UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

CRECIMIENTO DEL USO DE REDES WIRELESS VRS. SEGURIDAD REQUERIDA POR LAS ORGANIZACIONES EN GUATEMALA

RAMIRO RICARDO GIRÓN CASTILLO

ASESORADO POR LA INGA. ELIZABETH DOMÍNGUEZ ALVARADO

GUATEMALA, JUNIO DE 2004

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

CRECIMIENTO DEL USO DE REDES WIRELESS VRS. SEGURIDAD REQUERIDA POR LAS ORGANIZACIONES EN GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

RAMIRO RICARDO GIRÓN CASTILLO
ASESORADO POR: INGA. ELIZABETH DOMÍNGUEZ ALVARADO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, JUNIO DE 2004

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Ricardo Morales Prado
EXAMINADOR	Ing. Guillermo Rafael Sánchez Barrios
EXAMINADOR	Ing. César Fernández Cáceres
SECRETARIA	Ing. Pedro Antonio Aguilar Polanco

HONRABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la universidad de San Carlos de Guatemala, presento a su consideración mi trabajo graduación titulado:

CRECIMIENTO DEL USO DE REDES WIRELESS
VRS.
SEGURIDAD REQUERIDA POR LAS ORGANIZACIONES EN GUATEMALA

tema que me fuera asignado por la Coordinación de la Carrera de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería con fecha 16 de Febrero de 2004.

Ramiro Ricardo Girón Castillo

AGRADECIMIENTOS

A mis padres, quienes son mis motivadores y quienes siempre me han apoyado y me seguirán apoyando con sus consejos y vivencias para buscar siempre la superación.

Agradezco sinceramente a la Ingeniera Elizabeth Domínguez Alvarado, por su apoyo, confianza y sobre todo amistad que me brindó para la realización del presente trabajo de graduación.

A mis grandes amigos Juan Miguel Indekeu, Walter Michez, Héctor Mendía y Edgar González, por su apoyo incondicional y que todas las experiencias vividas las recordemos para siempre.

A mis catedráticos por el tiempo y dedicación que invirtieron en mi formación.

DEDICATORIA

A DIOS
Por darme la fe, sabiduría y espíritu para seguir adelante y continuar en los momentos difíciles.

A MIS PADRES JOSÉ ARTURO GIRÓN MALDONADO Y SONIA ELIZABETH CASTILLO DE GIRÓN, por darme primero que todo la vida y luego guiarme a través de ella, por todo el apoyo incondicional y comprensión que me brindaron en todo momento a lo largo de mi carrera.

A MIS HERMANOS MARVIN VINICIO E IVÁN ARTURO GIRÓN CASTILLO, por su comprensión y apoyo. Y que ésto sea un ejemplo para seguir adelante.

A MIS ABUELOS, TÍOS, PRIMOS Y FAMILIA EN GENERAL, por sus consejos y cariño.

A MIS AMIGOS dentro y fuera de la universidad, que siempre me apoyaron para lograr mis metas.

A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, por la formación académica recibida.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

802.11a Primer estándar de WLAN. Soporta de 1 a 2 Mbps.

802.11b Estándar mas utilizado para WLAN que trabaja a 2.4 Ghz y soporta 11Mbp.

802.11g Estándar de alta velocidad alternativo que trabaja en la banda de 2.4 Ghz con soporte de más de 20 Mbps.

802.11x Es un estándar de control de acceso a la red basado en puertos. Como tal, restringe el acceso a la red hasta que el usuario se ha validado.

ACL Significa *Access Control List*, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

AP Significa Punto de Acceso (*Access Point*).

ARP Sus siglas significan *Address Resolution Protocol* o protocolo de resolución de direcciones.

Beacomframes Los puntos de acceso mandan constantemente anuncios

	de la red, para que los clientes móviles puedan detectar su presencia y conectarse a la red *wireless*. Estos "anuncios" son conocidos como *BEACON FRAMES.*
Bluetooth	Estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDA's, teléfonos móviles de nueva generación y alguno que otro ordenador portátil.
CCMP	Sus siglas significan *Counter Mode with CBC-MAC Protocol* o modo contador con el protocolo CBC-MAC.
CDMA	Sus siglas significan *Code Division Multiple Access* o acceso múltiple por división de código. Sistema utilizado en las comunicaciones móviles.
CNAC	Significa *Closed Network Access Control*. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.
Coexistencia	Presencia simultánea en un mismo lugar de cosas o fenómenos que apenas tienen contactos o influencias entre sí, o carecen de ellos.
Cracker	El que rompe la seguridad de un sistema.
dBm	Decibel MiliWatt, medida utilizada para dar la fuerza de la señal en las redes inalámbricas.

DHCP Sus siglas significan *Dynamic Host Configuration Protocol* o protocolo de configuración de *host* dinámico. Distribuye un rango de número de IP's a varias máquinas en una o varias redes.

DMZ Significa *Demilitarized Zone* o Zona Desmilitarizada. Una DMZ es una zona que ha dividido un cortafuegos o *firewall* y es la zona que queremos mostrar al exterior o la zona desde la cual mostramos nuestros servicios o productos. También es llamada red protegida.

DoS Sus siglas significan *Denied of Service* o denegación de servicio. Tipo de ataque al 802.11 que bloquea o deniega el acceso a la red inalámbrica.

EAP Sus siglas significan *Extensible Authentication Protocol* o protocolo de autenticación extensible, que es un protocolo originalmente creado para realizar autenticación sobre enlaces PPP, soportando varios mecanismos de autenticación.

EAP-MD5 Método de autenticación por desafío. El servidor envía un mensaje "desafío" al cliente que quiere ser autenticado, el cliente debe responder a la petición con otro mensaje MD5 o con un mensaje NAK.

EAP-TLS Sus siglas significan *Extensible Authentication Protocol with Transport Layer Security* o protocolo de autenticación extensible con seguridad en la capa de

	transporte. Este protocolo proporciona autenticación mutua, negociación cifrada e intercambio de claves entre extremos. Soporta fragmentación y reensamblaje de mensajes.
EAP-TTLS	Sus siglas significan *Extensible Authentication Protocol with Tunneled Transport Layer Security* o protocolo de autenticación extensible con seguridad y túnel en la capa de transporte. En el intercambio de mensajes inicial se utiliza un ID de usuario y un *password*. Una vez realizada la autenticación inicial, se crea un túnel seguro que se utiliza para intercambiar información segura adicional.
Encriptar	Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor. Se usa para evitar el robo de información sensible, como números de tarjetas de crédito.
ESSID	Significa *Extended Service Set Identifier*, consta de cómo máximo 32 caracteres y es *case-sensitive*.
Frecuencia	Ritmo de recurrencia o rapidez de repetición de un fenómeno periódico. Representa el número de ciclos completos por unidad de tiempo para una magnitud periódica tal como corriente alterna, las ondas acústicas u ondas de radio.
Ghz	GigaHertz, es equivalente a mil millones de hertz.

GPRS Sus siglas significan *General Packet Radio Service* o Servicio General de Paquetes de Radio, la cual permite al GSM la integración de Internet con la Red Celular.

GPS Sus siglas significan *Global Positioning System* o sistema global de posición. Es un sistema de navegación por radio con recurso sobre una constelación de cerca de 24 satélites, que permiten a los utilizadores en el suelo, aire o mar determinar su localización exacta, velocidad y tiempo en cualquier instante, con todas las condiciones climáticas y en cualquier parte del mundo.

GSM Sus siglas significan *Global System for Mobile Communications* o Sistema Global para Comunicaciones Móviles. Es un sistema digital de telefonía móvil que es ampliamente utilizado en Europa y en otros países del mundo.

Hacker Un *hacker* es un curioso de la Red, todo un experto, un investigador, un explorador de sistemas. Básicamente se les conoce por sus penetraciones en ordenadores remotos. El buen *hacker* nunca hace daño. Cuando localiza un fallo, informa de ello. La ética *hacker* está basada en el aprendizaje y en la información libre y abierta.

HiperLAN Estándar Europeo de la ETSI equivalente a 802.11a de IEEE.

HotSpot	Un *hotspot* es un punto de acceso inalámbrico público donde los usuarios pueden conectarse a Internet. El servicio de *hotspot* se puede encontrar sin costo, o bien, con diferentes tarifas o renta del servicio.
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos (*Institute of Electrical and Electronics Engineers*).
Internet	Internet es el nombre de la red mundial de computadoras, que se encuentran en constante conexión.
IP	La transmisión de datos por Internet es hecha a través de *Information Packets* o paquetes de información. Cuando un mensaje es enviado se divide en paquetes de información que son transmitidos separadamente para el destinatario.
ISP	Sus siglas significan *Internet Service Provider* o proveedor de servicio de Internet.
IV	Sus siglas significan *Initialition Vector* o Vector de Inicialización. Son 24 bits que van en el paquete del protocolo WEP.
Kbps	Kilo bits por segundo.
Kilo	Un Mil.
LAN	Red de Area Local (*Local Area Network*).

LEAP	Sus siglas significan *Lightweigh* EAP o protocolo de autenticación extensible de bajo peso, propiedad de Cisco y diseñado para ser portable a través de varias plataformas *wireless*.
LLC	Control de Enlace Lógico (*Logic Link Control*).
MAC	Control de Acceso al Medio (*Medium Access Control*).
MAN	Red de Area Metropolitana (*Metropolitan Area Network*).
Mb.	Mega byte.
Mbps.	Mega bits por segundo.
Mega.	Un Millón.
Mhz	MegaHertz, es equivalente a un millón de hertz.
MS-CHAP	Protocolo Microsoft® de autenticación por desafío mutuo. Es conocido también como MS-CHAPv1.
OSA	Sus siglas significan *Open System Authentication* o sistemas abierto de autenticación. Es el protocolo de autenticación por defecto para 802.11b. Como su nombre indica, este método autentíca a cualquier cliente que pide ser autenticado, es decir, está abierto a cualquier usuario.
OSI	Interconexión de Sistemas Abiertos (*Open System*

Interconection)

PA Un punto de acceso es un dispositivo de hardware ubicado en óptima posición, que actúa como un punto central, y es capaz de proveer acceso de red *wireless* a un área circundante. Es un puente o *bridge* entre la *Ethernet* cableada y la *Ethernet* sin cable o *wireless*.

PCMCIA Significa *Personal Computer Memory Card International Association* o tarjeta internacional de memoria para computadora personal.

PDA Significa *Personal Digital Assistant* o asistente personal digital y se refiere a celulares, palmtops o similares que tengan acceso a Internet de alguna manera.

PDA's Plural de PDA.

PEAP Sus siglas significan *Protected Extensible Authetication Protocol* o protocolo de autenticación extensible protegido. Protocolo desarrollado por Microsoft®, CISCO® y RSA®. Similar a EAP-TTLS, al igual que éste, solamente el servidor de autentificación necesitaría un certificado.

QoS Sus siglas significan *Quality of Service* o calidad de servicio. Método de reservar ancho de banda y reducir la demora de la red para flujos de audio y video o de voz interactiva.

Radius Es un protocolo que implementa autentificación,

	autorización y contabilización para conexión a servidores. Autentifica y autoriza desde el propio switch inalámbrico o punto de acceso; conectado a un servidor, revisa que el usuario a conectarse esté dentro de la base de datos, permitiéndole el acceso a la red *wireless*.
RAM	Memoria de Solo Lectura (*Read Only Memory*).
Red	Colección de computadoras o dispositivos interconectados, no importando el medio por el cual lo estén.
Roaming	Dentro de una red, significa que el teléfono se conecta automáticamente a células diferentes cuando se halla en desplazamiento. Cuando su contacto o una determinada célula del teléfono se pierde o se debilita, busca inmediatamente otra célula que garantice una comunicación mejor.
SKA	Sus siglas significan *Shared Key Authentication* Se lleva a cabo mediante un mecanismo de desafío/respuesta cifrado, siendo necesario durante el proceso que ambas estaciones posean una clave común (autenticación simétrica).
SSID	Significa *Service Set IDentifier*, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica.
SSL	Significa *Secure Socket Layer* o *socket* de capa segura.

TCP/IP Protocolo de Control de Transmisión / Protocolo Internet. (*Transmission Control Protocol / Internet Protocolo*).

TDMA Sus siglas significan *Time Division Multiple* o multiplexión por división en el tiempo. Existe una multiplexión en el tiempo en que los usuarios esperan su turno por asignación cíclica, obteniendo uno en forma periódica la banda entera en poco tiempo.

TKIP Sus siglas significan *Temporal Key Integrity Protocol* o protocolo con llave íntegra temporal. Con este protocolo se pretende resolver las deficiencias del algoritmo WEP y mantener la compatibilidad con el hardware utilizado actualmente mediante una actualización del *Firmware*.

UDP Protocolo de Datagrama de Usuario (*User Datagrama Protocolo*).

ULA Sus siglas significan *Upper Layer Protocol* o protocolo de capa superior. Proporciona intercambio de autenticación entre el cliente y un servidor de autenticación.

USB Bus Universal de transmisión serial (*Universal Serial Bus*).

VPN Sus siglas significan *Virtual Private Network* o red privada virtual.

WAN Sus siglas significan *Wide Area Network* o red de área amplia.

WEP	Sus siglas significan *Wired Equivalet Privacy*, y fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Es inseguro debido a su arquitectura, por lo que el aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo.
WiFi	Significa *Wireless Fidelity* y es la institución encargada de tomar decisiones a cerca de nuevos estándares.
Wireless	Colección de computadoras o dispositivos interconectados de forma inalámbrica.
WLAN	Sus siglas significan *Wireless Local Area Network* o red inalámbrica de area local.
WMAN	Sus siglas significan *Wireless Metropolitan Area Network* o red inalámbrica de área metropolitana.
WPAN	Sus siglas significan *Wireless Personal Area Network* o red inalámbrica de área personal.
WWAN	Sus siglas significan *Wireless Wide Area Network* o red inalámbrica de área amplia.

RESUMEN

De una forma callada, las redes inalámbricas o *Wireless Networks*, se están introduciendo en el mercado de consumo gracias a unos precios populares y a un conjunto de entusiastas, mayoritariamente particulares, que han visto las enormes posibilidades de esta tecnología. Las aplicaciones de las redes inalámbricas son infinitas. De momento van a crear una nueva forma de usar la información, pues ésta estará al alcance de todos a través de Internet en cualquier lugar (en el que haya cobertura).

Existe una clasificación que nos muestra las diferentes variantes que podemos encontrar: Redes inalámbricas personales, Redes inalámbricas 802.11, Redes inalámbricas de consumo.

Las Redes inalámbricas personales son las redes que se usan actualmente mediante el intercambio de información con infrarrojos. Estas redes son muy limitadas dado su cortísimo alcance, necesidad de visión sin obstáculos entre los dispositivos que se comunican y su baja velocidad. También está el Bluetooth, estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDA's, teléfonos móviles de nueva generación y uno que otro ordenador portátil.

Las Redes inalámbricas 802.11 básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del IEEE.

Las Redes inalámbricas de consumo. Entre estas tenemos a las Redes CDMA (estándar de telefonía móvil estadounidense) y GSM (estándar de telefonía móvil europeo y asiático). Son los estándares que usa la telefonía

móvil empleados alrededor de todo el mundo en sus diferentes variantes. Y el 802.16 son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas (MAN) en la banda de entre los 2 y los 11 Ghz.

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado riesgos de seguridad en las redes inalámbricas. Varios son los riesgos derivados de este factor por ejemplo, se podría realizar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo, interceptando la red inalámbrica.

Para proteger los datos que se envían a través de las WLAN's, el estándar 802.11b define el uso del protocolo WEP (*Wired Equivalent Privacy*). WEP intenta proveer de la seguridad de una red con cables a una red *Wireless*, encriptando los datos que viajan sobre las ondas radioeléctricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace).

Siendo conscientes de las debilidades del estándar 802.11 en su protocolo WEP, se formó el comité 802.11i para combatir y mejorar los aspectos de seguridad en las redes inalámbricas. Existen algunos protocolos alternativos a este, que han sido muy exitosos entre los que se encuentran el ULA, 802.1x, TKIP, CCMP. Estos protocolos, aún están en su fase de estudio, por lo tanto que algunos no estén certificados por la IEEE, pero la mayoría ya está bien detallada y desarrollada.

OBJETIVOS

- **General**

Dar a conocer la importancia de la seguridad en las redes inalámbricas, para las empresas guatemaltecas, evaluando cómo mantenerla por medio de soluciones óptimas y efectivas. Hacer un análisis del crecimiento de las redes y análisis de costos que implica el mantenimiento de la seguridad.

- **Específicos**

1. Describir los conceptos importantes de una red inalámbrica y la importancia de su utilización en las empresas.

2. Dar a conocer los medios de seguridad para prevenir los daños que un Hacker o Cracker pueda provocar en una red inalámbrica.

3. Dar a conocer las tecnologías del Wardriving y el nuevo lenguaje del Warchalking.

4. Recomendar esquemas de seguridad para las redes inalámbricas, en base al costo y el rendimiento.

5. Plantear problemas específicos y dar una solución para estos de una manera práctica y en lo posible no costosa.

INTRODUCCIÓN

En la actualidad, la informática avanza a pasos agigantados, por lo que se necesita estar actualizado constantemente, las redes inalámbricas son una nueva tecnología que nos ayuda a mantener la comunicación.

La seguridad en la comunicación, ocupa un lugar muy importante dentro del mundo de las redes inalámbricas. Dentro de las empresas guatemaltecas, la información es importante, por lo que debe estar segura. Actualmente, los Hackers y Crackers están en búsqueda de vulnerabilidades dentro de las redes, con el objetivo de obtener información importante, lo cual puede ocasionar efectos desastrosos a la empresa.

Se explica con una amplia investigación el fácil acceso que se puede tener en una red interna, debido a que los protocolos que utiliza la red *wireless* son fáciles de burlar, especialmente, cuando existen errores de mala configuración, provocando una inseguridad para la empresa.

Se presenta un estudio de campo de una red inalámbrica situada en uno de los edificios más importantes en Guatemala, identificando los problemas de dicha red, en base a sus puntos de vulnerabilidad y presentando un análisis de costos y soluciones para combatir las vulnerabilidades encontradas.

1. REDES INALÁMBRICAS

1.1 Características generales, ventajas y desventajas

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante ondas de radio o luz infrarroja actualmente está siendo ampliamente investigada. Las redes inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

Pero la realidad es que esta tecnología está todavía en su nacimiento y se deben de resolver varios obstáculos técnicos y de regulación antes que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo.

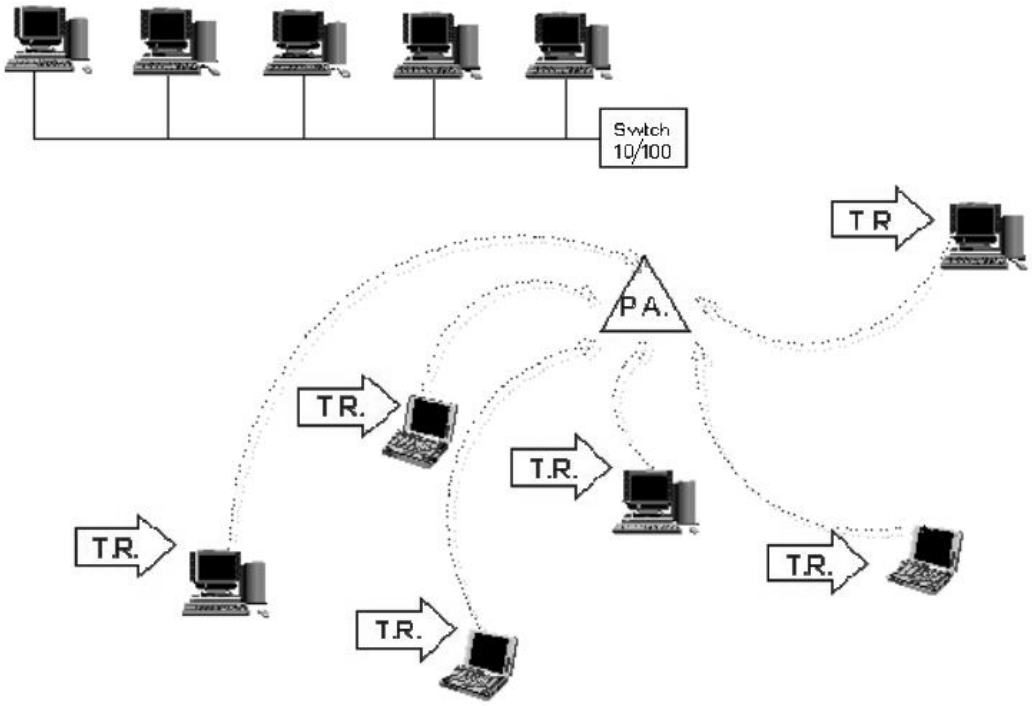
No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas, sino más bien complementarlas. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de cable de fibra óptica logran velocidades aún mayores, y pensando muy en el futuro se espera que las redes inalámbricas alcancen velocidades de solo 10 Mbps.

Se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una “red híbrida”. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al

equipo y que el operador se pueda desplazar con facilidad dentro de un almacén, oficina o centro comercial.

La siguiente figura, muestra gráficamente una red alámbrica y otra inalámbrica. Si nos damos cuenta, la primera tiene un *switch* que conecta todas las PC's unas con otras; todas llegan a éste de forma alámbrica. En cambio en la segunda, existe un punto de acceso (P.A.), el cual conecta a las demás PC's por medio de sus tarjetas de red *wireless*.

Figura 1. Red Alámbrica contra Red Inalámbrica



Fuente: Ander Otxoa Gilo. **Guía *wireless* para todos.** Pág. 4.

Ventajas sobre las redes inalámbricas:

- Movilidad.
- Facilidad en la Instalación.

- Flexibilidad de uso.
- Reducción de costos a largo plazo.

Desventajas sobre las redes inalámbricas:

- Elevado coste inicial, la inversión al inicio de un proyecto de instalación de una red inalámbrica es bastante elevado.
- Bajas velocidades de transmisión.

Existen dos amplias categorías de redes inalámbricas:

De larga distancia: Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.

De corta distancia: Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas son un medio para transmitir información de alto precio. Debido a que los *módems* celulares actualmente son más caros y delicados que los convencionales, ya que requieren de circuitos muy especiales, para mantener la señal. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos.

Otras desventajas de la transmisión celular son:

- La carga de los teléfonos se termina fácilmente.
- La transmisión celular se intercepta fácilmente (factor importante en lo relacionado con la seguridad).
- Las velocidades de transmisión son bajas.

Todas estas desventajas hacen que la comunicación celular se utilice poco, o únicamente para archivos muy pequeños como cartas y mensajes. Se espera que los avances en la compresión de datos, seguridad y algoritmos de verificación de errores permitan que las redes celulares sean una opción para algunas situaciones.

La otra opción que existe en redes de larga distancia son las denominadas: Red pública de conmutación de paquetes por radio. Estas redes no tienen problemas de pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en lugar de comunicaciones de voz. Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radiofrecuencias restringidas por la propia organización de sus sistemas de cómputo.

1.2 Clasificación de las redes inalámbricas

Vamos a hacer una primera clasificación que nos centre ante las diferentes variantes que podemos encontrar:

- Redes inalámbricas personales
- Redes inalámbricas 802.11
- Redes inalámbricas de consumo

1.2.1 Redes inalámbricas personales

Dentro del ámbito de estas redes podemos integrar dos principales actores:

- Infrarrojos
- *Bluetooth*

1.2.1.1 Infrarrojo

En primer lugar están las redes que se usan actualmente mediante el intercambio de información con infrarrojos. Estas redes son muy limitadas dado su corto alcance, necesidad de visión sin obstáculos entre los dispositivos que se comunican y su baja velocidad (hasta 115 Kbps). Se encuentran principalmente en ordenadores portátiles, PDAs (Agendas electrónicas personales), teléfonos móviles y algunas impresoras.
Los sistemas que funcionan mediante infrarrojos se clasifican según el ángulo de apertura con el que se emite la información en el emisor:

- Sistemas de corta apertura, de haz dirigido o de visibilidad directa que funcionan de manera similar a los controles remotos a distancia de los aparatos de televisión. Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse información.

- Sistemas de gran apertura, reflejados o de difusión que radian tal y como lo haría una bombilla, permitiendo el intercambio de información en un rango más amplio. La norma IEEE 802.11 especifica dos modulaciones para esta tecnología: la modulación 16 ppm y la modulación 4 ppm proporcionando velocidades de transmisión de 1 y 2 Mbps

respectivamente. Esta tecnología se aplica típicamente en entornos interiores para implementar enlaces punto a punto de corto alcance o redes locales en entornos muy localizados como puede ser un aula o laboratorio.

1.2.1.2 *Bluetooth*

En segundo lugar el bluetooth: Estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles de nueva generación y algún ordenador portátil.

Principal desventaja es que su puesta en marcha se ha ido retrasando desde hace años y la aparición del mismo ha estado plagada de incompatibilidades entre los dispositivos de comunicación de los distintos fabricantes que ha imposibilitado su rápida adopción. Opera dentro de la banda de los 2.4 Ghz.

Define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.

La tecnología bluetooth comprende *hardware*, *software* y requerimientos de interoperabilidad, por lo que para su desarrollo ha sido necesaria la

participación de los principales fabricantes en los sectores de las telecomunicaciones y la informática, tales como: Ericsson®, Nokia®, Toshiba®, IBM®, Intel® y otros. Posteriormente se han ido incorporando muchas más compañías, y se prevee que próximamente los hagan también empresas de sectores tan variados como: automatización industrial, maquinaria, ocio y entretenimiento, fabricantes de juguetes, electrodomésticos, etc., con lo que en poco tiempo se nos presentará un panorama de total conectividad de nuestros aparatos tanto en casa como en el trabajo.

1.2.2 Redes inalámbricas WLAN u 802.11

Una red de área local inalámbrica puede definirse como a una red de alcance local que tiene como medio de transmisión el aire. Por red de área local entendemos una red que cubre un entorno geográfico limitado, con una velocidad de transferencia de datos relativamente alta (mayor o igual a 1 Mbps tal y como especifica el IEEE), con baja tasa de errores y administrada de forma privada.

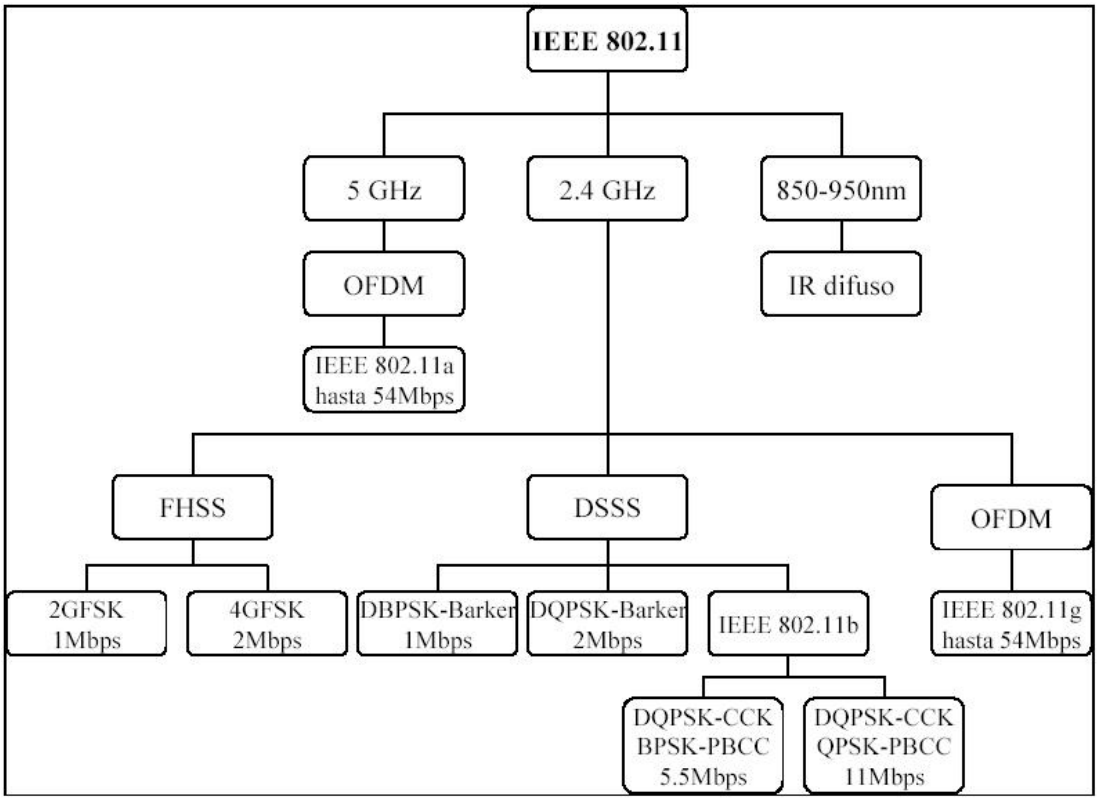
Por red inalámbrica entendemos una red que utiliza ondas electromagnéticas como medio de transmisión de la información que viaja a través del canal inalámbrico enlazando los diferentes equipos o terminales móviles asociados a la red. Estos enlaces se implementan básicamente a través de tecnologías de microondas y de infrarrojos.

En las redes tradicionales cableadas esta información viaja a través de cables coaxiales, pares trenzados o fibra óptica. Una red de área local inalámbrica, también llamada *Wireless* LAN (WLAN), es un sistema flexible de comunicaciones que puede implementarse como una extensión o directamente como una alternativa a una red cableada. Este tipo de redes utiliza tecnología

de radiofrecuencia minimizando así la necesidad de conexiones cableadas. Este hecho proporciona al usuario una gran movilidad sin perder conectividad.

El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así, debido a que sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 10 Mbps, frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general las WLAN se utilizarán como un complemento de las redes fijas.

Figura 2. Diagrama descriptivo de la capa física del 802.11 y sus extensiones



Fuente: Daniel Hernanz C. **Estudio de la capa física 802.11**. Pagina 3.

Las redes inalámbricas o WLAN básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del IEEE.

Como suele pasar siempre que un estándar aparece y los grandes fabricantes se interesan por él, surgen diferentes aproximaciones al mismo lo que genera una gran confusión.

Nos encontramos ante tres principales variantes:

- Estándar 802.11a
- Estándar 802.11b
- Estándar 802.11g

1.2.2.1 Estándar 802.11a

Fue la primera aproximación a las WLAN, llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE; hasta 72 y 108 Mbps con tecnologías de desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero que no están (al día de hoy) estandarizadas por la IEEE. Esta variante opera dentro del rango de los 5 Ghz. Inicialmente se soportan hasta 64 usuarios por punto de acceso.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y 802.11g, la no incorporación a la misma de QoS (*Quality of Service*,

que es la posibilidades de asegurar la calidad de servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos multimedia *online*), la no disponibilidad de esta frecuencia en Europa dado que está reservada a la HyperLAN2 y la parcial disponibilidad de la misma en Japón.

El hecho de no estar disponible en Europa prácticamente la descarta de nuestras posibilidades de elección para instalaciones en este continente.

1.2.2.2 Estándar 802.11b

Es la segunda aproximación de las WLAN. Alcanza una velocidad de 11 Mbps estandarizada por la IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes, pero sin la estandarización (al día de hoy) por la IEEE. Opera dentro de la frecuencia de los 2.4 Ghz. Inicialmente se soportan hasta 32 usuarios por punto de acceso.

Adolece de varios de los inconvenientes del 802.11a, como son la falta de QoS, además de otros problemas como la masificación de la frecuencia en que transmite y recibe; pues en los 2.4 Ghz funcionan también teléfonos inalámbricos, teclados y ratones inalámbricos, hornos de microondas, dispositivos *Bluetooth*, lo cual puede provocar interferencias.

En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a los muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo.

1.2.2.3 Estándar 802.11g

Es la tercera aproximación a las WLAN, y se basa en la compatibilidad con los dispositivos 802.11b y en ofrecer unas velocidades de hasta 54 Mbps. Funciona dentro de la frecuencia de 2.4 Ghz. Dispone de los mismos inconvenientes que el 802.11b además de los que pueden aparecer con la aún no estandarización del mismo por parte del IEEE (puede haber incompatibilidades con dispositivos de diferentes fabricantes).

Las ventajas de las que dispone son las mismas que las del 802.11b además de su mayor velocidad.

1.2.2.4 Comparación de los diferentes estándares 802.11X

La constante aparición de nuevas especificaciones 802.11 e HiperLAN pueden causar confusión. La tabla siguiente intenta aclarar conceptos básicos y poner un poco de orden en todo esto.

Tabla I. Comparación de los estándares 802.11X

Estándar	Estado	Definición
IEEE 802.11	Finalizado en 1997.	Primer estándar de WLAN. Soporta de 1 a 2 Mbps.
IEEE 802.11a	Finalizado en 1999	Estándar de Alta Velocidad para WLAN trabaja a 5GHz con una capacidad de 54 Mbps.
IEEE 802.11b	Finalizado en 1999	Estándar mas utilizado para WLAN que trabaja a 2.4 Ghz y soporta 11Mbp.
802.11c		Ofrece la información sobre 802.11 al estándar ISO/IEC 10038 (IEEE 802.1D).

802.11d		Añade los requerimientos y definiciones necesarias para permitir que redes 802.11 operen en redes heterogéneas.
IEEE 802.11e	Finalizado hace pocos meses	Expande el soporte para el uso de QoS en redes inalámbricas.
IEEE 802.11f	En proceso	Especifica qué información debe ser intercambiada entre los puntos de acceso para soportar la funciones de P802.11 DS.
IEEE 802.11g	Finalizado hace pocos meses	Estándar de alta velocidad alternativo que trabaja en la banda de 2.4 Ghz con soporte de más de 20 Mbps.
802.11h	En proceso	Pretende mejorar la capa 802.11 MAC y 802.11a PHY con el objetivo de mejorar los métodos de emisión de datos y minimizar las potencias de las señales para reducción de consumos.
802.11i	Finalizado hace pocos meses	Estándar que define la encriptación y la autentificación para complementar, completar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP).
802.11j	En Proceso	Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.
802.11m	Finalizado hace pocos meses	Estándar propuesto para el mantenimiento de las redes inalámbricas.
HiperLAN2	Finalizado en el año 2000.	Estándar Europeo de la ETSI equivalente a 802.11a de IEEE.

1.2.3 Redes inalámbricas de consumo

Dentro de esta clasificación de redes inalámbricas se encuentran dos principalmente, las redes CDMA – GSM y las redes del estándar 802.16 impuesto por la IEEE.

1.2.3.1 Redes TDMA, CDMA y GSM

Redes TDMA, CDMA (estándares de telefonía móvil estadounidense) y GSM (estándar de telefonía móvil europeo y asiático). Son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes.

TDMA (Acceso Múltiple por División en el Tiempo), es donde existe una multiplexión en el tiempo que los usuarios esperan su turno por asignación cíclica, obteniendo en forma periódica la banda entera en poco tiempo.

CDMA (Acceso Múltiple por División de Código), evita el problema de sincronización de tiempo y también el problema de reparto de canal; es completamente descentralizado y totalmente dinámico.

Entre sus características principales están:

- Se basa en s*pread spectrum*.
- Velocidades de datos alrededor de 144 Kbps.
- Puede actuar de dos modos el DSSS (Direct Secuence) y el FHSS (Frequency Hop).

GSM (Sistema Global para comunicaciones Móviles), es un sistema digital de telefonía móvil que es ampliamente utilizado en Europa y otros países del mundo. GSM utiliza una variación del acceso múltiple por división de tiempo (TDMA) y es la más utilizada de las tres tecnologías actuales de telefonía inalámbrica (TDMA, GSM y CDMA). GSM digitaliza y comprime voz y datos, y después los envía en un canal junto con otras dos series de datos del usuario en particular. Opera en las bandas de frecuencia de 900MHz, 1800MHz y 1900MHz.

GSM asegura que obtenga el estándar de sistema con los beneficios de una interfaz abierta, seguridad completa, *roaming* global, comunicación de datos, acceso a Internet, un sistema de tarifa y cobranza seguro y eficiente.

Naturalmente, GSM abastece otro tipo de datos (tales como WAP), protocolo de Internet (IP) y servicios empresariales con la técnica de 3G. GSM es un pilar en el camino hacia el Sistema Universal de Telecomunicaciones Móviles (UMTS) en la tercera generación tercera y cuarta generación.

Entre sus más relevantes características tiene:

- Su velocidad de transmisión está limitada por un uso ineficiente del canal.
- Brinda integración GSM – Internet, a esta unión se le llama GPRS (General Packet Radio Service), la cual permite a GSM la integración de Internet con la Red Celular.

Podemos comparar estas dos tecnologías, CDMA – GSM, que a la vista se ve que son las mejores, para ello listaremos algunas de las diferencias que tienen:

- GSM posee mayor facilidad de roaming (mayor cantidad de carriers), que CDMA.
- CDMA posee una implementación más fácil.
- CDMA sufre menor interferencia externa.

1.2.3.2 Redes 802.16a

Son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas (MAN) en la banda de entre los 2 y los 11 Ghz. Este estándar IEEE 802.16a fue aprobado en el mes de enero del año 2003.

El estándar IEEE 802.16a es una tecnología de red metropolitana inalámbrica (WMAN) que conecta *hotspots* inalámbricos, que ofrecen a los usuarios acceso a Internet inalámbrico vía estándar IEEE 802.11 o Wi-Fi, y otras ubicaciones como negocios y hogares a la columna vertebral de Internet por cable. Se espera que las redes basadas en el estándar 802.16a tengan un alcance de hasta 30 millas y la capacidad para transferir datos, sonido y video a velocidades de hasta 70 Mbps.

Los productos basados en la tecnología 802.16a pueden proporcionar conectividad de banda ancha inalámbrica a los negocios con niveles garantizados de servicio para las aplicaciones empresariales, y a los hogares para aplicaciones de banda ancha residenciales. Estos productos también permitirán que los proveedores de servicios ofrezcan servicios de voz y de datos.

1.3 Tecnología utilizada

La diferencia principal de los entornos *wireless* con los entornos de cable tradicionales, como *Ethernet*, radica únicamente en el medio en el que se transmiten los datos. Esto hace necesaria la redefinición del concepto de perímetro, ya que en las redes 802.11 el mismo no está establecido de forma

fija, sino que depende del alcance de una señal de radio, algo más complejo de medir.

Es conveniente hacer una división entre la topología y el modo de funcionamiento de los dispositivos WiFi.

Por topología nos referimos a la disposición lógica (aunque la física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida.

1.3.1 Topologías

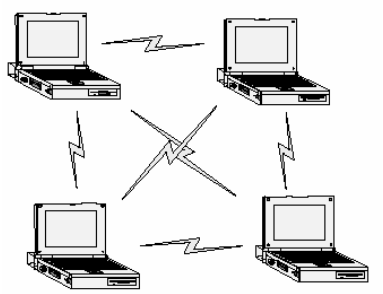
En el mundo *Wireless* existen dos topologías básicas:

- Ad-Hoc
- Modo Infraestructura

1.3.1.1 Ad-hoc

Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red *Peer to Peer* o de igual a igual, para lo cual sólo vamos a necesitar disponer de un SSID (*Service Set IDentifier*), igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre sí. La caída de un sólo nodo implica la caída de toda la red.

Figura 3. Gráfica de una topología ad-hoc

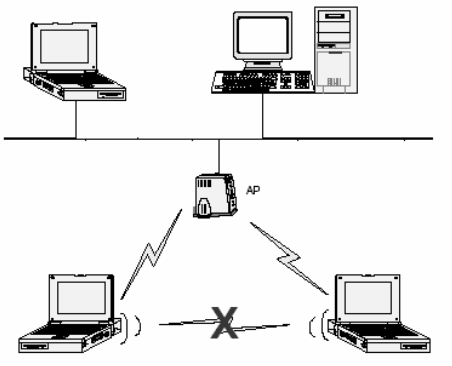


Fuente: Pau Oliva Fora. **(In)Seguridad en redes 802.11b**. Pagina 3.

1.3.1.2 Modo infraestructura

En el cual existe un nodo central (punto de acceso WiFi) que sirve de enlace para todos los demás (tarjetas de red WiFi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del punto de acceso. Este sí es tolerante a fallos, ya que la caída de un nodo no implica la caída de toda la red, en cambio si se desconecta por algún motivo el punto de acceso sí será trágico para la red.

Figura 4. Gráfica de una topología infraestructura



Fuente: Pau Oliva Fora. **(In)Seguridad en redes 802.11b**. Pagina 3.

1.3.2 Modos de funcionamiento

Todos los dispositivos, independientemente de que sean tarjetas de red o puntos de acceso tienen dos modos de funcionamiento.

Tomemos el modo infraestructura como ejemplo:

1.3.2.1 Modo managed

Es el modo en el que la tarjeta de red se conecta al punto de acceso para que éste último le sirva de concentrador. La tarjeta de red sólo se comunica con el punto de acceso.

1.3.2.2 Modo master

Este modo es el modo en el que trabaja el punto de acceso, pero en el que también pueden entrar las tarjetas de red si se dispone del *firmware* apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida. Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como puntos de acceso realmente las tarjetas de red, a las que se les ha añadido cierta funcionalidad extra vía *firmware* o vía *software.*

Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro y bajo una distribución especial de Linux llamada LINUXAP/OPENAP.

2. SEGURIDAD EN REDES INALÁMBRICAS

2.1 Riesgos de las redes inalámbricas

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha provocado nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del edificio donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la empresa y a la seguridad informática de la misma.

Varios son los riesgos derivados de este factor. Por ejemplo, se podría realizar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un PA ilegal más potente que capte las estaciones cliente en vez del PA legítimo, interceptando la red inalámbrica. También sería posible crear interferencias y una más que posible denegación de servicio con sólo introducir un dispositivo que emita ondas de radio a una frecuencia de 2.4 Ghz.

La posibilidad de comunicarnos entre estaciones cliente directamente, sin pasar por el PA permitiría atacar directamente a una estación cliente, generando problemas si ésta estación cliente ofrece servicios TCP/IP o comparte ficheros. Existe también la posibilidad de duplicar las direcciones IP o MAC de estaciones cliente legítimas.

Los PA están expuestos a un ataque de fuerza bruta para averiguar los *passwords*, por lo que una configuración incorrecta de los mismos facilitaría la irrupción en una red inalámbrica por parte de intrusos.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los materiales suficientes pueda introducirse en una red. Unos mecanismos son seguros,

otros, como el protocolo WEP (*Wired Equivalent Protocol*) fácilmente "rompibles" por programas distribuidos gratuitamente por Internet.

2.2 Proceso de conexión a una WLAN

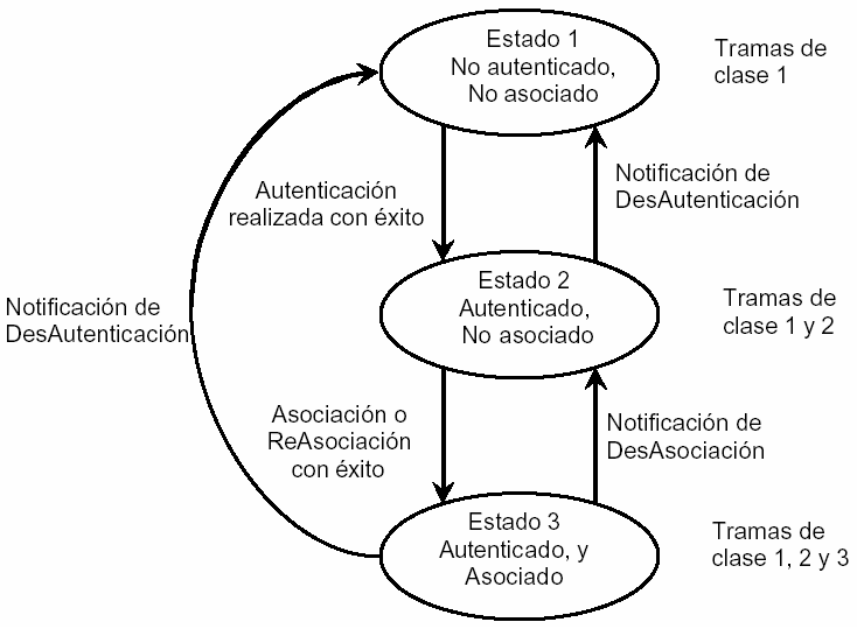
Antes de continuar estudiando la seguridad que implica una red inalámbrica, debemos conocer algunos términos importantes, los cuales se describen a continuación:

SSID o ESSID. Cada red *wireless* tiene un ESSID (*Extended Service Set Identifier*), que la identifica. El ESSID consta cómo máximo de 32 caracteres y es *case-sensitive*. Es necesario conocer el ESSID del PA para poder formar parte de la red *wireless*, es decir, el ESSID configurado en el dispositivo móvil tiene que concordar con el ESSID del PA.

BEACON FRAMES. Los PA mandan constantemente anuncios de la red, para que los clientes móviles puedan detectar su presencia y conectarse a la red *wireless*. Estos "anuncios" son conocidos como *BEACON FRAMES*, si pasamos un *sniffer* en las tramas de una red *wireless* podremos ver que normalmente el PA manda el ESSID de la red en los *BEACON FRAMES*, aunque esto se puede deshabilitar por *software* en la mayoría de los PA que se comercializan actualmente.

La siguiente gráfica muestra los estados en que debe estar un cliente para asociarse con un PA:

Figura 5. Estados para asociarse con un punto de acceso



Fuente: Pau Oliva Fora. **(In) seguridad en redes 802.11b.** Pág. 9.

El proceso de asociación tiene dos pasos, envueltos en 3 estados:

- No autenticado y no asociado
- Autenticado y no asociado
- Autenticado y asociado

En la transición por los diferentes estados, ambas partes (cliente y PA) intercambian mensajes llamados "*management frames*".

El proceso que realiza un cliente *wireless* para encontrar y asociarse con un PA es el siguiente:

Paso 1: Los PA transmiten *BEACON FRAMES* cada cierto intervalo de tiempo fijo. Para asociarse con un PA y unirse a una red en modo infraestructura, un cliente escucha en busca de *BEACON FRAMES* para identificar puntos de acceso. El cliente también puede enviar una trama

"*PROVE REQUEST*" que contenga un ESSID determinado para ver si le responde un PA que tenga el mismo ESSID.

Paso 2: Después de identificar al PA, el cliente y el PA realizan autenticación mutua intercambiando varios *management frames* como parte del proceso. Hay varios mecanismos de autenticación posibles que se describirán a detalle más adelante.

Paso 3: Después de una autenticación realizada con éxito, el cliente pasa a estar en el segundo estado (autenticado y no asociado). Para llegar al tercer estado (autenticado y asociado) el cliente debe mandar una trama "*ASSOCIATION REQUEST*" y el PA debe contestar con una trama "*ASSOCIATION RESPONSE*", entonces el cliente se convierte en un *host* más de la red *wireless* y ya está listo para enviar y recibir datos de la red.

2.2.1 Mecanismos de autenticación

Cuando se desea establecer una comunicación entre dos dispositivos, debe primero establecerse una asociación. Para ello el cliente solicita la autenticación y el PA responde identificando el tipo de autenticación presente en la red. Posteriormente, el cliente procede con la autenticación y, si es satisfactoria, se lleva a cabo la asociación.

El estándar 802.11b plantea dos posibles formas de autenticación:

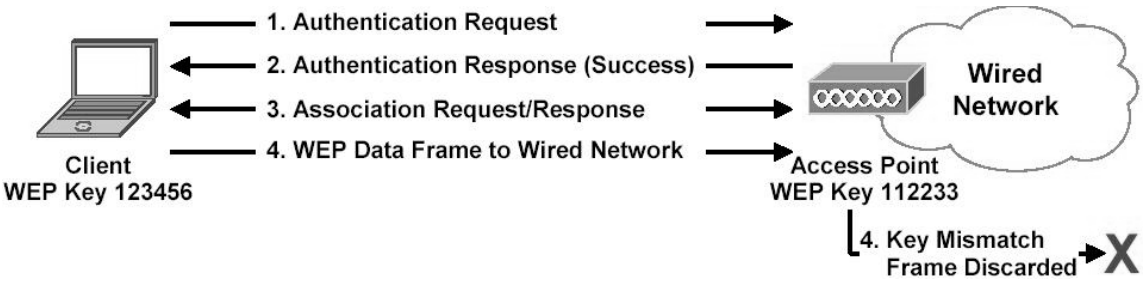
- *Open system authentication*
- *Shared key authentication*

2.2.1.1 *Open system authentication*

Open system authentication es el protocolo de autenticación por defecto para 802.11b. Como su nombre indica, este método autentica cualquier cliente

que pide ser autenticado, es decir, está abierto a cualquier usuario. Es un proceso de autenticación NULO, las tramas se mandan en texto plano aunque esté activado el cifrado WEP.

Figura 6. Estados del o*pen system authentication*



Fuente: Mike de Leo. ***Security* 802.11b *wireless networks*.** Pág. 23.

2.2.1.2 Shared key authentication

Se lleva a cabo mediante un mecanismo de desafío / respuesta cifrado, siendo necesario durante el proceso que ambas estaciones posean una clave común (autenticación simétrica). Para que una red 802.11b pueda utilizar este tipo de autenticación, debe emplear el protocolo WEP.

El siguiente esquema muestra el proceso de autenticación:

Figura 7. Estados del *shared key authentication*

Fuente: Mike de Leo. ***Security* 802.11b *wireless networks*.** Pág. 24

La estación que quiere autenticarse (cliente), envía una trama *AUTHENTICATION REQUEST* indicando que quiere utilizar una “clave compartida”. El destinatario (que es un PA) contesta enviando una trama que contiene 128 octetos de texto (desafío) al cliente.

El texto del desafío se genera utilizando el PRNG (generador de números pseudoaleatorios de WEP) con la clave compartida y un vector de inicialización (IV) aleatorio.

Una vez el cliente recibe la trama, copia el contenido del texto de desafío en el *payload* de una nueva trama, que encripta con WEP utilizando la clave compartida (*passphrase*) y añade un nuevo vector de inicialización (elegido por el cliente). Una vez construida esta nueva trama encriptada, el cliente la envía al PA, y éste desencripta la trama recibida y comprueba que:

- El ICV (*Integrity Check Value*) sea válido (CRC de 32 bits).
- El texto de desafío concuerde con el enviado en el primer mensaje.

Si la comprobación es correcta, se produce la autenticación del cliente con el PA y entonces se vuelve a repetir el proceso pero esta vez el primero que manda la trama con el *AUTHENTICATION REQUEST* es el PA. De esta manera se asegura una autenticación mutua.

2.3 Mecanismos de seguridad

2.3.1 Access Control List (ACL)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que existan en la Lista de Control de Acceso.

2.3.2 Closed Network Access Control (CNAC)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando ésta como contraseña.

2.3.3 Wired Equivalent Protocol (WEP)

Para proteger los datos que se envían a través de las WLANs, el estándar 802.11b define el uso del protocolo WEP (*Wired Equivalent Privacy*). WEP intenta proveer de la seguridad de una red con cables a una red *Wireless*, encriptando los datos que viajan sobre las ondas radioeléctricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace).

El protocolo WEP está basado en el algoritmo de encriptación RC4, y utiliza claves de 64 bits o de 128 bits. En realidad son de 40 y 104 bits, ya que los otros 24 bits van en el paquete como Vector de Inicialización (IV). Se utiliza un *checksum* para prevenir que se inyecten paquetes *spoofeados*. Más adelante se verá más a fondo como funciona la encriptación WEP.

2.3.3.1 **Llaves**

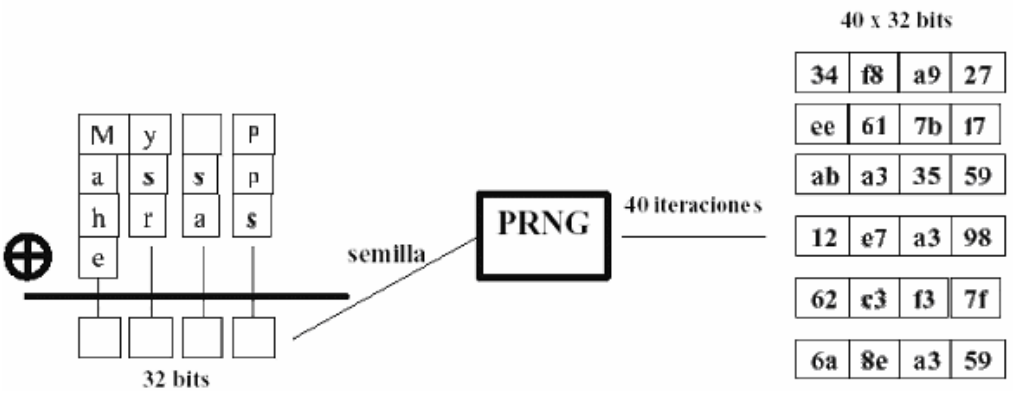
La llave de 40 ó 104 bits, se genera a partir de una clave (*passphrase*) estática de forma automática, aunque existe *software* que permite introducir esta llave manualmente. La clave o *passphrase* debe ser conocida por todos los

clientes que quieran conectarse a la red *wireless* que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente.

A partir de la clave o *passphrase* se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP.

Este es el proceso utilizado para generar las llaves:

Figura 8. Proceso para generar llaves en el WEP



Fuente: Pau Oliva Fora. **(In) seguridad en redes 802.11b.** Pág. 5.

Se hace una operación de exclusión con la cadena ASCII (*My Passphrase*) que queda transformada en una semilla de 32 bits que utilizará el generador de números pseudoaleatorios (PRNG) para generar 40 cadenas de 32 bits cada una. Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave, para que al final se generen 4 llaves de 40 bits.

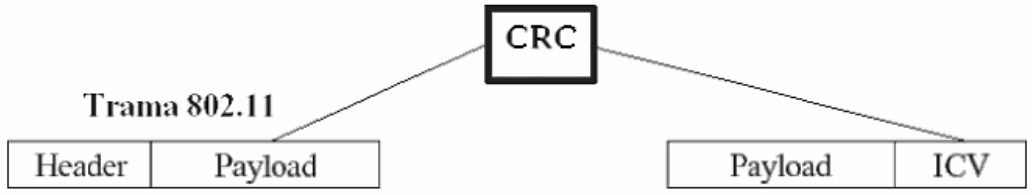
De estas 4 llaves sólo se utilizará una para realizar la encriptación WEP, como veremos a continuación.

2.3.4.1 Encriptación

Para generar una trama encriptada con WEP se sigue el siguiente proceso:

Partimos de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (*Header*) y contiene unos datos (*Payload*). El primer paso es calcular el CRC de 32 bits del *payload* de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único del *payload* en concreto, que nos servirá para verificar que el *payload* recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como valor de chequeo de integridad (ICV: *Integrity Check Value*).

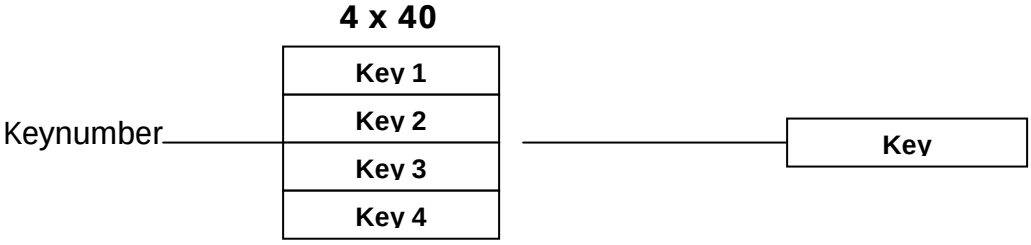
Figura 9. El CRC como generador de un identificador único



Fuente: Pau Oliva Fora. **(In) seguridad en redes 802.11b.** Pág. 5.

Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles:

Figura 10. Selección de una llave para el WEP.



Y se añade el Vector de Inicialización (IV) de 24 bits al principio de la llave seleccionada:

Figura 11. Vector de Inicialización más una llave seleccionada.

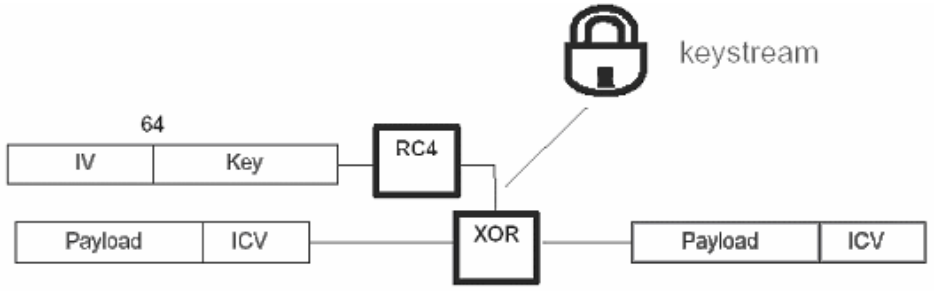
IV + Keynum	KEY
24	40

El IV es simplemente un contador que suele ir cambiando de valor a medida que se van generando tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para encriptar la trama. En el caso de utilizar encriptación de 128 bits tendríamos 24 bits del IV y 104 de llave.

Llegado a este punto, aplicamos el algoritmo RC4 al conjunto IV+Key y conseguiremos el *keystream* o flujo de llave. Realizando una operación de exclusión con este *keystream* y el conjunto *Payload*+ICV obtendremos el *Payload*+ICV cifrado, este proceso puede verse en el siguiente gráfico.

Se utilizan el IV y la llave para encriptar el *Payload* + ICV:

Figura 12. Proceso de encriptación WEP



Fuente: Pau Oliva Fora. **(In) seguridad en redes 802.11b.** Pág. 7.

Después añadimos la cabecera y el IV+*Keynumber* sin cifrar. Así queda la trama definitiva lista para ser enviada:

Figura 13. Trama lista para enviar, utilizando WEP

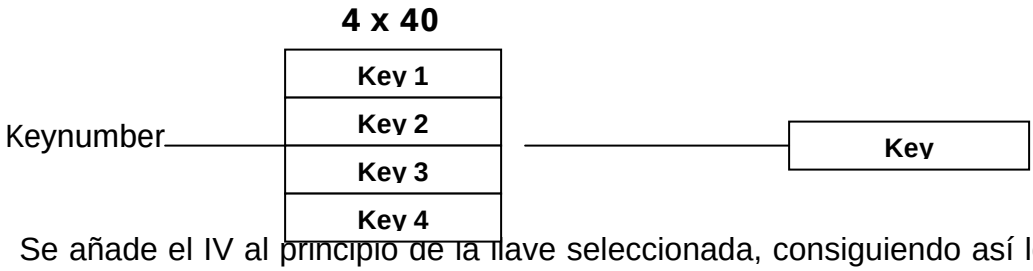
Header	IV + Keynumber	Payload	ICV

2.3.4.2 Desencriptación

Ahora vamos a ver el proceso que se realiza para desencriptar una trama encriptada con WEP:

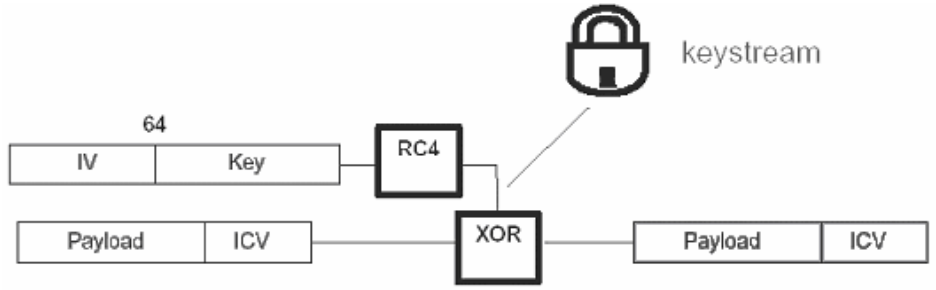
Se utiliza el número de llave que aparece en claro en la trama cifrada, junto con el IV para seleccionar la llave que se ha utilizado para cifrar la trama:

Figura 14. Selección de una llave para desencriptar el WEP



Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64 bits de llave. Aplicando RC4 a esta llave se obtiene el *keystream* válido para obtener la trama en claro (*plaintext*) realizando una operación de exclusión con el *Payload*+ICV cifrados y la llave completa como se describe a continuación:

Figura 15. Proceso de desencriptación WEP



Fuente: Pau Oliva Fora. **(In) seguridad en redes 802.11b.** Pág. 8.

Una vez obtenido el *plaintext*, se vuelve a calcular el ICV del *payload* obtenido y se compara con el original.

2.4 Vulnerabilidades en el 802.11 o WLAN

2.4.1 Deficiencias en la encriptación WEP

2.3.4.3 Características lineares de CRC32

Esta vulnerabilidad fue demostrada teóricamente por Nikita Borisov, Ian Goldberg y David Wagner (Universidad de Berkeley).

Como se ha visto anteriormente, el campo ICV (*Integrity Check Value*) de una trama encriptada con WEP contiene un valor utilizado para verificar la integridad del mensaje. Esto provee de un mecanismo de autenticación de mensajes a WEP, por lo tanto el receptor aceptará el mensaje si el ICV es válido. El ICV se genera simplemente haciendo un CRC (*Cyclic Redundancy Check*) de 32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas:

- Los CRC's son independientes de la llave utilizada y del IV.
- Los CRC's son lineares: CRC (m $\oplus$ k) = CRC (m) $\oplus$ CRC (k).

Debido a que los CRC's son lineares, se puede generar un ICV válido ya que el CRC se combina con una operación de exclusión que también es lineal y esto permite hacer el '*bit flipping*'.

2.3.4.4 Tamaño de vector de inicialización demasiado corto

Otra deficiencia del protocolo viene dada por la corta longitud del campo vector de inicialización (IV) en las tramas 802.11b. El vector de inicialización (IV) tiene sólo 24 bits de longitud y aparece en claro (sin encriptar).

Matemáticamente sólo hay 2^24 (16.777.216) posibles valores de IV. Aunque esto pueda parecer mucho, 16 millones de paquetes pueden generarse en pocas horas en una red *wireless* con tráfico intenso.

Un punto de acceso que constantemente envíe paquetes de 1500 bytes (MTU) a 11Mbps, acabará con todo el espacio de IV disponible después de 1500*8/(11*10^6)*2^24 = ~1800 segundos, o 5 horas. Este tiempo puede ser incluso más pequeño si la MTU es menor que 1500.

La corta longitud del IV, hace que éste se repita frecuentemente y da lugar a la deficiencia del protocolo WEP que se verá a continuación, basada en la posibilidad de realizar ataques estadísticos para recuperar el *plaintext* gracias a la reutilización del IV.

2.3.4.5 Reutilización de vector de inicialización

Esta vulnerabilidad fue demostrada teóricamente por David Wagner (Universidad de Berkeley). Se basa en que WEP no utiliza el algoritmo RC4 “con cuidado”: el vector de inicialización se repite frecuentemente. Se pueden hacer ataques estadísticos contra *cyphertexts* con el mismo IV.

El estándar 802.11 especifica que cambiar el IV en cada paquete es opcional. El IV normalmente es un contador que empieza con valor cero y se va incrementando de uno en uno, por lo tanto:

- Rebotar causa la reutilización de IV’s.

- Sólo hay 16 millones de IV's posibles, así que después de interceptar suficientes paquetes, seguro que hay IV's repetidos

Un atacante capaz de escuchar el tráfico 802.11 puede descifrar *cyphertexts* interceptados incluso sin conocer la clave.

2.4.2 Deficiencias en el método de autenticación *shared key*

El método de autenticación *shared key authentication* descrito anteriormente puede explotarse fácilmente mediante un ataque pasivo:

El atacante captura el segundo y el tercer *management messages* de una autenticación mutua (*authentication challenge* y *authentication response*). El segundo mensaje contiene el texto de desafío en claro, y el tercer mensaje contiene el desafío encriptado con la clave compartida. Como el atacante conoce el desafío aleatorio (*plaintext*, P), el desafío encriptado (*cyphertext*, C), y el IV público, el atacante puede deducir el flujo pseudoaleatorio (*keystream*) producido usando WEP con la siguiente ecuación:

Figura 16. Ecuación para obtener el *keystream*

$$WEP_{PR}^{K,IV} = C \oplus P$$

Fuente: Pau Oliva Fora. **(In) seguridad en redes 802.11b.** Pág. 15.

El tamaño del *keystream* será el tamaño de la trama de autenticación, ya que todos los elementos de la trama son conocidos: número de algoritmo, número de secuencia, *status code*, *element id*, longitud, y el texto de desafío. Además, todos los elementos excepto el texto de desafío son los mismos para todas las *authentication responses*.

El atacante tiene por lo tanto todos los elementos para autenticarse con éxito sin conocer la clave secreta compartida K. El atacante envía un *authentication request* al PA con el que se quiere asociar. El PA contesta con un texto de desafío en claro. El atacante entonces, coge el texto de desafío aleatorio, R, y el flujo pseudo-aleatorio WEP $^{k,IV}_{PR}$ y genera el cuerpo de una trama *authentication response* válido, realizando una operación de exclusión con los dos valores.

El atacante entonces debe crear un nuevo ICV válido aprovechando la vulnerabilidad de *características lineares de CRC32*. Una vez creado el nuevo ICV, el atacante acaba de completar la trama de *authentication response* y la envía, de esta manera se asocia con el PA y se une a la red.

Con este proceso el atacante sólo esta autenticado, pero todavía no puede utilizar la red. Como el atacante no conoce la clave compartida, para poder utilizar la red debe implementar algún ataque al protocolo WEP.

2.5 Ataques al 802.11 o WLAN

2.5.1 Romper ACL's basados en MAC

Una de las medidas más comunes que se utilizan para poner segura una red *wireless* es restringir las máquinas que podrán comunicarse con el PA haciendo filtrado por dirección MAC en éste. Para ésto se suele crear una tabla en el punto de acceso que contiene todas las MAC's de los clientes que están autorizados para conectar.

Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente envía, y hacernos pasar por uno de los equipos que sí tienen acceso a la red.

Para llevar a cabo el ataque basta con colocar un *sniffer* durante un momento en el tráfico y fijarnos en la MAC de cualquiera de los clientes. Sólo hace falta que nos pongamos su misma MAC y ya habremos saltado la restricción. Esto es sencillo de implementar, por ejemplo en el sistema operativo Linux se puede realizar con el comando *ifconfig* dependiendo del tipo de tarjeta que tengamos. También existen otras utilidades para cambiar la MAC como por ejemplo *setmac*.

Hay que tener en cuenta que si hay dos máquinas en la red con la misma dirección MAC podemos tener problemas, aunque generalmente en las redes *wireless* esto no suele ser un problema muy grave ya que el punto de acceso no puede distinguir que verdaderamente hay dos máquinas con la misma MAC. De todas formas, se puede "anular" a la máquina que le hemos "robado" la dirección MAC. Para hacer ésto, se debe implementar un ataque de Denegación de Servicio (DoS).

2.5.2 Ataque de Denegación de Servicio (DoS o *jamming*)

Para realizar este ataque basta con poner un *sniffer* durante un momento en la red y ver cual es la dirección MAC del punto de acceso. Una vez conocemos su MAC, nos la ponemos y actuamos como si fuéramos nosotros mismos el PA. Lo único que se tiene que hacer para denegarle el servicio a un cliente es mandarle continuamente notificaciones (*management frames*) de desasociación o desautenticación. Si en lugar de a un sólo cliente queremos denegar el servicio a todos los clientes de la WLAN, mandaremos estas tramas a la dirección MAC de *broadcast*.

2.5.3 Descubrir ESSID ocultados

Como se ha comentado anteriormente, para que un cliente y un PA se puedan comunicar, ambos deben tener configurado el mismo ESSID, es decir, deben pertenecer a la misma red *wireless*.

Una medida de seguridad bastante común es “ocultar” el ESSID, es decir, hacer que el PA no mande *BEACON FRAMES*, o en su defecto no incluya el ESSID en éstos.

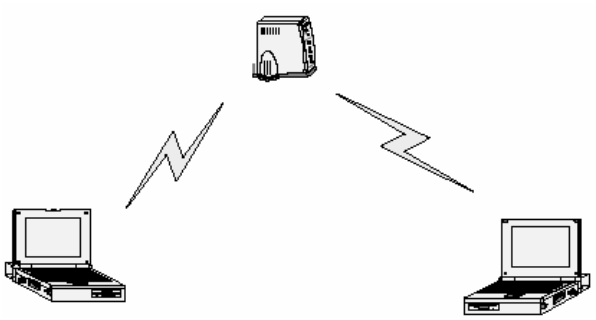
En este caso, para descubrir el ESSID deberíamos colocar un *sniffer* y esperar a que un cliente se conecte, y veríamos el ESSID en la trama *PROVE REQUEST* del cliente (en el caso de que no se manden *BEACON FRAMES*), o en la trama *PROVE RESPONSE* del PA.

Pero también se puede “provocar” la desconexión de un cliente, utilizando el mismo método que en el ataque DoS, pero mandando sólo una trama de desasociación o de desautenticación en lugar de mandarlas repetidamente, es decir, nos ponemos la dirección física del PA y mandamos una trama DEAUTH o DISASSOC a la dirección MAC del cliente (o a la de broadcast), entonces el cliente intentará volver a asociarse o autenticarse, con lo que se podrá ver el ESSID en los *management frames*.

2.5.4 Ataque de intercepción / inserción (*man in the middle*)

El ataque de *Man in the middle*, también conocido como *monkey in the middle* consiste en convencer al cliente (la víctima) de que el host que hay en el medio (el atacante) es el PA, y hacer lo contrario con el PA, es decir, hacerle creer al PA que el atacante es el cliente.

Figura 17. Red *Wireless* antes del ataque “*man in the middle*”



Fuente: Pau Oliva Fora. **(In) seguridad en redes 802.11b.** Pág. 23.

Para realizar este ataque, primero debemos tener el detalle de un *sniffer*, para obtener:

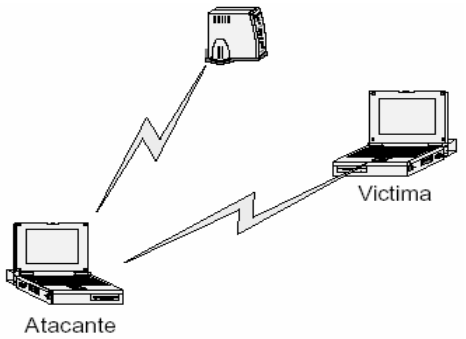
- El ESSID de la red (si estás ocultado, usaremos el método para obtener los ESSID).
- La dirección MAC del PA.
- La dirección MAC de la víctima.

Una vez conocemos estos datos, utilizaremos el mismo método que en el ataque DoS, para desautenticar a la víctima del PA real, es decir, realiza el ataque haciéndose pasar por el PA y manda tramas DEAUTH a la víctima. La tarjeta Wi-Fi de la víctima empezará entonces a escanear canales en busca de un PA para poderse autenticar, y ahí es donde entra el atacante.

El atacante hace creer a la víctima que él es el PA real, utilizando la misma MAC y el mismo ESSID que el PA al que la víctima estaba autenticada anteriormente, pero operando por un canal distinto. Para realizar esto la tarjeta Wi-Fi del atacante debe estar en modo master (como se vio en el capitulo 1).

Por otra parte, el atacante debe asociarse con el PA real, utilizando la dirección MAC de la víctima. De esta manera hemos conseguido insertar al atacante entre la víctima y el PA. Veamos como quedaría la WLAN después de realizar el ataque.

Figura 18. Red *wireless* después del ataque "*man in the middle*"



Fuente: Pau Oliva Fora. **(In) seguridad en redes 802.11b.** Pág. 24.

De esta manera todos los datos que viajan entre la víctima y el PA pasan a través del atacante. Como el ataque ha sido realizado a nivel de enlace de datos (nivel 2), el atacante puede ver, capturar e incluso modificar las tramas en los niveles superiores del modelo OSI.

Muchas soluciones de seguridad están pensadas asumiendo que las capas 1 y 2 son seguras, ésto como hemos visto es incierto para las redes *wireless,* por tanto el uso según qué tipo de solución podría no ser adecuado para estas redes.

Hay que ir con mucho cuidado sobre todo en implementaciones de VPN que no realizan las comprobaciones necesarias de autenticación para protegerse de ataques *Man in the middle* en redes *wireless*.

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

Las redes *wireless* son especialmente vulnerables a los ataques de monitorización, siendo el único requisito para su realización la conectividad, es decir, la posibilidad de acceso al flujo de datos. La identificación de redes es el método para detectar la existencia de un PA a una red inalámbrica.

Dentro del mundo *wireless*, no podemos dejar de lado dos prácticas que se han extendido rápidamente entre algunas comunidades de usuarios de esta tecnología, sobre todo con el ánimo de conseguir acceso gratuito a Internet.

2.5.5.1 Técnicas de búsqueda y marcado de redes *wireless*

Antes de salir en busca de una red *wireless*, hay que configurar el equipo que nos permitirá detectar la red.

Material a utilizar para la práctica de búsqueda y marcado de redes *wireless*:

- Ordenador portátil o PDA.
- Tarjeta Wi-Fi con *firmware* adecuado.
- Programa o *driver* que permita poner la tarjeta en modo monitor.
- *Sniffer*.

Se debe poner la tarjeta Wi-Fi o WNIC en modo monitor (visto en el capítulo 01); este modo es parecido al modo “promiscuo” de las tarjetas *Ethernet* convencionales, lo que hace es dejar la tarjeta “a la escucha” por la frecuencia utilizada en 802.11b (2.4 Ghz). El método para poner la tarjeta en modo monitor es distinto para cada sistema operativo, y para cada tipo de tarjeta (según *chipset*).

En este punto, ya estamos listos para salir a la calle en busca de una red *wireless*. Es aconsejable desplazarse a poca velocidad, moverse cerca de los edificios y hacerlo preferiblemente en horario laboral.

Según el medio de transporte que utilicemos, esta práctica se denomina de la siguiente manera:

- *WarWalking*: Caminando
- *WarSkating*: En patines
- *WarCycling*: En bicicleta
- *Wardriving*: En automóvil
- *WarFlying*: En avión

El *sniffer* más cómodo para estas prácticas es el Netstumbler (para ambiente Microsoft®), ya que emite un tono por la salida de audio cuando detecta una red *wireless*. Se suele colocar la computadora portátil en una mochila, con los auriculares conectados, y el monitor en modo *stand-by* (para ahorrar batería).

Podemos utilizar el *kismet* o el *Airsnort* (para ambiente Linux), que permiten comunicación directa con dispositivos GPS. Cuando el *sniffer* detecta una WLAN, guarda un registro con toda la información que ha podido obtener de la red mientras hemos tenido cobertura, si disponemos de GPS podemos saber en que posición exacta estaba situada la red y que área de cobertura tenía.

2.5.5.1.1 Wardriving

La implementación práctica de los ataques de escucha se conoce como *wardriving* (con su evolución de *drive-in hacking*), consiste en localizar e identificar puntos de acceso (PA) a lo largo del territorio. Carreteras, calles, aeropuertos, parques, centros comerciales, etc., cualquier ubicación puede ser rastreada. Adicionalmente, existen programas que pueden trabajar de forma conjunta con un receptor GPS, lo que permite que pueda localizarse de manera muy precisa (latitud, longitud, datos adicionales como SSID) la ubicación de los distintos PA.

2.5.5.1.2 Warchalking

Es un lenguaje de símbolos normalmente escritos con tiza en las paredes, que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto para que puedan localizarla fácilmente.

La sencillez del lenguaje ha sido uno de los factores que han hecho posible su proliferación en las grandes ciudades. Además otras características como la no perdurabilidad de las marcas durante grandes períodos de tiempo hacen que sea muy dinámico y se vaya adaptando constantemente a las características cambiantes de las redes sobre cuya existencia informa.

Una vez detectada la existencia de una red abierta, se suele dibujar en el suelo una marca con la anotación de sus características.

La convención de símbolos utilizada es la siguiente:

Tabla II. Simbología del *warchalking*.

Símbolo	Significado
SSID)(Ancho de banda	Nodo abierto
SSID ()	Nodo cerrado
SSID Contacto (W) Ancho de banda	Nodo WEP

Por ejemplo, si se colocara o se encontrara el siguiente dibujo, se debería entender así:

Genovia
)(
1.5

Indicaría un nodo abierto, que utiliza como SSID: “Genovia” y que dispone de un ancho de banda de 1.5 Mbps. Estos son los pasos para el marcado de un punto:

1. En primer lugar se identifica el nombre del nodo, o SSID.
2. En segundo lugar se identifica el tipo de red, bien sea abierta, cerrada o con WEP.
3. En último lugar se identifica el ancho de banda del mismo.

Esta simbología permite disponer de un mapa donde constan los puntos de acceso con sus datos (SSID, WEP, direcciones MAC,...). Si la red tiene DHCP, el ordenador portátil se configura para preguntar continuamente por una IP de un cierto rango; si la red no tiene DHCP activado podemos analizar la IP que figure en algún paquete analizado.

Este mecanismo de detección de redes inalámbricas nos muestra lo fácil que es detectarlas y obtener información (incluso introducirnos en la red).

2.6 Futuros cambios

Siendo conscientes de las debilidades del estándar 802.11 en su protocolo WEP, se formó el comité 802.11i para mejorar los aspectos de

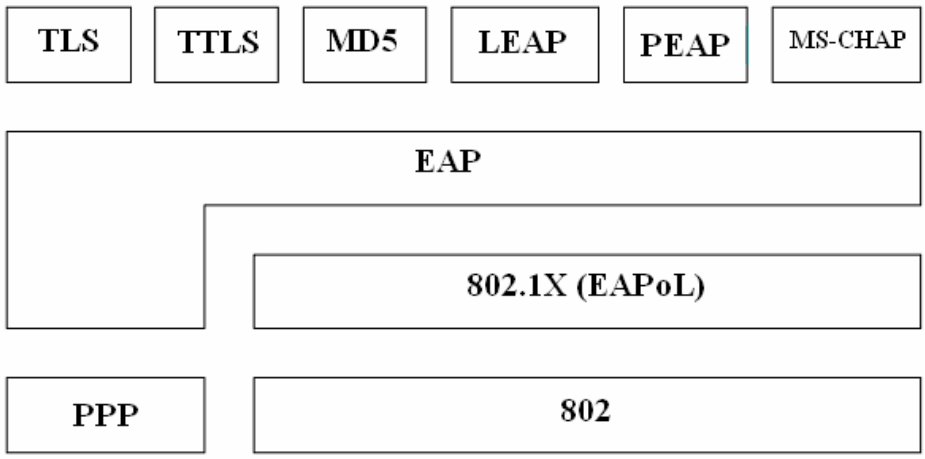
seguridad en las redes inalámbricas. A continuación se describirán algunos de los nuevos protocolos que pueden ayudar en este gran problema, como lo es la seguridad *wireless*. Estos protocolos, aún estén en su fase de estudio y por lo tanto que algunos no estén certificados por la IEEE, pero la mayoría ya está bien detallada y desarrollada.

2.6.1 Los protocolos ULA (*Upper Layer Protocol*)

Los protocolos ULA proporcionan intercambio de autenticación entre el cliente y un servidor de autenticación. Un ejemplo claro de esto es el EAP (*Extensible Authentication Protocol*), que es un protocolo originalmente creado para realizar autenticación sobre enlaces PPP, soportando varios mecanismos de autenticación. Este protocolo es una extensión del Protocolo Punto a Punto (PPP).

EAP se desarrolló como respuesta al aumento de la demanda de autenticación de usuarios de acceso remoto mediante otros dispositivos de seguridad. EAP proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. EAP, junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario e investigación de contraseñas, que otros métodos de autenticación.

Figura 19. Esquema de ubicación del protocolo EAP



Fuente: Gonzalo Galván, Manuel Ardoy**. EAP – PPP *Extensible Authentication Protocol*.** Pág. 02.

Entre los protocolos de autenticación sobre EAP:

EAP-TLS (*Extensible Authentication Protocol with Transport Layer Security*), Este protocolo proporciona autenticación mutua, negociación cifrada e intercambio de claves entre extremos. Soporta fragmentación y reensamblaje de mensajes. Está basado en certificados y soportado por Windows XP®. Necesita la configuración de la máquina para establecer el certificado e indicar el servidor de autentificación.

EAP-TTLS (EAP *With Tunneled Transport Layer Security*), este protocolo no necesita que ambas partes estén certificadas. Solo necesita certificado el servidor de autenticación. En el intercambio de mensajes inicial se utiliza un ID de usuario y un *password*. Una vez realizada la autenticación inicial, se crea un túnel seguro que se utiliza para intercambiar información segura adicional. Está

implementado en algunos servidores *Radius* y en *software* diseñado para utilizarse en redes 802.11 (inalámbricas).

PEAP (*Protected Extensible Authetication Protocol*). Protocolo desarrollado por Microsoft®, CISCO® y RSA®. Similar a EAP-TTLS, al igual que éste solamente el servidor de autentificación necesitaría un certificado. Proporciona canales seguros para otros protocolos de autenticación como MSCHAPv2.

EAP-MD5, Método de autenticación por desafío. El servidor envía un mensaje “desafío” al cliente que quiere ser autenticado, el cliente debe responder a la petición con otro mensaje MD5 o con un mensaje NAK. Si el cliente envía un paquete NAK está rechazando la autenticación. Es el más sencillo de implementar, pero el menos fiable.

LEAP (*Lightweigh* EAP), propiedad de Cisco® y diseñado para ser portable a través de varias plataformas *wireless*. Basa su popularidad por ser el primero y durante mucho tiempo el único mecanismo de autenticación basado en *password* y proporcionar diferentes clientes según el sistema operativo.

MS-CHAP, protocolo Microsoft® de autenticación por desafío mutuo. Es conocido también como MS-CHAPv1.

Proceso de desafío mutuo:

1. El autenticador envía al cliente un identificador de sesión y una cadena de desafío arbitraria.

2. El cliente envía como respuesta el nombre del usuario y un cifrado no reversible de la cadena de desafío, el identificador de sesión y la contraseña.

3. El autenticador comprueba la respuesta y, si es válida, se autentican las credenciales del usuario.

Las medidas que el comité 802.11i está estudiando intentarán mejorar la seguridad de las redes inalámbricas. Los cambios se fundamentan en tres puntos importantes, organizados en dos capas.

A un nivel más bajo, se introducen dos nuevos protocolos de encriptación sobre WEP totalmente compatibles entre sí, el protocolo TKIP (*Temporal Key Integrity Protocol*) y el CCMP (*Counter Mode with CBC-MAC Protocol*), que se describen a continuación, junto con el estándar 802.1x para el control de acceso a la red basado en puertos.

2.6.2 Estándar 802.1x

Es un estándar de control de acceso a la red basado en puertos. Como tal, restringe el acceso a la red hasta que el usuario se ha validado.

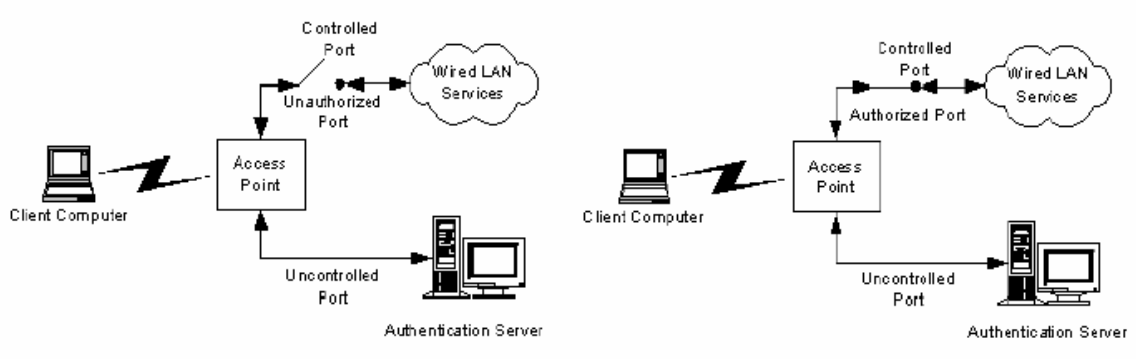
El sistema se compone de los siguientes elementos:

- Una estación cliente.
- Un punto de acceso.
- Un servidor de autenticación (AS).
- Entidad de puerto de acceso (*port access entity* o PAE)

Es este nuevo elemento, servidor de autenticación (AS), el que realiza la autenticación real de las credenciales proporcionadas por el cliente. El AS es una entidad separada situada en la zona cableada (red clásica), pero también implementable en un punto de acceso. El tipo de servidor utilizado podría ser el *Radius*, u otro tipo de servidor que se crea conveniente (802.1x no especifica nada al respecto).

El estándar 802.1x introduce un nuevo concepto, el concepto de puerto habilitado/inhabilitado, por el cual hasta que un cliente no se valide en el servidor no tiene acceso a los servicios ofrecidos por la red. El esquema posible de este concepto lo podemos ver a continuación:

Figura 20. Esquema puerto habilitado/inhabilitado 802.1x



Fuente: Vicent Alapont Miquel**. Seguridad en redes inalámbricas.** Pág. 11.

En sistemas con 802.1x activado, se generarán 2 llaves, la llave de sesión (*pairwise key*) y la llave de grupo (*groupwise key*). Las llaves de grupo se comparten por todas las estaciones cliente conectadas a un mismo punto de acceso y se utilizarán para el tráfico *multicast*; las llaves de sesión serán únicas para cada asociación entre el cliente y el punto de acceso y se creará un puerto privado virtual entre los dos.

El estándar 802.1x mejora la seguridad proporcionando las siguientes mejoras sobre WEP:

- Modelo de seguridad con administración centralizada.
- La llave de encriptación principal es única para cada estación, por lo tanto, el tráfico de esta llave es reducido (no se repite en otros clientes).
- Existe una generación dinámica de llaves por parte del servidor de autenticación (AS), sin necesidad de administrarlo manualmente.
- Se aplica una autenticación fuerte en la capa superior.

2.6.3 TKIP (*Temporal Key Integrity Protocol*)

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP y mantener la compatibilidad con el *hardware* utilizado actualmente mediante una actualización del *firmware*.

El protocolo TKIP está compuesto por los siguientes elementos:

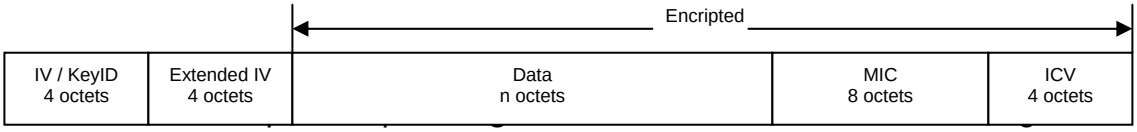
- Un código de integración de mensajes (MIC), encripta el *checksum* incluyendo las direcciones físicas (MAC) del origen, del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.

- Contramedidas para reducir la probabilidad de que un atacante pueda utilizar una determinada llave

- Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

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

Figura 21. Estructura de encriptación TKIP



Fuente: Vicent Alapont Miquel**. Seguridad en redes inalámbricas.** Pág. 13.

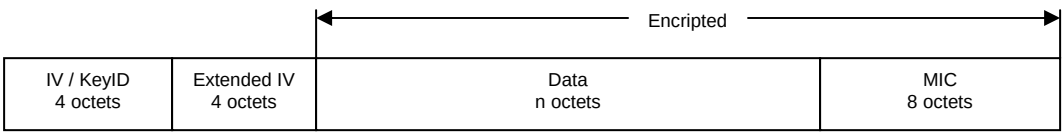
La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiarse 248 paquetes utilizando una sola llave temporal antes de ser reutilizada.

2.6.4 CCMP (*Counter Mode with CBC-MAC Protocol*)

Este protocolo es complementario al TKIP y representa un nuevo método de encriptación basado en AES (*Advanced Encryption Standards*), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizando 802.11i.

En la siguiente figura podemos observar el formato tras la encriptación CCMP:

Figura 22. Estructura de encriptación CCMP



Fuente: Vicent Alapont Miquel**. Seguridad en redes inalámbricas.** Pág. 13.

CCMP utiliza un vector de inicialización de 48 bits denominado Número de Paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

3. ESTUDIO DE CAMPO DE UNA RED *WIRELESS* Y SU SEGURIDAD

3.1 Descripción de la red real

Lugar: Hightech (centro de negocios y mercadeo).
Ubicación: Calzada Roosevelt 22-43 zona 11. Edificio Tikal Futura, torre Luna, nivel 2 Of. 267. Guatemala, Guatemala.

Este lugar es uno de los llamados “café Internet”, el cual presta servicio de Internet para los clientes que así lo deseen. Cuenta con la facilidad de proveer acceso a Internet en ese mismo centro y cuenta con un total de 40 máquinas con la última tecnología para poder accesar. También tiene en su disposición el servicio de *HotSpot* que hasta el momento es único verdadero en su clase, en Guatemala, ya que puede dar servicio de Internet por medio de una red inalámbrica que está colocada en los tres primeros niveles del edificio Tikal Futura.

Cuenta con puntos de acceso ubicados en lugares estratégicos, para poder prestar el servicio de Internet a cualquier persona que desee accesar, siempre y cuando cumpla con algunas especificaciones tanto de *hardware* como de *software*.

Qué es un *HotSpot*: Es un PA inalámbrico público donde los usuarios pueden conectarse a Internet. El servicio de *Hotspot* se puede encontrar sin costo, o bien, con diferentes tarifas o renta del servicio. Las redes inalámbricas son instaladas en lugares públicos (librerías, cafeterías, restaurantes, hoteles

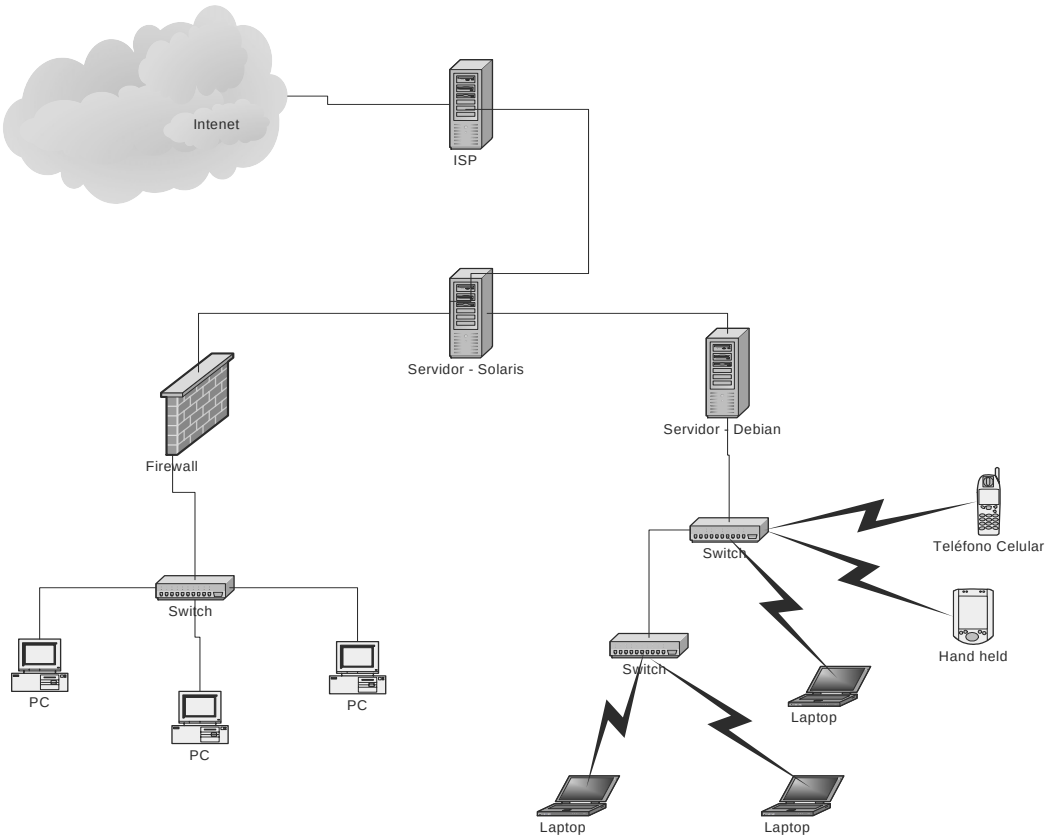
etc.) y permiten conectar a Internet computadoras portátiles entre otros dispositivos móviles sin necesidad de cables, siempre y cuando el usuario se encuentre dentro de la zona de cobertura de la red y cuente con el equipo adecuado.

Un servicio *Hotspot* se basa en el protocolo estándar de comunicación inalámbrica IEEE 802.11b, también conocido como Wi-Fi.

3.1.1 Arquitectura de la red

La arquitectura de red implementada es una de estrella, tanto para la red que es alámbrica como para la red inalámbrica.

Figura 23. Arquitectura de red, alámbrica e inalámbrica de Hightech



3.1.2 Topología de la red

La topología de red inalámbrica que se tiene implementada es una del tipo infraestructura, ya que cuenta con varios puntos de acceso los cuales son los que dan la señal a las computadoras personales, no así a los PDA's que llegan con la intención de conectarse a Internet, dado que para ello debería de estar implantada una topología *ad-hoc* o lo que es lo mismo punto a punto (por ejemplo *bluetooth*).

3.1.3 Cobertura

La cobertura que se tiene es amplia, llegando hasta los 50 metros a la redonda; este dato depende de la infraestructura del edificio, ya que cuenta con un PA que brinda conexión en cada uno de los tres primeros niveles del edificio Tikal Futura.

Se cuenta con cuatro puntos de acceso instalados en los siguientes lugares:

1. Se tiene instalado el primer PA dentro de las instalaciones de Hightech, debido a que es el encargado de dar el servicio, en parte del primero y segundo nivel de la torre Luna, del edificio de Tikal Futura.

2. El segundo PA está situado en el segundo nivel, que cubre toda la parte del *lobby* del edificio, y la parte de la torre Sol tanto el primero como el segundo nivel.

3. Un tercer PA está instalado en el tercer nivel del edificio. Éste le brinda servicio a toda el área de restaurantes que tiene el edificio Tikal Futura.

4. El último de los puntos de acceso está instalado en el segundo nivel del área de entretenimiento, donde están los cines y el área de boliches.

Figura 24. Colocación y cobertura de puntos de acceso dentro del edificio. Vista superior o planta

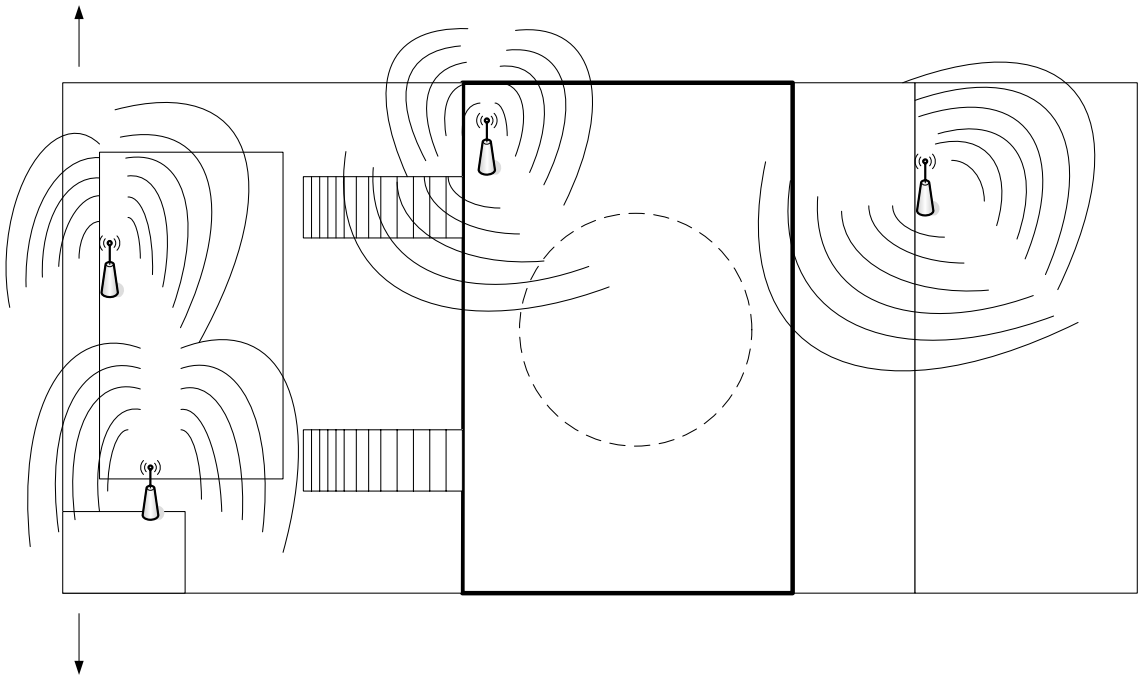
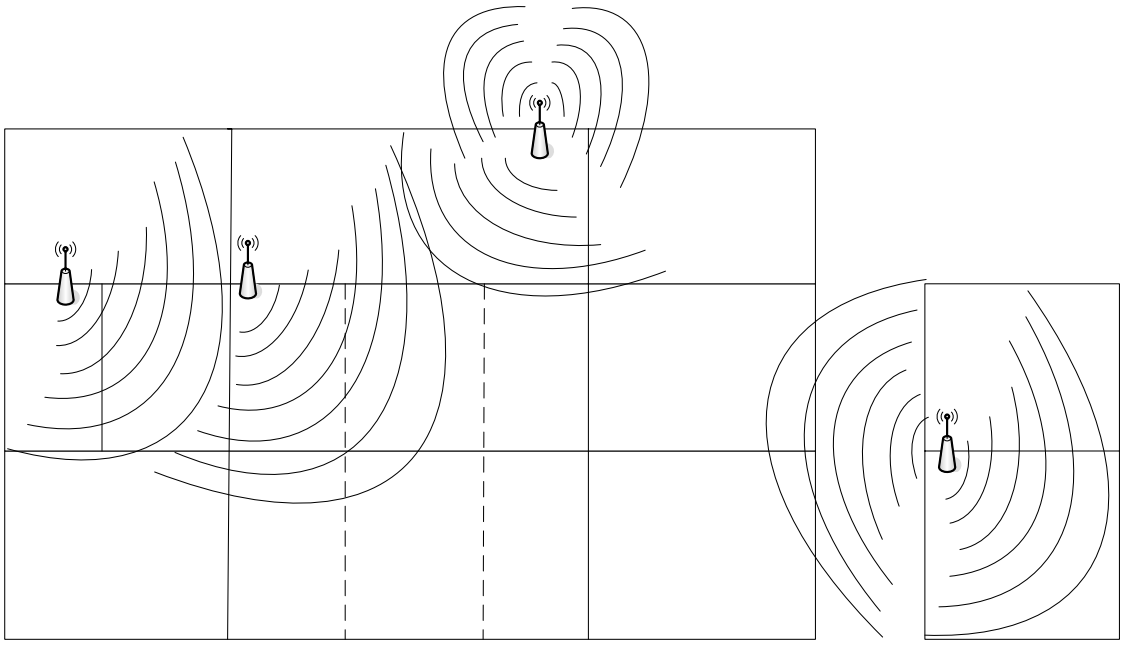


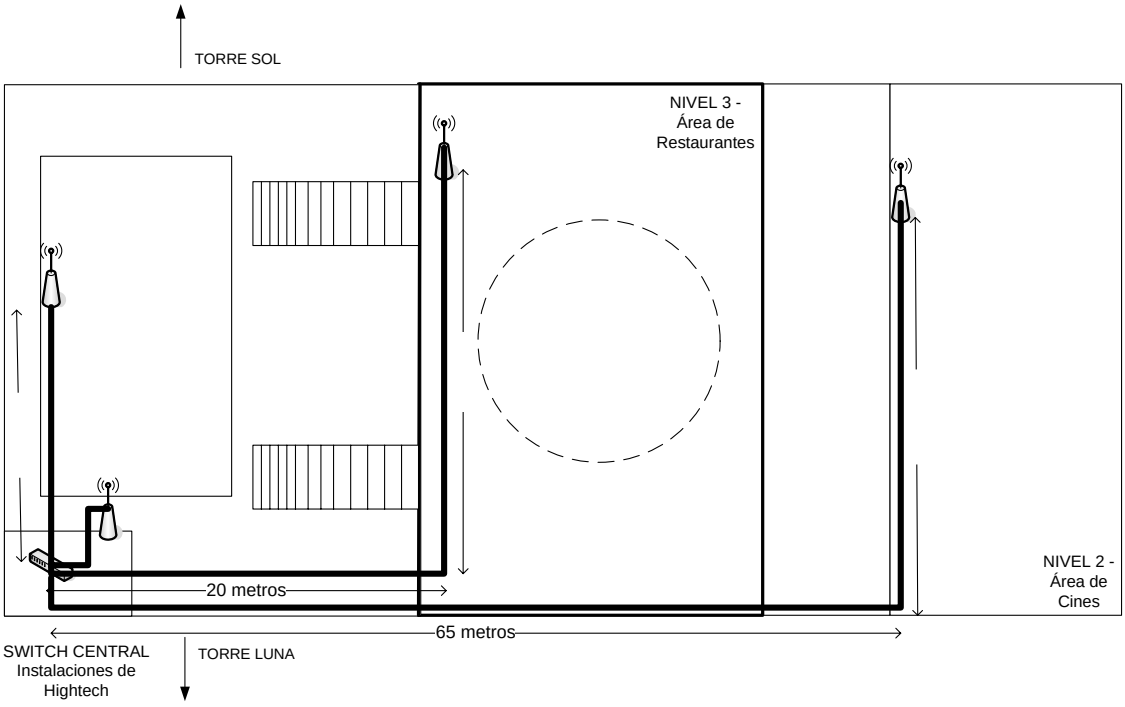
Figura 25. Colocación y cobertura de puntos de acceso dentro del edificio. Vista lateral derecha



Dentro de los ascensores que tiene el edificio, no se tiene muy buena recepción de la señal que lanzan los puntos de acceso, ya que estos están hechos de varias capas de materiales que aíslan el interior de cualquier señal externa. Por ello hasta los teléfonos celulares pierden la señal en esos lugares.

Algo importante a resaltar es que los adaptadores de red *wireless* o tarjetas de red inalámbricas buscan la señal que los puntos de acceso les otorgan, haciendo primero que todo un escaneo de señal, como se indicó en el capitulo 2, en la sección 2.2 Proceso de Conexión a una WLAN; esto lo hace la tarjeta para unirse como cliente del PA con la señal más intensa, para una buena comunicación en la red inalámbrica.

Figura 26. Distancia entre cada punto de acceso dentro del edificio. Vista superior o planta



Cada PA está conectado con un *switch* central que está instalado dentro de las instalaciones de Hightech por medio de cable UTP categoría 5. Este *switch* tiene ocho puertos en total, de estos solamente cinco están siendo utilizados, cuatro para conectar cada uno de los PA y uno que va directamente al servidor instalado con Linux Debian, el cual presta servicio de conexión inalámbrica.

3.1.4 Compatibilidad con redes existentes

La compatibilidad con las redes existentes es la adecuada, ya que se hicieron varias pruebas para poder llegar a una comunicación aceptable. Las

pruebas realizadas se llegaron a efectuar a través de varios pasos, los cuales se describen a continuación:

Paso 1. Se realizaron las pruebas con un punto de acceso y una *laptop*, se configuró el punto de acceso de la forma estándar, es decir, con las configuraciones que viene de fábrica, pero esto no funcionó de esta manera porque los puntos de acceso en su configuración para el "*performance*" o modo de actuación del punto de acceso en su opción de "*Basic Rates*" y "*TX Rates*", tenía colocado una velocidad de transmisión de 1 a 2 Mbps. Por lo tanto la transmisión no era lo suficientemente buena para poder dar señal de Internet a la *laptop*, en un radio mayor de los 5 metros. Para solucionar este problema se colocó en estas opciones la velocidad de transmisión de 1 – 2 – 5.5 – 11 Mbps.

Paso 2. Se probaron varios canales de transmisión, los cuales pueden oscilar para el punto de acceso desde el 1 hasta el 9. Debido a las demás redes inalámbricas configuradas en el edificio, se logró establecer una buena comunicación en los canales 1, 6 y 9.

Paso 3. Se colocó a todos los puntos de acceso el código de la red inalámbrica o SSID, igual a "Hightech". Con ésto lográbamos que todos los puntos de acceso estuvieran en la misma red.

Paso 4. Como último paso se colocaron los modos de encriptación del WEP y *Radius* en estado de no disponible. Esto porque es una red pública y no se necesita de esta configuración, ya que si la colocáramos, todas las personas que deseen entrar a la red para utilizar el Internet debería de tener ésto configurado y lo que se pretende es prestar el servicio con la mayor comodidad y facilidad posible.

Cabe mencionar que dentro del edificio de Tikal Futura existe otra red inalámbrica ubicada en el décimo nivel de la torre Luna, la misma torre en la cual está instalada la de Hightech, solamente que esta segunda tiene cobertura exclusiva para ese nivel, a diferencia de la red pública que trabaja Hightech, ésta es una red privada que pertenece a una empresa privada.

3.1.5 Interoperabilidad con dispositivos inalámbricos

Hasta el momento la red inalámbrica que tiene implementada Hightech, solamente puede dar acceso a Internet a computadoras portátiles o *laptops*, por lo que dispositivos como celulares o PDA's que tengan acceso a Internet no pueden accesar a la red.

3.1.6 Interferencia y coexistencia

La interoperabilidad con los distintos dispositivos inalámbricos que se manejan dentro del edificio de Tikal Futura, como por ejemplo los celulares o Palmtop's, antenas de radio frecuencia, radio transmisores o cualquier dispositivo inalámbrico que se utilice, tiene muy baja interferencia y hacen que la señal proporcionada por los puntos de acceso sea de muy buena calidad, es por ello que la velocidad de transmisión o ancho de banda es tan bueno que casi llega a los 5.5 Mbps. reales.

3.1.7 Simplicidad y facilidad de uso

El acceso al Internet, por ser un servicio público, su facilidad de uso y acceso debe ser muy fácil; esto no quiere decir que no se tomen las medidas respectivas para el acceso desde la red inalámbrica a la red interna que tiene los servidores de acceso.

El acceso se controla por medio del ESSID de la red, es decir el nombre de 32 caracteres que identifica a cada red inalámbrica; ésto se configura en la tarjeta de red inalámbrica que debe contar el usuario para la conexión.

Es por ello que cuando se tiene ya configurada la red a la que se quiere tener acceso inalámbrico, en el momento que se ejecuta el explorador de nuestra elección (Internet Explorer®, Netscape Navigator®, etc.), siempre tendrá como página de inicio la seleccionada por Hightech, esta página será la única a la que tenga acceso para navegar en Internet.

3.1.8 Seguridad

Esta es la parte más importante de la red y está construida confiable y segura. El procedimiento para que se lleve a cabo es de la siguiente manera:

Por medio de una página en la cual se ingresa un usuario y una contraseña válida que se compara contra una base de datos para recibir el tiempo de Internet estipulado para ese usuario en particular.

Este usuario y contraseña son enviados encriptados hacia el servidor que está en una plataforma Linux Debian, el cual hace la autenticación y la autorización para el usuario que acaba de ingresar.

3.2 Búsqueda e identificación de la red inalámbrica por medio de la herramienta Netstumbler.

Netstumbler es una herramienta que trabaja sobre la plataforma Windows® y su objetivo primordial es la búsqueda e identificación de redes inalámbricas. Existen dos versiones de éste programa, una para PC’s (0.29

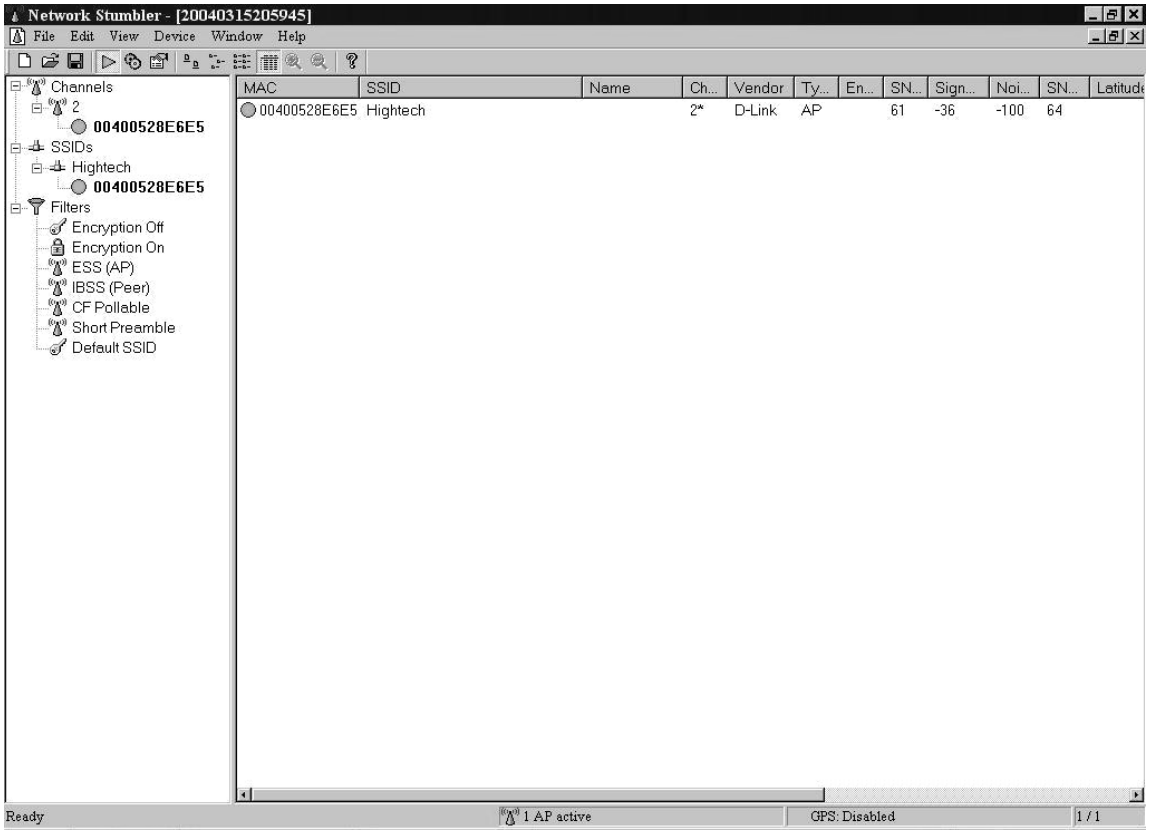
Mb.) y la otra que es para *PocketPC* (0.14 Mb.). Las dos se pueden conseguir en www.netstumbler.com y lo mejor es que son totalmente gratis.

Es muy fácil de utilizar ya que emite un tono por la salida de audio cuando detecta una red *wireless*, con estas características lo hacen especial para poder realizar un ataque a las redes inalámbricas llamado “de escucha y monitorización pasiva (*eavesdropping*)”, como se vio anteriormente consiste en la monitorización de la red *wireless*, lo cual es una vulnerabilidad de las redes inalámbricas, siendo el único requisito para su realización la conectividad, es decir, la posibilidad de acceso al flujo de datos. La identificación de redes es el método para detectar la existencia de un PA en una red inalámbrica.

Cuando el sniffer detecta una WLAN, guarda un registro con toda la información que ha podido obtener de la red mientras hemos tenido cobertura, si dispusiéramos de GPS podríamos saber en que posición exacta está situada la red y que área de cobertura tiene, para este caso como no contamos con un GPS debido al costo que implica, por ello no se describirá el funcionamiento de esta parte, pero sí la detección de la red y sus características.

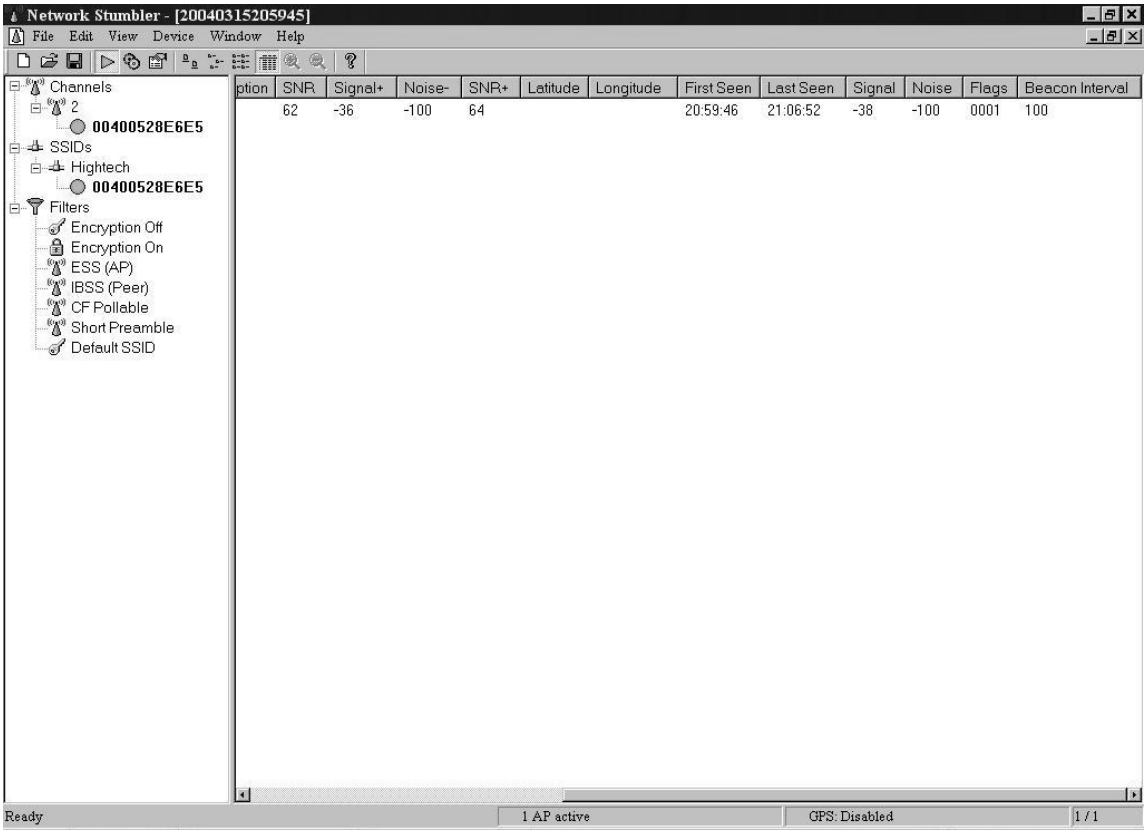
En la siguiente gráfica de la pantalla de resultados de Netstumbler se divide en dos partes, una muestra la descripción en forma de árbol de los diferentes PA encontrados en la red y la segunda parte muestra la descripción por dirección MAC de cada punto de acceso.

Figura 27. Netstumbler – Pantalla de identificación de redes. Primera parte



Se puede observar que existe activo un PA, el cual tiene como SSID asignado el nombre de Hightech, también está la dirección MAC y el número de canal por el que está transmitiendo señal, que para este caso es el número 2. En la parte *Vendor,* que significa el fabricante del PA; tiene D-Link®; como se dijo anteriormente, todos los PA en la red de Hightech son de la marca mencionada. En encriptación no tiene asignado ningún valor, ya que no está actualmente utilizando esta propiedad que trae el PA.

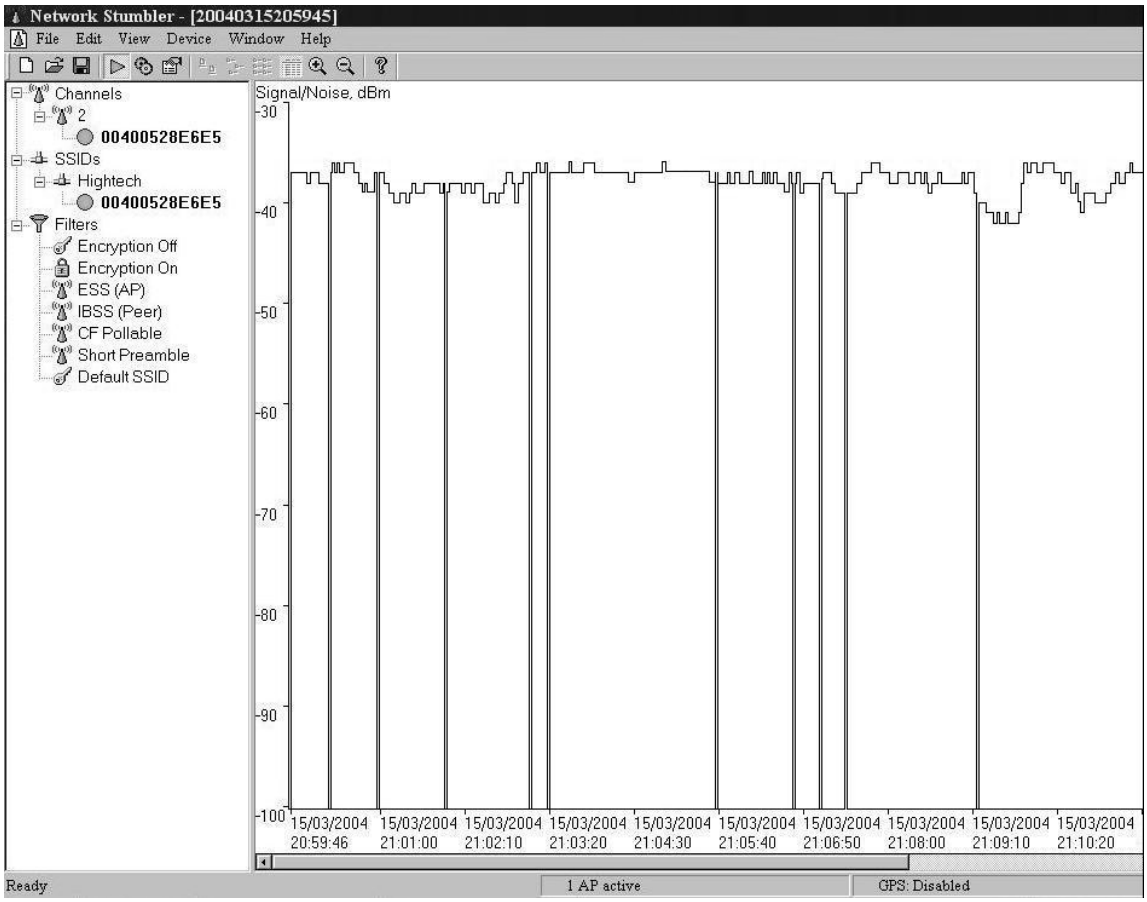
Figura 28. Netstumbler – Pantalla de identificación de redes. Segunda parte



La gráfica anterior es continuación de la ventana de características de un PA. Encontramos otros datos, por ejemplo, están los *Beacon Frames* igual a 100 milisegundos, son anuncios que el PA manda constantemente para que los clientes móviles puedan detectar su presencia y conectarse a la red *wireless*.

Si nos damos cuenta, existen dos características: *Latitude* que significa latitud y *Longitude* que significa longitud, estas no tienen ningún dato asignado, porque no contamos con un GPS instalado para obtener estos valores.

Figura 29. Netstumbler – Pantalla que muestra la gráfica de señal contra tiempo



La gráfica anterior muestra la fuerza de señal con que recibe la tarjeta *wireless* instalada en nuestra computadora personal, comparada contra el tiempo transcurrido cada minuto aproximadamente. La señal está dada en dBm, lo cual significan Decibel Miliwatt Como nos damos cuenta en esta gráfica, la señal indica un total de -38 dBm, la cual es una medida totalmente normal. Si tomamos el valor del ruido igual a -100 dBm junto con el valor de la señal nos dará un total de 62 dB (Decibeles). Según formulas, este valor se describe así:

Señal (*Signal*) = -38 dBm = 1mW - 38dB
Ruido (*Noise*) = -100 dBm = 1mW - 100dB
SNR = 38 dBm – (-100 dBm) = (1 mW – 38 dB) - (1 mW – 100 dB)
SNR = (1mW - 1mW) + (100 dB - 38dB)
SNR = 62 dB.

Para representar la fuerza de una señal inalámbrica no es muy común utilizar la medida Decibel, son más conocidos los dBm o Decibeles Miliwatt.

Con estos datos podemos puntualizar que la señal es lo suficientemente fuerte en el lugar donde se probó la herramienta *Netstumbler* y no deberíamos de tener problemas en lo que respecta a conexión a la red *wireless.*

3.3 *Software* y *hardware* utilizado

Los requerimientos de *software* y *hardware* que se utiliza en Hightech son los siguientes:

3.3.1 Configuración mínima de cliente inalámbrico

Todo cliente que desee conectarse en forma inalámbrica al Internet, debe contar con las siguientes especificaciones de *hardware* y *software,* mínimas para un buen rendimiento dentro en su navegación:

Hardware:

- Procesador de 1.0 Ghz. (Mínimo).
- Memoria RAM de 128 Mb. (Mínimo).
- Dispositivo para conectarse a una Red *Wireless* (preferiblemente que sean de marca D-Link):

- Tarjeta de Red *Wireless* PCI 2.4 Ghz. (802.11b).
  Transferencia de Datos de 11 y 22 Mbps.
  Soporte WEP para encriptación de 64/128/256 bits.

Figura 30. Tarjeta PCI 2.4Ghz. (802.11b), marca D-Link

Fuente: Accesorios *Wireless*. **Tarjeta PCI 2.4 Ghz**. www.d-link.com.

- Tarjeta de Red *Wireless* PCMCIA 2.4 Ghz. (802.11b).
  Transferencia de Datos de 11 y 22 Mbps.
  Soporte WEP para encriptación de 64/128/256 bits.

Figura 31. Tarjeta PCMCIA 2.4Ghz. (802.11b), marca D-Link

Fuente: Accesorios *Wireless*. **Tarjeta PCMCI 2.4 Ghz**. www.d-link.com.

- Adaptador USB *Wireless* 2.4 Ghz. (802.11b).
  Transferencia de Datos de 11 y 22 Mbps.
  Soporte WEP para encriptación de 64/128 bits.

Figura 32. Adaptador USB *wireless* 2.4Ghz. (802.11b), D-Link

Fuente: Accesorios *Wireless*. **Adaptador USB *Wireless* 2.4 Ghz**. www.d-link.com.

Software:

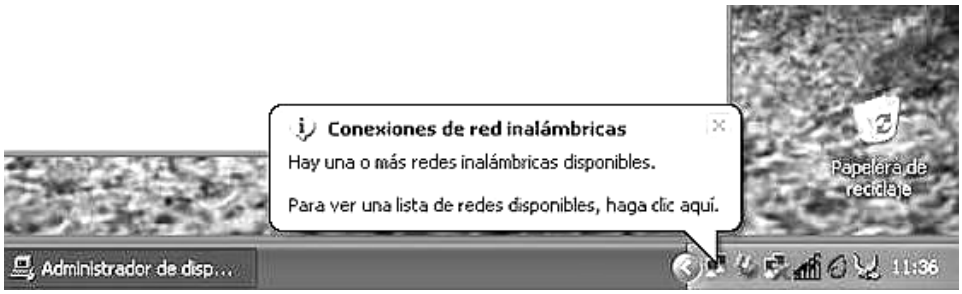
- Sistema Operativo Microsoft Windows 9x/2000/XP (preferiblemente) o Sistema Operativo Linux o Sistema Operativo Mac OS X (10.2 o superior).
- Controladores de Dispositivo para conectarse a la Red *Wireless* Instalados, de su respectiva marca.

3.3.2 Configuración de tarjeta de red inalámbrica

La configuración de una tarjeta de red inalámbrica en el sistema operativo Microsoft Windows XP® se hace de la siguiente manera:

Paso 1. Los equipos que cuentan con un sistema operativo Windows XP® reconocen por defecto la tarjeta inalámbrica y por lo tanto no hace falta instalarla (se instala sola al introducirla en la ranura PCMCIA). Una vez instalada, el propio sistema operativo hace una búsqueda de redes inalámbricas disponibles, por lo que si nos encontramos en alguna zona con cobertura de red *wireless*, esta la detectará y nos saldrá un aviso similar al siguiente:

Figura 33. Mensaje al instalar una tarjeta *wireless* en Windows XP

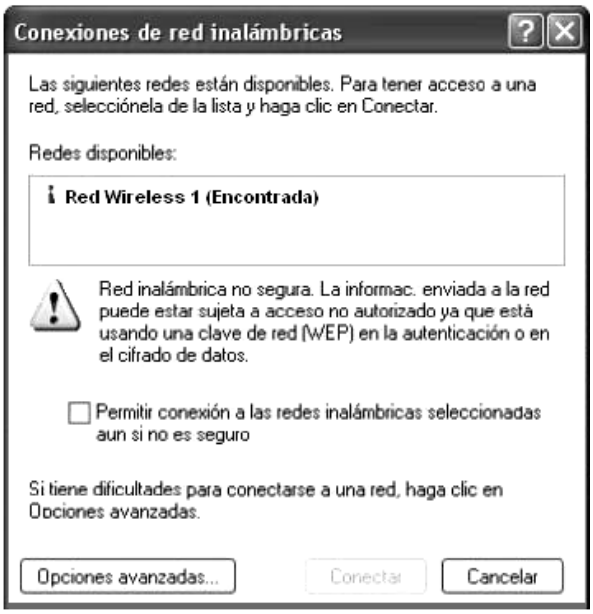


Fuente: Universidad Alicante. **Instalación *wireless* para Windows XP.** Pág. 1.

Como podemos observar: ahora Windows XP® nos informa que ha detectado una o varias redes inalámbricas disponibles.

Paso 2. Hacemos clic en el icono que se nos indica y luego aparece una ventana donde seleccionamos y pulsamos el botón de Conectar.

Figura 34. Ventana de conexiones encontradas por tarjeta *wireless* en Windows XP



Fuente: Universidad Alicante. **Instalación *Wireless* para Windows XP.** Pág. 1.

3.3.3 Configuración de un punto de acceso (a*ccess point*)

Los puntos de acceso que están instalados en Hightech tienen las siguientes especificaciones:

- D-Link *AirPlus Wireless Access Point* 2.4 Ghz. (802.11b) Modelo: DWL-900AP+.
  Soporta productos con encriptación WEP de 64/128/256 bits.
  Totalmente compatible con el estándar 802.11b.
  5 Diferentes modos de configuración.

Tabla III. Diferentes configuraciones para un PA

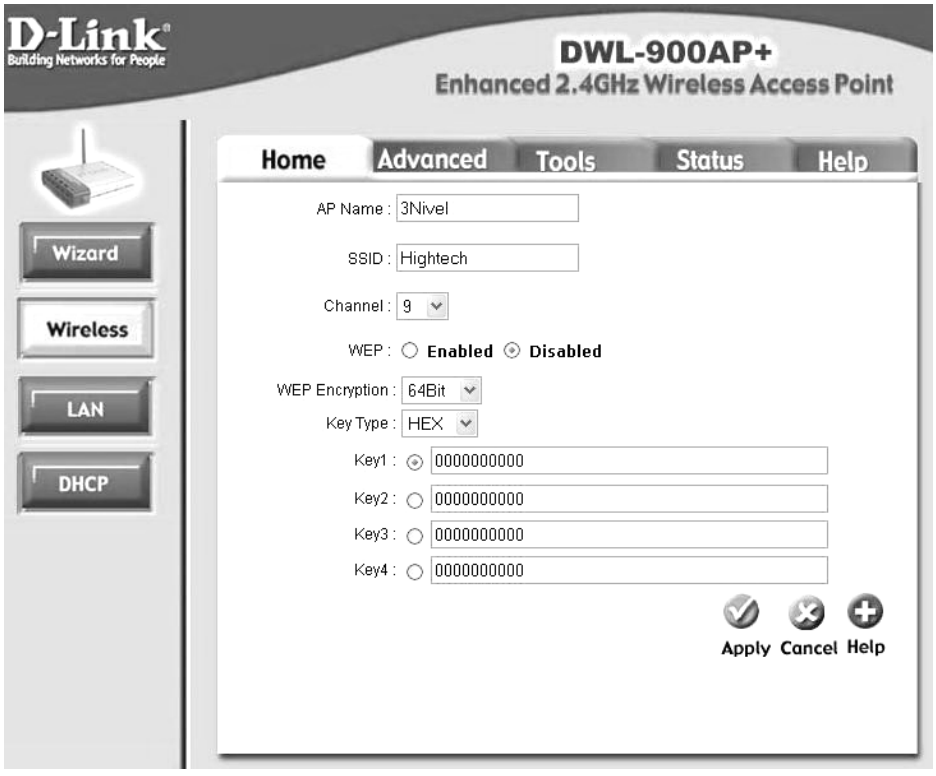
Punto de acceso – *access point*	Crea una red de área local.
Punto de acceso a punto de acceso - *Access point to access point (bridging).*	Inalámbricamente conecta dos redes diferentes. Provee una solución de costo-efectivo para interconectar redes, cuando tradicionalmente las soluciones alámbricas pueden ser muy costosas o prohibidas.
Punto de acceso a multipunto – *access point to multipoint (bridging)*	Inalámbricamente conecta multiredes. Actúa como un *Hub* inalámbrico que conecta múltiples redes.
Cliente *wireless*	Interconecta dispositivos *Ethernet*. Provee inmediata conexión para dispositivos *ethernet* sin la necesidad de un controlador del dispositivo.
Repetidor *wireless*	Extiende el rango de una red inalámbrica.

Como se mencionó anteriormente en este capítulo, existen en la red inalámbrica de Hightech 4 puntos de acceso, los cuales tienen la misma configuración.

Para acceder a cualquiera de lo PA que están instalados, el servidor DHCP les otorga un número de IP, el cual sirve para poder configurarlos desde un navegador de Internet, con solo acceder a él por el número de IP.

Páginas de configuración de un PA de la marca D-Link, con modelo DWL-900AP+.

Figura 35. Página de configuración PA – Datos de la red



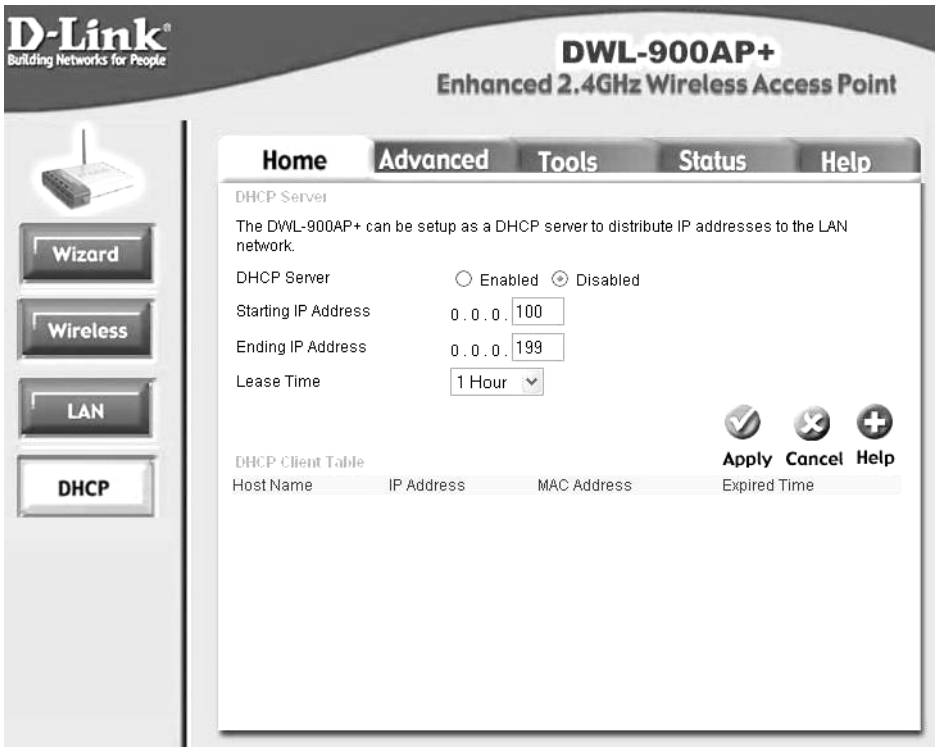
En esta página como se observa está configurado, primero que todo, el nombre del PA el cual para cada uno instalado en la misma red tiene que ser

diferente. Un nombre de red *wireless* o SSID, es el que identifica de cualquier otra red *wireless* que esté cerca. Cada punto de acceso tiene configurado como predeterminado el canal de transmisión No. 9.

Se puede observar como el protocolo de seguridad WEP está inhabilitado, dando oportunidad a que cualquier intruso pueda tomar el punto de acceso y hacer un ataque al 802.11b. En caso que el WEP estuviera habilitado, la configuración del punto de acceso en su encriptación puede cambiar; en este caso vemos que tiene 64 bits, pero también este modelo cuenta con encriptación de 128 y 256 bits.

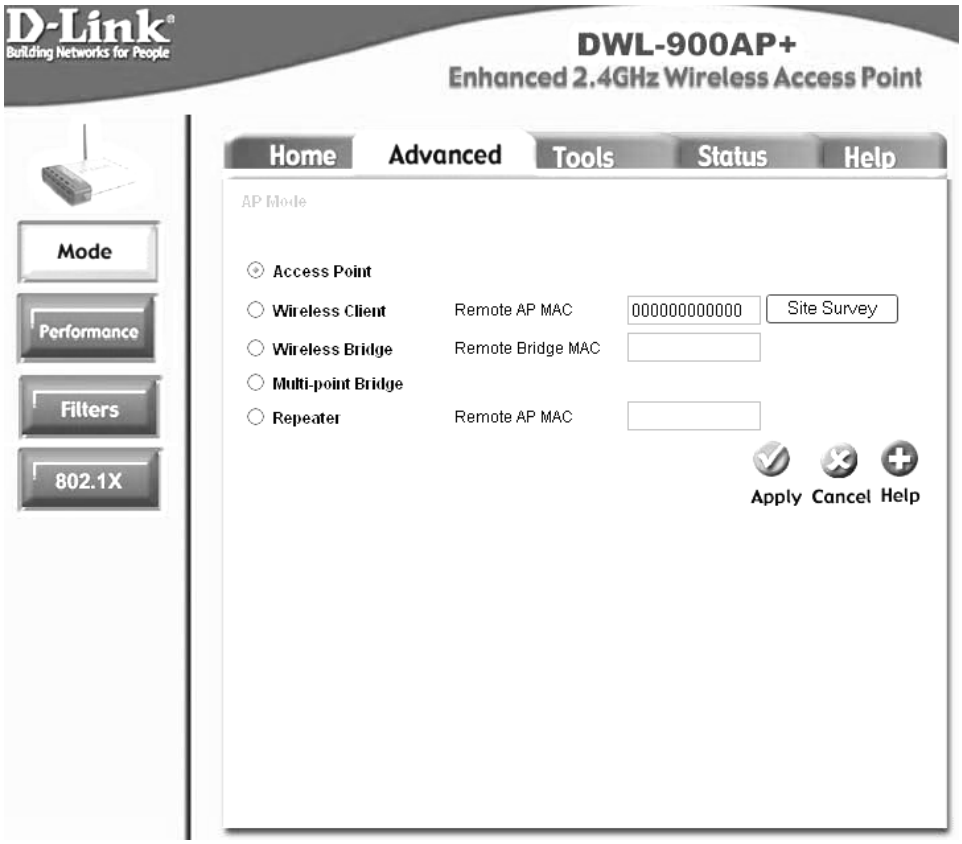
El espacio permite que se coloquen hasta un máximo de 4 llaves y se escoja la que se esté utilizando actualmente.

Figura 36. Página de configuración PA – Configuración de DHCP



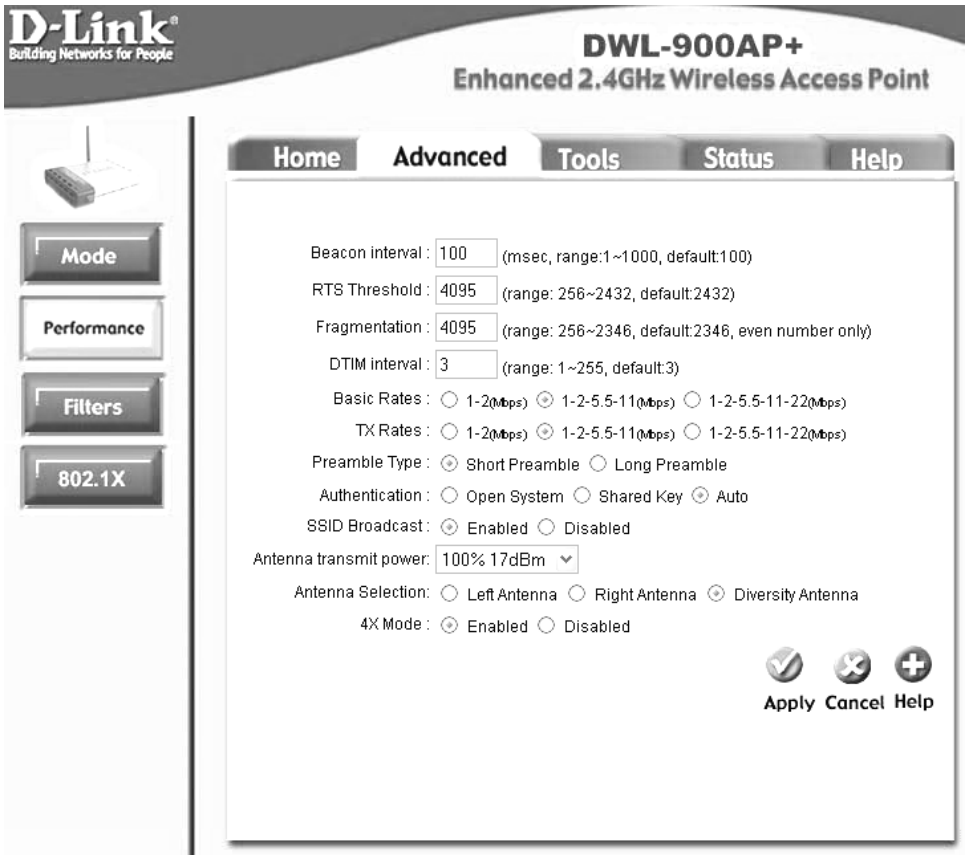
Esta página es donde se configura el DHCP que el PA puede otorgar, en caso no se tuviera un servidor DHCP en nuestra red. Se puede observar que para este caso de Hightech está inhabilitado, debido que se tiene un servidor de DHCP es el encargado de dar las direcciones IP, tanto para las computadoras que lo solicitan de la red interna alámbrica como para toda la parte de la red inalámbrica.

Figura 37. Página de configuración PA – Configuración del modo de funcionamiento



En la página anterior se observa como se configura el modo en que queremos que trabaje nuestro PA. Vimos anteriormente que en la tabla hay cinco modos de funcionamiento, para este caso tenemos configurado en la página el dispositivo como un punto de acceso o *access point.*

Figura 38. Página de configuración PA – Configuración de modo de actuación



La página anterior muestra toda la configuración de cómo se desea que el PA interactúe con los diferentes dispositivos de red inalámbricos. Se puede observar en la gráfica varios datos, los cuales pueden ser modificados para una aceleración o disminución de velocidad en la transmisión.

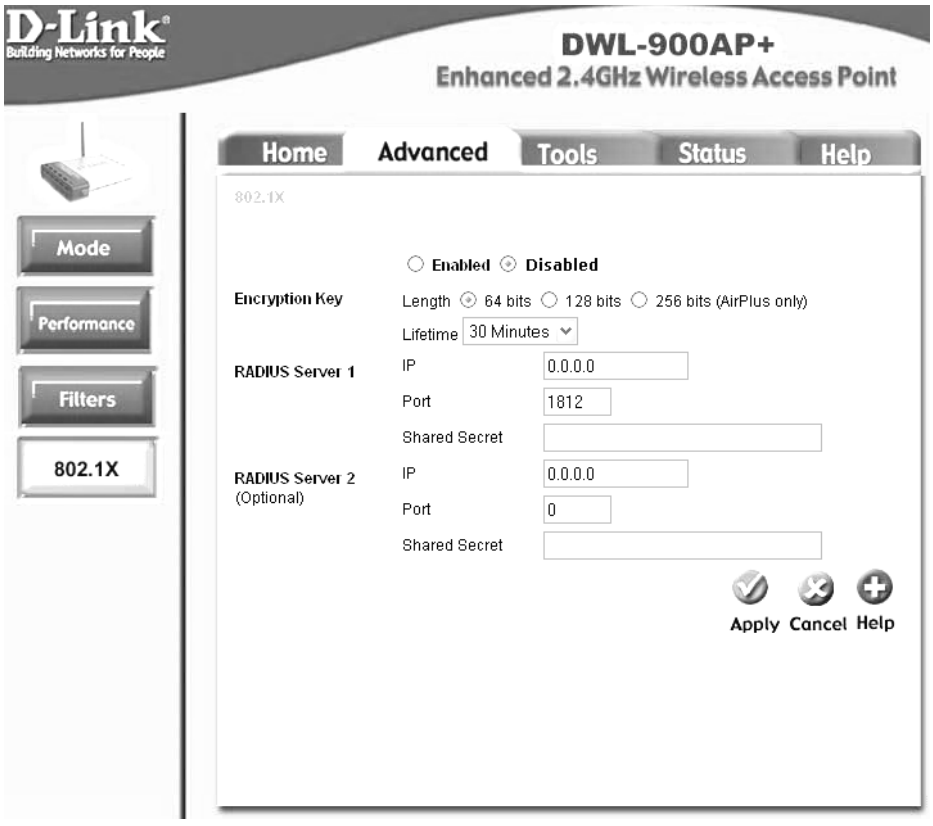
Vemos que hay una opción donde están los Rangos Básicos (*Basic Rates*), los cuales pueden ser los rangos siguientes:

- 1 - 2 Mbps.

- 1 - 2 - 5.5 - 11 Mbps.
- 1 - 2 - 5.5 - 11 - 22 Mbps.

Se debe tener cuidado al seleccionar estos rangos ya que hay diferentes tarjetas de red inalámbricas que no trabajan a todas las velocidades de transmisión descritas. Para poner un estándar se puede colocar la segunda opción que está entre 1 - 2 - 5.5 - 11 Mbps. Esta configuración la tiene Hightech y ha trabajado exitosamente.

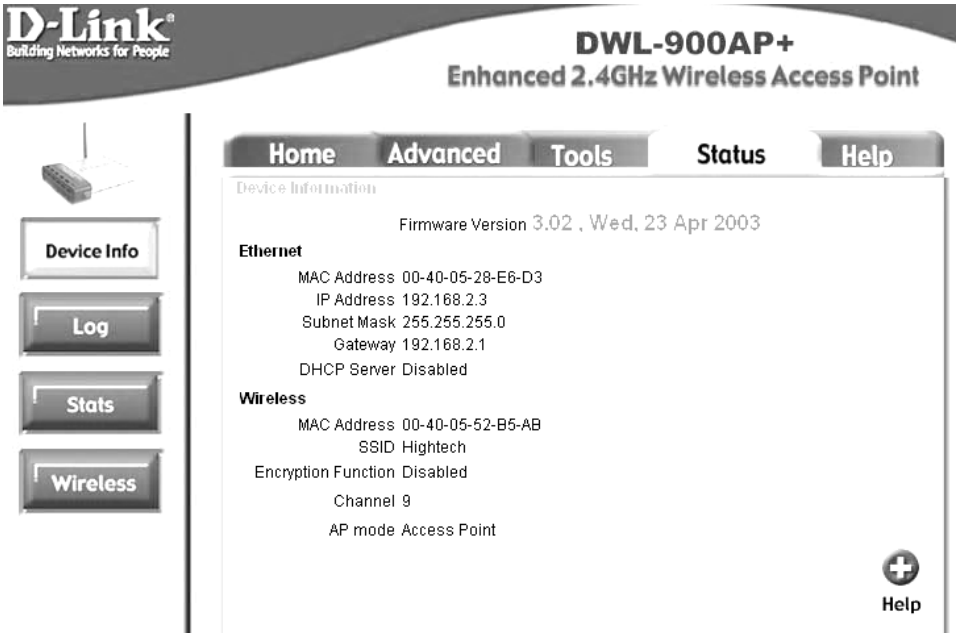
Figura 39. Página de configuración PA – Configuración de 802.1X y *Radius*



Como se ha mencionado, los PA pueden trabajar con el protocolo 802.1X que es uno de los más nuevos para redes inalámbricas.

Se observa en la figura que está inhabilitado para este caso, ya que Hightech no necesita de este servicio, debido a que el servicio que presta es para todo público y sería muy incómodo para el cliente estar configurando en cada momento que se conecta una configuración diferente, este es el objetivo de ser *hotspot*.

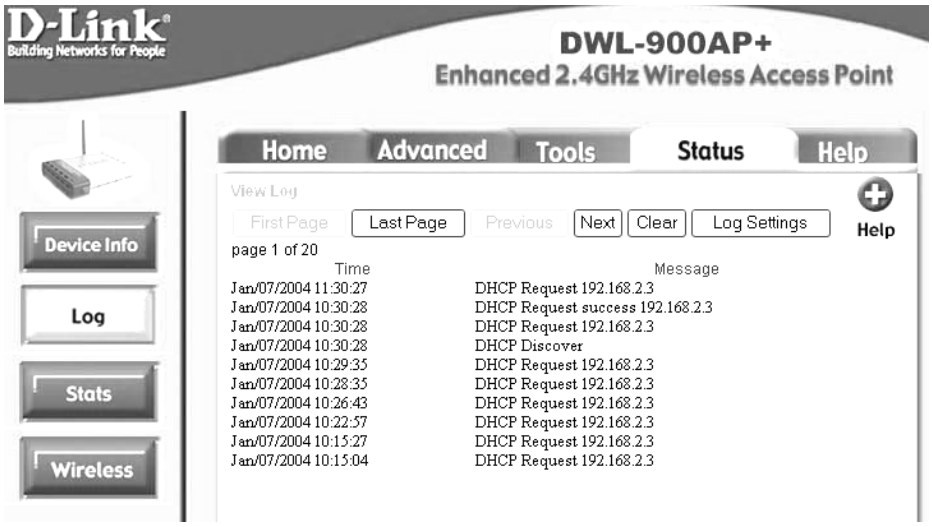
Figura 40. Página de configuración PA – Estado de la conexión del punto de acceso



La página anterior muestra como está todo el estado del PA. Como se puede observar nos indica cuál es su dirección MAC asignada, así como la dirección IP que le otorgó el servidor DHCP con su máscara de red y su número de puerta de salida o *gateway*.

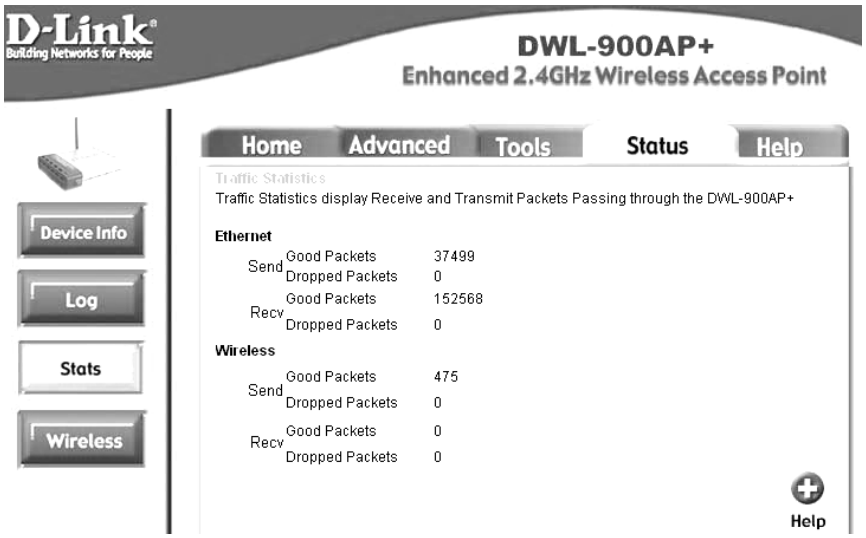
Nos muestra por separado toda la configuración que tiene para la parte de *ethernet* y la parte de *wireless*, esto para poder comunicarse tanto con la red alámbrica como con la red inalámbrica.

Figura 41. Página de configuración PA – Bitácora de estado del PA



El punto de acceso va guardando automáticamente en su bitácora todo lo sucedido desde que se activó, por lo que quedaran registrados todos los números de IP que acceden a él, por lo tanto los paquetes que recibe y reenvía.

Figura 42. Página de configuración PA – Estado de estadísticas



En esta página se tiene solamente una vista de los número de paquetes enviados exitosamente por el PA, tanto los paquetes buenos como los paquetes perdidos. En la página vemos que no hay ningún paquete perdido y todos han sido exitosamente entregados.

3.3.4 Servidores

Linux Solaris. Este servidor es el encargado de hacer la conexión entre el ISP y la red que distribuye el Internet a la red alámbrica e inalámbrica. Aparte de proporcionar el Internet a Hightech, tiene instalado DHCP con el que lleva la administración de que IP's ha otorgado a cada máquina que así lo solicite, tanto para la red alámbrica como para la red inalámbrica.

Tiene dos conexiones físicas con el ISP, ya que cuenta con dos números de IP públicos por los cuales salen la red alámbrica y la red inalámbrica al Internet. Esto se hace para que no disminuya demasiado el ancho de banda, cabe mencionar que para la red alámbrica se tiene actualmente disponible un ancho de banda de 1 Mbps. y para la red inalámbrica se da acceso a los clientes que la utilicen con un máximo de 128 Kbps.

Sus especificaciones son las siguientes:

- Procesador de 1.4 Ghz.
- 512 Mb. de RAM.
- 20 Gb. de Disco Duro.

Linux Debian. Este servidor es el encargado de administrar toda el área de la red inalámbrica, aquí es donde llegan las autenticaciones y autorizaciones que se dan a los diferentes usuarios que estén solicitando tiempo en Internet.

Este desencripta la información y compara el usuario ingresado con su respectiva *password* o contraseña contra una base de datos plana, donde se lleva actualmente la información de los tiempos de ingresos, fechas y estadísticas de velocidades alcanzadas.

Sus especificaciones son las siguientes:

- Procesador de 1.4 Ghz.
- 512 Mb. de RAM.
- 20 Gb. de Disco Duro.

Firewall. Se cuenta con un *firewall* dedicado exclusivamente para la red alámbrica; está configurado sobre Linux y solamente permite el acceso sobre algunos puertos como por ejemplo el 80 (http) o 21, 22 (ftp), los necesarios para una navegación satisfactoria.

3.4 Análisis de costos vrs. beneficios

La seguridad implementada hasta el momento por Hightech es bastante eficiente, por lo cual se debe seguir manteniendo el mismo nivel de seguridad en el que está para la parte de autenticación y autorización de personas que deseen accesar a Internet, desde cualquier parte de los tres primeros niveles del edificio de Tikal Futura.

Se recomendaría tomar alguna medida contra algunos de los ataques mostrados en el capitulo dos contra las redes *wireless* y el estándar 802.11b. Por ejemplo, estos son los problemas analizados en la arquitectura de la red:

Problema No. 1: Ataque de negación de servicio. Éste suele ser un ataque bastante frecuentado por los *hackers*, ya que le permite como cliente *wireless* poder hacerse pasar por un punto de acceso con una señal suficiente como para poder confundir a otro cliente y hacer que éste espere señal inalámbrica y no poder recibirla nunca, ya que se le está denegando y con ésto tener muy baja intensidad de señal por parte del cliente y piense que no tiene una red inalámbrica activa.

Solución al problema No. 1: Se puede llevar una mejor administración sobre las redes inalámbricas activas dentro del edificio por medio de un detector de redes inalámbricas. Éstos hacen un escáner sobre cada punto de acceso que estén detectando y verifican que éste sea autorizado por la empresa, ésta autorización puede ser por medio del número de dirección MAC que tiene cada punto de acceso asignado.

El costo que implicaría hacer este trabajo es bajo y los beneficios que se obtienen es considerablemente superior. De no hacer éste escaneo se tiene la probabilidad que un día se note baja la intensidad de señal en los clientes *wireless* y no se pueda saber la razón por que está sucediendo ésto, si ya se revisaron todas la conexiones alámbricas entre los puntos de acceso y el servidor de Internet y todo lo concerniente a la capa física está en su lugar, así como después de hacer un estudio de intercepción de señal que pueda existir para que no esté llegando la señal con toda su potencia hacia algún lugar en especial: se tiene que tomar en consideración que un *hacker* puede estar robando señal de un punto de acceso para poder así hacer que el negocio que tiene Hightech no pueda superarse.

Problema No. 2: Ataque de intercepción/inserción. Éste ataque es conocido también como “*man in the middle”* ya que consiste en colocar tres

actores, por una parte está el cliente *wireless* que lo único que quiere es obtener servicio de Internet, por otro lado está el punto de acceso instalado por las personas de Hightech y luego está el atacante para quien su mayor logro sería poder interceptar la señal de los dos y poder hacerse pasar por el punto de acceso, otorgándole al cliente su servicio de Internet sin ningún problema, pero este cliente no se daría cuenta que está exponiendo toda la información importante que tenga en su *laptop* o cualquier PDA que esté utilizando para la conexión inalámbrica y se la está otorgando sin ningún problema al *hacker*.

También el *hacker* tendría la posibilidad de poder obtener información de los servidores de Hightech que están prestando el servicio, pero ya que éstos cuentan con un *firewall* instalado, no le será tan fácil poder accesar a éste.

Solución al problema No. 2: Una solución fácil para ésto es que cada uno de los clientes que deseen conectarse a la red inalámbrica de Hightech tengan instalado un *firewall* para PC, éste haría que el *hacker* no pudiera entrar por algún puerto que esté abierto en la *laptop* por error, en cambio tendría solo permisos para los puertos más comunes para navegar en Internet como lo es el puerto 80 de http y el 21 de ftp.

Problema No. 3: Sobre la topología de la red. La red que se tiene instalada en Hightech utiliza medidas muy buenas sobre seguridad perimetral, como por ejemplo *firewall*, servidores de autenticación, etc. Sin embargo una vez en el interior de la red existen pocos mecanismos de seguridad para detectar un intruso. Esto pasa al conectar una red *wireless* directamente con la red interna, con esto estamos creando un punto de fallo, y entonces toda la seguridad que se tenía falla en un momento dado, haciendo que la red interna se vea comprometida por cualquier independencia de todas las medidas de seguridad perimetrales.

Solución al problema No. 3: Es importante resaltar que por cualquier medida que se tenga de seguridad instalada, hay que tratar de cualquier forma a una red inalámbrica como una red insegura. Una solución para este problema es muy sencilla de implementar, pero es costosa en cuestión de *hardware* que se tiene por instalar, ya que se debería en teoría poder separar ambas redes, tanto la red alámbrica como la red inalámbrica y hacerlas existir como áreas DMZ's seguras e independientes para cada una.

De esta forma se puede administrar mejor el envío de paquetes, clasificar el tipo de tráfico y recursos de la red interna que están accediendo desde la red inalámbrica.

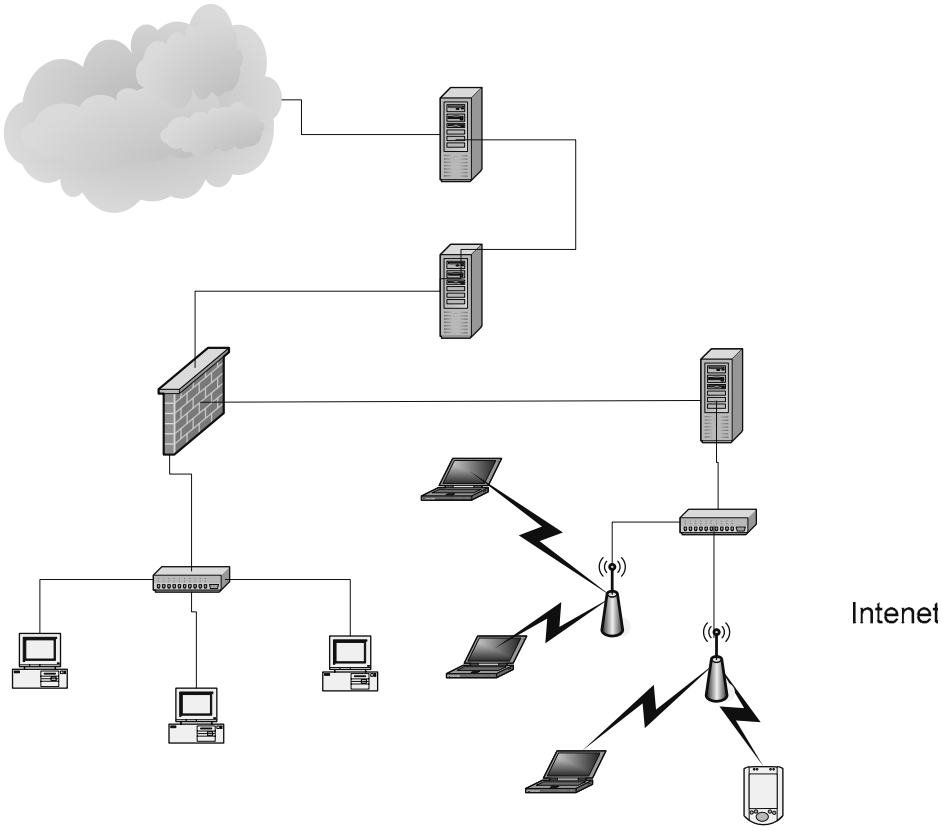
El costo que implicaría hacer una DMZ para cada red es elevado, ya que hay que empezar por cambiar la arquitectura de la red y hacer que todo el tráfico que viene del Internet pase por el *firewall* que sería el primero que recibiría la información para saber qué área puede comunicarse con qué otra área y a través de qué puertos lo tiene permitido.

3.5 Análisis de arquitectura y cobertura existentes.

La arquitectura de la red hasta el momento no ha dado ningún problema y está bien diseñada, ya que cuenta con un *firewall* separando la red que es alámbrica de los servidores, pero su funcionamiento no ha dado problemas en cuestión de seguridad, debido a que no hay mucha demanda actual de la red *wireless*; el problema va a surgir cuando ésta crezca.

Por ello, se muestra en la gráfica siguiente una arquitectura de red que se podría implementar para que no existan problemas más adelante cuando la demanda suba.

Figura 43. Arquitectura de red propuesta para implementar

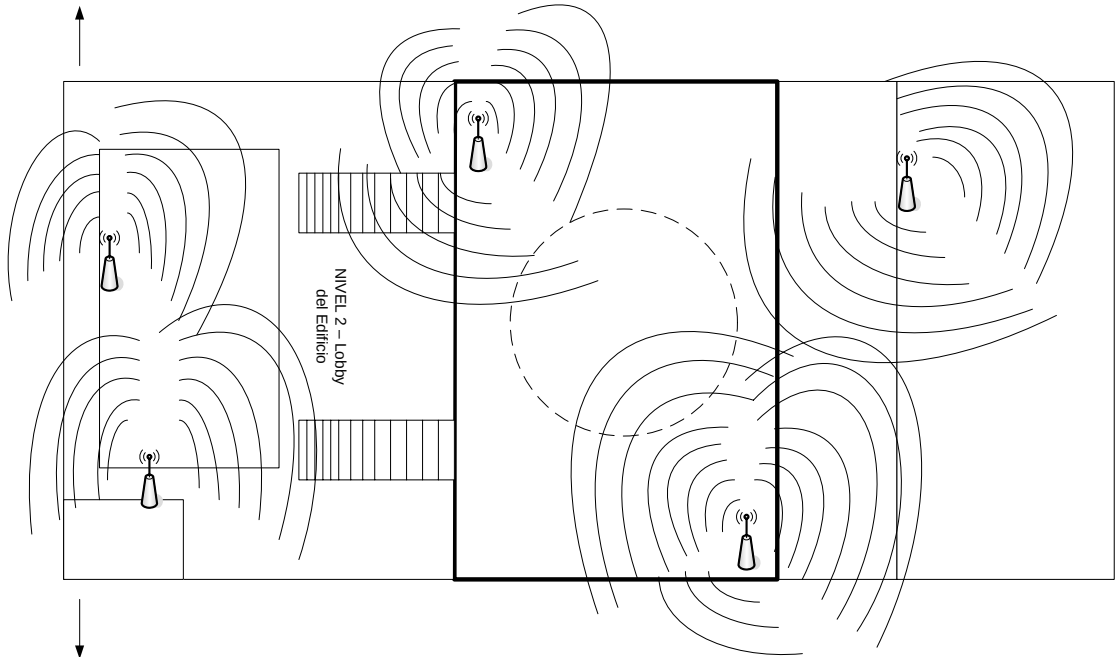


En esta arquitectura propuesta, se puede observar que a diferencia con la actual, tanto la red alámbrica como la inalámbrica están conectadas al *firewall*, desde el cual se podrá administrar de mejor manera la seguridad y los datos que pueden entrar o salir de cualquiera de estas dos redes.

Lo que se pudo observar también dentro de las conexiones entre puntos de acceso, es que se tiene que utilizar demasiado cable UTP para conectar un AP con el *switch* central. Debido a ésto se corre el riesgo que en algún momento se corte la señal en alguno de los puntos de acceso por algún cable que esté cortado o dañado de alguna manera.

Por no tener toda el área necesaria cubierta para el acceso a la red *wireless* del *hotspot*, se podría añadir un punto de acceso más para llegar a tener 5 en total, el cual estaría ubicado en el segundo nivel, pegado al edificio de la torre Luna; ésto haría que los puntos de acceso no estuvieran forzosamente conectados alámbricamente y en lugar de ésto, estarían conectados en cascada, a través de ellos mandando su señal hacia otro punto de acceso ubicado más adelante en el edificio. En una gráfica se vería de la siguiente manera.

Figura 44. Propuesta de colocación de cobertura de puntos de acceso dentro del edificio. Vista superior o planta



Con ésto se pretendería utilizar la propiedad que tienen lo puntos de acceso en poderse comunicar entre ellos y tomar la señal con mayor intensidad entre ellos mismos para lograr una red mucho más extensa. Lo mencionado anteriormente también tiene una desventaja y es que todos los puntos de

acceso para una mejor comunicación y que no existan problemas de compatibilidad deberían ser de la misma marca.

3.6 Siete Pasos para asegurar una red inalámbrica

En primer lugar hay que situarse dentro de lo que significa seguridad en el mundo informático. Se dice que una red es segura cuando casi nadie puede entrar a la misma, o los métodos de entrada son tan costosos que no muchos pueden llevarlos a cabo. Casi nadie puede significar que es segura en un 99.99%, por ello debemos desechar la idea de que los sistemas informáticos son seguros al 100%.

Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener. Se debe tener en cuenta que cuando se trabaja con una red convencional cableada se dispone de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos de comunicación de la misma. En nuestro caso no, de hecho vamos a estar desperdigando la información hacia los cuatro vientos con todo lo que ésto conlleva.

Paso 1, se debe activar el WEP. Parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado. Esto viene a ser como si el cajero de nuestro banco se dedicase a difundir por la radio los datos de nuestras cuentas cuando vamos a hacer una operación en el mismo. WEP no es completamente seguro, pero es mejor que nada.

Paso 2, se debe seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No se

deben usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando los ceros por o es.

Paso 3, uso del OSA (*Open System Architecture*). Esto es debido a que en la autenticación mediante el SKA (*Shared Key Authentication*), se puede comprometer la clave WEP, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos para recoger la suficiente información de la clave, como para exponer la seguridad del sistema.

Paso 4, desactivar el DHCP y activar el ACL (*Access Control List*). Se deben asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de *sniffing* de las direcciones MAC que podría permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones. Pero para la realización de ésto hay que tomar en cuenta la carga administrativa que tomaría llevar el control de inventario de cada tarjeta *wireless* y su dirección MAC asignada, ésto es parte de la responsabilidad que el administrador de la red tiene para con la red a su cargo. Por ello debe tener el debido control sobre ésto tomando en cuenta cada departamento de la empresa y cuantas computadoras conectadas a la red *wireless* existen.

Como en cualquier empresa, no toda la red necesita de la misma seguridad para todas las computadoras, es por ello que en algunos

departamentos se podría tomar esta opción y en otros dejar que el servidor DHCP le asigne un número de IP éstas máquinas; la decisión queda en el administrador de la red y su análisis de que se realizó previo a la instalación de la misma.

Paso 5, cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial preconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar la baja frecuencia de *broadcast* del SSID, deteniendo su difusión a ser posible

Paso 6, hacer uso de VPN's (Redes Privadas Virtuales) para contar con algo extra de seguridad que va a permitir la comunicación entre nuestros dispositivos con seguridad. Si es posible, añadir el protocolo IPSec.

Paso 7, aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un *firewall* que filtre el tráfico entre los dos segmentos de red. Actualmente el IEEE está trabajando en la definición del estándar 802.11i que permita disponer de sistemas de comunicación entre dispositivos *wireless* realmente seguros.

4. PROPLEMAS TÍPICOS Y SU SOLUCIÓN

Siete problemas típicos de seguridad y soluciones recomendadas basado en el artículo de Mathew Gast "*Seven Security Problems of 802.11 Wireless*", O'Reilly *Network*, Mayo 2002.

La rápida expansión de las redes inalámbricas (*wireless*) basadas en el estándar 802.1x ha añadido un nivel adicional de complejidad al problema de la seguridad de redes. Aunque los mencionados estándares incorporan ciertas funciones de seguridad y los diferentes fabricantes de equipos *wireless* han añadido diferentes mecanismos de protección, las redes inalámbricas representan un punto extremadamente vulnerable en la seguridad de una red.

A continuación se describen siete problemas básicos que padecen las redes basadas en el estándar 802.11.

4.1 Puntos de acceso vulnerables

Las redes inalámbricas son fáciles de detectar. Con el objetivo de facilitar la conexión a los usuarios las redes emiten gran cantidad de información acerca de su configuración. Esta información es exactamente lo que un *hacker* necesita para lanzar un ataque.

Las redes 802.11 no utilizan ninguna función de seguridad para proteger esta información. Por tanto, cualquier usuario con una tarjeta *wireless* estándar 802.11 puede acceder a estos datos. Atacantes con antenas amplificadoras pueden acceder a redes ubicadas en otros edificios y a algunas calles de cierta distancia.

Solución:

La solución ideal sería aislar la red inalámbrica de forma que las emisiones electromagnéticas de la red no salieran fuera del perímetro de la empresa o fuera de las habitaciones en las que se utilizase la red. Sin embargo, para la mayoría de empresas ésta no es una solución factible.

En muchos casos una solución eficiente es ubicar los puntos de acceso en redes DMZ (para mitigar cualquier intrusión) y en utilizar VPN's en la comunicación con los usuarios (para proteger el contenido de las transmisiones y poder contar con el sistema de autenticación del servidor de VPN's).

Otra medida de seguridad adicional es autenticar el acceso de los usuarios a través de la red inalámbrica con un servidor de autenticación. Por ejemplo, el estándar 802.1x soporta nuevos tipos de autenticación para integraciones con servidores *Radius*.

4.2 Puntos de acceso no autorizados

Las redes inalámbricas son fáciles de implementar y su precio está al alcance de cualquier usuario. Es relativamente sencillo comprar e instalar un punto de acceso *wireless* sin que éste sea advertido por los administradores de la red. En algunas ocasiones un departamento dentro de la empresa puede decidir instalar sus propios puntos de acceso sin coordinar dicha instalación con los responsables de seguridad.

Al funcionar prácticamente tan pronto como se conecta, la mayoría de puntos de acceso inalámbricos instalados sin supervisión utilizan la

configuración por defecto. El problema principal es que ésta configuración por defecto, normalmente carece de todas las medidas de seguridad aplicables.

Solución:

Auditar las oficinas de la empresa de forma regular con un detector de redes inalámbricas o un *wireless analyzer*. Por ejemplo ésto puede implicar asignar de forma regular un técnico para que se pasee por las oficinas con un ordenador portátil, o una agenda personal PDA, equipada con una herramienta para la detección de puntos de acceso *wireless*.

Existen varias herramientas en el mercado para escanear redes inalámbricas, como por ejemplo los programas Netstumbler® para Windows® y Airtraf para Linux. Algunas funcionan de forma pasiva detectando fuentes de emisión y analizando los datos transmitidos, mientras que otras intentan interrogar los puntos de acceso que encuentran buscando información sobre los mismos.

4.3 Accesos a la red no autorizados

Muchas instalaciones de redes inalámbricas utilizan la configuración por defecto de los equipos realizando los cambios mínimos para que funcionen. Por lo general estas configuraciones no hacen uso de la encriptación WEP (incluida en el estándar 802.11).

Sin WEP es prácticamente inmediato acceder a una red 802.11, aunque se haya restringido el acceso mediante listas de códigos MAC autorizados. Un *hacker* equipado con un *sniffer* puede obtener direcciones MAC válidas en cuestión de segundos, realizar un *spoof* (falsificación) de la dirección MAC de

su tarjeta *wireless* utilizando la de una tarjeta con acceso autorizado, y entrar en la red.

Solución:

La mejor forma para impedir los accesos no autorizados es utilizar un mecanismo de autenticación fuerte protegido mediante encriptación. Por ejemplo, *Transport Layer Security* (TLS), *Protected EAP* (PEAP) o *Tunneled TLS* (TTLS).

4.4 Rendimiento limitado

Las redes inalámbricas tienen una capacidad muy limitada. El estándar 802.11b permite una velocidad nominal de transmisión de 11Mbps, mientras que el 802.11a alcanza los 54Mbps. Debido a la información de control necesaria para mantener la comunicación, la velocidad real (práctica) suele ser la mitad que la velocidad nominal. Además, se trata de una capacidad de transmisión (ancho de banda) que es compartida entre todos los usuarios. La capacidad de transmisión inalámbrica puede saturarse de diferentes maneras:

- Un punto de acceso puede recibir a través de su conexión a la red física un flujo de datos superior al que el canal de radio puede emitir. Un atacante podría lanzar un ataque *ping flood* desde un segmento de red *Fast Ethernet* y saturar rápidamente el punto de acceso.

- Utilizando paquetes de *broadcast*, es posible saturar dos puntos de accesos conectados mediante cable.

- Sin estar conectado a ningún punto de acceso, un atacante puede inyectar datos en el canal de radio y saturar el medio. El estándar 802.11 ha sido diseñado para permitir la coexistencia de varias redes en un mismo canal de radio. Todo lo que el atacante ha de hacer es llenar de tráfico a un ritmo elevado el canal de radio utilizado por un punto de acceso, y este punto de acceso se saturará ya que intentará acomodar el nuevo tráfico.

Es especialmente importante recordar que en muchos casos el tráfico normal de una red es suficiente para saturar una red, y no tiene necesariamente que ser tráfico malintencionado o tratarse de un ataque. Aplicaciones Cliente/Servidor pueden transmitir ficheros de datos de gran tamaño en forma simultánea a varios clientes, provocando una saturación de los puntos de acceso *wireless*.

Solución:

Monitorizar las redes con un analizador de redes inalámbricas. Es necesario estudiar el tipo de conexiones según su velocidad y tipo de paquetes transmitidos. Un elevado porcentaje de conexiones de baja velocidad pueden indicar la existencia de una interferencia externa, o indicar que los puntos de accesos están demasiado lejos de los usuarios (o que existen obstáculos físicos entre los puntos de acceso y los usuarios).

También es interesante averiguar la velocidad en los diferentes canales de radiofrecuencia a lo largo del tiempo para determinar la evolución del ancho de banda disponible. La saturación de un canal en concreto puede indicar que existe demasiado tráfico y puede ser deseable asignar a los usuarios puntos de acceso alternativos.

4.5 MAC *spoofing* y secuestro de sesiones

Al igual que las redes *ethernet*, las redes 802.11 no realizan autenticación de "*frames*" (paquetes) de datos. Cada "*frame*" tiene una dirección de origen, pero no existe ninguna garantía de que la estación de origen fuese la que realmente emitió los datos. *Hackers* pueden falsificar paquetes de datos y alterar las tablas ARP de enrutamiento de datos, o pueden simplemente examinar el tráfico y extraer las direcciones MAC correspondientes a los usuarios para luego suplantar los usuarios reales.

Otra técnica de ataque también utilizada es instalar un punto de acceso que pretende formar parte de la red. No existe ningún mecanismo que permita verificar que se trate de un punto de acceso legítimo. Las tarjetas *wireless* de los usuarios automáticamente detectarán este punto de acceso e intentarán conectarse, revelando datos sobre su configuración y claves WEP (en caso de utilizar WEP).

Para evitar estos problemas se trabaja en estos momentos en mecanismos de autenticación para las redes 802.11. En junio del 2001 se aprobó el estándar 802.1x, que requiere que los usuarios se autentiquen antes de acceder a la red inalámbrica. Sin embargo todavía no hay acuerdo sobre los mecanismos de gestión de claves necesarios para implementar esta autenticación. Estos mecanismos se incluirán en el estándar 802.11i todavía pendiente de aprobación.

Solución:

Hasta que no se apruebe el estándar 802.11i, y se comercialicen equipos que los implementen, es necesario mitigar el problema de la falsificación

(*Spoofing*) de direcciones MAC. Para ello es necesario aislar la red *wireless* de la red física. En estos momentos la mejor forma de conseguirlo es implementar un protocolo VPN con encriptación fuerte, por ejemplo IPSec, y no permitir el tráfico en ningún otro protocolo.

4.6 Análisis de tráfico y *sniffing*

Nada impide a un atacante el “escuchar” el tráfico de radio de una red *wireless* y observar el tráfico de forma pasiva. Armado con esta información, o utilizando un analizador de redes, un *hacker* puede averiguar toda la información necesaria para realizar un ataque. El protocolo 802.11 no dispone de ningún mecanismo para evitar que los datos transmitidos sean interceptados. Desafortunadamente el *Wired Equivalente Privacy* (WEP), que inicialmente debía prevenir estos problemas, solamente encripta una parte de los paquetes. Los paquetes de datos para el control y gestión de las transmisiones no son encriptados ni autenticados. Además, el sistema de encriptación utilizado por WEP tiene fallos y es fácilmente descifrable.

Las implementaciones actuales del WEP han corregido muchos de los fallos originales que permitían a un usuario equipado con las herramientas *WEPcrack* o *AirSnort* calcular las claves criptográficas en unos pocos minutos. Algunos fabricantes también han implementado un sistema para cambiar las claves WEP cada 15 minutos. De esta manera aunque la red genere grandes cantidades de datos, estos no son suficientes para poder descifrar las claves WEP antes de que éstas sean cambiadas.
Solución:

Al igual que en el punto anterior, la mejor solución es emplear protocolos seguros como el SSH, SSL o IPSec. Hasta que el estándar 802.11i no esté

disponible, solamente el uso de éstos protocolos seguros puede garantizar la seguridad contra escuchas e interceptación del tráfico.

4.7 Topología de la red

Una red inalámbrica es difícil de contener, y el medio que utiliza se propaga más allá del espacio físico de la empresa. Muchas redes físicas disponen de extraordinarias medidas de seguridad perimetrales (VPN's, *firewalls*, detectores de intrusiones, servidores de autenticación, certificados digitales, monitorización contínua, etc.). Sin embargo, una vez en el interior existen pocos mecanismos de seguridad para detectar un intruso. Al conectar una red *wireless* directamente a la red interna estamos creando un punto de fallo único y si la seguridad de esta red *wireless* falla, entonces la seguridad de toda la red interna se ve comprometida, con independencia de todas las medidas de seguridad perimetrales.

Solución:

Es imperativo tratar a toda red inalámbrica, por muchas medidas de seguridad que tenga, como una red insegura. Una práctica muy recomendada es tratar a las redes *wireless* como redes DMZ, y conectar los diferentes puntos de acceso a una red DMZ independiente, que a su vez está conectada al *firewall* corporativo. De esta forma se puede regular exactamente que tipos de tráfico y que recursos de la red interna son accedidos desde la red inalámbrica.

CONCLUSIONES

1. Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica, pero la realidad es que ésta tecnología está todavía en su nacimiento y se deben resolver varios obstáculos técnicos y de regulación antes que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad. No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas, sino mas bien complementarlas.

2. Existen varios estándares, unos creados y otros por ser aceptados, como lo son entre los más importantes el 802.11a, 802.11b y 802.11g. Estos tienen diferentes características y hay que saber sus ventajas y desventajas a la hora de decidirnos por el equipo que se desea montar en una red inalámbrica. Se vio que el 802.11a puede alcanzar mayores velocidades de transmisión, pero no tiene el alcance del estándar 802.11b, el cual alcanza más espacio cubierto teniendo que sustituir ésto por velocidad de transmisión ya que alcanza solamente 11 Mbps., al contrario del 802.11a que llega a contar con 54 Mbps. de transmisión. Para concluir, tenemos el estándar más nuevo 802.11g, que tiene lo mejor de los dos anteriores, pero es más costoso. Por lo tanto, podemos concluir que la tecnología a utilizar depende mucho del área en el que estemos trabajando y la rapidez con que se desea trabajar.

3. Un atacante ya no requiere acceso físico a la red, las redes *wireless* están muchas veces situadas detrás de los *firewalls*, son redes muy

susceptibles a ataques de *Man In The Middle* y Denegaciones de Servicio (DoS) y el atacante puede marcharse con relativa impunidad.

4. El *wardriving* es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como un ordenador portátil o un PDA. Para dejar plasmado lo que en el *wardriving* se pudo observar, existe un lenguaje llamado *warchalking*, éste utiliza símbolos para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que pasen por esas zonas.

5. Tras los conceptos expuestos, es conveniente aclarar que sí es posible considerar ciertos entornos *wireless* como seguros, pero sólo tras la combinación inteligente de conocimiento técnico, procedimientos y uso en alcance correcto de límites de funcionalidad y tecnologías.

6. Esta tecnología tiene como mayor inconveniente la principal de sus ventajas: acceso al medio compartido por cualquiera con el material y los métodos adecuados, proporcionando un alto nivel de riesgo en la seguridad, lo cual debemos tener presentes a la hora de decidirnos por esta opción, pues crecerá en igual medida (o más rápido) que las soluciones aportadas para subsanar estos riesgos.

RECOMENDACIONES

1. Las redes inalámbricas y su inseguridad son un problema serio para tomarlas en cuenta a la hora de implementar nuestra red. Por lo tanto se recomienda la utilización de una política de seguridad homogénea y sin fisuras, que trate todos los aspectos que comparten riesgo, sin disminuir la rapidez y que sepa aprovechar las ventajas de las redes inalámbricas.

2. Siendo conscientes de las debilidades del estándar 802.11, existen diferentes tipos de seguridad entre los que destacan ACL (*Access Control List*), CNAC (*Closed Network Access Control*), WEP (*Wired Equivalent Protocol*), ULA (*Upper Layer Protocol*), Estándar 802.1x, TKIP (*Temporal Key Integrity Protocol*). Algunos muy conocidos, otros están siendo implementados; funcionan como protección para nuestra red inalámbrica y se deben tomar muy en cuenta, por que, siendo la red inalámbrica muy vulnerable para nuestra información vale la pena que estemos con la última tecnología en lo que concierne a seguridad.

3. Debe tenerse extremo cuidado en la configuración de los mecanismos de seguridad implementados para las redes inalámbricas, ya que de esto dependerá que la información almacenada a cargo de nuestra responsabilidad se mantenga siempre íntegra y no afecte de ninguna manera a la empresa. Por lo tanto la utilización de *wizards* o ayudantes en la configuración de los puntos de acceso debe ser descartada, ya que preferiblemente los puntos de acceso no deben ser configurados por usuarios inexpertos. Esto podría traer consecuencias desastrosas en la

seguridad y causar vulnerabilidad que una red inalámbrica puede llegar a tener.

4. Debe tenerse cuidado y experiencia cuando se decide el área a cubrir en una zona específica por una red inalámbrica, para ello se debe identificar los requerimientos que se desean con base al área cubierta, para poder definir el tipo de topología a utilizar, ya sea *ad-hoc*, Infraestructura o una combinación de ambas.

BIBLIOGRAFÍA

1. Alapont Miquel, Vicent. **Seguridad en Redes Inalámbricas**. www.seguridadenlared.org/programs/SeguridadWireless.pdf. 09/11/2003.

2. Caballé, Xavier. **Seguridad de las redes inalámbricas: Wardriving y Warchalking**. http://facom.udp.cl/CEM/TDC/fichas/seginalam/redinal.htm. 22/10/2003.

3. de Leo, Mike. **Security 802.11 Wireless Networks**. www.cisco.com. 04/05/2002.

4. Díaz, Gustavo. **GSM vs CDMA**. www.ieee.com. 28/12/2003.

5. Diaz, Toni. **Autenticación e Integridad en redes Wireless**. http://madridwireless.net. 14/08/2003.

6. Eschoyez, Maximiliano. **Seguridad en 802.11i**. http://lcd.efn.unc.edu.ar/frames/archivos/wep.pdf. 22/12/2003.

7. Fernández Bleda, Daniel. **Seguridad en Nuevas Tecnologías: Seguridad en Redes Inalámbricas 802.11b**. http://www.isecauditors.com/downloads/present/IGC2K3_Seg_Wireless.pdf. 15/05/2003.

8. Galván Alonso, Gonzalo. **Extensible Authentication Protocol y PPP**. www.infor.uva.es/~jvegas/docencia/ar/seminarios/EAP.pdf. 28/10/2003.

9. Garcia, Albert. **¿Que es Bluetooth?.** http://www.zonabluetooth.com/que_es_bluetooth.htm. 28/10/2003.

10. Gast, Mathew. **"Seven Security Problems of 802.11 Wireless".** www.totemguard.com. 10/05/2002.

11. Hernanz Chiloeches, Daniel. **Estudio de la capa física del 802.1.** http://bilbowireless.net/documentacion/estudio_wifi.pdf. 08/04/2002.

12. Intel. **Ethernet inalámbrica**. http://www.intel.com/es/home/trends/wireless/info/ethernet.htm. 10/11/2003.

13. KernelPanik Crew. **Entendiendo las Wireless Lan**. http://www.kernelpanik.org. 15/02/2002.

14. López Ortiz, Francisco. **El estándar IEEE 802.11 Wireless LAN**. http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf. 28/12/2003.

15. Martínez Veguillas, David. **REDES INALÁMBRICAS**. http://www.infosp.com/comunicaciones/articulos/redesinalambricas.doc. 15/10/2003.

16. Megías Perol, Javier. **Wireless: Seguridad en Redes Inalámbricas**. www.sgi.es/prensa/articulos_interes/sic52-art_javier_megias.PDF. 05/08/2003.

17. Microsoft Corporation. **Wireless Security**. www.microsoft.com. 30/10/2003.

18 Oliva Fora, Pau**. (In)seguridad en redes 802.11b**. www.eslack.org/pof/In-Seguridad_802.11b.pdf. 02/03/2003.

19. Otxoa Gilo, Ander. **Guía Wireless para todos/as**. http://el202.homeip.net/schedule.htm. 25 abril 2003.

20. Ribagorda, Dr. Arturo. **Seguridad en la red y el Comercio Electrónico: Seguridad en redes inalámbricas**. www.upsam.com/Doctorado/DIng/2002/calendarios/comercio_electronico.pdf. 20/09/2002.

21. Universidad de Alicante, España. **INSTALACIÓN DE WIRELESS EN WINDOWS 2000 Y XP.** http://www.ua.es/es/internet/wirelessua/ver_1_0/info.html. 12/12/2003.

22. Vaqué Martínez, Judith. **Comunications Sense Files**. http://assl.ath.cx/docs/docs/Comunidades%20Wireless.pdf. 17/05/2002.

23 Wi-Fi Alliance. **"Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks"**. www.wi-fi.com. 29/04/2003.

24 Wi-Fi. **Que son los "hot Spots"?**. http://www.wi-fi.com.ar/hotspots/hotspots.html. 15/08/2003.