UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

"IMPLEMENTACIÓN DE UNA RED INALÁMBRICA (WLAN), RIESGOS Y VULNERABILIDADES A ATAQUES EXTERNOS CON DIFERENTES SOFTWARE."

T E S I S

P A R A O B T E N E R E L T Í T U L O D E
I N G E N I E R O E N C O M P U T A C I Ó N

P R E S E N T A :

OSCAR ANTONIO RAMIRO APARICIO

ASESOR: ING. ENRIQUE GARCÍA GUZMÁN

MÉXICO 2011

AGRADECIMIENTOS

Agradezco primero a la vida por todas las experiencias brindadas.

A mis padres, que siempre han estado presentes, apoyándome en las buenas y las malas, ofreciéndome todo lo que estaba a su alcance para lograr un mejor futuro. Y aunque mi padre ya no está conmigo su enseñanza y su ejemplo me sigue impulsando. Y mi madre que con su cariño lo hace cada día de mi vida.

A mis hermanos que siempre están para apoyarme y compartiendo sus experiencias conmigo.

A Luftiye Wong que siempre me da su apoyo incondicional e impulsa a seguir adelante.

A mis compañeros de universidad por compartir innumerables experiencias en esos años inolvidables de estudio y sacrificios.

A la Universidad Nacional Autónoma de México por brindarme una oportunidad de formar parte de su alumnado y ofrecerme la oportunidad de una educación de calidad para un mejor presente y futuro, de igual forma a los profesores por compartir sus conocimientos.

A los ingenieros: Enrique García Guzmán, Antonio Nieto, Alberto Blanco, Narciso Acevedo y Jesús Hernández por apoyo en este trabajo de investigación.

A Alejandro Robles, Ing. Cuauhtémoc Romero Nava, Lic. Mayra Pérez Juárez, Ing. Manuel Arellano Orozco, Ing. Fernanda Aparicio López, Ing. Luis Cruz Morales, Ing. Eduardo Hilmenstein Castro por su apoyo y amistad.

Y a cada una de las personas que de alguna forma han pasado y marcado mi vida y siempre trataron de impulsarme a realizar mis metas.

ÍNDICE

OBJETIVO

Implementar una red local inalámbrica (WLAN) en una sala de cómputo, describir las características de dispositivos utilizados comúnmente, las normas establecidas y mostrar posibles vulnerabilidades a los ataques externos mediante software mal intencionado principalmente en el robo de acceso a internet.

DESCRIPCIÓN DE LA PROBLEMÁTICA

En la actualidad el uso de las redes inalámbricas se ha convertido en algo muy común, este crecimiento se debe en su mayor parte al auge experimentado por el mercado de los PC portátiles, para los que el empleo de una red de este tipo cobra pleno sentido en los hogares como en las escuelas, lugares públicos; en las empresas debido a la movilidad o por el difícil acceso de cableado estructurado.

La proliferación de salas de cómputo (café internet) los cuales son instalados como negocios rentables y en muchos casos los dueños solo lo ven como eso, sin tomar en cuenta la seguridad ya sea por ignorancia o por descuido, se convierten en objetivo de personas con interés de conexión a internet "gratis".

Dejando acceso a los modem inalámbricos sin protección de claves seguras o con claves vulnerables a diversos software que a pesar de ser diseñados para la auditoria de redes o para pruebas de seguridad, al salir al mercado, llegar a los usuarios "comunes" y sobre todo al estar disponibles en internet son un verdadero peligro para los usuarios de las WLAN que sin darse cuenta pueden estar permitiendo que alguna persona pueda descifrar sus contraseñas, conectarse a su punto de acceso y de esta forma pueda hacer un uso de su servicio de internet principalmente afectando de esta forma el desempeño de dicha red. Esta problemática también aplica en el ámbito domestico y es más común de lo que se piensa, ya que se dejan modem con las contraseñas que traen por default, permitiendo que otras personas utilicen sus servicios de internet.

JUSTIFICACIÓN

En la presente investigación busco dar a conocer las características de una WLAN así como sus componentes más comúnmente utilizados, de igual forma la implementación de dicha red, las vulnerabilidades a las que pueden estar expuestas si no se toman medidas de seguridad, en este caso se usa una sala de cómputo para mostrar la problemática a la que puede enfrentar, más aún ahora que la proliferación de estas salas (ciber cafes).

Hablare en particular del robo de la conexión de internet que ha generado gran interés para infinidad de personas que ya sea por medio de cd´s vendidos en los establecimientos dedicados a la comercialización de software, en los cuales les prometen descifrar claves WEP o WAP de módems inalámbricos o bien por medio de paquetería disponible en Internet que fue diseñada para auditorias y supervisión de redes; en manos curiosas y con los conocimientos necesarios se pueden dar robos en la conexión a los puntos de acceso de servicios de internet. Afectando en el menor de los casos el rendimiento.

En particular este tema me intereso por que he instalado varias salas de este tipo y en mi experiencia y convivencia con estudiantes y el ver como se venden dvd´s con la leyenda “internet gratis” me di cuenta que ya sea por economía o simple curiosidad, las herramientas con las que se supervisan y audita la seguridad de WLAN han llamado la atención para la decodificación de las contraseñas WEP y WAP sobre todo de los módems inalámbricos de Prodigy. También en los hogares se tienen estos módems sin ningún tipo de seguridad salvo la que viene por default en esos dispositivos.

Dichas herramientas, hardware adecuado y videos en los que se muestra indiscriminadamente vía Internet el procedimiento, sino descifran las contraseñas al menos afectan las conexiones al hacer uso de programas que “inyectan” flujo de información al punto de acceso afectando seriamente en el rendimiento de la conexión atacada.

Por lo tanto creo que es necesaria la descripción de dichas vulnerabilidades de este tipo de conexiones que al contrario de lo que dicen los Proveedores de Servicios de Internet, no son seguros. Sumado a las contraseñas seguras se debe contar con algún software o hardware destinado a la protección de los puntos de acceso al servicio de internet.

INTRODUCCIÓN

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Debido al rápido crecimiento de las WLAN en el mundo, el IEEE formó el grupo de trabajo 802.11 para definir los protocolos necesarios para soportar las redes inalámbricas, tanto para la capa física como para la capa de enlace (MAC). El primer paso importante en el desarrollo evolutivo de las tecnologías de redes inalámbricas se dio a partir de la aprobación del primer estándar del IEEE 802.11 en junio de 1997. Este estándar internacional define las características de una WLAN y cuyo propósito es proporcionar conectividad inalámbrica entre los diferentes tipos de dispositivos.

Debido a un uso indebido de los términos y por razones de marketing el nombre WLAN y Wi-Fi, que es el nombre de la certificación que otorga la alianza Wi-Fi que anteriormente era la WECA (Alianza para la compatibilidad de Ethernet inalámbrica), han sido confundidos; es decir una WLAN es una red certificada por Wi-Fi que cumple con el estándar 802.11 de IEEE.

Una red LAN inalámbrica (WLAN), es un sistema flexible de comunicación de datos implementado como extensión o alternativa a una red de área local cableada, dando la movilidad sin las correspondientes restricciones físicas. Lo anterior se logra ya que las WLAN utilizan las ondas electromagnéticas del espectro de Radio Frecuencia (RF) e Infrarrojos (IF) para transmitir datos de un punto a otro. Debido a que los infrarrojos no permiten, por sus limitaciones construir redes prácticas no se utilizan ampliamente dejando el camino libre a las frecuencias de radio.

Las redes WLAN se pueden dividir en dos categorías:

1. Larga distancia: Estas son las utilizadas para grandes distancias como pueden ser de una ciudad o de un país.
2. Corta distancia: son las utilizadas en un mismo edificio o en varios cercanos.

Las redes se pueden dividir en los tipos Ad-hoc e infraestructura que es la más utilizada. En la primera, las estaciones de trabajo se comunican a través de la configuración peer to peer, no hay Puntos de acceso (AP) y no se requieren permisos para la comunicación. En el modo de infraestructura un AP actúa como concentrador para los nodos o estaciones de la red, estos puntos de acceso pueden estar conectados a las redes cableadas para proporcionar o compartir recursos entre dichas redes. Cualquiera que sea el tipo red en uso se estará utilizando el estándar IEEE 802.11 que es el que define las características y la conectividad inalámbrica.

Las WLAN´s utilizan o deberían utilizar alguno de las alternativas de seguridad basadas en los protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, WPA, o WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad que son proporcionados por los dispositivos inalámbricos. Un elevado porcentaje de redes son instaladas sin tener en consideración la seguridad convirtiendo las en redes abiertas y dejando sin protección la información que por ellas circula.

En la actualidad el uso de las redes inalámbricas se ha convertido en algo muy común, este crecimiento se debe, en su mayor parte, al auge experimentado por el mercado de los PC portátiles, para los que el empleo de una red de este tipo cobra pleno sentido en los hogares como en las escuelas, en lugares públicos; en las empresas debido a la movilidad o por el difícil acceso de cableado estructurado.

La proliferación de salas de cómputo (café internet) los cuales son instalados como negocios rentables y en muchos casos los dueños sólo lo ven como eso; sin tomar en cuenta la seguridad ya sea por ignorancia o por descuido dejando acceso a los modem inalámbricos sin protección de claves seguras o vulnerables a diversos software que a pesar de ser diseñados para la auditoria de redes o para pruebas de seguridad que al salir al mercado y llegar a los usuarios “comunes”, y sobre todo al estar disponibles en internet son un verdadero peligro para los usuarios de las WLAN que sin darse cuenta pueden estar permitiendo que alguna persona con los conocimientos necesarios o bien guiados por la información existente en internet pueda descifrar sus contraseñas, conectarse a su punto de acceso y de esta forma pueda hacer un uso de su servicio de internet principalmente afectando de esta forma el desempeño de dicha red. En las WLAN domesticas también se corre el riesgo ya que sin saberlo se puede estar “compartiendo” el servicio de internet a terceras personas.

En la presente investigación busco dar a conocer las características de una WLAN así como sus componentes más comúnmente utilizados, de igual forma la implementación de dicha red, las vulnerabilidades a las que pueden estar expuestas si no se toman medidas adecuadas de seguridad; en este caso se usa una sala de cómputo para mostrar la problemática a la que puede enfrentar.

Hablare en particular del robo de la conexión de internet que ha generado gran interés para infinidad de personas que ya sea por medio de cd´s vendidos en los establecimientos dedicados a la comercialización de software, en los cuales les prometen descifrar claves WEP o WAP de módems inalámbricos o bien por medio de paquetería disponible en Internet que fue diseñada para auditorias y supervisión de redes; en manos curiosas o con los conocimientos necesarios se pueden dar robos en la conexión a los puntos de acceso de servicios de internet. Afectando en el menor de los casos el rendimiento.

Dichas herramientas, combinadas con los conocimientos necesarios, hardware adecuado y videos en los que se muestran procedimientos indiscriminadamente vía Internet, sino descifran las contraseñas al menos afectan las conexiones al hacer uso de programas que "inyectan" flujo de información al punto de acceso afectando seriamente en el rendimiento de la conexión atacada.

Existen herramientas gratuitas que facilitan el trabajo de romper la clave secreta de enlaces protegidos con WEP y WPA o hasta WPA2 algunos ejemplos son*:*

WEPCrack: *que consiste* en una serie de scripts escritos en lenguaje Perl[1] diseñados para analizar un archivo de captura de paquetes de un sniffer o bien AirSnort hace lo mismo, pero integra las funciones de sniffer y analizador de claves y por lo tanto es más fácil de usar. AirSnort captura paquetes pasivamente y obtiene la clave WEP cuando ha capturado suficientes datos

Backtrack: Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

[1] Perl es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación. Estructuralmente, Perl está basado en un estilo de bloques como los del C o AWK, y fue ampliamente adoptado por su destreza en el procesador de texto y no tener ninguna de las limitaciones de los otros lenguajes de script.

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Wifislax: Es una distribución GNU/Linux en formato *.iso con funcionalidades de LiveCD y LiveUSB pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. WiFislax incluye una lista de herramientas de seguridad y auditoría listas para ser utilizadas, entre las que destacan escáner de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría wireless, además de añadir una serie de útiles lanzadores.

Speedtouch: Lanzador de contraseñas WEP que solo puede descifrar contraseñas de 6 dígitos siempre y cuando la contraseña sea la que viene por default; al utilizar dicho lanzador se ejecuta la aplicación, colocando el nombre de la red a "atacar" y genera después de unos minutos, el número de serie y las posibles contraseñas las cuales sólo se prueban una a una y listo, se conecta al punto de acceso sin problema: se teclea la ruta de la puerta de enlace (192.168.1.254) y se puede acceder al modem.

Wifiway

Es una distribución de seguridad Wi-Fi basada en Linux From Scratch. Con Wifiway, podremos realizar auditorías en nuestras redes inalámbricas Wi-Fi utilizando herramientas como Kismet, Aircrack, Airodump o Wireshark. La gran ventaja de la distribución WifiWay, radica en la integración de todas las herramientas necesarias a la hora de realizar ataques y análisis de redes inalámbricas Wi-Fi bajo GNU/Linux. WifiWay a diferencia de Wifislax su hermana pero basada en la distribución Slax, está creada desde cero, y está optimizada en tamaño y rendimiento, aunque soporta menor cantidad de hardware que Wifislax. Otra ventaja de WifiWay, es el idioma, Backtrack es una estupenda distribución de seguridad Wi-Fi, sin embargo, siempre es apreciada esta traducción al castellano que permite a los hispanohablantes conseguir un mayor entendimiento de qué es lo que se está cociendo en su instalación de Linux.

CAPITULO I

FUNDAMENTOS Y NORMAS DE REDES INALÁMBRICAS (WLAN)

I.1 Definición de Red Inalámbrica y Antecedentes de las WLAN

WLAN son las siglas en inglés de Wireless Local Area Network. Es un sistema de comunicación de datos flexible muy utilizado como alternativa a las redes LAN cableada o como una extensión de ésta. En términos sencillos, una WLAN hace exactamente lo que su nombre implica; proporciona todas las características y ventajas de las tecnologías LAN tradicionales, pero sin las limitaciones que suponen los hilos o cables; Así las WLAN redefinen la visión que la industria tiene de las LAN. La conectividad ya no implica estar "atado".

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología. Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del spread spectrum (espectro extendido), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la Agencia Federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400- 2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en spread spectrum. (IMS es una banda para uso comercial sin licencia).

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps que es el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

Las primeras tecnologías WLAN eran de baja velocidad y ofrecían de 1 a 2 Mbps. A pesar de estas limitaciones, la libertad y la flexibilidad que ofrece la tecnología inalámbrica permitieron que estos productos encontraran un lugar en los mercados comerciales.

Los trabajadores móviles utilizaban los dispositivos portátiles para administrar los inventarios y recopilar datos en los comercios y los almacenes. Más tarde, los hospitales aplicaron la tecnología para obtener y distribuir la información de los pacientes. De hecho, muchas de estas tecnologías inalámbricas "pre-estándar" todavía se siguen utilizando porque los dispositivos que recopilan los datos no requieren velocidades de datos altas.

A medida que las computadoras fueron dejando sitio en las aulas y las oficinas, los colegios y las empresas empezaron a instalar redes inalámbricas para evitar los costos de un cableado al tiempo que habilitan el acceso compartido a Internet. Al darse cuenta de la necesidad de un estándar del tipo de Ethernet, los fabricantes de tecnología inalámbrica se asociaron en 1991 y formaron la Alianza para la compatibilidad de Ethernet inalámbrica (WECA, Wireless Ethernet Compatibility Alliance). La WECA propuso y construyó un estándar basado en las tecnologías cooperantes. Más tarde, la WECA cambió su nombre por el de Wi-Fi Alliance (Alianza Wi-Fi). En junio de 1997, el IEEE hizo público el estándar 802.11 para las redes inalámbricas de área local. La imagen I.1 ilustra la evolución de las WLAN.

En 1997 el IEEE añadió la norma 802.11 que se encargaba de definir a las redes de área local inalámbricas. La primera norma 802.11 utilizaba infrarrojos como medio de transmisión y no tuvo buena aceptación en el mercado. Posteriormente, salieron otras dos normas basadas en 802.11 basadas en el uso de radiofrecuencia en la banda de 2,4 GHz. Ambas se diferencian del método de transmisión de radio utilizado. Pero la tecnología podía ir mucho más allá de lo que estos estándares estaban brindando. En 1998 aparecieron en el mercado los primeros sistemas que funcionaban a 11Mbps, siguiendo el borrador de la norma 802.11b, que fue finalmente aprobada en septiembre de 1999, junto con la 802.11a que especifica el funcionamiento en la banda de 5GHz. a velocidades de hasta 54Mbs. En la imagen. I.1 se muestra la cronología de acuerdo a las velocidades.

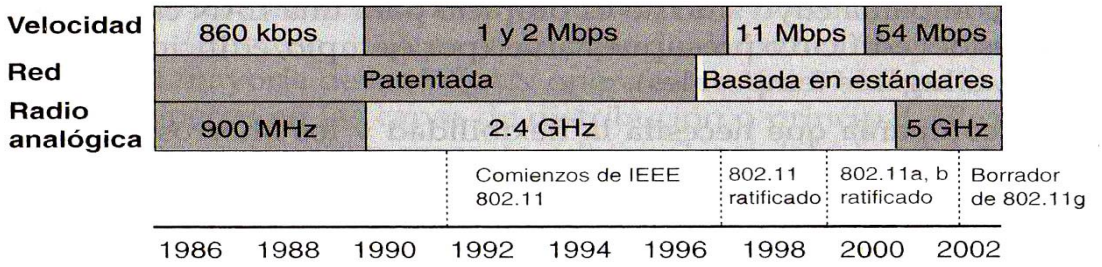

Imagen I.1 Cronología de acuerdo a las velocidades

En 1999, el IEEE finalizó el estándar 8021.11b, aumentando el rendimiento de las redes inalámbricas a 11Mbps. Aunque hubo muchas compañías implicadas en la creación de le especificación, Lucent Technologies y Apple Computer abrieron el camino para producir dispositivos de red inalámbrica asequibles para los pequeños consumidores.

El momento decisivo para las redes inalámbricas llegó en julio de 1999, con el lanzamiento por parte de Apple de su tecnología AirPort, que era una versión de IEEE 802.11b ajustada al estándar de la industria y la puso en el mercado cobrando sólo cien dólares y el punto de acceso por tres cientos dólares que Apple llamaba Estación Base AirPort.

En el 2001 destaca 802.11e, que especifica mecanismos de calidad de servicio en WLANS, y en el 2003 802.11g que especifica el funcionamiento de velocidades de hasta 54Mbs en la banda de 2,4Ghz.

El cuadro I.1 muestra la cronología de las redes WLANs.

FECHA	EVENTO
1986	Primeras WLANs. 900Mhz(860Kbs) no disponible en Europa
1993	WLANs de 1 y 2 Mbs en banda de 2,4Ghz. primeras en Europa
7/1997	IEEE aprueba 802.11 1 y 2Mbs banda de 2,4Ghz. e infrarrojos
1998	Primeros sistemas de 11Mbs a 2,4Ghz. Pre-estándar 802.11b.
9/1999	IEEE aprueba: 802.11b (hasta 11Mbs, 2,4Ghz.) 802.11a (hasta 54Ghz, 5Ghz.) no disponible en Europa. Nace Wi-Fi
12/2001	Primeros productos comerciales 802.11a
12/2001	Borrador 802.11e (QoS en WLANs)
2003	IEEE aprueba 802.11g (hasta 54Mbs, 2,4Ghz.

Cuadro I.1 Cronología de WLAN

I.2 Características de las WLAN.

Las señales inalámbricas son ondas electromagnéticas que pueden viajar por el espacio. No se necesita un medio físico para este tipo de señales que también viajan por el aire de un edificio de oficinas. La capacidad de las ondas de radio de atravesar paredes y cubrir grandes distancias convierte a la tecnología inalámbrica en una forma versátil de construir una red. En una configuración típica de LAN sin cable los puntos de acceso conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos (dependiendo de diversos factores).

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores, estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas mediante una antena.

La tecnología WLAN puede ocupar el lugar de una red cableada tradicional o ampliar sus límites y capacidades. De una forma muy parecida a las redes cableadas, el equipamiento WLAN de un edificio consta de adaptadores cliente y AP que llevan a cabo funciones parecidas a las de los hubs o concentradores de las redes cableadas.

Las redes inalámbricas tienen características fundamentales que las hacen significativamente diferentes a las LAN cableadas tradicionales. En el diseño de las LAN cableadas se asume implícitamente que una dirección MAC es equivalente a una ubicación física. En el IEEE 802.11, la unidad direccionable es una estación. La estación es un destino de mensaje, pero generalmente no es una ubicación fija. Las capas físicas utilizadas en el IEEE 802.11 son fundamentalmente diferentes a las utilizadas con los medios cableados.

Las redes inalámbricas de área local, WLAN (Wirelees Local Area Networks), están pensadas para crear un entorno de red local entre computadoras o terminales situados en un mismo edificio o grupo de éstos. En el mercado existen distintas tecnologías que dan respuesta a esta necesidad.

La transferencia de datos por medios inalámbricos pueden emplear uno de los distintos estándares, pero algo que todos estos tienen en común es su capacidad de ordenar señales de datos que se solapan.

Los dispositivos inalámbricos utilizan una de dos estrategias distintas para hacer frente al solapamiento de las señales: espectro extendido con salto de frecuencia (FHSS) o espectro extendido de secuencia directa (DSSS). Ambas formas de transmisión de espectro extendido son resistentes a las interferencias, pues no hay una sola frecuencia en uso constante, y el salto de frecuencias también puede ser resistente a los intrusos, pues los patrones de salto pueden evitar todos los analizadores de espectro excepto los de gama industrial y militar.

I.2.1 Tipos de comunicación inalámbrica

Las comunicaciones inalámbricas, pueden clasificarse tomando en cuenta su alcance, que es la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica. En Cuadro I.2.1 se muestra los tipos de comunicación de a cuerdo a su alcance.

WPAN	WLAN	WMAN	CELULAR
< 10 metros	**edificio-campus**	**Ciudad**	**región global**
Bluetooth	Wi-Fi	LMDS	2,5G
ZigBee	HomeRF	MMDS	3G
IrDA	HiperLAN	WiMax	4G

Cuadro I.2.1 tipos de comunicación por su alcance.

Por tanto, las comunicaciones inalámbricas se dividen en los siguientes grupos de acuerdo con su alcance:

Las redes inalámbricas de área personal o WPAN *(Wireless Personal Área Network)* cubren distancias inferiores a los 10 metros. Estas soluciones están pensadas para interconectar los distintos dispositivos de un usuario (por ejemplo, el PC con la impresora). Éste es el caso de la tecnología Bluetooth.

Las redes inalámbricas de área local o WLAN *(Wireless Local Área Network)* cubren distancias de unos cientos de metros. Estas redes están pensadas para crear un entorno de red local entre computadoras o terminales situados en un mismo edificio o grupo de edificios. Éste es el caso de Wi-Fi o HomeRF, por ejemplo.

Las redes inalámbricas de área metropolitana o WMAN *(Wireless Metropolitan Área NetworK)* pretenden cubrir el área de una ciudad o entorno metropolitano.

Los protocolos LMDS *(Local Multipoint Distribution Service,* 'Servicio local de distribución multipunto') o WiMax *(Worldwide Interoperability for Microwave Access,* 'Interoperatividad mundial para accesos de microondas') ofrecen soluciones de este tipo.

Por último, tenemos las **redes globales** con posibilidad de cubrir toda una región (país o grupo de países). Estas redes se basan en la tecnología celular y han aparecido como evolución de las redes de comunicaciones de voz. Éste es el caso de las redes de telefonía móvil conocidas como 2,5G o 3G.

En comunicaciones móviles de voz se les llama 1G (primera generación) a los sistemas analógicos (tipo NMT o AMPS), 2G a los digitales (tipo GSM o CDMA), 2,5G a los digitales con soporte para datos a alta velocidad (tipo GPRS, IS-95B o EDGE, *Enhanced Data for GSM Evolutiorí)* y 3G o tercera generación a los nuevos sistemas de telefonía celular con capacidad de gran ancho de banda.

Este último es el caso de UMTS *(Universal Mobile Telecommunications Service,* 'Servicio universal de telecomunicaciones móviles') o CDMA-2000 *(Code División Múltiple Access,* 'Acceso múltiple por división de código').

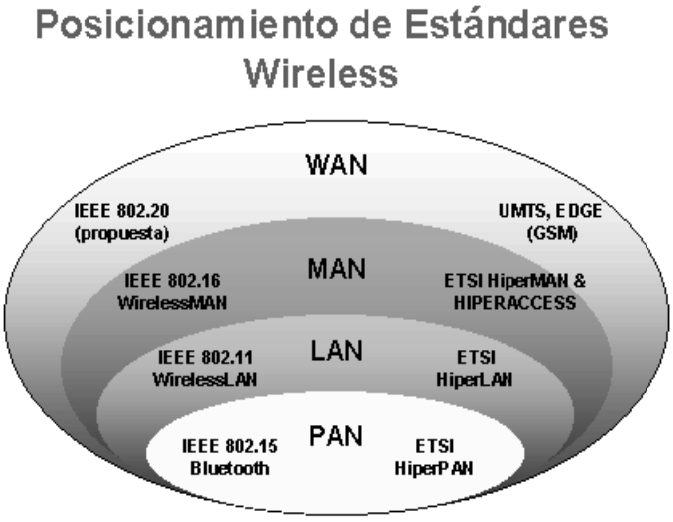

Imagen I.2.1 Estándares wireless

Las tecnologías más comunes en la actualidad que son:

HomeRF

En 1998 varias empresas entre las cuales se encontraron Compaq, HP, IBM, Intel y Microsoft, crearon el llamado HomeRF (Home Radio Frequency, 'Radio Frecuencia del hogar') que en 1999 salió la versión 1.0 con su protocolo SWAP (Sharep wireless Acces Protocol, 'protocolo de acceso compartido inalámbrico').

El SWAP trabaja en la banda de frecuencias de 2,4Ghz y permite configuraciones de comunicación punto a punto y en red. Permite transmitir datos a 1,6Mbps y mantener hasta cuatro comunicaciones dúplex de voz. Tiene un alcance de 50 metros y una potencia de 100mW. Utiliza un protocolo similar a IEEE 802.11 para datos y otro similar a DECT (Digital Enhanced Cordless Telecommunications, 'Telecomunicaciones digitales inalámbricas mejoradas') y su versión 2.0 alcanza los 10Mbps.

HiperLAN

HiperLAN (High-Performance Radio Local Area Network, 'Red de área local de radio de alto rendimiento') es el resultado del trabajo del Instituto europeo de normalización en telecomunicaciones para conseguir un estándar de red de área local inalámbrica vía radio. La primera versión publicada en 1996, trabajaba en la banda de frecuencias de 5Ghz. y alcanzaba velocidades de hasta 24Mbps.

En 2000 se obtuvo HiperLAN/2 que ofrece velocidades de transmisión de 54Mbps, La capa física es prácticamente idéntica a IEEE 802.11a. La mayor diferencia radica en la capa MAC. HiperLAN está diseñada de forma ambiciosa soportando aplicaciones en las que el tiempo de respuesta es crítico, define interfaces de redes de tercera generación, redes ATM (Asynchrinous Transfer Mode, 'Modo de transferencia asíncrono) y Firewire' (IEEE 1394).

Wi-Fi ("*Wireless Fidelity*"): en lenguaje español significa literalmente fidelidad sin cables. También se les denomina WLAN ("*Wireless Local Area Network*") ó redes de área local inalámbrica. Se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio con muy buena calidad de emisión para distancias cortas (hasta teóricamente 100 m). Este tipo de transmisión se encuentra estandarizado por la IEEE, siglas en inglés del Instituto de Ingenieros en Electricidad y Electrónica, la cuál es una organización internacional que define las reglas de operación de ciertas tecnologías.

Para la transmisión es necesario el uso de antenas integradas en las tarjetas, además este tipo de ondas son capaces de traspasar obstáculos sin necesidad de estar frente a frente el emisor y el receptor. Actualmente son 3 estándares básicos: IEEE 802.11b, IEEE 802.11g y IEEE 802.11n.

En el caso de las redes locales inalámbricas, el sistema que se utiliza es el propuesto por la WECA (Wireles Ethernet Compatibility Alliance, 'Alianza de compatibilidad Ethernet inalámbrica') y normalizado por IEEE con el estándar 802.11b. A esta norma se le conoce más habitualmente como Wi-Fi o Wireles Fidelity. Con este sistema se alcanza una velocidad máxima de 11Mbps, alcanzando varios cientos de metros. No obstante, versiones más recientes de esta tecnología permite alcanzar los 22, 54 y hasta los 100Mbps. El gran éxito de WiFi, es fruto de muchas de las ventajas que ofrece a los usuarios, entre las cuales podemos destacar:

- **Movilidad:** Permite conectarse desde cualquier lugar que tenga cobertura inalámbrica, esto hace que WLAN sea muy práctica sobre todo para los dispositivos portátiles.

- **Costo reducido y fácil instalación.** La instalación de una red inalámbrica es muy barata ya que sólo hay que añadir uno o varios puntos de acceso para que los equipos puedan conectarse a la red.

- **Escalabilidad.** Para escalar la red tan sólo debe añadir más puntos de acceso para que aumente la cobertura inalámbrica y el número de usuarios que se pueden conectar al mismo tiempo.

- **Flexibilidad.** Las redes WLAN, al ser inalámbricas, permiten llegar a zonas de complicado acceso a través del cableado. Esta característica puede ser útil para instalar dispositivos de seguridad, como por ejemplo cámaras de vigilancia.

Pero también tiene sus inconvenientes:

- **Seguridad.** La seguridad es uno de los principales temas que se tienen que mejorar en las redes inalámbricas, ya que cualquier persona que se encuentre dentro del radio de cobertura puede "escuchar" el tráfico o acceder a la red. Para disminuir el riesgo existen los protocolos de cifrado WEP, WPA y WPA2 que han disminuido uno de los puntos débiles de las WLAN.

- **Velocidad de transmisión.** Las redes inalámbricas no ofrecen en la actualidad un ancho de banda tan elevado como las redes cableadas. La velocidad de transmisión máxima de una red inalámbrica es de 5OOMbps en el caso de la versión IEEE 802.1n, mientras que en una red cableada la velocidad puede llegar a superar 1 Gbps.

- **Interferencias.** Una gran desventaja de las redes inalámbricas es que los obstáculos o las condiciones climatológicas pueden atenuar la señal de forma que no pueda utilizar la red inalámbrica de forma correcta.

- **Cobertura limitada.** La cobertura de una red inalámbrica depende de varios factores: apantallamiento de la señal, potencia del punto de acceso y del adaptador de red, etc.

I.2.2 Topologías

Comprender las topologías es muy importante a la hora de diseñar una red. Las redes inalámbricas, al igual que las redes cableadas, sirven para interconectar no sólo computadoras, sino también cualquier otro tipo de equipo informático al que se puede instalar un dispositivo inalámbrico. Las redes inalámbricas Wi-Fi admiten dos tipos de configuración desde el punto de vista del equipamiento:

- **Modo ad hoc.** Es una configuración en la cual solo se necesita disponer de tarjetas o dispositivos Wi-Fi en cada equipo, estos se comunican unos con otros directamente, sin necesidad de que existan puntos de acceso intermedios.

  Esta configuración que no tiene AP, se denomina BSS independiente (IBSS, Independent IBSS). En sistemas operativos como Windows xp es fácil configurar este tipo de red entre iguales. Esta topología se puede utilizar para conectar una portátil al Pc principal, o para que varias personas compartan archivos.

Sin embargo las limitaciones de cobertura son un inconveniente en este tipo de red, porque todos deben poder escuchar a todos los demás. Como dato extra, se debe tener cuidado al conectarse con otros clientes a través de esta configuración, ya que muchos mecanismos de autenticación no están disponibles

- **Modo infraestructura.** Esta configuración, además de las tarjetas Wi-Fi en las computadoras, se necesita disponer de un equipo conocido como punto de acceso. El punto de acceso lleva a cabo una coordinación centralizada de la comunicación entre los distintos terminales de la red como se muestra en la imagen I.2.3. Si el área a cubrir es extensa se pueden instalar más de un punto de acceso interconectados. De esta forma se pueden llegar a cubrir ciudades enteras.

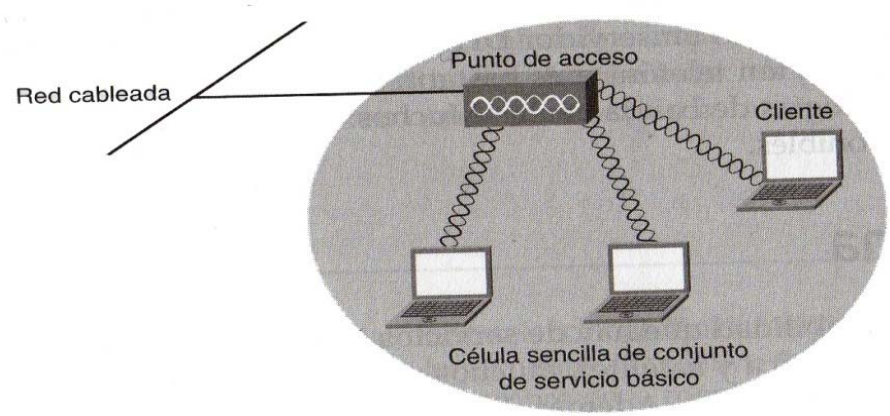

Imagen I.2.3 Modo Infraestructura

El conjunto de servicio básico (BSS, Basic Service net) es el bloque constructivo de una WLAN 802.11.

El BSS abarca una sola célula. Cuando uno de sus miembros se mueve fuera de su BSS, ya no puede comunicarse con los demás miembros del BSS. Todas las estaciones se comunican a través del AP, las estaciones no se *comunican* directamente. Un BSS tiene un ID de conjunto de servicio (SSID, Service Set ID).

Con el bajo costo de los AP inalámbricos SOHO (Small Office/ Home Office) y los routers inalámbricos, una topología BSS es el método más seguro y escalable para configurar una WLAN, en comparación con una red ad hoc.

La imagen I.2.3 muestra un BSS con tres estaciones que son sus miembros además del AP.

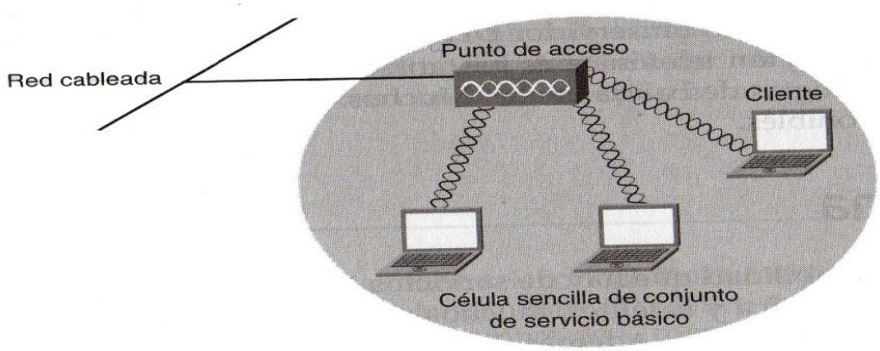

Imagen I.2.3 muestra un BSS con tres estaciones

- **Modo de Infraestructura Extendida (ESS)**

  Modo de Infraestructura extendida (ESS, Extended Service Set) se define como dos o más BSS que están conectados mediante un sistema de distribución común, como se observar en la imagen I.2.4, esto permite la creación de una red inalámbrica de un tamaño y una complejidad arbitraria. Como ocurre con un BSS, todos los paquetes de un ESS deben pasar uno de los AP.

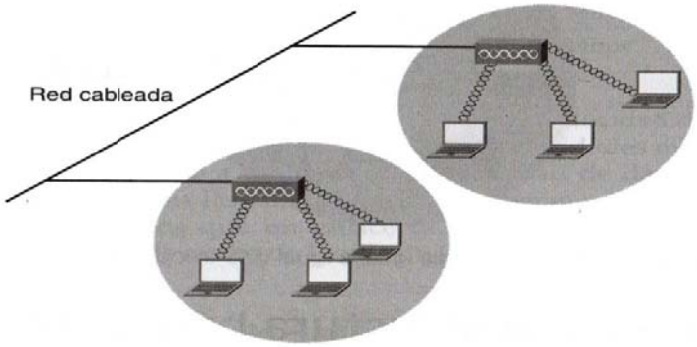

Imagen I.2.4 Infraestructura extendida

Como la cobertura de un AP no suele pasar de algunas decenas de metros en interiores y algunos cientos en exteriores, si la extensión a cubrir es extensa serán necesario disponer de múltiples puntos de accesos interconectados entre sí, en esta configuración las terminales pueden desplazarse por toda el área de cobertura sin perder la comunicación.

Los distintos AP que forman la red deben estar conectados entre sí para lo que existen diferentes alternativas:

- Utilizar una conexión cableada tipo Ethernet. en este caso, los puntos de acceso son unos terminales más de la red local, haciendo de puente entre los terminales fijos y móviles.

- Utilizar enlaces inalámbricos Wi-Fi. Existen equipos conocidos como bridges (puentes) que establecen un enlace dedicado entre dos o más puntos.

- Utilizar enlaces inalámbricos de tipo metropolitano, los distintos puntos de acceso podrían estar interconectados mediante tecnología WiMax o LMDS.

- Utilizar internet como medio de interconexión. En este caso cada punto de acceso se conecta a Internet con banda ancha (ADSL) y se establecen conexiones de red privada (VPN) entre ellos. Las conexiones de red privada virtual garantizan la privacidad de las comunicaciones.

Para que todos los AP formen parte de una misma red se deben configurar con el mismo nombre de red y los mismos parámetros de seguridad. Los AP de acceso vecinos, concierta intersección de su cobertura, deben configurarse con distintos canales de radio para evitar interferencias.

Cuando una terminal se mueve fuera del alcance del punto de acceso con el que está asociado originalmente, automáticamente se reasocia con un nuevo AP con el que tenga cobertura.

I.3 Normalización

Uno de los factores más importantes para que una tecnología sea aceptada es la normalización, el hecho de que la tecnología esté perfectamente definida para que los distintos fabricantes de equipos, componentes o software puedan hacer su trabajo con la seguridad de ser aceptados en el mercado. El organismo de normalización que más ha avanzado en la definición de normas de redes de área local es el IEEE (Institute of Electrical and Electronics Enginners, 'Instituto de Ingenieros Eléctricos y Electrónicos').

El IEEE empezó a tratar el tema de la normalización de redes locales y metropolitanas en 1980. Para ello creo el grupo de trabajo llamado 802. La norma 802 fue aprobada en 1990. Esta norma sentaba las bases para el establecimiento de redes de área local y redes metropolitanas basadas en el modelo de Interconexión de Sistemas abiertos conocido como OSI (Open Systems Interconnection).

El modelo OSI se basa en estructurar el proceso de comunicación en siete áreas independientes a las que llama capas (física, enlace, red, transporte, sesión, presentación y aplicación). De las siete capas del sistema OSI, la norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas: física y de enlace. Uno de los temas que se definen en estas dos capas son las técnicas de acceso, las cuales definen como cada terminal puede hacer uso del medio de comunicación común.

El grupo de trabajo 802.11 se estableció específicamente para las redes locales inalámbricas creadas con la tecnología Wi-Fi. El principal problema que resolvió la normalización IEEE 802.11 fue la incompatibilidad entre los dispositivos inalámbricos de distintos fabricantes

Dentro del grupo de trabajo IEEE802.11 se pueden encontrar diferentes versiones, aunque las más importantes son las siguientes:

Wireless A	IEEE 802.11a	54Mbps hasta 108Mbps	Trabaja en la banda de frecuencia de 5Ghz utiliza la técnica de transmisión denominada OFDM
Wireless B	IEEE 802.11b	11 Mbps (Megabits por segundo)	Trabaja en la banda de frecuencia de 2.4 GHz solamente compatible con velocidades menores.
Wireless G	IEEE 802.11g	11 / 22 / 54 Mbps	Trabaja en la banda de frecuencia de 2.4 GHz.
Wireless N	IEEE 802.11n	300 Mbps	Utiliza una tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente.

Tabla I.3.1 normas wireless

IEEE 802.11

Fue el primer estándar que se definió. Opera en la banda ISM (Industrial, Scientific and Medica). El estándar especifica una secuencia de Barker de chipping empleada para ensanchar el espectro. Cada secuencia de 11 bits representa un símbolo el cual, a su vez, está asociada a un solo bit de datos (1 ó 0). Las modulaciones empleadas son BPSK y APSK, Éstas han caído en desuso puesto que las velocidades de transmisión no resultan atractivas y existen otras variantes de mayores prestaciones.

El estándar 802.11 establece los niveles inferiores del modelo OSI para las conexiones inalámbricas que utilizan ondas electromagnéticas, por ejemplo:

•La capa física (a veces abreviada capa "PHY") ofrece tres tipos de codificación de información.

•La capa de enlace de datos compuesta por dos subcapas: control de enlace lógico (LLC) y control de acceso al medio (MAC).

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos mientras que la capa de enlace de datos define la interfaz entre el bus del equipo y la capa física, en particular un método de acceso parecido al utilizado en el estándar Ethernet, y las reglas para la comunicación entre las estaciones de la red.

En realidad, el estándar 802.11 tiene tres capas físicas que establecen modos de transmisión alternativos:

- Capa de enlace de datos (MAC): 802.2 (cableado) y 802.11 (WLAN)
- Capa física (PHY): DSSS, FHSS o Infrarrojo.

Cualquier protocolo de nivel superior puede utilizarse en una red inalámbrica Wi-Fi de la misma manera que puede utilizarse en una red Ethernet.

Dentro de la normativa 802.11 existen otras versiones que se muestran en la tabla I.3.2.

Versión	Características
802.11a	54Mbps WLAN en la banda de 5Ghz.
802.11b	11Mbps WLAN en la banda de 2,4Ghz.
802.11c	Cruce sin cables
802.11d	"modo mundial" adaptación de los requerimientos regionales
802.11e	QoS y extensiones que fluyen a través de 802.11 a/g/h
802.11f	Transito para 802.11 a/g/h
802.11g	54Mbps WLAN en banda 2,4Ghz.
802.11h	802.11 con DFS y TCP (Europa)
802.11i	Autentificación y cifrado AES
802.11j	802.11a con canales adicionales por encima de 4-9 Ghz.
802.11k	Intercambio de información de capacidad entre clientes y AP
802.11m	Mantenimiento, publicación de actualizaciones estándar
802.11n	Nueva generación WLAN en banda 2,4Ghz. que permite velocidades superiores a 500Mbps.

Tabla I.3.2 versiones del 802.11

Siendo que las IEEE 802.11b y IEEE 802.11g son las que se han extendido en las redes Wi-Fi debido sobre todo a la banda de frecuencia que utilizan para la comunicación. Esta banda corresponde a ISM (medico-científica internacional) y está disponible en cualquier parte del planeta, por lo tanto al utilizar esta misma banda de WiFi se aseguran que los dispositivos funcionan correctamente en todos los países del mundo.

I.3.1 IEEE 802.11a

La gran diferencia con el estándar 802.11b es su trabajo en la banda de los 5Ghz. y su ventaja es que alcanza velocidades de hasta 54Mbps llegando en algunos casos hasta los 108Mbps.Las características de esta norma son principalmente las siguientes:

- Velocidad máxima de hasta 54Mbps.
- Opera en el espectro de 5Ghz.
- Menos saturado
- No es compatible con las normas 802.11b y 802.11g.
- Modulación OFDM

En 1997 el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) crea el estándar con velocidades de 2Mbps. En 1999 se aprobaron los estándares 802.11a y el 802.11b. En 2001 fue el año en que se lanzaron los productos al mercado del estándar 802.11a. Utiliza protocolos, opera en la banda de 5Ghz y utiliza 52 subportadoras (OFDM) 'Orthogonal frequency-division multiplexing' con una velocidad máxima de 54Mbps, lo que lo hace el estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20Mbps. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbps en algunos casos. No puede interoperar con equipos del estándar 802.11b, excepto que se disponga de equipos que implementen ambos estándares (tarjetas NIC a/b). La utilización de esta banda tiene sus desventajas ya que restringe el uso de dichos equipos a únicamente puntos en línea de vista, lo que hace necesaria la instalación de un mayor número de puntos de acceso y esto significa que no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

I.3.2 IEEE 802.11b

Introducida en 1999 con una velocidad de transmisión de 11Mbps a pesar de su baja velocidad y de operar en la banda de 2.4Ghz. Es muy sensible a las interferencias con otras tecnologías inalámbricas como por ejemplo bluetooth.

Características principales

- Velocidad máxima de hasta 11Mbps
- Opera en el espectro de 2.4Ghz. sin necesidad de licencia.
- Esta norma es la conocida como WiFi
- Compatible con los equipos del estándar 802.11

Esta norma utiliza el método de acceso CSMA/CA, este estándar funciona en la banda de 2.4 a 2.497 Ghz. del espectro radioeléctrico y su método de modulación se le conoce como espectro de difusión de secuencia directa complementaria (DSSS) y utiliza la llave de código complementario (CCK). Debido a la utilización de CSMA/CA en la practica la velocidad máxima de transmisión de este estándar es de aproximadamente 5.9Mbps sobre TCP y 7.1Mps sobre UDP.

I.3.3 IEEE 802.11g

Características generales del estándar

- Velocidad máxima de hasta 54Mps
- Opera en la banda de los 2.4Ghz. sin licencia.
- Compatible con 802.11b
- Utiliza la modulación DSSS y OFDM

En junio de 2003 se ratifico el estándar 802.11g, que utiliza la banda de 2.4Ghz. al igual que el 802.11b pero operando con una velocidad teórica máxima de 54Mps o cerca de 24.7Mps de velocidad real de transferencia similar a la del estándar 802.11a, su compatibilidad con el 802.11b se logró con un proceso adecuado sin embargo en redes usando ambos estándares reduce significativamente la velocidad de transmisión. El principal problema que puede plantear un despliegue masivo de los estándares 802.11b y 802.11g se basa en la necesidad de realizar una normalización estricta desde entornos reguladores oficiales, puesto que la división de canales establecida para el rango de frecuencia utilizado por estos dispositivos (2.4Ghz.) provoca interferencias de equipos cuyas zonas de cobertura se solapen, que puede llegar a impedir el uso de ambas redes de una forma eficiente.

El futuro de las nomas esta dado en **802.11n**. En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b.

También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input – Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. Existen también otras propuestas alternativas que podrán ser consideradas. El estándar ya está redactado, y se viene implantando desde 2008.

A principios de 2007 se aprobó el segundo boceto del estándar. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial este estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo estuviera implantado). Ha sufrido una serie de retrasos y el último lo lleva hasta noviembre de 2009. Habiéndose aprobado en enero de 2009 el proyecto 7.0 y que va por buen camino para cumplir las fechas señaladas. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

I.4 Capa Física y MAC

El nivel Físico se encarga de resolver los aspectos relacionados con las particularidades del medio de transmisión radioeléctrico. En IEEE 802.11 se emplean cuatro tecnologías de transmisión diferentes, todas ellas incompatibles entre sí. La norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del sistema OSI (International Standards Organization): Capa física y capa de Enlace, a ésta última se hace una división por que resultan tres capas:

- **PHY** (Physical Layer, "capa física") es la capa que se encarga de definir los métodos por los que se difunde la señal.
- **MAC** (Medium Access Control, "control de acceso al medio") es la capa que se ocupa del control de acceso al medio físico. En el caso de WiFi el medio físico es el espectro radioeléctrico. La capa MAC es un conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso de este espectro radioeléctrico.
- **LCC** (Logical Link control, "control del enlace lógico") es la capa que se ocupa del control del enlace lógico definiendo cómo pueden acceder múltiples usuarios a la capa MAC.

La tabla I.4.1 muestra características de los medios físicos.

	Infrarrojos	**FHSS** Frecuecy-Hopping Spread Spectrum	**DSSS** Direct-Sequence Spread Spectrum	**OFDM** Orthogonal Frecuency Division Multiplexing
Banda	850-950nm	2,4Ghz.	2,4 Ghz	2,4 y 5 Ghz.
Velocidades	1 y 2Mbps (802.11)	1 y 2Mbps (802.11)	1 y 2Mbps (802.11) 5,5 y 11Mbps (802.11b	6,9,12,18,24,36,48 y 54 Mbps (802.11a) Hasta 54Mbps (802.11g)
Alcance (velocidad máxima)	20 m	150m	30m	5m
Utilización	Muy rara	Poca / a extinguir	Mucha	Poca /creciente
Características	No atraviesa paredes	Interferencias Bluetooth y hornos de microondas	Buen rendimiento y alcance	Máximo rendimiento

Tabla I.4.1 medios físicos

Una vez seleccionada la banda de frecuencia, el paso siguiente es elegir una tecnología de transmisión.

I.4.1 Tecnologías de Transmisión

Las tecnologías más utilizadas son las de espectro ensanchado y OFDM (Orthogonal Frecuency Division Multiplexing). Existen dos variantes:

- **DSSS** Espectro ensanchado por secuencia directa (Direct-Sequence Spread Spectrum): En este caso, la secuencia pseudoaleatoria se emplea para generar un bit redundante (chipping code). Estos códigos Chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits. Entre las señales eliminadas se encuentra el ruido y las interferencias, este código permite identificar los datos como pertenecientes a un emisor determinado.

  El emisor genera los chips y sólo los receptores que conocen dicho código pueden descifrar los datos. La norma 802.11 dice que la longitud mínima del código de chips debe ser de 11.

  El resultado es un código de mayor frecuencia, al ensanchar el canal, cuando se produce una interferencia, el receptor puede traer la información útil por que dicha interferencia aparece como si fuera de banda estrecha, Se muestra en la imagen I.5.1.

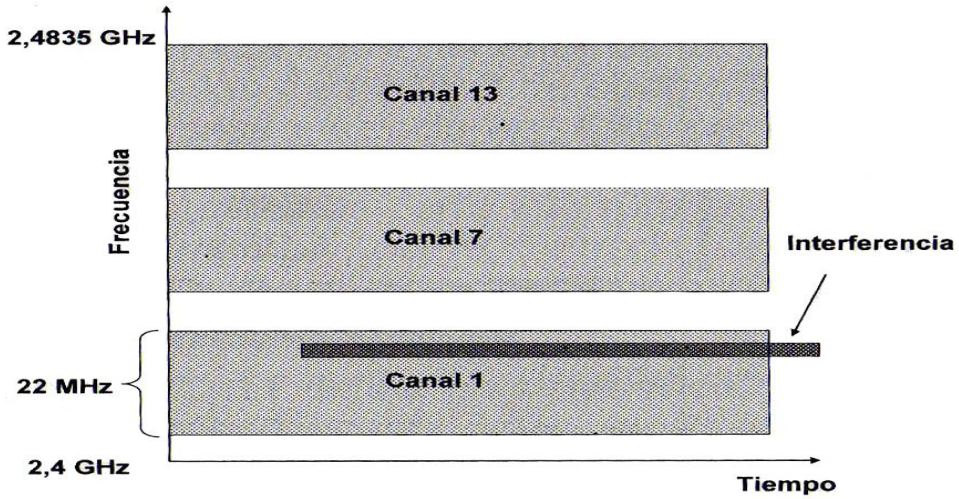

Imagen I.5.1 Canal Ensanchado

- **FHSS** espectro ensanchado por salto en frecuencia (Frecuecy-Hopping Spread Spectrum): Se basa en ir cambiando de portadora (aproximadamente unas 50 veces por segundo) en función de un patrón conocido por los extremos de la comunicación, de manera que cada tramo de la información se transmite a una frecuencia durante un corto intervalo de tiempo (dwell time).

  A todos los efectos es como si se dispusiera de un solo canal lógico mucho más inmune a las interferencias de este tipo, únicamente se perderían algunos saltos. La ventaja en estos sistemas es que si se cumplen dos comunicaciones distintas nunca utiliza la misma portadora simultáneamente, podremos tener más de un punto de acceso en la misma zona geográfica sin que existan interferencias, sin embargo, su principal problema es que complica el diseño de la capa MAC debido a que se requiere más información de control. En la imagen I.5.2 se muestra los saltos que se dan en la frecuencia.

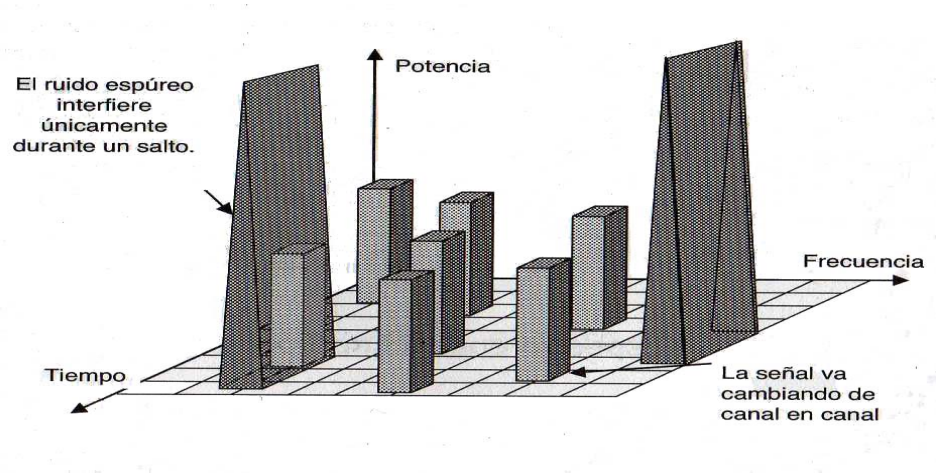

Imagen I.5.2 Saltos de Frecuencia

Los sistemas de espectro ensanchado son los que consumen más ancho de banda, pero la señal resulta más fácil de detectar.

El inconveniente de FHSS es la necesidad de sincronizar el emisor y el receptor en las frecuencias a utilizar en cada momento, este problema fue resuelto por los ingenieros de Sylvania Electronics system a finales de los años 50`s.

La modulación OFDM: emplea un conjunto de subportadoras ortogonales cada una de las cuales se modulan de manera individual y combinada para formar la señal final, el inconveniente principal es que se requiere una mayor precisión en frecuencia.

Esta técnica divide el ancho de banda en subcanales más pequeños que trabajan en paralelo de esta forma se consigue llegar a velocidades de hasta 54Mbps, divide la portadora en 48 subportadoras que son utilizadas para transmitir datos y otras 4 para poder alinear las frecuencias en el receptor, este sistema consigue un uso muy eficiente del espectro radioeléctrico.

Una ventaja de este sistema es que consigue una alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno (eco o multipath) Para poder transmitir la señal hace primero falta definir el método de difusión y posteriormente un método de modulación de la misma.

La modulación consiste en modificar una señal pura de radio para incorporarle la información a transmitir. La señal base a modular recibe el nombre de portadora (Carrier).Lo que se le cambia a la portadora es su amplitud, frecuencia, fase o una combinación de éstas.

Las técnicas de modulación utilizadas en 802.11 son:

- BPSK: Modulación binaria por salto de fase (binary phase-shift keying)
- QPSK: Modulación binaria por salto de fase en cuadratura (Quadrature phase-shift keying)
- GFSP: Modulación gausiana por salto de frecuencia (Gaussian frequency-shift keying)
- CCK: Modulación de código complementario (Complementary code keying)

Otra posibilidad aunque no muy extendida, es la tecnología infrarroja, se emplean frecuencias muy altas, el problema es que no pueden traspasar objetos opacos, lo que reduce su utilización a enlaces punto a punto o punto a multipunto con visión directa entre los extremos de la comunicación.

I.4.2 Nivel MAC

MAC (Control de acceso al medio), define los procedimientos que hacen posible que los distintos dispositivos compartan el uso de este espectro radioeléctrico. Mientras que las distintas versiones del estándar 802.11 utilizan distintos sistemas para difundir su señal (su capa física es diferente), la capa MAC es la misma para todas ellas.

Sobre el nivel físico, se encuentra el nivel MAC encargado de funciones tales como la fragmentación, el arbitrio del acceso al medio compartido o la retransmisión de paquetes.

La MAC es muy similar a la utilizada por la red Ethernet, ambas utilizan la técnica conocida como CSMA (Carrier Sense Multiple Access, 'Acceso Múltiple por Detección de Portadora') la diferencia radica en el uso de la tecnología CD (Collision Detection, 'Detección de Colisión') para Ethernet y en la inalámbrica es usada la tecnología CA (Collision Avoidance, 'Evitación de Colisión'). Una colisión se produce cuando dos terminales intentan hacer uso del medio simultáneamente. La CA dispone de procedimientos para evitar que se produzcan colisiones mientras que la CD detecta la colisión y retransmite los datos.

La razón por la cual hay dos sistemas es que cuando el medio es un cable, una terminal puede transmitir y recibir al mismo tiempo, por lo que debe detectar colisiones. Por el contrario en el medio radioeléctrico un terminal no puede transmitir y recibir al mismo tiempo por el mismo canal, por lo tanto al no poder detectar colisiones, la solución es disponer de una técnica que las evite.

I.4.2.1 CSMA/CA

Evitar las colisiones

EL método CSMA/CA utiliza un mecanismo tanto físico como virtual para detectar la portadora; el físico funciona como en CSMA/DC y el virtual se logra distribuyendo información de reserva que anuncia el uso inminente del medio. El cambio de tramas RTS (request to send) 'Solicitud para enviar' y CTS (Cleat to send) 'listo para enviar', antes de la trama de datos real es una forma de distribuir esta información de reserva del medio.

Estas tramas contienen un campo de duración que define el periodo de tiempo que necesita el medio para transmitir la trama de datos real.

El intercambio RTS/CTS realiza un tipo de deducción rápida de colisiones y una comprobación de la ruta de transmisión.

El nivel de MAC se basa en el concepto de función de coordinación. Genéricamente la función de coordinación se encarga, dentro de cada celda (BSS), de decidir en qué instantes las estaciones pueden acceder al canal. Se divide en dos niveles: la función de coordinación puntual (PCF, *Puntual Coordination Function)* y la función de coordinación distribuida (DCF, *Distributed Coordination Function).*

MAC tiene dos funciones distintas para coordinar la transferencia de datos:

PCF *(Point Coordination Function,* 'Función de coordinación del punto') facilita un sistema para poder transmitir el tráfico que es sensible a los retardos y que requiere un tratamiento especial para evitar las demoras.

DCF *(Distributed Coordination Function,* 'Función de coordinación distribuida') facilita un sistema que permite compartir el medio físico (radioeléctrico, infrarrojos, etc.) entre todas las estaciones de la red. Para ello, DCF define los mecanismos que le permiten a las estaciones negociar el acceso al medio físico, así como los mecanismos que aseguran la entrega de los datos a las estaciones. A través de DCF se transmiten los datos que no son sensibles a los retardos.

La función DCF se encuentra con un problema y es que una de las diferencias de los medios cableados frente a los inalámbricos es que en estos últimos es mucho más complicado detectar las colisiones.

El IEEE aprobó a finales de 2005 el estándar que define las características de calidad de servicios de las redes inalámbricas. Se trata de 802.11e. Este estándar mejora las técnicas PCF y DCF con una nueva función conocida como HCF *(Hybrid Coordination Function,* 'Función Híbrida de Coordinación').

HCF define dos métodos de acceso al canal: HCCA *(HCF Controlled Channel Access,* 'Acceso Controlado al Canal HCF') y EDCA *(Enhanced DCF Channel Access,* 'Acceso al Canal Mejorado DCF'). Ambos métodos definen las distintas clases de tráfico (TC, *Traffic Classes)* a considerar. Con EDCA, el tráfico de alta prioridad se transmite antes al aplicar la estación unos tiempos de espera menores después de enviar el paquete anterior. Por su parte, HCCA funciona de forma similar a PCF, en el que existe un coordinador híbrido (HC, *Hybrid Coordinator)* que controla el acceso al medio.

I.4.2.2 Servicios de MAC

La subcapa MAC proporciona tres servicios en IEEE802.11:

- Servicio de datos asíncrono.
- Servicio de Seguridad.
- Ordenamiento MSDU (MAC Service Data Units).

I.4.2.2.1 *Servicio Asíncrono*

Este servicio permite a las entidades LLC (Logical Link Control) vecinas intercambiar las MSDU (MAC Service Data Units), para soportar el servicio, MAC actual utiliza un nivel físico subyacente para transportar una MSDU a una entidad MAC vecina, donde es entregada al LLC vecino.

El transporte por difusión (*broadcast*) o multidifusión (*multicast*) es parte del servicio de datos asincrónicos proporcionados por la subcapa *MAC.* A causa de esta característica del medio inalámbrico, la difusión y multidifusión de *MSDUs* podría experimentar una reducción en la calidad del servicio en comparación con la unidifusión (*unicast*) *de MSDUs*. Todas las estaciones soportan el servicio de datos asincrónicos.

I.4.2.2.2 Servicio de Seguridad

El servicio de autenticación y el mecanismo WEP (Privacidad equivalente al cableado, Wired Equivalent Privacy) suministran los servicios de seguridad del IEEE 802.11. El ámbito de los servicios de seguridad proporcionados está limitado al intercambio de datos entre estaciones. El servicio de privacidad ofrecido por una implementación WEP IEEE 802.11 es el cifrado de la MSDU.

Para propósitos del estándar IEEE 802.11, WEP es visto como un servicio lógico ubicado en la subcapa MAC. La implementación real del servicio WEP es transparente para las capas que se encuentra sobre la subcapa MAC. WEP proporciona tres servicios de seguridad:

- Confidencialidad.
- Integridad de los datos.
- Control de acceso.

El servicio WEP se explica detalladamente más adelante.

I.4.2.2.3 Ordenamiento de MSDU

Los servicios suministrados por la subcapa MAC permiten y en ciertos casos requiere el reordenamiento de las MSDUs que se realiza solamente cuando se necesita mejorar la probabilidad de entrega de una manera satisfactoria, basado en el modo operativo "administración de energía" actual de la estación o estaciones receptoras.

I.4.3 Formato de la Trama de MAC

La trama es la unidad de transmisión a nivel de MAC y define qué información debe adjuntarse a los paquetes generados por las aplicaciones de usuario para que sea transportada de manera adecuada por la red. En la imagen. I.4.1 se muestra como es la trama. En 802.11 la trama de MAC, contiene una cabecera que incluye campos de control, duración, direccionamiento y control de secuencia, un cuerpo de longitud variable y, finalmente, un campo de FCS para el control de errores.

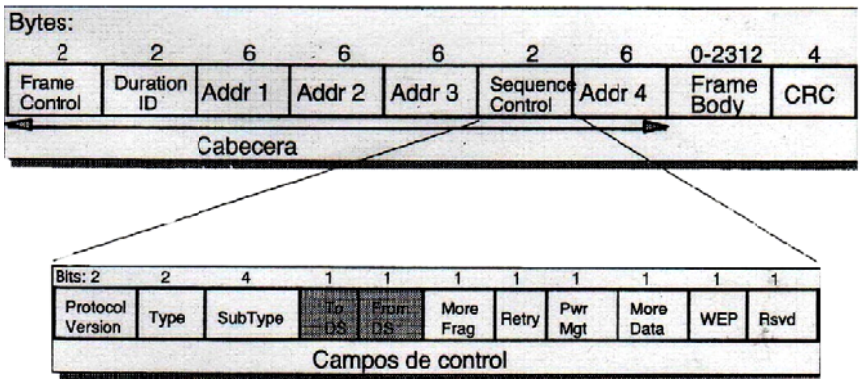

Imagen I.4.1 Trama de 802.11

Además de las tramas de datos, existen dos tipos de tramas de MAC: tramas de control (por ejemplo, reconocimientos o ACK, las tramas para el acceso múltiple con gTS y CTS y las tramas libres de contienda) y tramas de gestión (por ejemplo, el servicio de asociación, las tramas de *Beacon* o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso).

Uno de los aspectos más importantes a nivel de MAC es direccionamiento puesto que esta funcionalidad es la que permite a los nodos de la red reconocer que una trama va dirigida hacia ellos y quién es el responsable de su transmisión.

En 802.11, junto con las direcciones origen y destino, se emplean los bits *ToDS y FromDS del* campo de control de la cabecera de la trama. El primero de ellos indica si la trama se envía al sistema de distribución mientras que el segundo especifica que la trama procede de éste. En redes *ad hoc,* al no existir sistema de distribución, ya que la conexión es directa entre los nodos, estos bits siempre son nulos.La sincronización de los nodos de la red resulta fundamental para tareas de vital importancia como los saltos en frecuencia o el control de potencia.

Por ello, 802.11 ha definido la función de sincronización (TSF, ‘Time Synchronization Function’) que se encarga de gestionar todos los aspectos relacionados con la temporización. Su modo de trabajo va a depender de si la red es una red ad-hoc o si se trata de una configuración con punto de acceso.

La situación más sencilla se presenta con los puntos de acceso. En este caso, todos los nodos deben actualizar sus relojes internos de acuerdo al reloj del punto de acceso, que es el que marca la sincronización. Para ello, el punto de acceso envía periódicamente tramas de beacon con el valor de su reloj en el momento de la transmisión.

El nodo, al recibirla, comprueba el valor de su reloj y lo corrige para sincronizarlo con el del punto de acceso. Este proceso de ajuste puede ser pasivo, si el nodo espera a recibir la trama de beacon del punto de acceso al que está asociado o, activo cuando el nodo envía tramas de prueba y espera la respuesta de algún punto de acceso.

En el modo *ad-hoc,* el funcionamiento es más complejo. En este caso, el control está distribuido y es responsabilidad de todos los nodos de la *red* mantener la sincronización. Cuando un nodo no detecta una trama de *beacon* durante un tiempo superior al tiempo de *backoff,* generará una con el fin de evitar que no desincronice la red.

El estándar 802.11 define un funcionamiento en modo limitado de potencia según el cual las estaciones pueden permanecer "dormidas" sin pérdida de información, de modo similar a lo que sucede en Bluetooth. La idea es sencilla: el punto de acceso mantiene una lista de los nodos que, en cada momento, se encuentran en este estado y, además, almacena las tramas destinadas a dichos nodos hasta que éstos soliciten el envío de las tramas que les corresponden o cambien a un modo de potencia normal.

Periódicamente, el punto de acceso envía información sobre las estaciones en modo limitado de potencia de las que tiene tramas almacenadas utilizando para ello la trama de *beacon.* Al recibir esta trama, las estaciones despiertan y, en caso de que tengan pendiente la recepción de alguna trama, deben solicitar al punto de acceso. Cuando el punto de acceso decida enviar la trama, lo hará previa transmisión de una trama TIM (*Traffíc Indication Map)* para que el nodo despierte en el próximo intervalo de portadora. De esta manera, estas estaciones recibirán la información con un desgaste mínimo de potencia.

El estándar define cuatro servicios elementales que deben proporcionar las WSTA (*Wireless Stations)* para interactuar con un AP:

- Autenticación: el primer paso para conectarse a una BSS es la identificación de la WSTA mediante la entrega al AP de algún tipo de credencial (SSID, dirección de MAC, certificado digital, etc.). El AP verificará esta credencial y denegará o permitirá el acceso.
- Desautenticación: proceso inverso al anterior.
- Envío de datos: transmisión de la información de los usuarios por la red.
- Privacidad: protección de la información a través del cifrado de la misma.

Una de las ventajas de las redes inalámbricas es la movilidad. Sin embargo, la movilidad de los usuarios se consigue a costa de una mayor complejidad de los protocolos. Uno de estos procesos es la itinierancia o *roaming.* A medida que el usuario se desplaza, puede ocurrir que abandone la celda de un punto de acceso y entre dentro de la celda de otro punto de acceso. En ese momento, la red efectúa un *handover* mediante el cual el usuario pasa a estar asociado al segundo punto de acceso.

El *handover es* muy similar al que tiene lugar en las redes de telefonía móvil, pero con dos diferencias principales. Una red WLAN es una red de datos y, dado que éstos se generan a ráfagas, y el *roaming* puede efectuarse en los intervalos en los que no se intercambian tramas de datos, a diferencia de lo que ocurre en las redes de telefonía móvil en las que el *roaming* tiene lugar durante la conversación utilizando canales de señalización dedicados, lo que facilita notablemente el proceso. Por otra parte, en una red de voz la pérdida temporal de conexión no afecta demasiado a la conversación. Sin embargo, en una red de datos se reducen las prestaciones de la red debido a las retransmisiones de las tramas extraviadas o erróneas que solicitarán los protocolos de nivel superior.

El estándar 802.11 no estipula ninguna implementación del *roaming,* aunque sí ofrece algunos mecanismos que simplifican su puesta en marcha. Cuando un dispositivo móvil (PC, PDA, PocketPC, etc.) envía una trama de datos, existe una ventana temporal dentro de la cual espera recibir un reconocimiento. Si éste no llega, se asume que la trama de datos se ha perdido y reenvía, los puntos de acceso envían periódicamente unas tramas de gestión llamadas tramas de *beacon.* Estas tramas contienen el SSID *(Service Set Identifier),* las velocidades soportadas, si el punto de acceso trabaja con salto en frecuencia o con secuencia directa y la capacidad de dicho punto de acceso.

El modo de manejar esta información para tomar la decisión final depende del criterio del fabricante. Para evitar problemas de incompatibilidad entre puntos de acceso de fabricantes distintos, se ha definido la norma 802.11f, que especifica un protocolo para el punto de acceso que proporciona la información necesaria para efectuar el *roaming* entre puntos de acceso de diferentes vendedores. Una red 802.11, al igual que ocurre con cualquier tipo de red inalámbrica, es una red inherentemente insegura puesto que el medio de transmisión es el aire y las señales viajan libres, de manera que cualquier individuo equipado con una antena de las características adecuadas podría recibir la señal y recogerlas en un equipo para su posterior análisis. Sin embargo, esa capacidad de recibir la señal no equivale a poder extraer la información que contiene, siempre y cuando se tomen las medidas oportunas, por ejemplo, mediante el cifrado de la misma.

I.5 Protocolo

Un protocolo no es más que un conjunto de reglas que emplean dos equipos informativos para dialogar entre sí, de forma que puedan establecer y mantener una comunicación sin errores.

Para que los protocolos puedan llevar a cabo sus objetivos, necesitan añadir ciertos datos de control a la información original a transmitir. Estos datos adicionales son incluidos por el terminal emisor y suprimidos por el terminal receptor antes de entregar la información al destino.

Anteriormente cada fabricante establecía sus criterios para sus dispositivos, siendo casi imposible la comunicación entre dispositivos de distintos fabricantes, por lo tanto se evidenciaba la necesidad de una normalización par que las conexiones informáticas fueran posibles y de esa forma se lograran independientemente del fabricante.

I.5.1 Protocolos de cifrados de datos

El acceso sin necesidad de cables que ofrece la tecnología Wi-Fi es la razón por la cual las redes han tenido un auge muy significativo, sin embargo el problema más importante radica en la seguridad. Una red inalámbrica, es una red inherentemente insegura puesto que el medio de transmisión es el aire y las señales viajan libres, de manera que cualquier individuo equipado con una antena de las características adecuadas podría recibir la señal y recogerlas en un equipo para su posterior análisis. Sin embargo, esa capacidad de recibir la señal no equivale a poder extraer la información que contiene, siempre y cuando se tomen las medidas oportunas, por ejemplo, mediante el cifrado de la misma. Para que los datos que se transmiten en la comunicación inalámbrica vayan cifrados existen tres protocolos de encriptación: WEP, WAP y WPA2.

- **WEP**

  (Wired Equivalent Privacy) fue el primer protocolo de encriptación introducido en el estándar IEEE 802.11 del año 1999 y se ha mantenido sin ningún cambio en las diferentes versiones de dicho estándar (IEEE 802.11b, IEEE 802.11g). El protocolo WEP está basado en el algoritmo RC4[2] usando claves de 64 y 128 bits (40+24 ó 104+24, donde el número 24 es un vector de inicialización, conocido como IV, de 24 bits).

  El cifrado de WEP en una red inalámbrica realiza los siguientes pasos:

  - En primer lugar, se elige una clave secreta estática que afectará a todos los puntos de acceso y las PC de la red WiFi.
  - Dicha clave secreta se utiliza, junto con un vector de inicialización IV, para generar una clave pseudoaleatoria.
  - Por último se aplica la operación lógica XOR entre los datos originales y la clave pseudoaleatoria anteriormente creada, produciendo como resultado los datos cifrados, que tienen una longitud adicional de cuatro caracteres, que posteriormente se utilizan durante la fase de descifrado para comprobar la integridad de la información. Estos cuatro caracteres adicionales reciben el nombre de ICV (Integrity Check Value).

[2] El algoritmo RC4 es un cifrador de flujo inventado por Ronald Rivest, uno de los creadores del conocido algoritmo de criptografía asimétrica RSA.

Para descifrar la información encriptada con el protocolo WEP se realizan los siguientes pasos:

- en primer lugar se genera una semilla a partir de la combinación de la clave secreta con el vector de inicialización IV.
- A continuación se utiliza dicha semilla en el algoritmo de descifrado PRGN para obtener unos datos a los que, aplicándole la operación lógica XOR junto con el mensaje cifrado, permiten obtener el texto plano.
- Por último, el receptor comprueba la integridad de los datos, aplicando el algoritmo CRC-32 al ICV que añadió durante el cifrado WEP.

El protocolo WEP no ofrece unas barras de seguridad demasiado potentes en la actualidad, ya que existen en Internet numerosas herramientas gratuitas fáciles de utilizar que permiten obtener la clave secreta WEP en apenas minutos.

- **WPA**

WPA (Wi-Fi Protected Access, 'Acceso Protegido Wi-Fi') es un sistema para proteger las redes inalámbricas creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy, 'Privacidad Equivalente a Cableado').

Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP. WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado.

La información se cifra utilizando el algoritmo RC4 con una clave de 128 bits y un vector de inicialización de 48 bits.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil.

El algoritmo fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques.

Para limitar este riesgo, los drivers de las estaciones se desconectarán un tiempo definido por el fabricante, si reciben dos colisiones en menos de 60 segundos, el algoritmo podrán tomar medidas, como por ejemplo reenviar las claves o dejar de responder durante un tiempo específico.

Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

- **Para el uso personal doméstico:** El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

- **Para el uso en empresarial/de negocios:** El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor RADIUS

A pesar de protocolo WPA ofrece muchas más garantías de seguridad que el WEP, la inmensa mayoría de redes inalámbricas Wi-Fi utilizan el protocolo WEP por desconocimiento o por que los fabricantes. Lo ponen por defecto en sus dispositivos.

- **WPA2**

En junio de 2004, fue adoptado el estándar IEEE 802.11i con la intención de responder a las precauciones empresariales ante la seguridad inalámbrica. Este estándar introdujo varios cambios fundamentales, como la separación de la autentificación de usuarios de la integridad y privacidad de los mensajes proporcionando una arquitectura segura para las redes inalámbricas.

Utiliza una nueva arquitectura para las redes wireless llamada Robust Securityy Network (RSN) y utiliza autentificación 802.11x, distribución de claves robustas y nuevos mecanismos de integridad y privacidad. Para el cifrado de datos utiliza el algoritmo de cifrado por bloques AES (Advance Encryption estándar).

Hasta ahora el momento el algoritmo de cifrado WPA2 es un algoritmo seguro y se aconseja su utilización frente a otros algoritmos que ya han sido “rotos” como es el caso de WEP o WPA.

CAPITULO II

DESARROLLO E IMPLEMENTACIÓN DE WLAN EN UNA SALA DE CÓMPUTO

Wi-Fi permite establecer dos tipos de redes: interconexión directa entre todos los equipos, conocida como ad hoc, o interconexión a través de una estación base central conocida como punto de acceso. Las redes inalámbricas con punto de acceso son más convenientes cuando se pretende crear una red permanente, aunque sea con pocos terminales, cuando se desea disponer de un área de cobertura más amplia o crear una red inalámbrica con muchos usuarios. El modo normal de configuración de las redes inalámbricas Wi-Fi es con puntos de acceso, es decir redes inalámbricas Wi-Fi infraestructura.

La instalación y configuración de una red inalámbrica es algo relativamente simple; sin embargo, uno de los motivos de crear una red es compartir algún recurso: una impresora, carpetas, etc.

Es importante tener en cuenta que no sólo se trata de establecer una conexión entre dos o más equipos, sino que hace falta que el equipo que comparte sus recursos permita el acceso de los usuarios remotos y que los archivos o dispositivos a compartir estén configurados de forma adecuada. Dicho de otra forma, no todo es Wi-Fi a la hora de crear una red.

Para poder interconectar equipos/y compartir recursos, es necesario realizar las siguientes acciones. Más adelante se explicara a fondo.

1. Asegurarse de que cada equipo dispone de su dispositivo Wi-Fi y que tenemos los elementos de red necesarios (punto de acceso, etc.). La existencia de los certificados Wi-Fi garantizan la compatibilidad de todos los dispositivos.

2. Configurar los distintos dispositivos Wi-Fi para permitir una interconexión inalámbrica entre los equipos.

3. Permitir que los usuarios remotos puedan conectarse al equipo que comparte los recursos.

4. Configurar los recursos a compartir (archivos, carpetas, impresoras) para que puedan ser utilizados de forma remota.

En la imagen II.1 podemos observar los pasos a seguir en la configuración de nuestra red wlan.

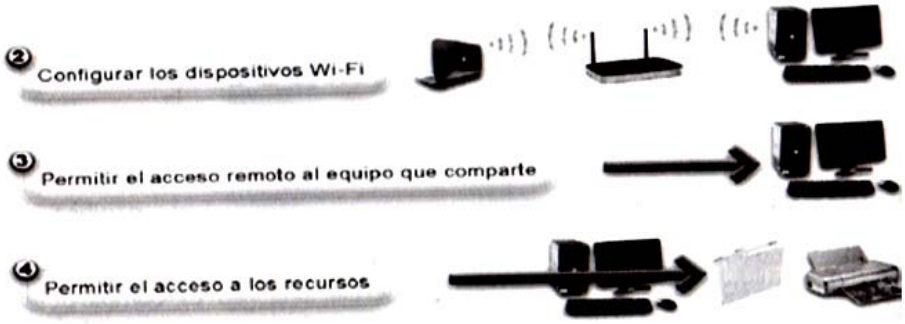

Imagen II.1 Configuración de red Wlan

II.1 Dispositivos utilizados en la Wlan.

La mayoría de las redes inalámbricas que hay en el mercado funcionan de manera similar: tienen unas estaciones base que normalmente se conocen como puntos de acceso (AP) que se encargan de coordinar las comunicaciones y unas tarjetas de red, conocidos como adaptadores de red que se instalan en los equipos de computo, mediante las cuales se comunican entre sí y forman parte de la red.

Adicionalmente existen antenas que permiten aumentar el alcance de los equipos Wi-Fi, así como software especializado que permite facilitar la labor de gestión y mantenimiento de la red inalámbrica.

II.1.1 Puntos de Acceso

Características internas. Si se tuvieran unas necesidades particulares, antes de elegir el punto de acceso, sería interesante comprobar que sus características son las adecuadas para darles respuesta. Por ejemplo, puede ser interesante lo siguiente:

- Comprobar las características del *router* del punto de acceso. DHCP, NAT o propiedades de *firewall* (cortafuegos) son facilidades que nos ayudarán en la configuración y manejo de las comunicaciones con internet o con otras redes.

- En el entorno corporativo suelen coexistir una red inalámbrica para darle movilidad a los usuarios que la necesitan, junto con una red cableada para darle conectividad al resto de usuarios. Generalmente, las redes corporativas utilizan el protocolo TCP/IP; no obstante, hay que tener en cuenta que en el mercado existen otros protocolos. Por tanto, conviene comprobar que el punto de acceso que se va a comprar sea compatible con el protocolo de red cableada con el que se va a conectar.

- Los puntos de acceso Wi-Fi funcionan sin problema con los adaptadores de red (tarjetas de red) de cualquier fabricante. No obstante, hay cierta incompatibilidad cuando se desea crear una red con varios puntos de acceso de distintos fabricantes.

- La falta de entendimiento aparece a la hora de mantener en servicio una comunicación cuando un usuario pasa del área de cobertura de un punto de acceso al de otro (a esto se le llama itinerancia o *roaming,* en inglés).

- Si los puntos de acceso son de distinto fabricante, es muy posible que se corte la comunicación. Aunque esta comunicación se volverá a establecer con el nuevo punto de acceso, lo cierto es que no se habrá producido una transferencia sin interrupciones, que es de lo que se trata. Para evitar este problema, es recomendable que los puntos de acceso vecinos sean del mismo fabricante. Además, cuando todos los dispositivos son del mismo fabricante, es posible utilizar alguna característica adicional propietaria o particular del fabricante.

- Es importante saber que algunos puntos de acceso no utilizan una interfaz web, sino que requieren de la introducción directa de líneas comandos (lo que se conoce como CLI, *Command Une Interface,* 'Interfaz de línea de comandos') o, incluso, requieren de un sistema operativo particular.

El punto de acceso es la parte central de las comunicaciones de la mayoría de las redes inalámbricas, no solo es el medio de intercomunicación de todas las terminales inalámbricas, sino también es el punto de interconexión con la red fija e internet.

Un AP puede enlazar redes cableadas e inalámbricas, en instalaciones grandes se pueden configurar varios AP para que los usuarios tengan movilidad sin tener interrupciones. Un AP puede actuar como repetidor inalámbrico, o como un punto de extensión de la red inalámbrica.

Un AP se puede configurar de varias formas:

- Puerto de consola: requiere un cable totalmente cruzado
- Telnet: requiere que el AP tenga una dirección IP conocida
- Navegador web: requiere que el AP tenga una dirección IP conocida.

Existen dos categorías de puntos de accesos en la figura II.2 se muestran algunos de ellos:

- **Puntos de acceso profesionales:** diseñados para crear redes corporativas de tamaño medio o grande. Éstos suelen ser los más caros, incluyen mejores características, como son mejoras en la seguridad y una más perfecta integración con el resto de equipos. Los líderes de este tipo de equipamiento son Cisco, 3Com, Agere/Orinoco (antiguamente conocidos como Lucent) y Nokia.

- **Puntos de acceso económicos** dirigidos a cubrir las necesidades de los usuarios de pequeñas oficinas o del hogar. Estos puntos de acceso ofrecen exactamente los mismos servicios que los anteriores, con la misma cobertura y las mismas velocidades, pero ofrecen unas posibilidades de configuración y gestión más limitadas. Los que más puntos de acceso de tipo económico venden son Intel, 3Com, D-Link, Agere/Orinoco, NetGear Proxim y Linksys.

  Cada equipo tiene sus propias características externas. Algo que diferencia claramente a unos puntos de acceso de otros es el número y tipo de puertos exteriores que ofrece. Existen puntos de acceso que disponen hasta de un puerto de impresora (con su servidor de impresión), mientras que otros se limitan a ofrecer una conexión para red cableada o Internet.

Imagen II.2 puntos de acceso

Es habitual que los puntos de acceso se utilicen también como pasarela de conexión con otras redes en estos casos es importante que se tengan en cuenta los siguientes puntos:

- Comprobar las características del *router* del punto de acceso. DHCP, NAT o propiedades de *firewall* son facilidades que nos ayudarán en la configuración y manejo de las comunicaciones con Internet o con otras redes.

- Los puntos de acceso Wi-Fi funcionan sin problema con los adaptadores de red (tarjetas de red) de cualquier fabricante. No obstante, existe cierta incompatibilidad cuando se desea crear una red con varios puntos de acceso de distintos fabricantes. Los puntos de acceso son de distinto fabricante, es muy posible que se corte la comunicación. el IEEE está trabajando para solucionar este problema (grupo de trabajo IEEE 802.11f). Las tarjetas inalámbricas que se conectan a los equipos; estas últimas sí pueden proceder de fabricantes distintos sin problemas.

Características de Puntos de Acceso

Los puntos de acceso consiste cableada básicamente en un equipo de radio que dispone de una o varias antenas que se usan para transmitir y recibir información, con varios conectores RJ-45 que sirven de enlace físico a la red.

Los puertos R-J45 se pueden usar para conectar la red inalámbrica a una red cableada o internet, incorporan en su interior un switch, y a veces incluso incorporan puertos paralelos o usb para poder compartir impresoras sin necesidad de conectarlas a una PC. Al igual que un switch, incorpora usan serie de LED que indican en cada memento la actividad del enlace. La figura II.3 nos muestra un ejemplo de un punto de acceso comúnmente usado.

En su interior podemos encontrar el mismo equipamiento:

- Un equipo de radio (de 2,4 GHz en el caso de 802.11b y 802.11g, o 5 GHz en el caso de 802.11a)
- Una o dos antenas (que pueden o no apreciarse exteriormente)
- Un *software* de gestión de las comunicaciones
- Puertos para conectar el punto de acceso a Internet o a la red cableada
- Los puntos de acceso hardware suelen ofrecer múltiples servicios como servidor DHCP, filtrado de direcciones MAC, cifrado WEP, Cifrado WPA2.

En la actualidad la mayoría de los AP incorporan un servidor web que permite configurar el AP de una forma fácil y cómoda.

Los parámetros de configuración más importantes de un AP son:

- **Nombre de la red (SSID):** Nombre que identifica la red inalámbrica.

- **Canal de trabajo:** Existen 11 canales de funcionamiento y puede configurarse el AP para que utilice un canal predeterminado o que seleccione alguno de forma automática.

- **Protocolo de cifrado:** Existen protocolos de cifrado (WEP,WPA y WPA2), por seguridad se debe utilizar el protocolo WPA ó WPA2 ya que WEP es el más vulnerable.

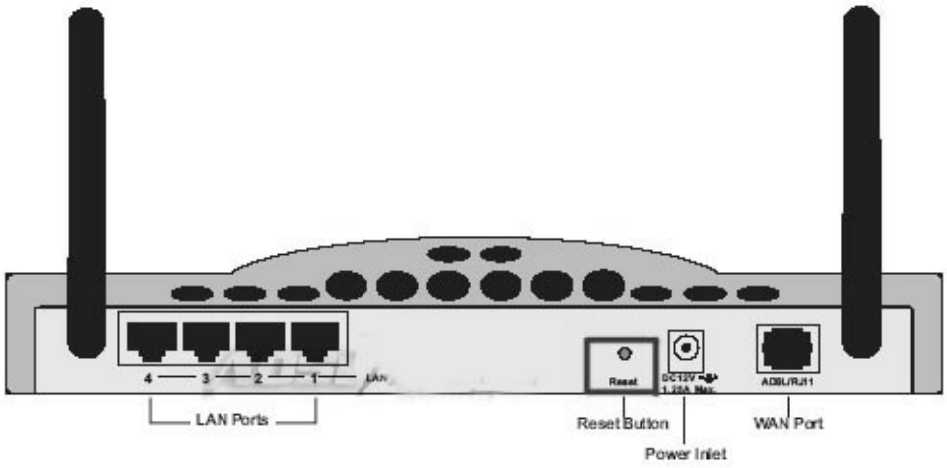

Imagen II.3 Parte trasera de un AP

Dependiendo del modelo, nos podemos encontrar con los siguientes puertos:

- Un puerto especial para conectarse a un hub o switch de red de área local Ethernet (uplink port).

- Disponer internamente de un *hub,* por lo que ofrecen de dos a cuatro puertos exteriores para conectarles los equipos de red Ethernet de que disponga el usuario. Esto es ideal para el hogar o la pequeña oficina ya que evita la necesidad de disponer de un *hub* o *switch* independiente.

- Un puerto serie RS-232 para que se le pueda conectar un módem de red telefónica (RTB o RDSI). Esta conexión a Internet a 56 Kbps o 64 Kbps puede ser utilizada como acceso principal a Internet o como acceso de seguridad en el caso de que falle la conexión de banda ancha (ADSL o cable).

- Un puerto paralelo o USB para conectarle una impresora. Esto permite compartir una impresora sin la obligación de tener una PC encendido para poder mantenerla disponible. Además, la impresora no le ocuparía recursos a ninguna PC.

- Puerto para conectarle una antena exterior que le provea de un mayor alcance. En el mercado existe una gran variedad de antenas externas que pueden dar respuesta a muchas necesidades distintas. Si se necesita que el punto de acceso ofrezca cobertura a una distancia superior a unos 100 metros, es importante contar con un punto de acceso que disponga de un conector de este tipo.

Los puntos de acceso ofrecen determinadas características que son configurables, como son las opciones de seguridad o de gestión de la red. La mayoría permiten llevar a cabo esta configuración a través de una interfaz basada en páginas Web. Para hacer uso de esto, sólo se necesita instalar el *software* que incluye el punto de acceso o introducir el número IP del punto de acceso en el navegador de Internet de cualquiera de sus terminales.

II.1.2 Adaptadores inalámbricos de Red (Wireless card)

Un adaptador de red inalámbrico es un componente hardware que permite a una PC conectarse a una red inalámbrica.

Son tarjetas o dispositivos que se instalan en los equipos de cómputo ya sea en su interior o externamente, estos dispositivos son un tipo de tarjeta especial NIC (Network Interface Controller) que permite al usuario conectarse a una red sin necesidad de cables. Son fundamentalmente unas estaciones de radio que se encargan de comunicarse con otros adaptadores (modo ad hoc) o con un punto de acceso (modo infraestructura). Como todos los equipos de radio, los adaptadores de red necesitan de una antena la cual puede o no apreciarse claramente, algunos adaptadores incluyen un conector para poder disponer una antena externa.

En el mercado existen numerosos modelos de adaptadores que se diferencian dependiendo del bus de expansión que utilizan (PCMCIA, PCI, USB, etc) y la normativa 802.11 que utilizan (802.11b, 802.11g o 802.11n) la imagen II.1.2.1 nos muestra una tarjeta pcmcia.

Tarjeta PCMCIA:

Imagen II.1.2.1 tarjeta PCMCIA

Por sus siglas en ingles (Personal Computer Memory Card International Association) 'Asociación Internacional de Tarjetas de Memoria para equipos portátiles'. Son tarjetas que tienen un tamaño similar al de una tarjeta de crédito que se insertan en los puertos PCMCIA (pc card) tipo II. Se utilizan para expandir la funcionalidad en aspectos variados y en este caso para añadir una tarjeta de red. Las tarjetas fueron creadas en 1989 con el propósito de desarrollar una norma de hardware y software para tarjetas de memoria. Todas las tarjetas tienen un ancho de 54 milímetros, siendo su largo variable, pero con un mínimo de 85,6 milímetros.

El hecho de ser variable se debe a que algunas tarjetas necesitan sobresalir hacia el exterior para mostrar algún tipo de conectar, una antena o, simplemente, porque necesitan más espacio.

En cuanto al grosor de las tarjetas existen tres tipos: las tarjetas tipo I con un grosor de 3,3 milímetros (utilizadas, por ejemplo, para ampliaciones de memoria), las de tipo II con un grosor de 5 milímetros (son las habituales en los adaptadores de red inalámbricos) y las de tipo III con un grosor de 10,5 milímetros (utilizadas, por ejemplo, por los discos duros).

Otra de las características que aportan las tarjetas PCMCIA es su bajo consumo de energía y ser resistentes a los golpes típicos de los dispositivos móviles.

Los adaptadores Wi-Fi PCMCIA suelen ser de tipo II (con *bus* de 32 bits tipo *CardBus) y* la mayoría de las PC portátiles incluyen una o dos ranuras PCMCIA de este tipo. Las PC portátiles modernos integran un adaptador Wi-Fi, por lo que no haría falta instalarles ninguna tarjeta adicional.

Adaptadores PCI e ISA:

Dispositivos PCI (Peripheral Component Interconnect) 'Interconexión de componentes periféricos') componentes de hardware que se conectan directamente a la placa base del equipo, por lo que es necesario abrir el equipo para su instalación. La imagen II.1.2.1 nos muestra una tarjeta PCI.

Imagen II.1.2.1 tarjeta pci inalámbrica

También hay tarjetas de red inalámbricas ISA (Industry Estándar Architecture) 'Arquitectura normalizada de la industria', sin embargo este tipo de dispositivos no son tan eficientes como PCI, estos últimos se configuran solos al reiniciar el sistema y los ISA hay que configurarlos y en esta época son obsoletos totalmente.

Adaptadores USB: Conector USB (Universal Serial Bus) 'bus serial universal' es un puerto de comunicaciones que se diseño para poder mejorar la forma en cómo los periféricos se conectaban a las PC, en 1996 apareció, creado por IBM, Intel, Compaq, Microsoft, digital, Northem Telecom y Nec. La imagen II.1.2.2 nos muestra un adaptador use inalámbrico.

Se aplica a casi todos los dispositivos que pueden comunicarse con una PC, ya que se trata de un estándar extendido por todo el orbe y garantiza la compatibilidad entre dispositivos, las características de USB son muy parecidas a las de PCMCIA, excepto el precio ya que los USB son muy económicos.

Imagen II.1.2.2 adaptador usb inalámbrico

USB vino a traer las siguientes ventajas:

- No hace falta apagar el equipo para conectar o desconectar un periférico USB.

- El equipo reconoce automáticamente los periféricos que se conectan y, si es preciso, instala automáticamente los controladores necesarios para que funcione adecuadamente.

- Ofrecen una alta velocidad de transferencia de datos: hasta 12Mbps con USB 1.1 y hasta 480Mbps con USB 2.0.

- Permite conectar hasta 127 dispositivos USB. Incluso, aunque la PC disponga de un solo puerto, basta con instalar un multiplicador de puertos (un *hub)* para disponer de más puertos USB.

- Ofrece alimentación eléctrica a los periféricos a través del propio conectar USB (hasta 500 mA).

- Los periféricos USB pueden apagarse automáticamente cuando detectan que no se están utilizando.

- Los periféricos USB se instalan automáticamente, sin necesidad de abrir el equipo.

- Algunos adaptadores inalámbricos USB se conectan al equipo mediante un cable, lo que permite que se pueda jugar con su orientación hasta conseguir el mejor nivel de recepción.

Adaptadores PDA. En el mercado se pueden encontrar adaptadores de red inalámbricos SD que permiten conectar PDA's, estos adaptadores que usualmente son usados están basados en IEEE 802.11b, que disponen de encriptación WEP de 64/128-bit para proteger la información que se transmite durante la comunicación.

Adaptadores inalámbricos COM y LPT. También pueden encontrarse en el mercado adaptadores inalámbricos que se conectan a través de puerto paralelo (LPT) y puerto serie (COM). Las características de estos conectores son muy similares a otras tarjetas de red pero el costo suele dispararse.

En la actualidad los equipos portátiles traen integrado un adaptador de red inalámbrico para poderse conectar a una red Wi-Fi, sin necesidad de algún dispositivo adicional, todo esto a causa de la necesidad social y tecnológica y que supone la formación de redes sin necesidad de una instalación cableada.

Los adaptadores de red, como cualquier dispositivo, para su correcto funcionamiento requieren de un pequeño software (driver o controlador), este es específico y debe ser compatible con cada sistema operativo ya sea instalado automáticamente o desde el cd de que contiene dicho software.
Los sistemas operativos suelen disponer de los controladores de dispositivos de los periféricos más comunes del mercado.

Por lo tanto es importante asegurarse que el dispositivo contenga el driver compatible con el sistema operativo que se va a utilizar en el equipo de cómputo.

Instalación de los adaptadores de red

La instalación de la tarjeta Wi-Fi o adaptador de red depende del modelo de tarjeta de que se disponga: los modelos PCMCIA hay que insertarlos en su ranura, en los modelos USB hay que conectar el cable en el puerto USB del equipo y en los modelos PCI o ISA hay que abrir el equipo e insertar la tarjeta en una de las ranuras disponibles.

En el caso de los adaptadores USB no hay ningún problema para conectarlos con el equipo encendido, pero, antes de conectarlos, conviene asegurarse de que el otro extremo del cable USB está conectado al adaptador de red.

La instalación de las tarjetas PCI o ISA requiere que se apague el equipo (incluso que se desenchufen los cables de la comente eléctrica), se abre el CPU y de acuerdo al tipo de tarjeta es el tipo de ranura que utilizaremos, una vez identificada se conecta la tarjeta y se sujeta firmemente a la mother board, esto es importante ya que si quedara mal conectada podría ocasionar un corto circuito en el dispositivo y causar daños.

Si el sistema operativo tiene dificultades para instalar automáticamente el nuevo dispositivo, se deberá recurrir al cd de instalación que el proveedor entrega en el paquete del dispositivo.

Los fabricantes sacan continuamente mejoras en firmware (es un código que se graba en las unidades de hardware de la tarjeta), de sus equipos, de sus controladores y sus aplicaciones de utilidad. A través del firmware el fabricante logra actualizar las características del hardware sin cambiar el chip.

Hay que tomar en cuenta que el firmware y el controlador deben trabajar juntos, por lo tanto si se consigue una nueva versión de uno, seguramente se deberá instalar la nueva versión del otro.

II.1.3 Antenas

Todos los dispositivos inalámbricos, tanto puntos de acceso como los adaptadores de red, ya incorporan su antena propia, en muchas ocasiones es necesario ampliar el tamaño de la red para ofrecer una mayor cobertura.

Una forma de clasificar a las antenas es de acuerdo a su radiación, como omnidireccionales o direccionales; las primeras se utilizan para conexiones punto a multipunto y las segundas en conexiones direccionales.

Dentro de las antenas omnidireccionales y direccionales, pueden encontrarse otros tipos:

- **Antena de sector***:* Direccionales que se utilizan en conexiones punto-punto. Se consigue mejorar la ganancia de las omnidireccionales. En la imagen II.1.3.1podemos observar un ejemplo de antena de sector

Imagen II.1.3.1 Antena de sector

- **Antena de panel:** Con este tipo de antenas se consiguen conexiones punto-punto con una ganancia comparable a las antenas de sector. En la imagen II.1.3.2 podemos observar un ejemplo de antena de panel.

Imagen II.1.3.2 Antena de panel

- **Antena parabólica:** Estas antenas tienen una ganancia muy elevada y son las más potentes en el mercado. En la imagen II.1.3.3 podemos observar un ejemplo de antena de parabólica.

Imagen II.1.3.3 parabólica

- **Antena yagui**: Son bidireccionales con forma de tubo y una buena ganancia. En la imagen II.1.3.4 podemos observar un ejemplo de antena de sector.

Imagen II.1.3.4 antena de sector

- **Antena omnidireccional***:* son antenas que tienen poca potencia, por lo que están indicadas para usarse cuando se requiere comunicar dispositivos cercanos.

Una antena otorga al sistema inalámbrico tres propiedades fundamentales:

- Ganancia: Es el aumento de la potencia
- Dirección: Es la forma del patrón de transmisión
- Polarización: Es la orientación física del elemento de la antena que realmente emite la energía RF.

II.1.4 Bridges

Un *bridge* (puente) que podemos observar en la imagen II.1.4.1 en la es un dispositivo que interconecta dos redes. Una vez interconectadas, los equipos de una red pueden ver y comunicarse con los equipos de la otra como si todos formaran parte de la misma red. La mayoría de los puntos de acceso hacen las funciones de *bridges* al poder interconectar una red local cableada con la red inalámbrica.

Imagen II.1.4.1 Puente inalámbrico

Existe un equipo conocido como *bridge* inalámbrico *(Wireless Bridge)* que es algo distinto a un punto de acceso. Un *bridge* inalámbrico interconecta dos redes remotas (cableadas o no) mediante una conexión inalámbrica punto a punto. Estas dos redes pueden ser interconectadas también mediante cable, pero los *bridges* inalámbricos evitan la necesidad de tener que instalar o alquilar el cable. La solución inalámbrica requiere de dos equipos *bridges,* uno en cada extremo.

Los puentes conectan sitios difíciles de cablear por ejemplo, sucursales, los edificios de un campus o de un parque empresarial, redes temporales y almacenes. Se pueden configurar para aplicaciones punto a punto o punto multipunto.

Una implantación de puente típica utiliza el mismo tipo y marca de un puente en cada ubicación. Es así porque los dispositivos puentes que proporcionan enlaces que exceden de 1,6 kilómetros deben modificarla trama inalámbrica para soportar el retardo de un tiempo generado por unas distancias mayores.

II.1.5 Repetidores inalámbricos

En entornos donde es necesario ampliar la cobertura y no se puede usar otro dispositivo, se puede utilizar un repetidor inalámbrico que podemos observar en la imagen II.1.5.1, que no es más que un AP que no está conectado al backbone cableado.

Imagen II.1.5.1 Repetidor inalámbrico

Esta configuración requiere un 50% de superposición del AP en el backbone y el repetidor inalámbrico.

Se pueden configurar cadenas de varios puntos de acceso repetidores, pero el rendimiento de los dispositivos clientes al final de la cadena será bastante bajo, ya que cada repetidor recibe y emite los paquetes de información por el mismo canal, al añadir un repetidor el rendimiento se reduce a la mitad. Por lo que no es recomendable recurrir a más de dos saltos.

Al configurar los puntos de acceso de repetición hay que tomar los siguientes pasos:

- Utilizar repetidores donde no se requiere alto rendimiento, ya que estos dispositivos amplían la cobertura pero reducen drásticamente el rendimiento.

- Tratar de tener conectados dispositivos compatibles con los repetidores, ya que de lo contrario puede ocasionar problemas.

- Se pueden utilizar en coberturas temporales fuera y dentro de la red.

II.1.6 Switch

El switch que podemos observar en la imagen II.1.6.1, es un dispositivo de red que opera en la capa 2 del modelo OSI, es decir, pertenece a la capa de enlace de datos; es un dispositivo de interconexión de redes de computadoras. Este interconecta dos o más segmentos de red, pasando datos de una red a otra, de acuerdo a la dirección MAC destino de los datagramas en la red y un switch no difunde tramas por todos los puertos, sino que las retransmite sólo por los puertos necesarios.

Fig. II.1.6.1 Switch

I.2 Instalación de una WLAN

Para instalar nuestra red inalámbrica necesitamos tomar en cuenta algunos aspectos importantes. Para esto, se establecerán parámetros como: alcance de los equipos y causas de posibles limitaciones de estos, áreas de cobertura de la red, ubicación de la instalación, espaciado entre los AP, interferencia y coexistencia con otras redes, seguridad de la red, ancho de banda requerido por las aplicaciones y velocidad de transmisión, y número de usuarios a servir, además de una eficiente administración, calidad de servicio en las aplicaciones que lo requieran. Con el fin de instalar correctamente la red cuando sea implementada para tener un acceso inalámbrico consistente y fiable.

Un sitio Web, puede emitir contenidos de muchos formatos, tales como documentos HTML, imágenes, sonidos y videos. El tamaño del contenido, la estructura y los enlaces que contiene, inciden en el rendimiento. Cuando se realiza el diseño de una red inalámbrica es importante conocer la cantidad de usuarios que utilizarán los servicios que se brindarán a través de la red, para estimar la capacidad. En Ethernet, la planeación de capacidad es un valor absoluto.

Por otro lado en Wi-Fi la cantidad de usuarios puede variar enormemente en la medida que estos entren y salgan del área de cobertura, por lo tanto la planeación de la capacidad para las WLAN está representada por una aproximación. Debido a las diferencias en la configuración, colocación y entorno físico de los componentes, cada infraestructura es una instalación única. Antes de instalar el sistema, debe realizarse una inspección del emplazamiento para determinar la mejor ubicación para los puntos de acceso en la red inalámbrica y maximizar el alcance, la cobertura y el rendimiento de la infraestructura.

A continuación se describe algunas condiciones operativas y ambientales que se debe tener en consideración. Velocidades de transmisión de datos. La sensibilidad y el alcance son inversamente proporcionales a las velocidades de transmisión de datos (bits). El alcance de radio máximo se consigue con la velocidad más baja que sea factible. A medida que aumenta la velocidad, el receptor requiere un nivel de señal más fuerte.

- Tipo de antena y ubicación. Un factor importante para maximizar el alcance de la radio es la configuración correcta de la antena, teniendo en cuenta que el alcance de la antena aumenta en proporción a la altura de la misma.

- Entornos Físicos. Las áreas despejadas o abiertas proporcionan un mejor alcance de la radio que las áreas cerradas.

- Obstáculos. Una obstrucción física, puede disminuir el rendimiento del adaptador inalámbrico del cliente.

Una vez tomadas estos factores en consideración, procederemos a identificar que dispositivos usaremos tanto, en equipos pc´s como en dispositivos como router o switch, para la implementación de nuestra red.

En el mercado existe una gran variedad de equipos Wi-Fi que ofrecen diversas características y presentaciones de acuerdo a las necesidades. Los precios de estos equipos, varían dependiendo de las características y marcas.

II.3 Configuración de una WLAN

La utilidad de las redes inalámbricas en el hogar y las pequeñas empresas ofrece ventajas evidentes. Con una red inalámbrica no es necesario instalar cables para conectar los distintos equipos entre sí y los equipos portátiles pueden trasladarse de un lado a otro de la casa o la pequeña oficina y mantener su conexión a la red.

Las redes inalámbricas, tanto si funcionan en modo de infraestructura como en modo ad hoc, utilizan un nombre que se denomina identificador del conjunto de servicios (SSID) para identificar una red inalámbrica específica. Cuando los clientes inalámbricos se inician por primera vez, exploran la banda de frecuencias inalámbricas en busca de tramas de señalización especiales que envían los puntos de acceso inalámbricos o los clientes inalámbricos en modo ad hoc. Las tramas de señalización contienen el SSID, también denominado nombre de red inalámbrica. En la lista acumulada de nombres de red inalámbrica recopilados durante el proceso de exploración, el cliente inalámbrico puede determinar la red inalámbrica con la que se intentará establecer conexión. Uno de los elementos de la configuración de una red inalámbrica es seleccionar un nombre para la red inalámbrica. Si va a crear una nueva red inalámbrica, el nombre que elija debe ser distinto de los nombres de las demás redes dentro del intervalo de exploración.

II.3.1 Red AD-Hoc

Como las redes ad hoc no disponen de puntos de acceso, la red estará formada por aquellos equipos que se pretenden interconectar. Estos equipos deben situarse a poca distancia unos de otros para no tener problemas con la calidad de la señal. En cualquier caso, esta distancia dependerá del tipo de adaptador de red que tengan los diferentes equipos.

El procedimiento de configuración consiste en elegir uno de los equipos y configurarle manualmente los parámetros Wi-Fi. A continuación se abre la aplicación Wi-Fi en cada uno de los restantes equipos, se le indica que explore las redes existentes, se selecciona la red ad hoc configurada en el primer equipo y se hace clic sobre el botón Conectar, si se desea, también se puede repetir en cada equipo la configuración realizada en el primero. El resultado debe ser el mismo.

Para configurar los parámetros Wi-Fi de la tarjeta de red es necesario ejecutar el programa de utilidades Wi-Fi que viene incluido en el CD del fabricante o utilizar la herramienta Wi-Fi que incluye el sistema operativo. Cada uno de estos programas tiene su propia estética y su manejo puede variar. Estas diferencias también afectan a la terminología empleada.

Para acceder a la aplicación Wi-Fi con Windows XP se debe hacer clic en *Inicio, Configuración, Panel de control.* A continuación, se hace clic sobre *Conexiones de red y,* con el botón derecho del ratón, se hace clic sobre *Conexión de red inalámbrica.* Se elige la opción *Propiedades* y se selecciona la ficha *Redes inalámbricas.* Aquí Windows mostrará una lista de todas las redes inalámbricas del entorno que ha podido detectar de forma automática. Si no se encuentra la red buscada se puede hacer clic en el botón *Actualizar.* Si se trata de una red nueva que todavía no está en funcionamiento, deberemos hacer clic en el botón *Agregar.* Antes hay que asegurarse de que está señalada la opción *Usar Windows para establecer mi configuración de red inalámbrica.* En la nueva pantalla se deben introducir los parámetros Wi-Fi y asegurarse de marcar la opción *Ésta es una red de equipo a equipo.*

Los parámetros Wi-Fi a configurar son los siguientes:

- **Tipo de red.** Se refiere a si la red va a ser de tipo *ad hoc* o con punto de acceso. En este caso se elige la primera opción. Esta opción puede estar indicada con cualquiera de los siguientes nombres: *ad hoc, peer-to-peer,* IBSS, igual a igual, independiente, equipo a equipo o término similar.

- **Nombre de red.** La red debe tener un nombre. Se puede elegir cualquier nombre, siempre que no esté siendo utilizado por otra red del entorno. Al parámetro nombre de red también se le conoce como *Network Name* 'Nombre de red' o *SSID (Service Set Identifier,* 'Identificador del conjunto de servicios').

- **Canal.** Los equipos Wi-Fi disponen de distintos canales de radio por los que comunicarse. Estos canales están identificados por un número. Se puede elegir cualquiera de ellos.

- **Seguridad.** Con las redes Wi-Fi se pueden configurar ciertas características de seguridad. Lo cierto es que no hay mucho dónde elegir, pero es importante habilitar el cifrado de paquetes WEP o WPA y elegir una clave que no resulte demasiado evidente.

En las redes Wi-Fi *ad hoc* todos los equipos son iguales (de ahí su otro nombre *peer-to-peer).* No hay PC principal ni secundario, cualquier equipo puede apagarse o desconectarse que, mientras haya dos PC conectadas, seguirá existiendo la red.

El parámetro que identifica a la red es el nombre de red o SSID, mientras que el que identifica a cada PC que forma parte de la red se conoce como BSSID *(Basic Service Set Identifier,* 'Identificador básico del conjunto de servicios'). Este identificador se genera de forma automática y aleatoria.

Si se establece una conexión entre varias computadoras, es porque se tiene la intención de compartir recursos: carpetas, impresoras, unidades de disco, etc. Por defecto, ninguno de estos recursos está compartido, por lo que explícitamente se debe indicar lo que se desea compartir y cómo se desea compartir.

Para compartir un recurso, simplemente se debe abrir el *Explorador de Windows,* buscar el recurso a compartir (el archivo, la carpeta, etc.) y hacer clic sobre él con el botón derecho del ratón (bueno, con el botón secundario). Aparecerá una lista de opciones donde podremos ver una con el nombre *Compartir.* Haciendo clic sobre esta opción, veremos una ventana con todas las opciones de compartición.

Probar la conexión

Para saber si una conexión Wi-Fi está funcionando adecuadamente después de haberla configurado, simplemente hay que ir a uno de las PC, abrir el *Explorador de Windows y* comprobar si se pueden ver los recursos que se han compartido en otros equipos.

Qué hacer en caso de problemas

Lo primero es comprobar lo evidente:

- Ver si el equipo remoto está encendido.
- Ver si alguno de los equipos no tiene conectada la tarjeta o dispositivo Wi-Fi.
- Asegurarse de que el equipo al que se pretende acceder está configurado correctamente.

Si el fallo no es tan evidente, podemos probar otras causas:

- Sitúe los equipos más cerca uno de otro evitando que haya obstáculos entre ellos. Una vez establecida la conexión en estas condiciones, se podrán ir separando los equipos hasta situarlos en la localización deseada.

- Comprobar las luces de la unidad Wi-Fi para comprobar si se están portando como indican las instrucciones. Quizás esto nos dé una pista sobre lo qué está funcionando mal.

- Apague y encienda ambas PC. Algunas veces los propios registros de Windows o de los controladores no funcionan adecuadamente inmediatamente después de ser instalados y necesitan que se reinicie el equipo.

- Comprobar que el *software* de utilidad que venía con la unidad Wi-Fi está instalado y funcionando correctamente.

- Desconecte y vuelva a conectar su unidad Wi-Fi. Esto hará que se reinicie esta unidad. A veces es necesario este tipo de reinicio aunque la unidad haya estado funcionando bien durante mucho tiempo.

- Compruebe que los siguientes datos son los mismos en ambas computadoras: el tipo de red debe estar fijado a *ad hoc* (o a cualquiera de

los otros nombres de esta modalidad), se tiene el mismo nombre de grupo de trabajo (deben coincidir incluso mayúsculas y minúsculas), se tiene el mismo número de canal y se tienen fijados los mismos parámetros de seguridad.

- Comprobar que el nombre de cada PC es diferente y que no coincida con el grupo de trabajo.

- Comprobar que las direcciones TCP/IP son distintas en ambos equipos.

- Comprobar que las unidades Wi-Fi están instaladas correctamente en el equipo. Se puede comprobar esto haciendo clic con botón derecho del ratón sobre "mi pc", luego "propiedades", gestor de dispositivos y comprobar que la unidad Wi-Fi se encuentra en la lista de de hardware conectado al equipo y que no tiene signo de exclamación sobre él.

II.3.2 Red con un Punto de Acceso

Punto de Acceso. Un punto de acceso es un dispositivo que funciona en las redes inalámbricas Wi-Fi como si fuera una estación base central que sirve de intermediario de todas las comunicaciones entre las PC de la red. Los puntos de acceso permiten interconectar la red inalámbrica con una red local cableada e internet como se muestra en la imagen II.3.2.1. Los AP disponen de equipos de radio y antena para comunicarse con sus PC inalámbricos y de puertos Ethernet 10/100BaseT (Rj45) para comunicarse con la red cableada.

En la figura II.3.2.1 se puede observar una red con un punto de acceso y conectada a una red Ethernet y a internet. Cada AP dispone de un área de cobertura, esta es la zona dentro de la cual un equipo puede comunicarse con el AP de forma inalámbrica, el tamaño depende de distintos factores como son:

- Localización del punto de acceso
- Obstáculos entre el punto de acceso y el equipo de cómputo.
- Interferencias radioeléctricas
- Tipos de antenas utilizadas

Si se sitúan distintos puntos de acceso complementando sus coberturas, se puede llegar a crear una red local inalámbrica con un área de servicio tan extensa como se desee.

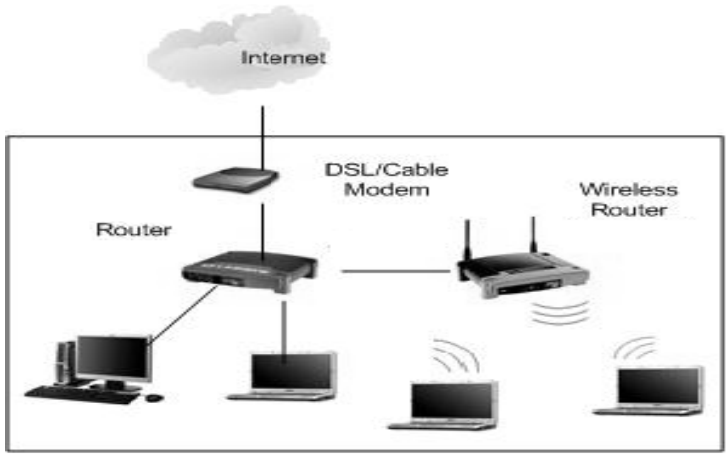

Imagen II.3.2.1 Red infraestructura conectada a LAN

Donde colocar los puntos de acceso

Si pretendemos cubrir una pequeña área como puede ser una casa o una pequeña oficina lo más probable es que se deba utilizar un solo AP, en el lugar más céntrico y alto del lugar.

La colocación de los AP viene dado principalmente por el lugar en donde este el acceso ADSL, modem cable, etc. Y también se toma en cuenta la base técnica y artística, esto debido a que hay muchos factores que afectan la propagación de las ondas electromagnéticas, sin embargo ya que generalmente no se puede realizar estudios sobre este factor, suele basarse en el método de prueba y error.

En todo caso, se debe tener muy claro el área que se quiere cubrir y cuantos usuarios simultáneos habrá en dicha área. Se tiene que tomar en cuenta la cobertura y la coexistencia.

Configuración del punto de acceso

Una vez que se dispone del punto de acceso, es conveniente proceder a su configuración. La mayoría de los fabricantes ya facilitan el punto de acceso con una configuración por defecto, para comprobar que todo funciona, desde el punto de vista de la seguridad es muy importante configurar valores propios, sobre todo, en los parámetros de seguridad (claves WEP/WPA/WPA2 y nombre de usuario y claves para acceder a las opciones de configuración).Hay que tomar en cuenta que los valores por defecto pueden obtenerse vía internet para todos los modelos de PA.

En los puntos de acceso hay que configurar dos conjuntos de parámetros:

Aquellos que gestionan la red inalámbrica (*Wireless setting, AP setting* o similar) y aquellos otros que permiten establecer la conexión con la red cableada o Internet *(Internet setting, IP setting, network setting* o similar).

La forma de configurar las propiedades propias del punto de acceso depende de cada fabricante o, incluso, del modelo del equipo.

La configuración de un punto de acceso consta de dos pasos:

1. Conectar un equipo con el punto de acceso. Para acceder al menú de configuración hay que realizar algunas configuraciones previas en la computadora.

2. Configurar los distintos parámetros. Una vez conectados con el punto de acceso bastará moverse por los distintos menús y opciones para dar con los parámetros a configurar.

Acceder a la configuración

Para configurar un punto de acceso es acceder a sus opciones de configuración. Esto puede llevarse a cabo de las siguientes formas:

- Utilizar un **cable USB** o cable específico.

- Utilizar un **cable de red Ethernet** (10/100 BaseT). Los puntos de acceso suelen incluir uno o más puertos RJ45 para conectar computadoras de forma cableada. Este equipo forma parte de la red de la misma forma que aquellos otros que se conectan de forma inalámbrica.

  Lo importante en este caso es configurar el equipo para que obtenga las direcciones IP de forma automática.

A continuación, sólo hay que abrir el explorador de Internet (Internet Explorer, Netscape o Firefox, por ejemplo) e introducir el número IP del punto de acceso en la barra de direcciones. Este número vendrá indicado en el manual de usuario y suele ser de la forma 192.168.1.1.

- Utilizar un **acceso inalámbrico.** Una vez encendido el punto de acceso, se exploran desde la PC las redes Wi-Fi disponibles y se selecciona la del punto de acceso a configurar. El nombre de la red del punto de acceso (SSID), así como los parámetros de acceso (código WEP/WPA/WPA) vendrán indicados en el manual de usuario. No obstante, el nombre SSID estará relacionado con el fabricante, marca o modelo del punto de acceso. La clave WEP/WPA/WPA2 puede venir en el manual del equipo o en el manual de usuario. Una vez conectados, al igual que con la conexión por cable Ethernet, habrá que abrir el navegador de Internet e introducir el número IP del punto de acceso.

- Utilizar un **acceso remoto.** Si el punto de acceso está activo y conectado a Internet, existe la posibilidad de acceder a él desde cualquier PC conectado Internet. Para ello será necesario que se pueda acceder a él desde el exterior sin que un *firewall* o *router* intermedio bloquee las comunicaciones entrantes. Por otro lado, este tipo de acceso remoto debe estar específicamente permitido en el punto de acceso, de lo contrario, sólo admitirá los accesos locales.

Si el punto de acceso ha sido configurado anteriormente, lo más probable es que no conserve los valores por defecto. Si tenemos el acceso a la información se utiliza, en caso contrario se puede utilizar el botón que restablece los valores de configuración de fábrica que suelen traer estos dispositivos.

Generalmente, los puntos de acceso no sólo disponen de la funcionalidad de interconectar los equipos inalámbricos de los usuarios, sino que también incluyen otras funciones como las de *router, switch* o módem.

Las propiedades principales propias de la función de punto de acceso son las siguientes:

- **Nombre de red** *(Network name).* Al nombre de red se le conoce también como *SSID (Service Set Identifier,* 'Identificador del conjunto de servicios'). Los puntos de acceso suelen incluir un nombre de red por defecto.
  Es recomendable sustituir este nombre por cualquier otro que se considere adecuado.

Este nombre de red debe ser el que se configure en cada PC. Es importante recordar que en los nombres de red se diferencian las letras mayúsculas de las minúsculas.

- **Canal** *(Channel).* Aquí se deberá introducir el número de canal que se considere apropiado. El sistema permite elegir cualquier canal, o bien que esta asignación se haga de forma automática o dinámica. Una opción antes de decidirse por un número concreto de canal es explorar las redes de la zona y elegir un número de canal que no esté siendo utilizado.

- **Seguridad** *(Security).* Los equipos Wi-Fi disponen de determinadas características de seguridad para cifrar el intercambio de información con los equipos de los usuarios. Los parámetros de seguridad que se establezcan aquí deben ser configurados posteriormente en cada equipo de usuario. Establecer los parámetros de seguridad consiste en elegir el tipo de cifrado deseado: WEP 64, WEP 128 o WPA/WPA2 e introducir la clave de cifrado. En cuanto a la clave de cifrado, existen distintos procedimientos para introducirla:

Adicionalmente, los puntos de acceso ofrecen distintas características que ayudan a gestionar la red. Algunas de estas características son las siguientes:

- **Bajada automática de velocidad** *(Auto rate fall back).* Esta característica permite que, cuando empeoren las condiciones de difusión de la señal radioeléctrica, el sistema pueda bajar la velocidad de transmisión para mantener la comunicación abierta.

- **Filtro MAC o selección de los equipos autorizados** *(Authorised MAC address).* Algunos puntos de acceso incluyen la facilidad adicional de incluir una lista de los equipos autorizados (lista de direcciones MAC) a conectarse al punto de acceso. Las direcciones MAC son unos números únicos que los fabricantes asignan a cada dispositivo inalámbrico. Este número identifica al dispositivo de forma inequívoca. Las direcciones MAC están formadas por 12 caracteres alfanuméricos (por ejemplo, 12-AB-56-78-90-FE).

- **Emitir el nombre de red** *(Broadcast SSID to associate).* Los puntos de acceso emiten generalmente su nombre de red (SSID) para permitirles a los posibles usuarios que puedan asociarse a la red con facilidad. No obstante, si se desea "aumentar" la seguridad de la red, puede deshabilitarse

- **Clave de acceso** *(Password).* El punto de acceso dispone de una clave para impedir el acceso a sus funciones de configuración.

- **Habilitar la red inalámbrica** *(Enable Wireless Networking).* Algunos equipos permiten que su función de punto de acceso pueda ser habilitada o deshabilitada. Esto es útil, fundamentalmente, cuando el punto de acceso dispone también de las funciones de *router* o *switch.* En algún caso podría ser interesante mantener sus funciones *de router y* deshabilitar sus funciones de punto de acceso.

- **Servidor DHCP.** Los puntos de acceso suelen tener habilitado el servidor DHCP para asignar automáticamente las direcciones IP a los equipos que se conectan. No obstante, este servicio puede deshabilitarse si se cree conveniente.

- **Potencia de transmisión.** (transmit power).Algunos puntos de acceso permiten que les configure la potencia de transmisión. Esto tiene la ventaja de que si con poca potencia cubrimos el área deseada, para que extender el área de cobertura emitiendo más potencia. Esto aumenta el riesgo de intrusión y el consumo de electricidad.

- **Registro de actividad** *(Log file).* Algunos puntos de acceso ofrecen la posibilidad de guardar un registro de actividad. En este registro se guarda, fundamentalmente, los accesos de los distintos usuarios, lo que es de utilidad para comprobar la actividad de la red y detectar posibles intrusos.

Conexión con la red local cableada

Cuando se desea conectar un punto de acceso a una red local cableada (o a Internet), los parámetros que hay que configurarle son los mismos que los que se le configuran a cualquier otro equipo de la red cableada. Quiere esto decir que el punto de acceso será un equipo más de la red cableada. El punto de acceso tendrá dos números IP (y máscaras de subred), uno que lo identifica dentro de la red inalámbrica y otro que lo identifica dentro de la red cableada.

Los puntos de acceso incluyen entre sus opciones de configuración todos los parámetros necesarios que le permiten conectarse a una red cableada (o Internet). Existen dos posibilidades: que estos parámetros se obtengan automáticamente del *switch (router)* de la red o introducir estos valores manualmente.

En el primer caso bastará con seleccionar la opción *Obtener una dirección IP automáticamente* o similar. Si las opciones le "parecen en inglés, el equivalente sería *Obtain an IP automatically* o similar.

Manualmente, los parámetros a configurar son los siguientes:

Dirección IP *(IP Address).* Es la dirección IP del punto de acceso como componente de la red local cableada o la que el proveedor de acceso a Internet ha facilitado.

Máscara de subred *(Subnet Mask).* Es la máscara de la red local cableada o la que facilite el proveedor de acceso a Internet. Un número de máscara muy común es el 255.255.255.0.

Puerta de enlace *(Gateway).* Es el número IP del equipo al que el punto de acceso tiene que enviarle los datos con destino a Internet o red local cableada.

Servidor DNS *(DNS Server).* Son las direcciones IP de los DNS (servidor de nombres de dominio). Este dato lo facilita el proveedor de acceso a Internet. Las direcciones IP de los dos servidores DNS (principal y secundario) pueden configurarse en cada equipo de la red inalámbrica, en el *router* inalámbrico (punto de acceso) o en el *router* de acceso a Internet (módem *router* ADSL o cable).

Cualquier PC que se desee conectar de forma inalámbrica a una red con puntos de acceso necesita disponer de un adaptador de red (tarjeta Wi-Fi) y configurarse adecuadamente para que el adaptador se entienda con el punto de acceso de la red deseada. Si el punto de acceso ya está instalado y funcionando, la forma más simple de configurar el equipo del usuario es buscar la opción de exploración de redes existentes, localizar el nombre del punto de acceso en cuestión, seleccionarlo y hacer clic sobre el botón Conectar. El punto de acceso dispone de una configuración particular que no admite este tipo de conexión automática.

Hay que realizar una configuración manual del adaptador de red:

- Configurar los parámetros Wi-Fi. Esta configuración hace posible que se pueda establecer una conexión entre el equipo del usuario y el punto de acceso.

- Configurar el protocolo TCP/IP. Esta configuración hace posible que el equipo se pueda comunicar con el resto de equipos de la red inalámbrica e Internet.

Cualquier PC con un adaptador Wi-Fi que tenga configurados correctamente los parámetros anteriores y que esté dentro del área de cobertura radioeléctrica de cualquier punto de acceso de la red formará parte de ella y, por tanto, podrá compartir sus recursos y tener acceso a los recursos (configurados como compartidos) del resto de equipos.

Configurar los parámetros Wi-Fi

En caso de ser necesario configurar los parámetros Wi-Fi de forma manual, éstos se configuran con la aplicación que viene en el CD incluido con el equipo adaptador de red o con la herramienta Wi-Fi del propio sistema operativo. Una de las medidas de seguridad que se puede activar en un punto de acceso es que no emita su SSID (siempre como complemento de otras). Por lo que la única manera de establecer la conexión es introduciendo los parámetros a mano.

Los parámetros a configurar son los siguientes:

Tipo de red. En este caso, el tipo de red que hay que configurar es el modo infraestructura, BSS o con puntos de acceso.

- **Nombre de red.**
- **Canal.**
- **Seguridad.**

Que ya se han mencionado anteriormente.

Configurar el protocolo TCP/IP

Estos datos le permiten la computadora formar parte de la red IP de Wi-Fi. Aunque esta configuración puede hacerse de forma manual, suele ser más habitual que estos valores los tome automáticamente del punto de acceso. Para ello, el punto de acceso debe estar configurado para ofrecer automáticamente esta información (DHCP habilitado). En el lado del equipo sólo hay que indicar que obtenga las direcciones IP de forma automática.

La forma de configurar la PC para obtener las direcciones IP de forma automática depende del sistema operativo de que se dispone.

Con **Windows 2000/Me** haremos clic con el botón derecho sobre el icono Mis sitios de red, seleccionamos la opción Propiedades, en el botón Propiedades, la lista de componentes marcamos el componente Protocolo Internet (TCP/IP) y presionamos el botón Propiedades. Marcamos la opción Obtener la dirección IP automáticamente. Hay que verificar también que está marcada la opción Obtener la dirección del servidor DNS automáticamente.

Con Windows NT pulsamos Inicio; elegimos Configuración y después la opción Panel de control. Paso seguido localizamos el icono Red y hacer doble clic sobre él, aquí en la ventana Red debemos seleccionar la ficha de protocolos. En la lista de protocolos de red debe aparecer Protocolo TCP/IP, seleccionamos propiedades. Nos aparecerá una nueva ventana donde seleccionamos la ficha Dirección IP. Marcamos la opción Obtener la dirección IP de un servidor DHCP. Para terminar, cierre todas las ventanas pulsando Aceptar.

Con Windows XP hay que hacer clic en *Inicio, Configuración, Conexiones de red.* A continuación se hace clic con el botón derecho sobre *Conexión de área local* y se elige *Propiedades.* También se puede llegar aquí eligiendo *Cambiar la configuración de esta conexión* en la ficha *Tareas de red.* Se continúa haciendo clic sobre *Protocolo Internet (TCP/IP)* y, luego, sobre el botón *Propiedades.* Se marca la opción *Obtener una dirección IP automáticamente.* Hay que verificar también que está marcada la opción *Obtener la dirección del servidor DNS automáticamente.* Para terminar, cierre todas las ventanas pulsando *Aceptar.*

Si el punto de acceso no está configurado para ofrecer los datos de configuración de forma automática, no habrá más remedio que configurar estos datos en la PC de forma manual. Los datos a configurar son los siguientes:

- **Número IP de la PC.** Cualquier número, siempre que esté dentro del rango de numeración de la red local inalámbrica. Eso sí, cada PC debe disponer de un número IP distinto.

- **Máscara de subred.** Generalmente, se suele utilizar como máscara de subred el número 255.255.255.0. Este número es válido para redes que dispongan de menos de 255 terminales.
- **Puerta de enlace.** Aquí habría que indicar el número IP del punto de acceso.
- **DNS.** En este caso tenemos dos opciones: o se configura para que los tome automáticamente del punto de acceso o se introducen los números IP de los DNS primario y secundario. Aunque el punto de acceso pueda asignar estos números, el usuario podría preferir introducir sus propios DNS.

Estas propiedades se configuran en las propiedades de la tarjeta de red. Con Windows XP habría que hacer clic en *Inicio, Configuración, Conexiones de red,* botón derecho sobre *Conexión de área local* y elegir *Propiedades.* Clic sobre *Protocolo Internet (TCP/IP) y Propiedades.*

Conexión a Internet se puede comprobar si se tiene conexión con otros equipos de la red.

Antes de comprobar el acceso a Internet hay que asegurarse de haber configurado el protocolo TCP/IP en la PC.

Para comprobar la conexión con otros equipos de la red, con Windows se lleva a cabo abriendo *Explorador de Windows* desde uno de los equipos y buscando los recursos compartidos de otros. Es posible que para hacer esto se tenga que hacer clic sobre la opción *Entorno de red, Toda la red y* sobre el grupo de trabajo que haya definido. Si la PC remota tiene definido un nombre de usuario y clave de acceso para acceder a sus recursos, se tendrá que introducir.

Si se conoce el número IP del punto de acceso, se puede comprobar que una computadora está en comunicación con el punto de acceso abriendo un navegador de Internet (Internet Explorer, por ejemplo) e introduciendo este número como dirección. Si se obtiene cualquier respuesta distinta de *página no encontrada,* es que funciona la conexión. Incluso, todavía sería más fiable la utilización del comando *ping* o *tracert.*

Abra una ventana del DOS desde Windows y teclee *ping* seguido del número IP del punto de acceso (por ejemplo, *ping 192.168.1.1);* si aparece una línea que empieza por *reply from,* es que la conexión funciona. Si la línea empieza por *Request timed out,* es que no funciona.

La velocidad máxima a la que transmite una red inalámbrica es de 11 ó 54 Mbps. Independientemente de que esta velocidad puede ser menor dependiendo de la distancia entre emisor y receptor.

De las condiciones del entorno o de si los equipos se encuentran en el interior de un edificio o en el exterior en espacio abierto, lo cierto es que dicha velocidad se refiere exclusivamente a la conexión entre los equipos inalámbricos de los usuarios y el punto de acceso correspondiente. Adicionalmente, el punto de acceso puede disponer de una conexión con Internet con una velocidad diferente.

La velocidad real de una comunicación entre un usuario de una red inalámbrica y un servidor situado en Internet depende de muchos factores, entre los que se encuentran los siguientes:

- Velocidad efectiva de la conexión inalámbrica.
- Conexión del punto de acceso con el módem *router* ADSL o cable.
- Ancho de banda de la conexión ADSL o cable.
- Dimensionado de la infraestructura del proveedor de acceso.
- Rendimiento de Internet en ese momento.
- Ancho de banda de la conexión del servidor con internet.
- Hardware del servidor donde esté situado el servicio de Internet utilizado.
- Número de usuarios simultáneos que tenga el servidor en ese momento.
- Número de usuarios simultáneos que tenga el servidor en ese momento.

Si después de hacer todo el trabajo de instalación y configuración no es posible ver los recursos compartidos por el resto de los equipos.

Lo primero que hay que hacer es comprobar lo evidente: comprobar que todos los dispositivos están encendidos, que están bien conectados y funcionando. Si hubiese una antena exterior, se deberá comprobar que está conectada. Las tarjetas PCMCIA *(PC Card)* o unidades USB deben estar insertadas o conectadas al equipo. Se pueden mover estas conexiones para comprobar que están firmemente conectadas.

- Sitúe las computadoras más cerca del punto de acceso evitando que haya obstáculos en medio.

- Comprobar las luces de las unidades Wi-Fi (adaptadores de red y puntos de acceso) para comprobar si están funcionando como indican los manuales de usuario de los equipos.

- La mayoría del *hardware* (impresoras, equipos Wi-Fi, etc.) dispone de una utilidad que permite comprobar de forma local que dicho *hardware* está operativo.

- Apague y encienda ambas PC. Algunas veces los propios registros de Windows o de los controladores no funcionan adecuadamente inmediatamente después de ser instalados y necesitan que se reinicie el sistema.

- Comprobar que el *software* de utilidad que venía con la unidad Wi-Fi está instalado y funcionando correctamente.

- Desconecte y vuelva a conectar su unidad Wi-Fi. Esto hará que se reinicie esta unidad.

- Comprobar que los parámetros de la comunicación (tipo de red, SSID y canal) están configurados adecuadamente en ambos equipos.

- Comprobar que los parámetros de seguridad están configurados en los mismos valores en ambos equipos.

- Comprobar que el nombre de cada equipo es distinto al nombre del otro y que no coinciden con el nombre del grupo de trabajo.

- Comprobar que las direcciones TCP/IP son distintas en todos los equipos, o. bien, que están configurados para obtener las direcciones IP de forma automática.

- Comprobar que los adaptadores de red están instalados correctamente en el equipo.

- Si ninguna de las comprobaciones anteriores nos ha dado la solución, posiblemente estamos ante un fallo de hardware, y este, puede estar en el equipo de cómputo, el punto de acceso o en la tarjeta Wi-Fi.

II.4 Acceso a Internet

Las redes inalámbricas permiten que todos los dispositivos conectados a la red puedan compartir una única conexión a Internet. Esto no significa que todos los usuarios tengan que ver las mismas páginas Web. Cada usuario puede navegar por sus propias páginas, leer su correo o hacer cualquier otro uso de Internet. En la imagen II.4.1 se muestra una conexión común de una red con acceso a internet.

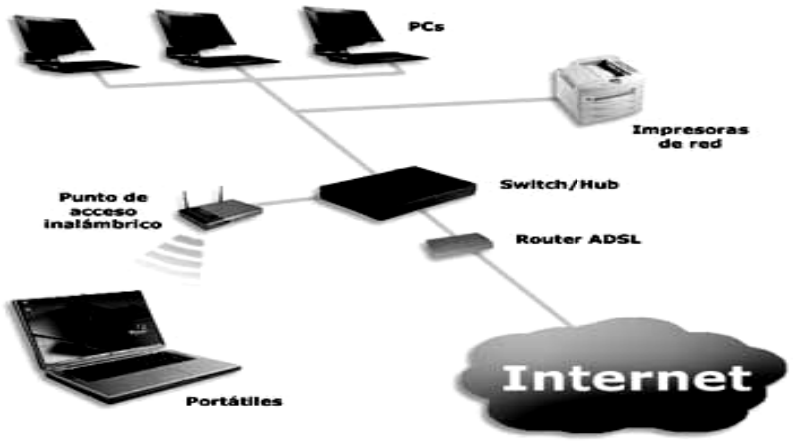

Imagen II.4.1 Red con acceso a internet

El ancho de banda de la conexión será compartido entre todos. Por tanto, es posible que en algunos momentos la conexión vaya algo más lenta de lo habitual. La inmensa mayoría de los modelos de punto de acceso ya tienen integrada la posibilidad de compartir una conexión a Internet (o a cualquier otra red). Es posible porque el punto de acceso tiene integrada la función de router. El router es un equipo que hace de intermediario entre dos redes (Wi-Fi e Internet).

Para compartir un acceso .a Internet, lo primero es disponer del acceso. Las empresas que facilitan los servicios de acceso a Internet se conocen con el nombre de proveedores de acceso (ISP, Internet Service Provider). Aunque existen puntos de acceso que permiten compartir una conexión a Internet de baja velocidad (56 Kbps), lo más recomendable es disponer de un acceso de banda ancha: ADSL, módem cable, satélite, WiMax, etc.

II.5 IMPLEMENTACIÓN DE LA RED EN LA SALA DE CÓMPUTO

En nuestra red inalámbrica se dispondrá de equipos finitos aunque sin dejar de lado la posibilidad de conectar nuevos clientes. Por lo tanto es necesario hacer una tabla de cantidades aproximadas de equipos (usuarios fijos) equipos (usuarios visitantes).

En el sentido de las aplicaciones que se utilizaran, son variadas y tomando en cuenta que se tiene un servicio contratado de ADSL a una velocidad de 2Mb, el ancho de banda que consumirá cada equipo es difícil de calcular, y no debemos olvidar que la velocidad de bajada y subida varia y esto sumado a que las conexiones inalámbricas tienen un límite de velocidad definido en los estándares que hemos visto anteriormente nos proporcionara una velocidad considerable en cada equipo, y en nuestro caso existirán equipos conectados a una red LAN cableada en la cual su velocidad variara de acuerdo a los dispositivos de conexión.

Para estimar el ancho de banda requerido, por la red inalámbrica, se debe analizar las aplicaciones (http, correo, chat, etc.), es difícil establecer el verdadero ancho de banda que ocuparían, ya que estas dependan exclusivamente de la calidad y cantidad de información que contiene la página.

A continuación en el cuadro II.5.1 se presentan los dispositivos que serán utilizados en nuestra Wlan:

Equipos Fijos	**Características**	**Aplicaciones utilizadas**
9 equipos de renta	Procesador Dual core 1gb de memoria RAM 80gb de disco duro Quemador dvd Tarjeta wireless pci	Email, www, chats,otros
1 equipo principal	Procesador Core 2 Duo. 3gb de memoria RAM 160 gb de disco duro Lector y quemador dvd. Tarjeta wireless pci Multilector de memorias.	Email, www, chats, control de tiempo de renta, impresiones, etc.

Multifuncional laser en negro hp M1319mfp	Fotocopia, digitalización, impresión, fax	
Multifuncional de inyección Epson stylus cx4700	Fotocopia, digitalización e impresión.	

El Router inalámbrico a 54Mbps TL-WR340G

Está diseñado para su uso en redes inalámbricas en las oficinas en casa o pequeñas oficinas (SOHO).

Integra un Punto de Acceso Inalámbrico, un conmutador incorporado de 4 puertos full-duplex a 10/100Mbps y el NAT-Router.
Permite que conecte su red, y que todos sus aparatos con cable o inalámbricos compartan una conexión a Internet por Cable o DSL a alta velocidad, o compartan archivos u otros recursos como impresoras y espacio de almacenamiento en disco duro.

Cumple con la IEEE 802.11g y IEEE802.11b Es compatible con todos los dispositivos IEEE 802.11g y IEEE 802.11b.

También cuenta con cortafuegos que incluye filtrado de direcciones IP, filtrado de direcciones MAC y filtrado de Nombre de Dominio, permitiéndole que administre con facilidad el acceso a Internet de otros usuarios.

Proporciona seguridad por encriptación de LAN inalámbrica WEP 64/128/152-bit y autenticación WPA/WPA2 y WPA-PSK/WPA2-PSK así como seguridad por encriptación TKIP/AES. También soporta transferencia VPN para una transmisión segura de datos confidenciales.

Modem 2wire		

Cuadro II.5.1 Dispositivos utilizados en la WLAN.

Ahora debemos observar y analizar la disposición de los equipos tanto los AP como los clientes que se conectaran al mismo, en nuestro caso dichos equipos estarán de la siguiente forma:

En la imagen II.5.1se muestra la disposición de los equipos y dispositivos utilizados en la Wlan.

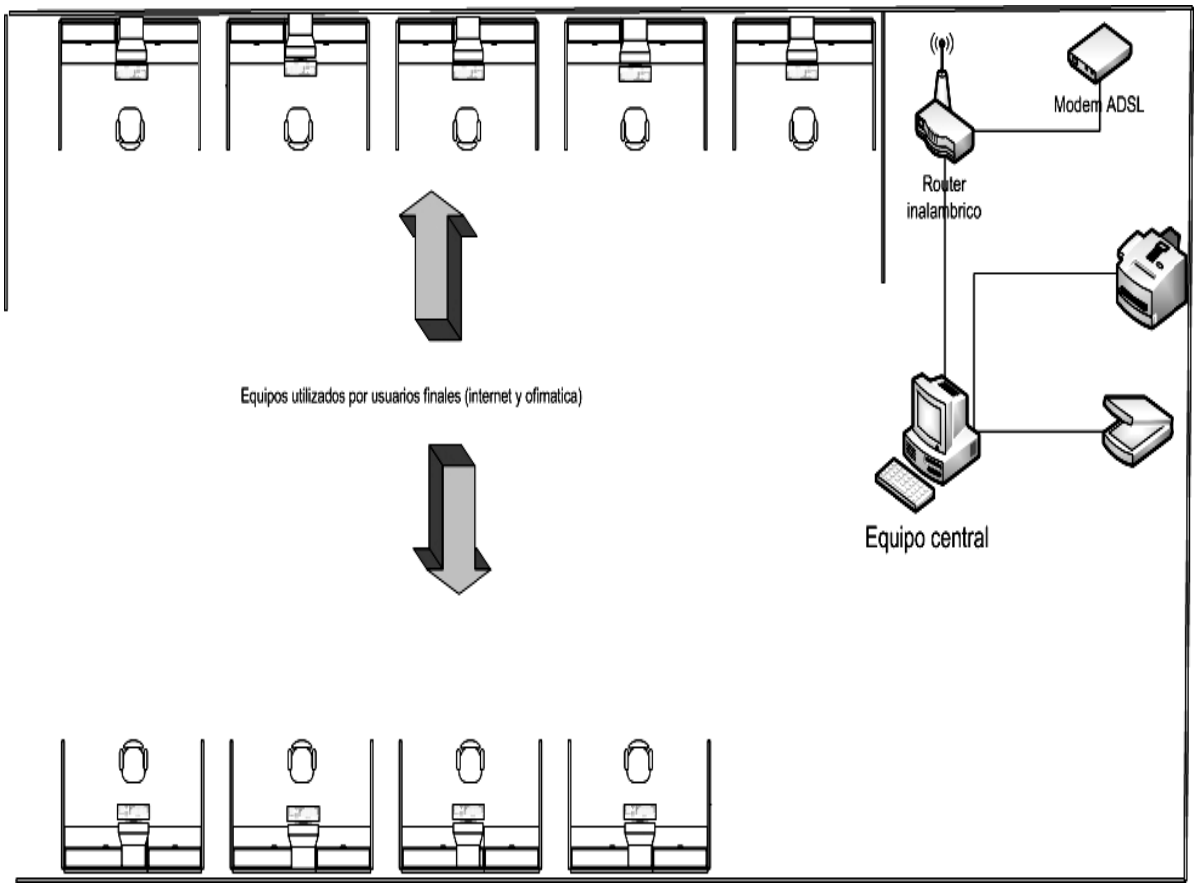

Imagen II.5.1se muestra la disposición de los equipos y dispositivos

Una vez que se tienen dispuestos los dispositivos en los lugares que seleccionamos anteriormente, se configurara el modem, router y estaciones de trabajo.

II.5.1 Configuración del router

Se conecta al modem del ISP a través del cable Ethernet y de igual forma a la computadora de escritorio o laptop que utilizaremos para la configuración inicial. Una vez conectado utilizaremos ya sea la interface web o el disco de instalación de nuestro router (usaremos la interface web) y la imagen II.5.1muestra la entrada a la web de configuración.

Imagen II.5.1 web de configuración del router

Cualquiera que sea el método seleccionado vamos encontrar las siguientes áreas: LAN, WAN,WLAN, DHCP que vamos a configurar de acuerdo a los datos proporcionados por el ISP y nuestras necesidades de conexión y protección en la WLAN que vamos a instalar. La imagen II.5.1 nos muestra un ejemplo de los datos que nos aparecen dentro de la web de configuración.

Imagen II.5.1 Interface Web del router

Dentro de WLAN aparece la ip lan 192.168.1.1 nos indica que coloquemos de forma opcional los DNS, aquí ingresaremos los proporcionados por el ISP que es por ejemplo: 10.3.1.125 y 1.3.1.100

También podemos ver lo referente a wireless settings que podemos observar en la imagen II.5.2 es en la cual colocaremos el SSID de nuestra red, el canal en la que transmitirá, el estándar a utilizar y finalmente el área de seguridad que nos indica la encriptación WEP/WPA y la modulación en la figura muestra como quedan en nuestra red los siguientes datos:

SSID: asgard
Canal: 5
802.11g
Encriptación: WEP (utilizaremos esta para demostrar vulnerabilidad de la misma que es uno de los puntos clave del presente trabajo).

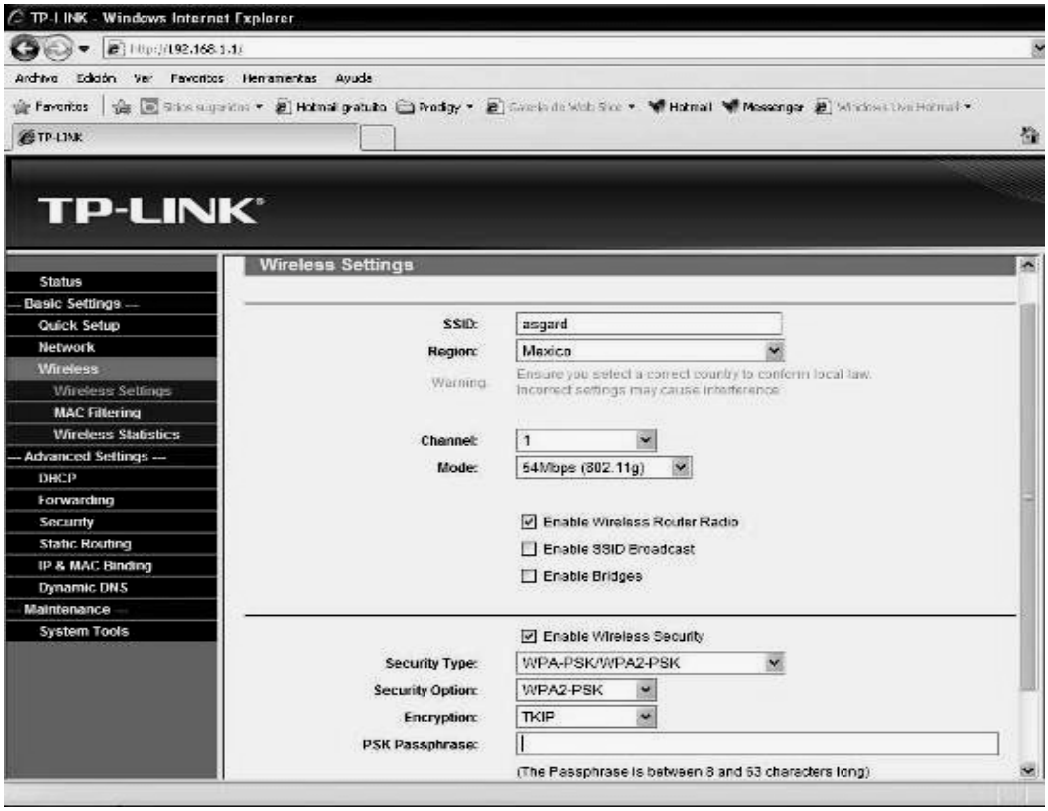

Imagen II.5.2, configuración inalámbrica "wireless settings"

En el router utilizado da opciones de claves de 64 y 128bits hexadecimal o ASCII. Nos proporciona la posibilidad de utilizar el filtrado MAC y filtrado IP, que será explicado más adelante.

Una vez que tenemos configurado nuestro router procedemos a que nuestros equipos (estaciones) queden listas en la red, tanto los portátiles como los fijos. Configuramos el acceso a internet y la integración de la red local, para poder compartir recursos que es uno de los objetivos de una WLAN.

En WAN nos da varias opciones como Dinamic ip, stactic ip, PPPoE, que debemos seleccionar de acuerdo a nuestro ISP .La imagen II.5.3 nos muestra esta opción en el router.

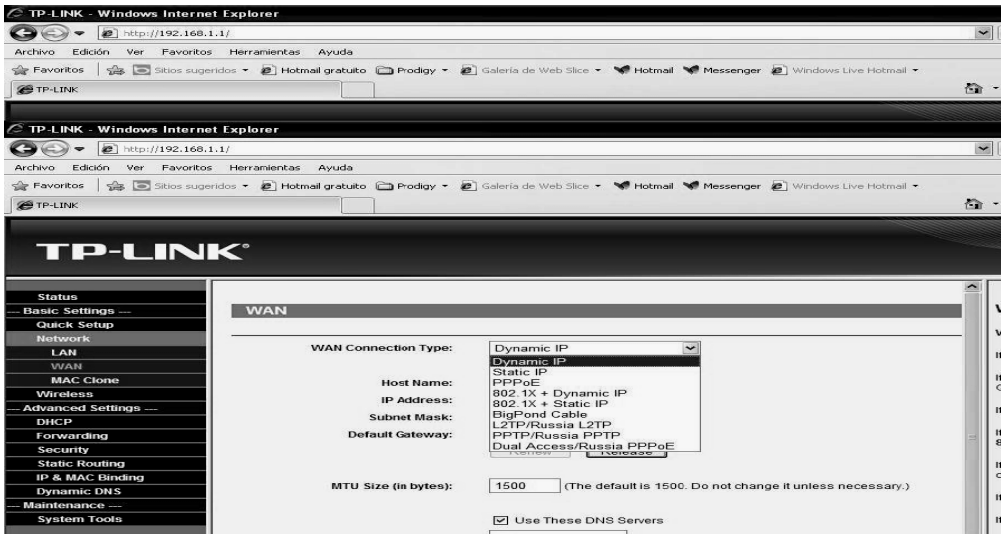

Imagen II.5.3 opciones de configuración WAN

En nuestro caso, al desactivar el DHCP, se pierde acceso total al router. La imagen II.5.4 muestra el área donde se configura.

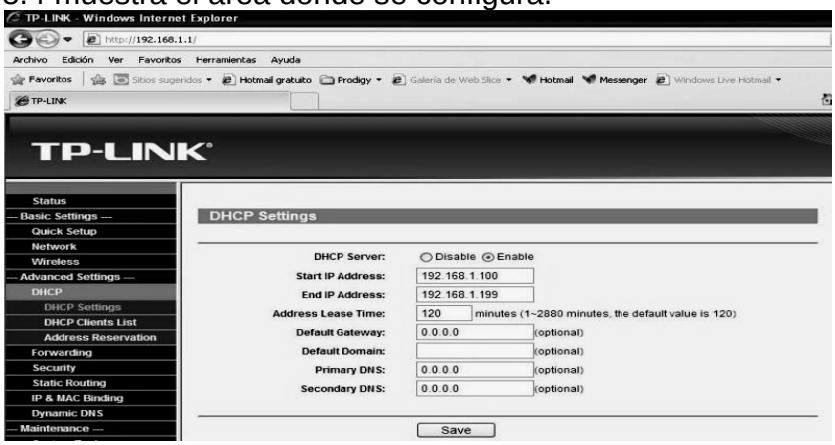

Imagen II.5.4 Configuración de DHCP

II.5.2 Configuración de estaciones de trabajo (utilizando Windows xp)

Se identifica la red creada a través del software de gestión wireless o del propio xp, una vez detectada bastara darle clic sobre ella para indicar que queremos conectarnos y cuando nos solicita la clave ingresaremos la misma que configuramos en el router; esperaremos a que realice la conexión.

La configuración de las estaciones de trabajo se pueden realizar de dos formas:

- Configuración con ip y DNS automática.
- Configuración con ip fija y DNS fijos.

En la primera opción no tenemos que configurar ningún dato ya que el router proporciona dicha información, aunque para compartir recursos se debe asignar un grupo de trabajo.

En la segunda opción se realiza el proceso siguiente: imagen II.5.2.1 muestra el menú principal en donde vamos a ingresar a la configuración ya sea en conexiones de red o a través del panel de control.

Imagen II.5.2.1 menú de inicio

Nos dirigimos a conexiones de red y cuando hayamos seleccionado redes inalámbricas damos clic secundario y propiedades allí nos aparecerá la siguiente imagen, en la imagen II.5.2.2 podemos observar la pantalla de conexiones de red desde donde vamos a ingresar a nuestra red inalámbrica para configurar.

Imagen II.5.2.2 pantalla de conexiones de red.

Al dar clic en las propiedades de redes inalámbricas vamos a buscar el área en donde vamos a poder configurar el protocolo TCP/IP y nos aparece una ventana como la que observamos en la imagen II.5.2.3.

Imagen II.5.2.3. Propiedades de conexiones inalámbricas

En la pantalla que se muestra en la imagen II.5.2.4 que al nos ejecuta nos da la oportunidad de configurar la ip y DNS.

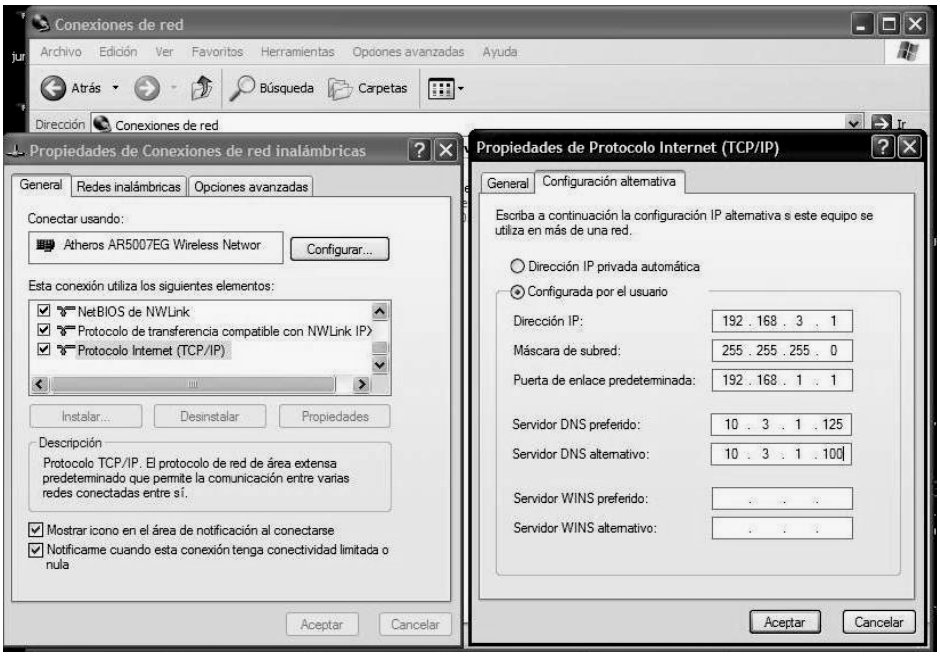

Imagen II.5.2.4 Propiedades de TCP/IP

IP asignado: 192.168.3.1
Sub mascara de red: 255.255.255.0
Puerta de enlace predeterminada: 192.168.1.1 (ip del router)
DNS: 10.3.1.125
10.3.1.100

Una vez colocados estos datos se reinicia el equipo; se verifica el funcionamiento, abriendo explorer internet (si funciona la "navegación") se puede continuar con la configuración de nuestra red WLAN ya que en este punto nuestro acceso al router y al servicio de internet ha sido concretado.

Paso seguido se configurara cada uno de los equipos que integran nuestra WLAN para que se pueda compartir recursos (impresoras, archivos, etc) entre éstos.

II.5.3 Configuración de recursos compartidos

Una vez que tenemos configurado el router, creamos la red (SSID) y colocamos claves de acceso y tipo de encriptación agregamos las estaciones de trabajo al AP y ya tenemos la red WLAN creada y nos resta compartir recursos (archivos de imagen, música, datos, impresoras). Como toda red se necesita saber a que grupo de trabajo se pertenece así que vamos a crear nuestro grupo (independiente de la conexión inalámbrica). Empezamos identificando ya sea por el panel de control o por el icono en el escritorio a “mi pc”; en este caso damos clic secundario en el icono de mi pc y seleccionamos propiedades, la imagen II.5.3.1 muestra la pantalla que nos da la oportunidad de ver las propiedades del sistema.

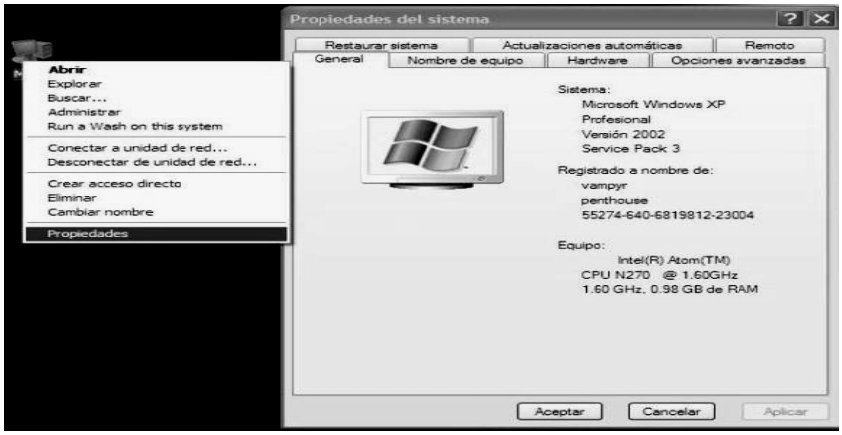

Imagen II.5.3.1Propoedades del Sistema

Una vez que se ha abierto la pantalla no presenta varias pestañas la general nos proporciona datos del sistema (tipo de sistema, versión, nombre de equipo) la pestaña que se utiliza para crear el grupo de trabajo es *nombre de equipo* que nos muestra la imagen II.5.3.2.

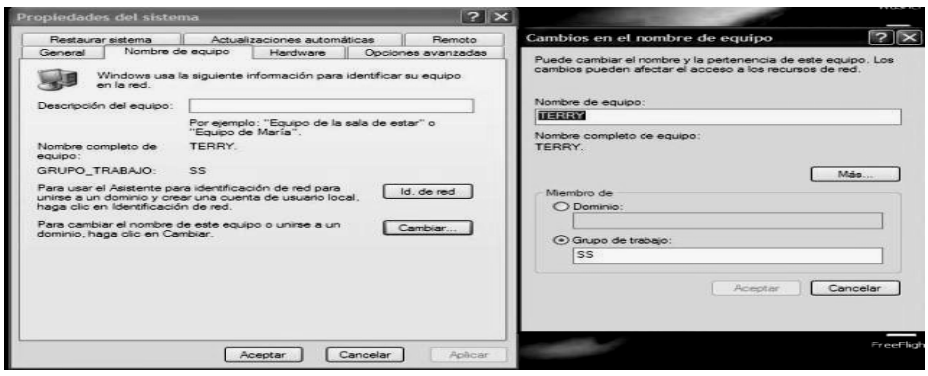

Imagen II.5.3.2 Nombre de Equipo

Al asignar nombre de equipo y grupo de trabajo estamos definiendo nuestra red inalámbrica local que podrá interactuar con la red Ethernet. Se genera ahora el poder compartir los recursos y para esto dando clic en *"mis sitios de red/propiedades/tarea de red/configurar una red domestica/* se abre el asistente para configuración de red que nos da las instrucciones para la configuración presentándonos diferentes pantallas de las cuales, las más significativas se muestran a continuación en las imágenes II.5.3.3 y II.5.3.4.

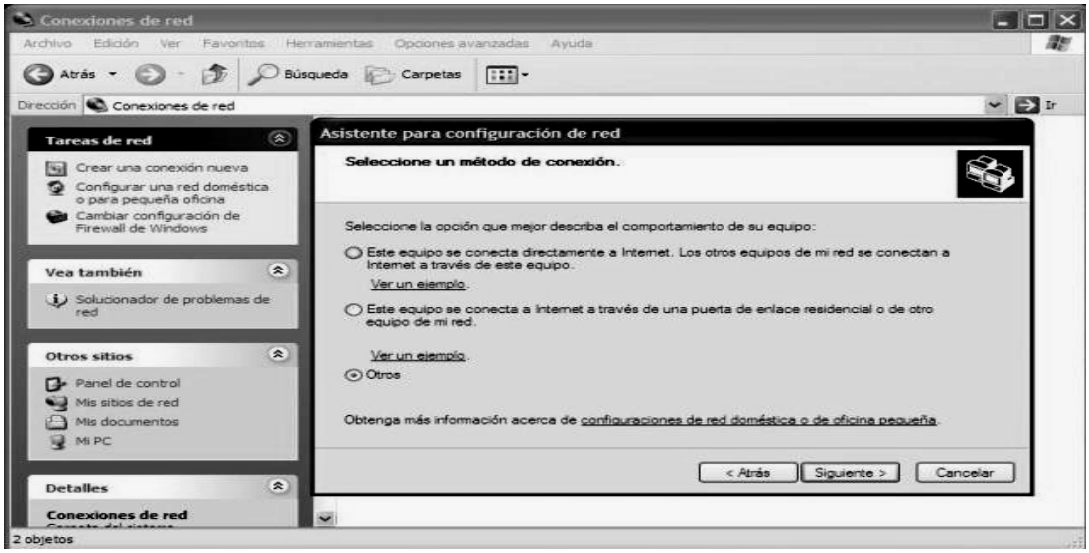

Imagen II.5.3.3

Imagen II.5.3.4

Posteriormente al seleccionar dichas opciones nos aparece el área para asignar el nombre del equipo y el grupo de trabajo como lo muestran las imágenes II.5.3.5 y II.5.3.6 Estos parámetros deben ser los mismos en todos nuestros equipos que integran la red.

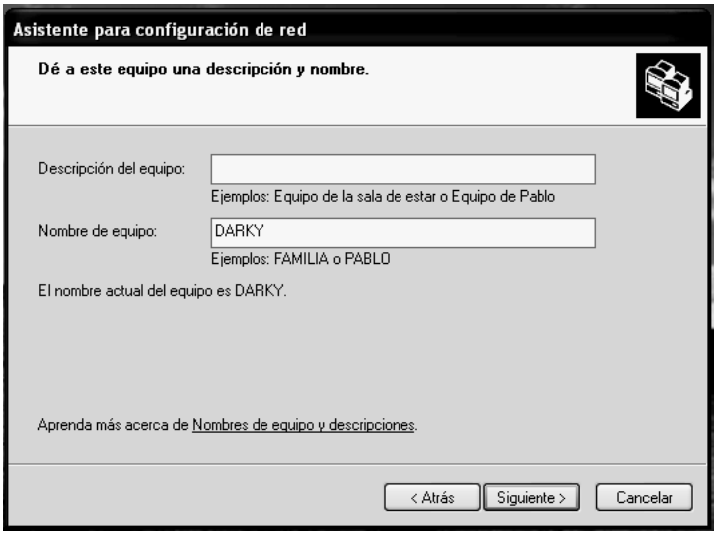

Imagen II.5.3.5 Ingresar nombre de equipo

Imagen II.5.3.6 Ingresamos el grupo de trabajo.

En esta última pantalla colocamos el nombre de grupo de trabajo para que este conformada nuestra red, paso seguido el sistema ejecutara procesos para compartir recursos y una vez finalizados, podemos seleccionar carpetas, dispositivos y archivos que queremos compartir en nuestra red.

En Windows seven, es similar la configuración solo que algunas ventajas que se tienen es que lo automatiza en gran manera este sistema operativo, ya que al detectar la red, y dar conectar (proporcionando la clave) da la opción de configurar una red domestica, empresarial o pública; en el caso de la red local, se agrega automáticamente un grupo de trabajo y nos proporciona una contraseña para ingresarla cuando se pretenda compartir recursos con algún equipo de nuestra red.

Como en todo se debe configurar lo que es nuestro grupo de trabajo para que todos estén dentro del mismo, ya sea con sistemas iguales o diferentes. Una ves hecho esto solo vamos a seleccionar los archivos y dispositivos que se requiere compartir. El procedimiento es el mismo tanto en xp como en seven, solo cambia la interface. Cuando se quiere compartir de Windows seven a xp, se debe hacer un procedimiento sencillo para que no pida usuario y contraseña al intentar acceder de xp a seven; Aquí voy a explicar como hacerlo:

Esta forma posiblemente sea la que más se adecúe en el caso de poseer varios equipos y es la siguiente, se ejecuta la imagen II.5.3.7.

- Desde nuestro equipo con Windows 7, nos dirigimos a Panel de Control > Redes de Internet > Centro de Redes y Recursos Compartidos.
- Apenas se abra el cuadro del Centro de Redes vamos a ver en el menú izquierdo “Cambiar configuración de uso compartido avanzado”.

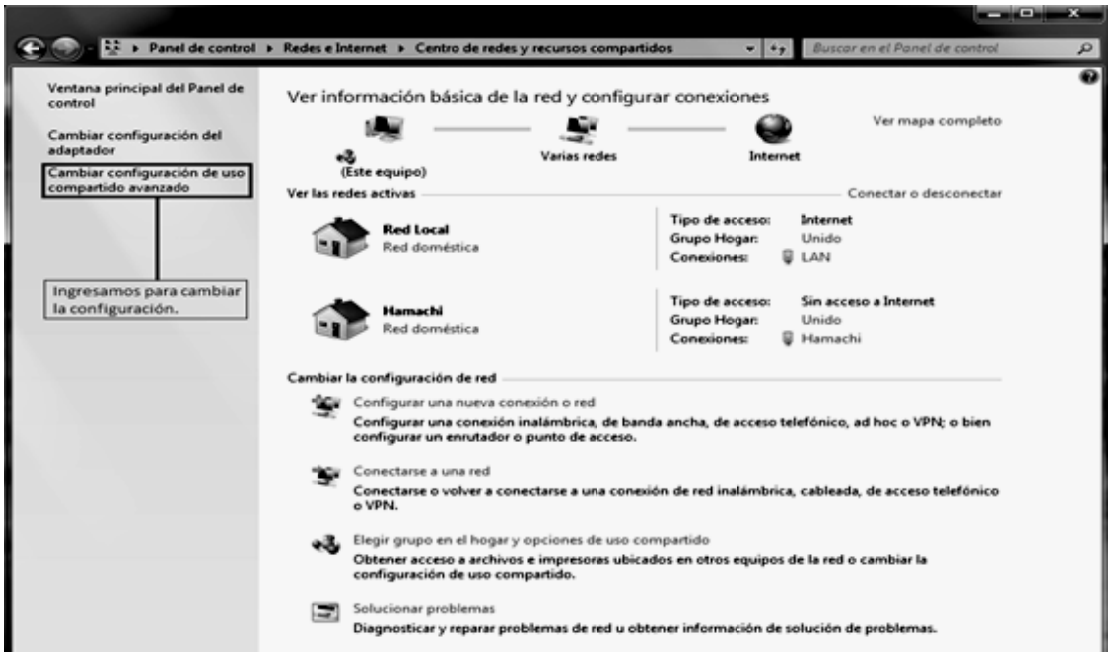

Imagen II.5.3.7. Centro de recursos compartidos

- Buscamos “Uso compartido con protección por contraseña” y le damos en “Desactivar el uso compartido con protección por contraseña”. Que se muestra en la imagen II.5.3.7. Le damos a “Guardar cambios” y listo.

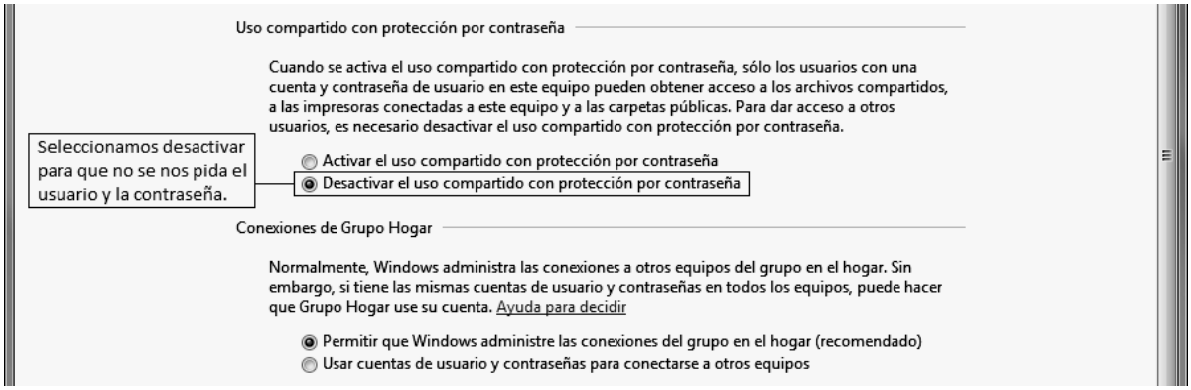

Imagen II.5.3.7 Usos compartidos (activar o desactivar contraseña)

CAPITULO 3

III. VULNERABILIDADES DE UNA RED WLAN Y SOFTWARE UTILIZADO

La seguridad en una red es el proceso por el que los recursos de información digitales son protegidos. Los objetivos de la seguridad son mantener la integridad, proteger la confidencialidad y garantizar la disponibilidad. La seguridad también significa garantizar que los usuarios no puedan dañar los datos, aplicaciones o entorno operativo de un sistema. La seguridad implica protegerse contra ataques malintencionados, así como controlar los efectos de los errores y de los fallos del equipo.

El auge del comercio móvil y de las redes inalámbricas hace que el modelo antiguo sea inadecuado. Un solo dispositivo *firewall* ya no es apropiado para proporcionar seguridad porque es difícil aislar físicamente las señales inalámbricas. Es por ello que al ser la seguridad de redes un tema muy amplio y que su detenido análisis está fuera de los alcances de este proyecto. Solo se mencionará la seguridad que concierne a las redes inalámbricas 802.11, indicando una corta descripción de los mecanismos y estándares que se utilizan en la actualidad, los principales tipos de ataques conocidos y recomendaciones de las medidas seguridades que se deben aplicar en una red inalámbrica.

III.1 Mecanismos de seguridad

III.1.1 OSA

OSA (Sistema de autenticación abierto, *Open System Authentication*), este mecanismo de autenticación abierta ejecuta todo el proceso de autenticación en texto plano. La autenticación abierta se puede configurar para utilizar o no *WEP*.

Un cliente se puede asociar a un *AP* con el SSID correcto, por lo cual resulta un mecanismo de seguridad deficiente ya que no realiza comprobación del cliente y las tramas son enviadas en texto plano.

III.1.2 SKA

SKA (Autenticación por clave compartida, *Shared Key Authentication*), este mecanismo requiere que el cliente y el *AP* tengan la misma clave WEP. Sin embargo, un *AP* que utiliza *SKA* envía un paquete de texto de desafío al cliente.

Si el cliente tiene la clave errónea o no tiene la clave, falla en esta parte del proceso de autenticación. El cliente no tiene permitido asociarse al *AP*.
La autenticación por clave compartida utiliza el cifrado *WEP* durante el proceso de asociación del cliente.

III.1.3 ACL (filtrado de MAC)

ACL (Lista de control de acceso, *Access Control List*), 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 consten en la *ACL*.

Se utiliza para minimizar el riesgo de conexión de dispositivos no autorizados. Se debe utilizar con un número no muy elevado de dispositivos móviles. Este método no es recomendable porque una dirección MAC se puede duplicar, o si se daña la tarjeta de un cliente hay que dar de baja la antigua MAC y declarar la nueva dirección MAC; este proceso puede complicarse en medida del tamaño de la empresa.

También sufre el llamado MAC Spoofing, que es el saltar este filtro clonando o modificando la MAC del equipo atacante por una valida para el ACL

III.1.4 CNAC

CNAC (Control de acceso por red cerrada, *Closed Network Access Control*), 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 éste como contraseña.

El *SSID* es el nombre que le asignamos a nuestra red inalámbrica y es conocido por los dispositivos autorizados. Se utiliza para determinar por parte del dispositivo móvil, a qué punto de acceso está conectado y autenticarse en el mismo. También se denomina ESSID (Identificador de conjunto de servicios extendido, *Extended Service Set Identifier*).
Se debe tener claro que el *SSID* no es un método de autentificación, más bien es un nombre común para los subsistemas wireless (clientes y otros AP), como un identificador. Este nombre debe ser conocido por los dispositivos a conectar.

A todos los dispositivos que no tienen por defecto ese SSID no los deja pasar, es la forma de cómo se diferencian las redes wireless. Por defecto este SSID está en broadcast y por lo tanto cualquier cliente puede identificar y unirse al *SSID* existente. Si se elimina la opción de broadcast del *AP*, un intruso sin un sniffer no puede identificar el *SSID* y unirse al *AP*.

III.1.5 Cortafuegos o "Firewall"

Los firewalls son soluciones basadas en software o en hardware que residen en una máquina y pueden ser administradas por el cliente de manera centralizada. Permiten definir filtros para denegar o permitir el acceso a ciertos usuarios o a ciertos hosts de la red.

Un firewall tiene dos componentes:

· *Filtrado de paquetes,* revisa cada paquete, tanto entrante como saliente, permitiendo la transmisión únicamente de aquellos que cumplan con determinadas condiciones y desechando a los que no lo hagan. Los criterios considerados pueden ser: direcciones IP, números de puertos, etc.

· *Puerta de enlace de aplicación,* toma decisiones basadas en los datos de aplicación, por ejemplo, se puede establecer qué grupos de usuarios tienen permiso de ejecutar Telnet hacia y desde el exterior, y cuáles no. Todos los datos de aplicación deberán pasar por la puerta de enlace de aplicación para su análisis.

III.1.6 VLAN

Una *VLAN* es una red conmutada segmentada de forma lógica en funciones, equipos de proyecto o aplicaciones, en lugar de estar dividida física o geográficamente. Por ejemplo, todas las estaciones de trabajo y servidores utilizados se pueden conectar a una misma *VLAN*. Las *VLAN* se utilizan para reconfigurar la red con ayuda de software, en lugar de hacerlo físicamente desconectando y moviendo los dispositivos o cables. La imagen III.1.6.1 Muestra un solo punto de acceso con tres *VLAN*.

Imagen III.1.6.1 Vlan con un solo AP [3]

El AP y configuración se podría explicar de la siguiente forma:

- Varios SSID
- Varios tipos de seguridad.
- Propaga las VLAN desde los *switches*.
- Protocolo de *trunking 802.1Q*.

Una VLAN consta de cierta cantidad de sistemas finales, hosts o equipos de red (como puentes y routers), conectados por un solo dominio de puenteado. El dominio de puenteado está soportado en varias piezas del equipo de red, como los *switches* LAN que operan puenteando protocolos entre ellos con un grupo separado por cada VLAN.

Las VLAN ofrecen los servicios de segmentación tradicional proporcionado por los routers en las configuraciones LAN. Las VLAN ofrecen escalabilidad, seguridad, administración de la red. Esto resulta útil para separar los clientes WEP básicos de una *VLAN* de los usuarios que no utilizan ningún tipo de cifrado. Si las VLAN están correctamente configuradas, son seguras. El tráfico de una VLAN no puede atravesar otra *VLAN*.

[3] Referencia: Cisco Systems, Inc. *Fundamentos de redes inalámbricas.* Traducido por: Díaz, José Manuel. Madrid (España), 2006. Traducido de: Fundamentals of Wireless LANs Companion Guide (Cisco Networking Academy Program), 1st Edition. ISBN: 1-58713-119-6

III.2 Protocolos de autenticación de capa superior

Los protocolos ULA (Autenticación de capa superior, *Upper Layer Autentication*) proporcionan intercambio de autenticación entre el cliente y un servidor de autenticación.

Los protocolos ULA son:

- **EAP-TLS** (Protocolo de autenticación extensible con Seguridad de la capa de transporte, *Extensible Authentication Protocol with Transport Layer Security*), es un protocolo de autenticación basado en certificados digitales, los cuales deben estar instalados tanto en el servidor como en el cliente ya que la autenticación es mutua. EAP-TLS está basado en los certificados X.509[4].

- **LEAP** (EAP Ligero, *Lightweight EAP*), el EAP ligero también se denomina EAPCisco el cual es propiedad de Cisco y fue diseñado para ser portable 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 seguridad a diferentes clientes según el sistema operativo. LEAP también se puede utilizar cuando se necesita una clave *WEP* dinámica y la autenticación mutua. Se debe utilizar *TKIP* para asegurar *LEAP*. *LEAP* es el método menos complicado de implantar 802.1x; sólo requiere un servidor RADIUS.

- **PEAP** (EAP Protegido, *Protected EAP*), es un protocolo EAP diseñado para permitir la autenticación híbrida. *PEAP* emplea la autenticación PKI (Infraestructura de clave pública, *Public Key Infrastructure*) del lado del servidor. Para la autenticación del lado del cliente, *PEAP* puede utilizar cualquier otro tipo de autenticación EAP. Como PEAP establece un túnel seguro a través de la autenticación del lado del servidor, pueden utilizar los tipos EAP de autenticación no mutua para la autenticación del lado del cliente.

[4] X.509: Es una norma internacional publicada por la UIT-T, que trata algunos de los requisitos de seguridad en los ámbitos de autenticación, y otros servicios de seguridad mediante la introducción de un conjunto de marcos sobre los que se pueden basar servicios completos. De forma específica, esta norma define marcos para: certificados de clave pública; certificados de atributo y servicios de autenticación.

- **EAP-TTLS** (EAP con Seguridad de la capa de transporte en túnel, *EAPTunneled Transport Layer Security*), parecido al PEAP, está implementado en algunos servidores Radius y en software diseñado para utilizarse en redes 802.11.

- **EAP-MD5**, no se debe utilizar porque no proporciona una autenticación mutua.
- EAP-MD5 es una autenticación de una sola dirección que duplica la protección de contraseña CHAP (Protocolo de autenticación de intercambio de señales por desafío), en una WLAN. EAP-MD5 se utiliza como bloque constructivo en EAPTTLS.

- **MIC** (Código de integridad de mensaje, *Message Integrity Code*), es un valor de 64 bits generado por una función de cifrado de clave simétrica usando el algoritmo de Michael. Si se cambian los datos de entrada, un nuevo valor no puede ser calculado correctamente sin el conocimiento de la clave simétrica. Así pues, la clave secreta que protege los datos de entrada no es detectable. Las claves WEP más sólidas son proporcionadas por las mejoras de TKIP y MIC. El controlador del adaptador cliente y el *firmware* deben soportar la funcionalidad MIC, y en el AP debe activarse MIC.

- **TKIP** (Protocolo de integridad de clave temporal, *Temporal Key Integrity Protocol*), establece una clave temporal de 128 bits que se comparte entre los clientes y los *AP*. TKIP añade un vector de inicialización (IV) de 16 octetos relativamente largo a la clave base para producir la clave con la que se cifrarán los datos. Este procedimiento garantiza que cada estación utiliza flujos de clave diferentes para cifrar los datos.

  Al igual que WEP, TKIP está basada en el algoritmo de encriptación RC4 para realizar el cifrado. No obstante una gran diferencia a WEP es que TKIP cambia la clave temporal con cada paquete. TKIP permite a los sistemas WEP la actualización para instalar un protocolo más seguro. TKIP se requiere para la certificación WPA y se incluye como parte de RSN 802.11i como una opción. TKIP añade medidas correctoras para cada una de las vulnerabilidades de WEP.

CCMP (*CTR with CBC-MAC Protocol*), proporciona confidencialidad, autenticación, integridad, y protección en la reproducción. CCMP es obligatorio para el cumplimiento de la certificación WPA2. WPA2 nombre comercial dado por la Alianza Wi-Fi al estándar de seguridad IEEE 802.11i para redes RSN. CCMP se basa en la suite de cifrado de bloques *AES* en su modo de operación CCM, con la clave y los bloques de 128 bits de longitud. AES es a CCMP.

III.3 WEP

WEP (Privacidad equivalente al cableado, *Wired Equivalent Privacy*) fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11 en el año de 1999 para proteger a los usuarios autorizados de una WLAN ante una escucha casual. WEP está basado en el algoritmo de encriptación RC4, con una clave secreta de 40 o 104 bits, combinada con un *Vector de Inicialización* (IV) de 24 bits.

Al utilizar WEP, tanto el cliente inalámbrico como el *AP* deben tener una clave *WEP* coincidente, es decir una clave estática. A partir de la clave estática se generan 4 llaves, en función de si se van a utilizar llaves de 40 o 104 bits. De las 4 llaves generadas se selecciona solo una de ellas para la encriptación WEP. Permite dos modos de operación, uno como un sistema de autenticación abierto (*OSA*), en el que todos los usuarios tienen permiso para acceder a la red de área local inalámbrica y otro mediante una autenticación de clave compartida (*SKA*), que controla el acceso a la WLAN.
El proceso de encriptación de WEP es el siguiente:

- Se calcula un CRC-32 de los datos.
- Se agrega un vector de inicialización (IV) aleatorio de 24 bits concatenándolo con la clave compartida para generar la llave de cifrado (*seed*).

- Se encriptan los datos utilizando RC4, el cual genera una secuencia de caracteres pseudoaletorios (*keystream*) a partir de la clave generada (*seed*).
- Se realiza una *operación XOR* entre el *keystream* y los datos para obtener el texto cifrado.
- Se transmite el vector de inicialización en texto plano y el texto cifrado dentro de la trama de datos IEEE 802.11.

En la actualidad se han encontrado grandes debilidades en la seguridad ofrecida por este protocolo, por lo que en el caso de utilizarlo es conveniente hacerlo en conjunto con otros mecanismos de seguridad.

Los fallos de seguridad de WEP pueden resumirse de la siguiente manera:

- Debilidades del algoritmo RC4 dentro del protocolo WEP debido a la construcción de la clave.
- Los IVs son demasiado cortos (24 bits – hacen falta menos de 5000 paquetes para tener un 50% de posibilidades de dar con la clave) y se permite la reutilización de IV (no hay protección contra la repetición d mensajes).

- No existe una comprobación de integridad apropiada (se utiliza CRC32 para la detección de errores y no es criptográficamente seguro por su linealidad).

- No existe un método integrado de actualización de las claves.

III.4 WPA (Pre 802.11i)

Al igual que WEP utiliza cifrado RC4, se emplea TKIP para la generación temporal de claves y MIC (en reemplazo de CRC-32) para asegurar la integridad de la información, y soporte del estándar 802.1x.

Antes de la introducción del estándar IEEE 802.11i, los fabricantes de WLAN intentaron compensar los fallos internos de WEP usando una solución conocida como WPA (Acceso Protegido Wi-Fi, *Wi-Fi Protected Access*), desarrollado al amparo de la Alianza Wi-Fi.

Las características más importantes de WPA son la Anulación de Llaves Débiles ("WEPplus"), Habilitación de la Autentificación EAP y el Protocolo Temporal de Integración de Llaves (TKIP). TKIP está diseñado para evitar los puntos débiles reemplazando las llaves estáticas con llaves modificadas dinámicamente e implementando comprobaciones de integridad ampliamente incrementadas. Por razones de compatibilidad descendente TKIP aún usa el débil flujo de codificación RC4.

Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

En la siguiente tabla III.4.1 podemos observar la comparación entre WEP y WPA

Característica		WEP	WPA
Cifrado	Sistema de algoritmo de cifrado	RC4	TKIP (RC4)
	Longitud	40 bits	128 bits
	Generación de claves	Estática: la misma para todos los dispositivos	Dinámica por usuario
	Distribución de claves	Manual en cada dispositivo	Automática: gestionada por 802.1x/EAP
Autenticación	Entorno	802.11	802.1x/EAP
	Método	Abierta/clave compartida (autentica el equipo)	EAP-TLS, PEAP, EAP-TLS (autentica al usuario)

Tabla III.4.1[5]

III.5 IEEE 802.11i (WPA2)

Esta enmienda fue aprobada el 24 de junio de 2004 y está incluida en la nueva versión IEEE 802.11, para las *WLANs* y recibió el nombre comercial WPA2, por parte de la Alianza Wi-Fi. Los mecanismos de seguridad para IEEE 802.11 son definidos en esta enmienda, que incluye una definición de WEP para garantizar la compatibilidad con el estándar original IEEE 802.11, edición 1999.

Esta enmienda define los protocolos TKIP y CCMP, que proporcionan mecanismos de protección de datos más robustos que WEP. Donde CCMP es obligatorio para que un dispositivo tenga la certificación WPA2 por parte de la Alianza Wi-Fi. CCMP se basa en la suite de cifrado de bloques *AES*[6] en su modo de operación CCM, con la clave y los bloques de 128 bits de longitud. AES es a CCMP lo que RC4 a TKIP que se diseño para acomodar el hardware WEP existente.

[5] Referencia: SINCHE M. Soraya MSc. Curso de Capacitación Tecnológica WIRELESS LAN-WAN. ATI. Octubre 2007

[6] AES (Estándar de cifrado avanzado, *Advanced Encryption Standard*), utiliza el algoritmo de Rijndael, que es un cifrador de bloques con soporte para claves de 128, 192 y 256 bits, y es mucho mas solido que RC4. AES es el sucesor de Triple-DES (3DES) e incluye MIC y funciona con claves estáticas y dinámicas patrocinado por el Instituto de estándares y tecnología (NIST). Para que los dispositivos WLAN utilicen AES, el hardware debe estar diseñado para soportar AES, y no WEP.

El estándar abarca los protocolos 802.1x, TKIP y CCMP. La nueva arquitectura para las redes wireless se llama RSN[7] y utiliza autenticación 802.1x, distribución de claves robustas y nuevos mecanismos de integridad y privacidad. Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica.

Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red transicional de seguridad (TSN, *Transitional Security Network*), arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo en el futuro.

El establecimiento de un contexto seguro de comunicación consta de cuatro fases:

- Acuerdo sobre la política de seguridad.
- Autenticación 802.1X.
- Derivación y distribución de las claves.
- Confidencialidad e integridad de los datos RSNA.

III.6 AMENAZAS Y ATAQUES CONTRA LAS WLANs IEEE 802.11

III.6.1 Amenazas

Hay cuatro clases principales de amenazas a la seguridad inalámbrica:

· Amenazas no estructuradas.

· Amenazas estructuradas.

· Amenazas externas.

· Amenazas internas.

Las amenazas no estructuradas, consisten principalmente en individuos inexpertos que utilizan fácilmente las herramientas de pirateo disponibles, como los *scripts* de *shell*, los programas *war-driving* y los *crackers* de contraseñas.

[7] RSN (Red de seguridad sólida, *Robust Segurity Network*), es una red que solo permite la creación de Asociaciones de red de seguridad sólida (RSNAs). Una RSN puede ser identificada por la indicación en el elemento de información RSN de tramas Beacon.

Las amenazas estructuradas, vienen de intrusos más motivados y técnicamente más competentes. Estas personas conocen en profundidad las vulnerabilidades del sistema inalámbrico y pueden entender, así como desarrollar *scripts* y programas.

Las amenazas externas, son individuos y organizaciones que trabajan desde el exterior de la empresa. No tienen acceso autorizado a la red inalámbrica. Trabajan a su manera sobre una red, principalmente desde el exterior del edificio (parqueaderos, edificios adyacentes o áreas comunes).

Las amenazas externas son el tipo de amenazas en el que las personas invierten la mayoría del tiempo y el dinero para protegerse contra ellas.
Las amenazas internas, se producen cuando alguien tiene acceso autorizado a la red con una cuenta en un servidor, o tiene acceso físico al cableado. Según el FBI, el acceso interior y el mal uso de las cuentas representan del 60 al 80 por ciento de los incidentes denunciados.

III.6.2 Ataques contra las WLAN

Los métodos de ataque inalámbricos más conocidos se describe a continuación:

Espionaje (surveillance)

Este tipo de ataque consiste simplemente en observar el entorno donde se encuentra instalada la red inalámbrica. No se necesita ningún tipo de "hardware" o "software" especial. Sirve para recopilar información y se puede combinar con otros tipos de ataques.

War-Chalking

Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que "pasen por allí". Es decir, es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.

War-driving

Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como una notebook o un PDA. El método es realmente simple: el atacante pasea con el dispositivo móvil, y en el momento en que detecta la existencia de la red, se realiza un análisis de la misma.

El dispositivo móvil puede estar equipado con un sistema GPS para marcar la posición exacta donde la señal es más fuerte, o incluso una antena direccional para recibir el tráfico de la red desde una distancia considerable. Existen varias herramientas útiles para detectar redes inalámbricas, las más conocidas son el AirSnort o Kismet para Linux y el NetStumbler para sistemas Windows.

Para realizar el War driving se necesitan realmente pocos recursos. Los más habituales son una computadora portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el punto de acceso (AP) en un mapa y el software apropiado (AirSnort para Linux, BSD- AriTools para BSD o NetStumbler para Windows).

"Sniffing" y "Eavesdropping" (escuchas-intercepción)

El programa monitoriza los datos y determina hacia donde van, de donde vienen y qué son, siempre que haya una tarjeta de red que actúa en "modo promiscuo". El modo promiscuo es un modo de operación en el que una computadora conectada a una red compartida captura todos los paquetes, incluyendo los paquetes destinados a otras computadoras. Es muy útil para supervisar la red, pero presenta un riesgo de seguridad dentro de una red de producción.

Denegación de servicio (DoS, Denial of Service)

La denegación de servicio sucede cuando un atacante intenta ocupar la mayoría de los recursos disponibles de una red inalámbrica. Impide a los usuarios legítimos de ésta, disponer de dichos servicios o recursos. Puede producirse a través de:

· Ataques por sincronización (SYN Flooding).

· Ataque "smurf".

· Sobrecarga del sistema.

· Falsedad de nombres de dominio (DNS spoofing).

Ataques de AP falso

La mayoría de clientes se asocia al AP que tiene la señal más fuerte. Si un AP no autorizado, que normalmente es un AP falso, tiene una señal fuerte, los clientes se asocian a él. El AP falso tendrá acceso al tráfico de red de todos los clientes asociados. Por lo tanto el AP falso se puede utilizar para llevar a cabo ataques "manin- the-middle" (hombre en el medio) contra el tráfico cifrado.
"Spoofing" (burla) y "Hijacking" (secuestro)

El atacante falsifica información, un identificador de usuario o una contraseña permitidos por el sistema atacado. Esto lo hace redefiniendo la dirección física o MAC de la tarjeta inalámbrica por una válida ("hijacking"). De esta manera, asocia una dirección IP válida del sistema atacado. La idea es secuestrar la comunicación entre dos sistemas suplantando a uno de ellos, para lo que es necesario estar situado en la ruta de comunicación.

En cuanto a este tipo de ataques o amenazas se puede evitar en cierto grado a través del filtrado de MAC que ya se incorpora en los routers actuales, sin embargo si se enfrenta a una persona con conocimientos y medios adecuados pueden ser burlados y terminar por conectarse al AP que selecciono mediante procedimientos y comandos basados en Linux básicamente.

A continuación se muestra un ejemplo de lo que se puede realizar para este tipo d ataques (tomados desde la web). En la web se encuentran manuales de cómo clonar las MAC autorizadas y poder atacar y autentificarse a algún AP y poder tener el servicio de internet, que es un punto fundamental en la presente investigación, a continuación se muestra un ejemplo encontrado en la WEB para clonar la MAC

> *El escenario es el siguiente: tenemos acceso a una red inalámbrica sin autentificación ni cifrado a la cual queremos entrar. Intentamos entrar en la red wireless de forma normal. Todo parece ir bien pero no conseguimos conectarnos.Tras varios intentos de conexión fallidos llegamos a la conclusión de que el router tiene un filtrado de MAC.*

Lo primero que hay que hacer es poner nuestra tarjeta wireless en modo promiscuo. No todos los chipset soportan este modo en Windows, así que dependiendo de la tarjeta que tengamos podremos utilizar Windows o decantarnos luego utilizaré la distribución wifiway que me permite poner la tarjeta en modo monitor.

El siguiente paso es ver la MAC del cliente al cual queremos suplantar. Para ello lanzamos un programa que nos permita ver que clientes están conectados a las estaciones o bssid (además de darnos información adicional como la direcciones MAC de los clientes. Uno de ellos podría ser el ariodump de la suite aircrak. Tras lanzarlo podemos ver el cliente (con la MAC xx:xx:xx:xx:xx:xx) que queremos spoofear y la anotamos.

El siguiente paso será cambiar nuestra dirección MAC verdadera, a la dirección que hemos anotado, mediante un pequeño programa que nos permita hacer esto.

Existe software tanto para Linux como para Windows.

Para Windows tenemos varias opciones. Si vamos a las propiedades de nuestro adaptador de red, algunos fabricantes (la mayoría) permiten cambiar directamente la dirección MAC. Otra opción sería modificar el registro del Windows.

Por último podríamos utilizar también programas de terceros tipo MacShift, Etherchange, Smac, etc para cambiar nuestra dirección. Hay que señalar que es posible que algunos de los métodos no funcionen y por consiguiente tendríamos que aplicar otro hasta que veamos que nuestra MAC a cambiado realmente. Para comprobar que se ha cambiado correctamente nuestra MAC solo tenemos que ejecutar una consola y escribir en ella "ipconfig /all" y ver si realmente la dirección física se ha cambiado.

Por contra, para el sistema operativo Linux el cambio resulta más fácil, con solo ejecutar estos tres comandos habremos cambiado nuestra dirección a la que especifiquemos por xx:xx:xx:xx:xx:xx.

Los comandos son: "ifconfig eth0 down" (deshabilitamos la interfaz de red) , "ifconfig eth0 hw ether xx:xx:xx:xx:xx:xx" (cambiamos la dirección hardware de la tarjeta), e "ifconfig eth0 up" (volvemos a levantar la interfaz de red). También existen programas en Linux que permiten hacer el cambio y otras cosas más como GNU Mac Changer. De nuevo podemos ver si el cambio se ha realizado con éxito si hacemos un "ifconfig" y vemos que la MAC ha cambiado.

III.7 Descripción y aplicación del uso de software malintencionado

Los ataques más comunes es el conectarse a un AP para obtener la clave para tener acceso al servicio de internet (punto central de la presente investigación) Usando herramientas especificas y de adquisición fácil en nuestro país o a través de internet se "ataca" dicho AP, se autentifica y se inyecta trafico para capturar paquetes de información con el objetivo de descifrar la contraseña con la cual el dispositivo "atacado" permitirá el tener una conexión a internet sin necesidad de pagar el costo que conlleva ese servicio.

En algunos casos las claves utilizadas son los números de serie del dispositivo o las que vienen por default de fábrica, que son fácilmente obtenidas en internet. En estos tipos de situaciones basta con tener el equipo adecuado para escanear redes, detectar las vulnerables y "atacarlas" en el caso de que tengan una clave vulnerable.

Hay redes en las que sus claves pueden ser descifradas hasta por un simple teléfono móvil como es el caso del Samsung Galaxy Ace que con un software descargado en el mismo teléfono de nombre HHG5xx default wepkey scanner free.

Con este software fue posible en pocos minutos descifrar claves wep predeterminadas en los módems 2wire en su mayoría, el cual nos dio los datos siguientes: ESSID, BSSID y la key predeterminada.

III.7.1 Wifislax

A continuación se muestra el uso de **Wifislax** para la obtención de la clave del modem 2wire proporcionado en el servicio de prodigy infinitum

Wifislax es un CD de arranque que contiene al sistema operativo Linux. Puede hacer correr Linux directamente desde el CDROM sin instalación. Aunque lleva incorporado herramientas de instalación en el disco duro o en llaveros USB, o una emulación en Windows. Wifislax está basado básicamente y principalmente en SLAX[8] (basado en la distribución Slackware Linux[9].

Con este liveCd, que se puede manipular de acuerdo a las necesidades y estar en cd o usb, podemos con los comandos necesarios y dispositivos adecuados monitorear las redes inalámbricas que estén al alcance de nuestro equipo, y una

[8] **Slax** es un sistema operativo Linux moderno, portable, pequeño y rápido con un enfoque modular y un diseño excepcional. A pesar de su pequeño tamaño, Slax proporciona una amplia colección de software pre-instalado para uso diario, incluyendo una interfaz gráfica de usuario bien organizada y útiles herramientas de recuperación para administradores de sistemas.

[9] **Slackware** Linux es la distribución Linux más antigua que tiene vigencia. En su última versión, la 13.37, Slackware incluye la versión del núcleo Linux 2.6.37.6 y Glibc 2.11.1. Contiene un programa de instalación sencillo de utilizar aunque puede ser compleja para los nuevos en sistemas linux, extensa documentación, y un sistema de gestión de paquetes basado en menús. Una instalación completa incluye una implementación de X Window System para el sistema de ventanas (X.Org ; entornos de escritorio como KDE (4.5.5) (hasta la versión 10.1 estuvo incluido GNOME) y XFce (4.6.2); entornos de desarrollo para C/C++, Perl, Python, Java, LISP y Ruby; utilidades de red, servidores de correo, de noticias (INN), HTTP (Apache) o FTP; programas de diseño gráfico como The GIMP; navegadores web como Konqueror, Firefox y Mozilla SeaMonkey, entre otras muchas aplicaciones

vez monitoreado lograremos después de un tiempo, obtener las claves WEP de los AP que queremos en este caso "descifrar".

En las siguientes páginas se mostrara con imágenes el procedimiento que se siguió para lograr obtener la clave de acceso al dispositivo ADSL de prodigy infinitum. En este ejemplo realizado para documentar el presente trabajo, no se "ataco" un AP ajeno, se utilizo el de la red existente antes instalada, teniendo claves de acceso para comprobar la efectividad de la herramienta aquí mostrada.

PROCEDIMIENTO

- Paso 1: Se instala wifislax en la Usb
- Paso2: Se inicia la pc desde la usb (para este procedimiento, es necesario realizar los cambios necesarios en el BIOS, esto para que el equipo inicie desde el dispositivo USB). Ya que se inicio desde el dispositivo externo y se ejecuta la herramienta Wifislax aparece la pantalla de inicio de la misma donde en algunos casos se debe ingresar lo siguiente para que se carguen los drivers necesarios para el entorno grafico que más adelante se observara. Al dar "TAB" escribimos "nohotplug" (se pueden utilizar otros).

- Paso 3: Ya que se da enter en la pantalla anterior se presenta la pantalla de inicio en donde se debe ingresar el usuario y contraseña necesarios.

- Paso 4: Se escribe el comando "startx" para iniciar la carga del entorno grafico de Wifislax.

- Paso 5: Se coloca la tarjeta inalámbrica en modo monitor, como se muestra en la imagen III.7.1.

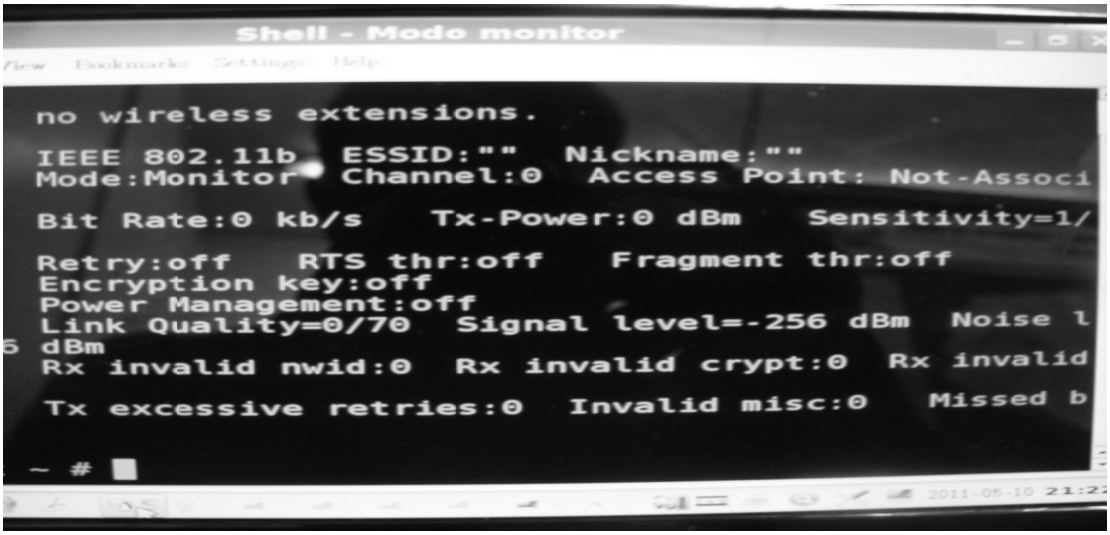

Imagen III.7.1 Shell- monitor

Se da en el botón de inicio, se del menú que aparece se selecciona *Asistencia al chipset/ Asistencia del chipset Atheros/ modo monitor.*
Se abre Shell monitor.

- Paso 6: En este paso se iniciara el *airoscript*; se abre un nuevo Shell siguiendo la secuencia *incio/wifislax/Herramientas wireless/ airoscript .*En la imagen III.7.2 se muestra la pantalla de Shell airoscript en donde nos da la bienvenida y también es el inicio de una serie de comandos que serán utilizados para obtener las claves.

Imagen III.7.2 Shell airoscript

Nos indicara que seleccionemos la interface a utilizar (si no se detecto previamente la interface inalámbrica no funcionara el procedimiento, debido a la incompatibilidad entre wifislax y la tarjeta inalámbrica).

En el ejemplo que se está utilizando, elegimos la opción 1 que nos muestra ath0 (que es nuestra interface inalámbrica).En la imagen III.7.3 se muestra la pantalla que nos ofrece dicha opción

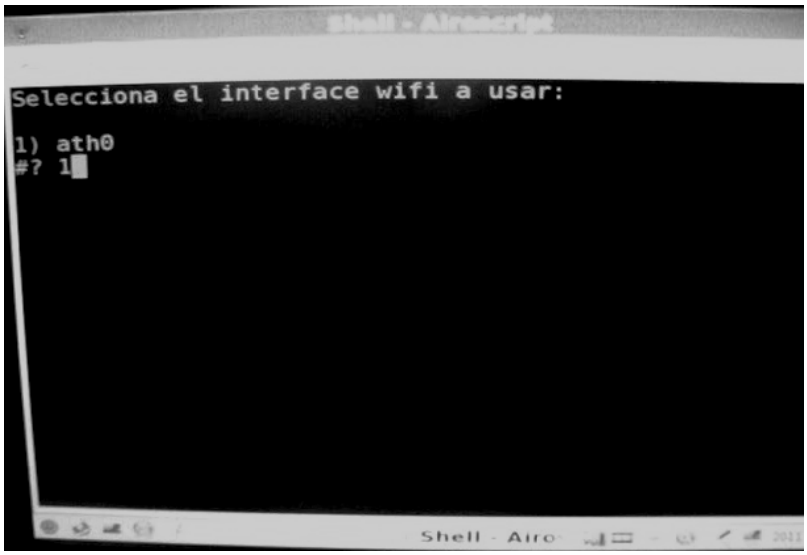

Imagen III.7.3 Airoscript detectando la interface wifi

- Paso 7: Al elegir nuestra interface nos mostrara la siguiente pantalla en la cual nos ofrece 15 opciones desplegadas del 1 al 15 del cual seleccionaremos la 1, con la cual escaneara los objetivos, la imagen III.7.4 nos muestra el listado de opciones.

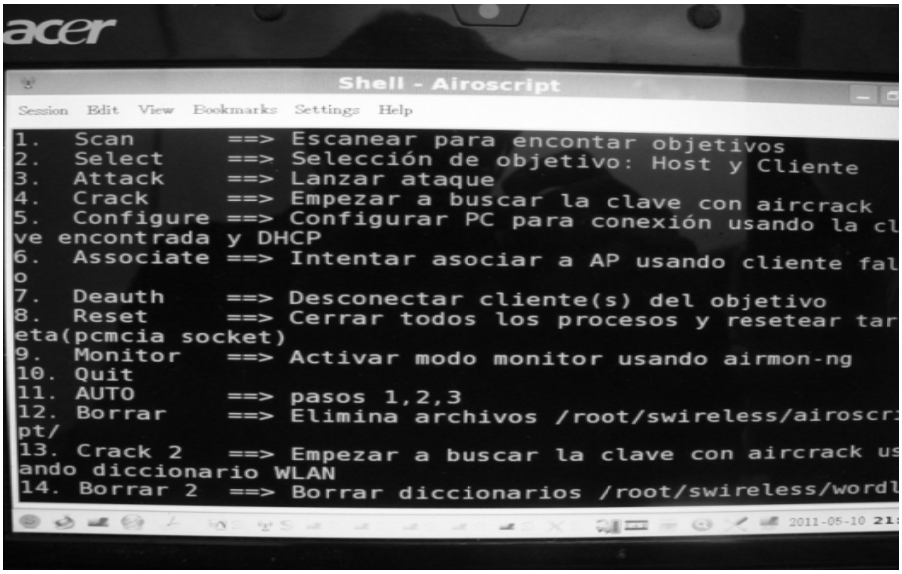

Imagen III.7.4 Lista de opciones Airoscript

- Paso 8: Indicara que airodump será ejecutado y nos indica si queremos escanear múltiples canales o uno especifico. En la imagen III.7.5 muestra la pantalla que nos indicara que tipo de escaneo se llevará a cabo.

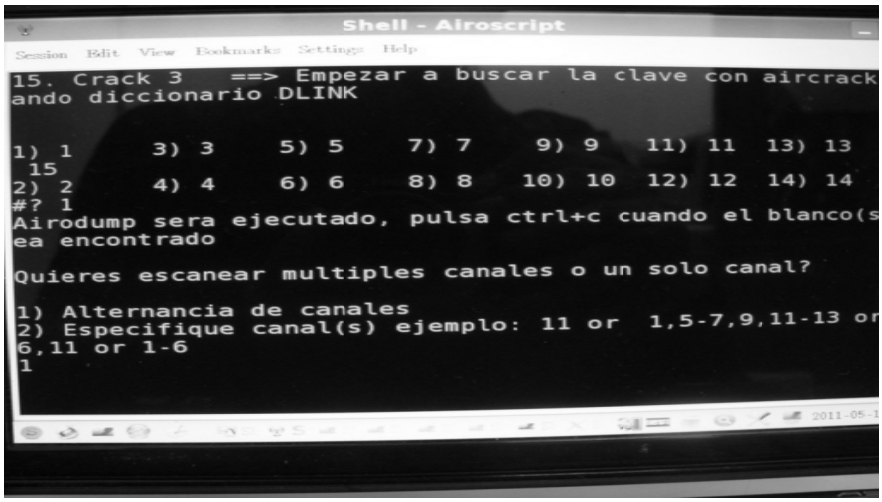

Imagen III.7.5 Tipo de escaneo a ejecutar en airodump.

- Paso 9: Seleccionaremos “alternancia de canales” para poder escanear diferentes objetivos, se abrirá una pantalla donde nos mostrara datos de las redes dentro del alcance. La imagen III.7.6 muestra como se ejecuta el escaneo de posibles objetivos.

Imagen III.7.6 Escaneo de objetivos.

De esta pantalla los datos importantes que debemos anotar son los siguientes:
ESSID: que es el nombre de la red (posible objetivo)
BSSID: MAC del posible objetivo.
CH: canal en el cual está transmitiendo.

La siguiente tabla III.7.1 nos muestra los datos que proporciona la ejecución del airodump-ng:

BSSID	PWR	Beacons	# Data	CH	MB	ENC	ESSID
00:13:10:30:24:9C	46	15	3416	6	54.	WEP	the ssid
00:09:5B:1F:44:10	36	54	0	11	11	OPN	NETGEAR

BSSID	STATION	PWR	Packets	Probes
00:13:10:30:24:9C	00:09:5B:EB:C5:2B	48	719	the ssid
00:13:10:30:24:9C	00:02:2D:C1:5D:1F	190	17	the ssid

Tabla III.7.1 Datos proporcionados por airodump-ng

BSSID
Dirección MAC del punto de acceso.

PWR
Nivel de señal reportado por la tarjeta. Su significado depende del controlador, pero conforme te acercas al punto de acceso o a la estación la señal aumenta. Si PWR == -1, el controlador no soporta reportar el nivel de señal.

Beacons
Número de paquetes-anuncio enviados por el AP. Cada punto de acceso envía unos diez beacons por segundo al ritmo (rate) mínimo (1M), por lo que normalmente pueden ser recogidos desde muy lejos.

Data
Número de paquetes de datos capturados (si es WEP, sólo cuenta IVs), incluyendo paquetes de datos de difusión general.
CH
Número de canal (obtenido de los paquetes beacon). Nota: algunas veces se capturan paquetes de datos de otros canales aunque no se esté alternando entre canales debido a las interferencias de radiofrecuencia.

MB
Velocidad máxima soportada por el AP. Si MB = 11, entonces se trata de 802.11b, si MB = 22 entonces es 802.11b+ y velocidades mayores son 802.11g.

ENC
Algoritmo de encriptación en uso. OPN = sin encriptación, "WEP?" = WEP o mayor (no hay suficiente datos para distinguir entre WEP y WPA), WEP (sin la interrogación) indica WEP estática o dinámica, y WPA si TKIP o CCMP están presentes.

ESSID
Conocida como "SSID", puede estar vacía si el ocultamiento de SSID está activo. En este caso airodump-ng tratará de recuperar el SSID de las respuestas a escaneos y las peticiones de asociación.

STATION
Dirección MAC de cada estación asociada. En la captura de más arriba se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).

Nota: podemos encontrar algunas variaciones según las versiones, pero lo fundamental siempre es lo mismo, que son los datos que hemos definido.

Una vez seleccionado los AP cerramos este Shell.

- Paso 10: Abrimos un Shell y en este escribimos el siguiente comando: airmon-ng star ath1 ch. En la imagen III.7.7 se muestra el comando utilizado para iniciar la tarjeta inalámbrica.
-

Donde:

ath1 (nombre de nuestra interface)

Ch: canal del objetivo

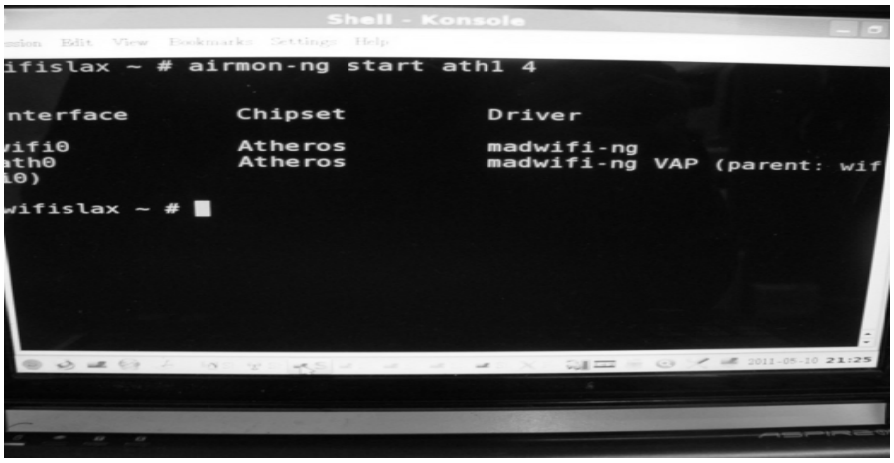

Imagen III.7.7 comando airmong-ng iniciando la interface wireless.

- Paso 11: en otro Shell que abrimos y en el que vamos a escribir el siguiente comando

Airodump-ng –w hola1 –c ath0

-w : indica que se va a guardar información en el archivo “hola1” (este nombre lo elegimos al azar)

Hola1: nombre del archivo

-c : es el canal atacado.

Ath0: interfaz inalámbrica

Esta parte del proceso es importante ya que de este archivo que se esta creando se va a extraer la clave y la pantalla que se ejecuta se observa en la imagen III.7.8

Nos abre una pantalla como la siguiente

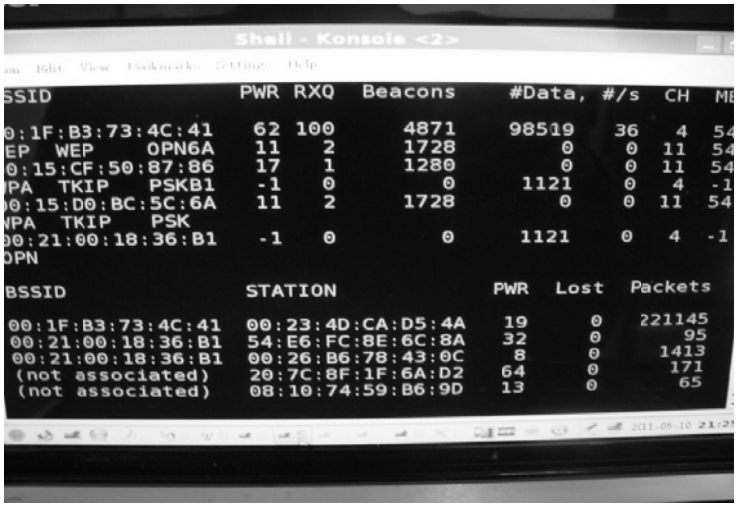

Imagen III.7.8 Airodump ejecutándose

- Paso 12: Abrimos nuevamente un Shell como observamos en la imagen III.7.9 en el cual vamos a escribir lo siguiente: aireplay-ng -1 30 -e ESSID -a BSSID -h MAC ath0

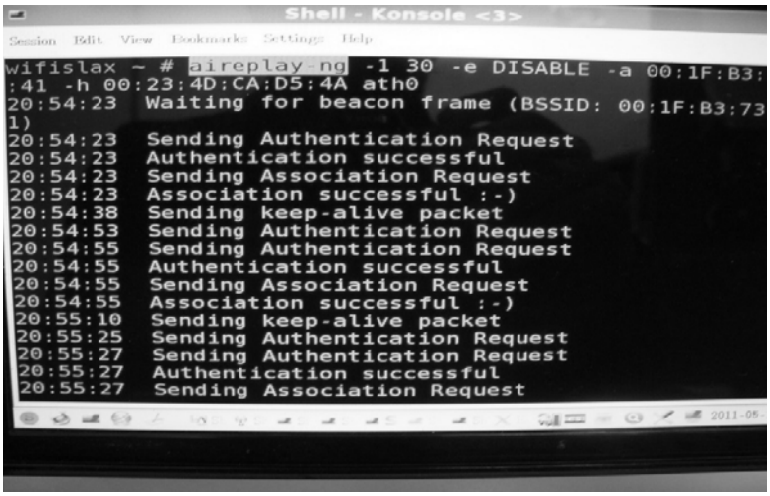

Imagen III.7.8 Ejecución de aireplay-ng

En donde:
-1 30: tipo de ataque e indica que enviara 30 paquetes de autentificación
-a BSSID: mac de la victima
ESSID: nombre de la red victima
-h MAC: indica la dirección propia falsa.

En este paso, para poder hacer el inyectado de paquetes va a autentificarse y asociarse con un cliente ficticio de la red.

- Paso 13: una vez asociados vamos a ejecutar otra consola Shell y en esta vamos a ejecutar el aireplay-ng que podemos observar en la imagen III.7.9 pero ahora con otros parámetros, esto es para acelerar el proceso de captura, mediante el inyectado de tráfico desde el equipo del atacante.

Hay que esperar a que se capture un paquete ARP-request, para luego inyectarlo nuevamente para que aumente el número de paquetes capturados.
Escribiremos el siguiente comando:

Aireplay-ng -3 -x600 -b BSSID -h MAC ath0

Donde:

-3 :indica el tipo de ataque
-x600 : permite indicar la velocidad con la que reinyecta Paquetes.

Nos mostrara una pantalla como la siguiente:

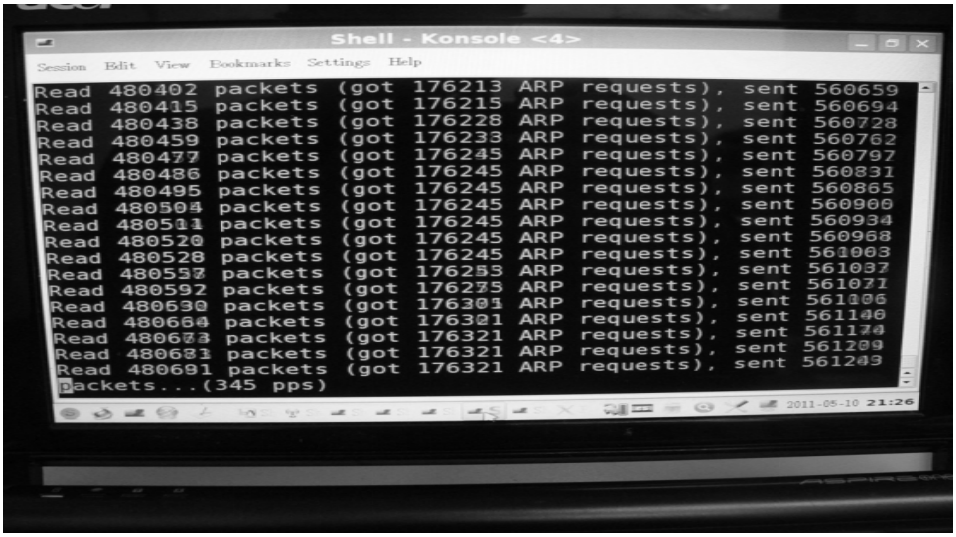

Imagen III.7.9 una vez autentificado se inyecta tráfico.

- Paso 14: Una vez que se ésta inyectando y capturando paquetes, se esperara a tener el número suficiente de ellos para poder ejecutar el

comando aircrack que después de analizar los paquetes guardados en el archivo generado con airodump-ng lograremos obtener la clave.

Escribiremos el comando siguiente:

Aircrack-ng -ptw hola1-01.cap

En la imagen III.7.10 se observa la pantalla que se abre al ejecutar un Shell nuevo e ingresar el comando para obtener la clave a través de la información obtenida en el proceso antes descrito, verificando el archivo creado al inicio del procedimiento.

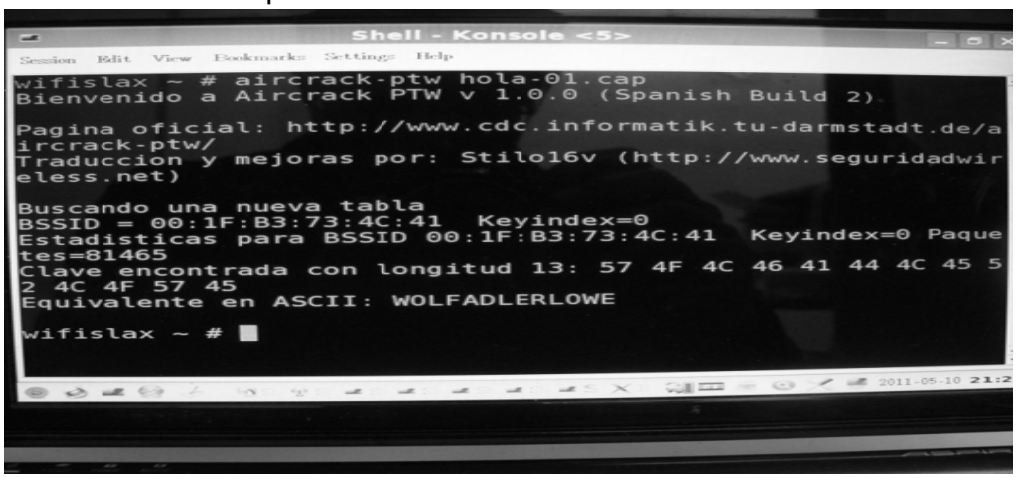

Imagen . III.7.10 Clave descifrada por el aircrack-ng

El proceso puede tardar varios minutos (aproximadamente 10min) para contraseña WEP de 64 bits y (aproximadamente 20min).
Para contraseñas WEP de 128 bits. La velocidad de descrifrado va a depender de la potencia del AP, la distancia de la computadora atacante.
A continuación se explica la primer pantalla de escaneo donde indicamos cada uno de los parámetros.

III.7.2 BACKTRACK

En general, otras herramientas como backtrack que esta basado en Linux, se utilizan comandos similares por ese motivo solo se utilizan estas pantallas. La imagen III.7.2.1 nos muestra las herramientas básicas de esta suite.

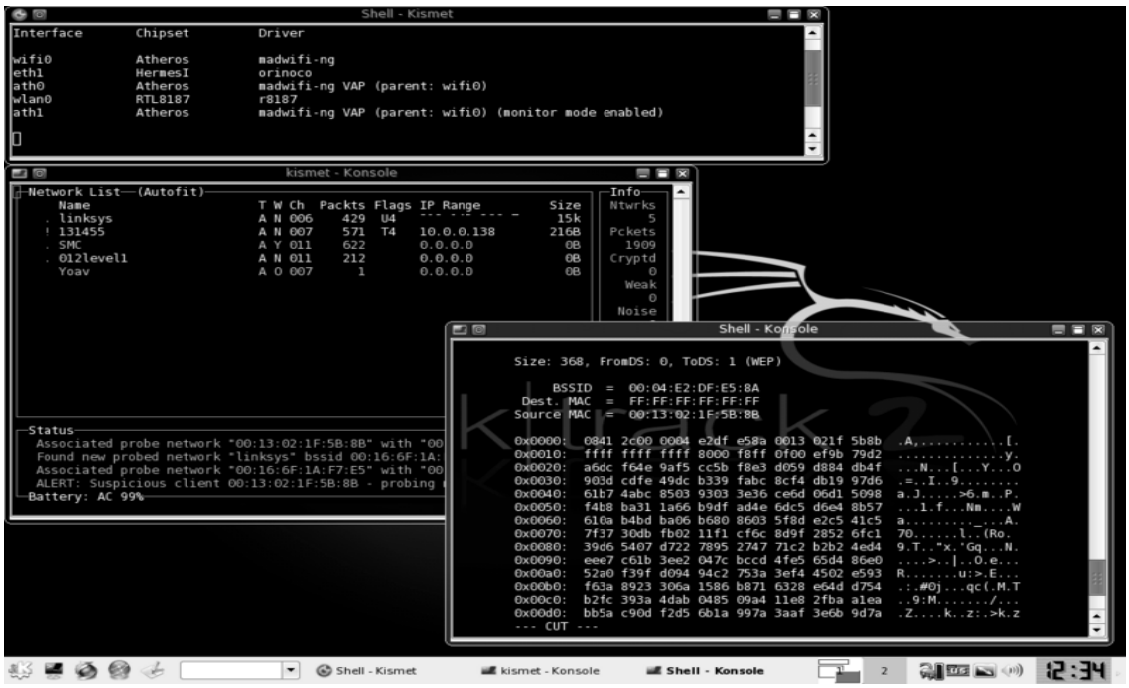

Imagen III.7.2.1 herramientas básicas

BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Backtrack le ofrece al usuario una extensa colección de herramientas completamente usables desde un Live CD o un Live USB por lo que no requiere una instalación para poder usarse. O bien, se ofrece la opción de instalar en un disco duro.

Entre las herramientas ofrecidas se encuentran:

- Aircrack-ng, Herramientas para auditoría inalámbrica

- Kismet, Sniffer inalámbrico
- Ettercap, Interceptor/Sniffer/Registrador para LAN
- Wireshark, Analizador de protocolos
- Medusa, herramienta para Ataque de fuerza bruta
- Nmap, rastreador de puertos
-

Y una larga lista de otras herramientas, que se agrupan en 11 familias:

- Recopilación de Información
- Mapeo de Puertos
- Identificación de Vulnerabilidades
- Análisis de aplicaciones Web
- Análisis de redes de radio (WiFi, Bluetooth, RFID)
- Penetración (Exploits y Kit de herramientas de ingeniería social)
- Escalada de privilegios
- Mantenimiento de Acceso
- Forenses
- Ingeniería inversa
- Voz sobre IP
- Según su registro de desarrollo, Remote Exploit liberó las siguientes versiones de BackTrack.

La tabla III.7.2.1 muestra dichas versiones por fecha de liberación.

Fecha	Lanzamiento
05/02/2006	BackTrack v.1.0 Beta
26/05/2006	The BackTrack 1.0 Final.
13/10/2006	BackTrack 2 primer beta.
19/11/2006	BackTrack 2 segundo beta.
06/03/2007	BackTrack 2 final.
17/12/2007	BackTrack 3 beta.
19/06/2008	BackTrack 3 final.
11/02/2009	BackTrack 4 beta.
19/06/2009	BackTrack 4 final.
09/01/2010	BackTrack 4 final.
08/05/2010	BackTrack 4 R1 final
22/11/2010	BackTrack 4 R2 final
10/05/2011	Backtrack 5 R1 FINAL

Tabla III.7.2.1 Versiones de Backtrack

III.7.3 Wifiway

Es una distribución de seguridad Wi-Fi basada en Linux From Scratch. Con Wifiway, podras realizar auditorías en nuestras redes inalámbricas Wi-Fi utilizando herramientas como Kismet, Aircrack, Airodump o Wireshark. La gran ventaja de la distribución WifiWay, radica en la integración de todas las herramientas necesarias a la hora de realizar ataques y análisis de redes inalámbricas Wi-Fi bajo GNU/Linux.

WifiWay a diferencia de WifiSlax su hermana pero basada en la distribución Slax, está creada desde cero, y está optimizada en tamaño y rendimiento, aunque soporta menor cantidad de hardware que WifiSlax.

Origen de la distribución www.wifiway.org

Entre los drivers más destacados soportados por la distribución WifiWay, se encuentra el de la tarjeta inalámbrica ipw3945 el que está parcheado para soporta la inyección y WifiWay fue una de las primeras distribuciones en soportar la inyección con este tipo de tarjeta inalámbrica. Además su integración con el sniffer Wi-Fi Kismet y el sencillo panel de control que permite en sencillos pasos realizar tareas que con otras distribuciones de seguridad requerirían una gran cantidad de pasos adicionales.

La imagen III.7.3.1 nos muestra las tres ventanas que se utilizan en esta suite para descifrar las claves wep

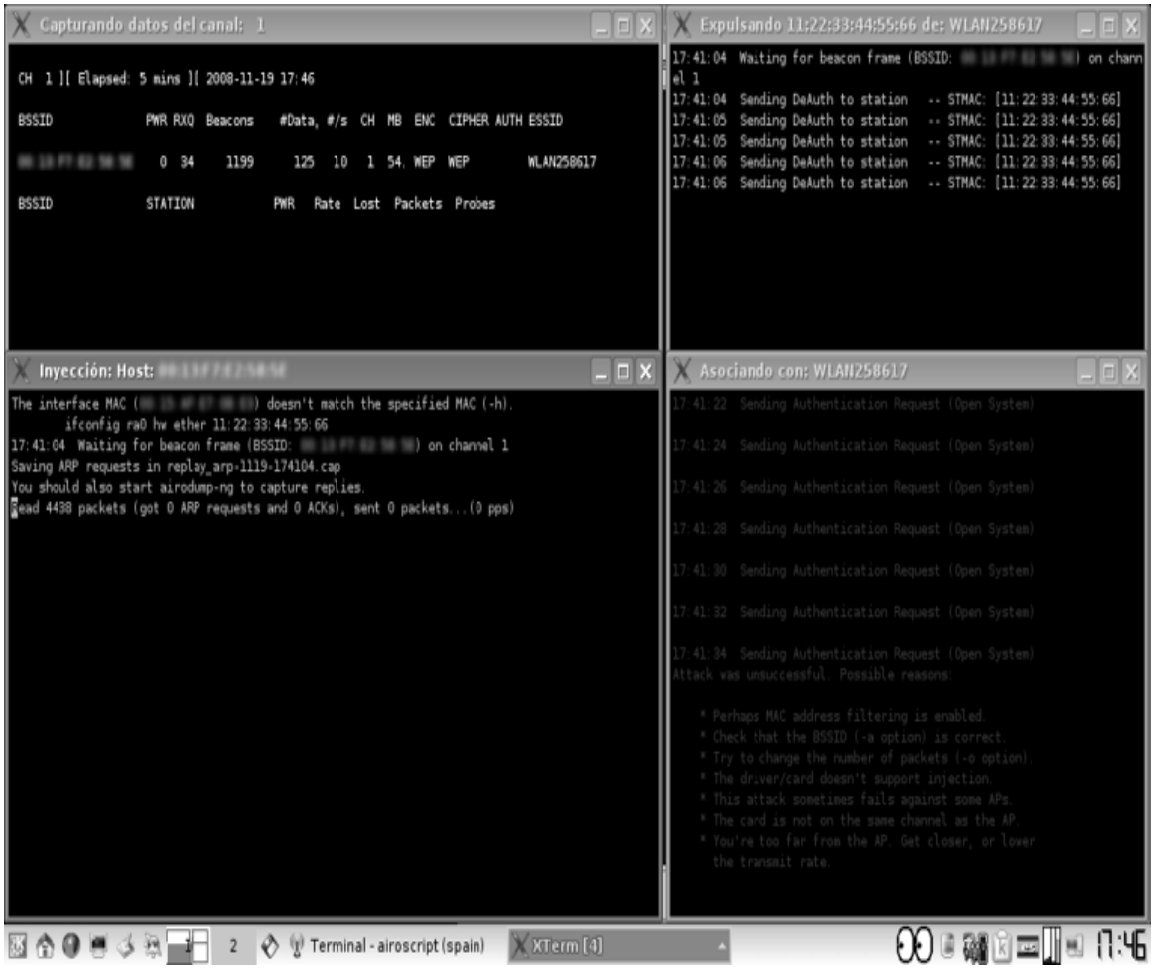

Imagen III.7.3.1 pantalla de las tres ventanas usadas por esta suite

Otra ventaja de WifiWay, es el idioma, Backtrack es una estupenda distribución de seguridad Wi-Fi, sin embargo, siempre es apreciada esa traducción a castellano que permite a los hispanohablantes conseguir un mayor entendimiento de qué es lo que se está cociendo en su instalación de Linux. Gracias al staff de Seguridad Wireless, podemos acceder a esta estupenda distribución de seguridad Wi-Fi que nos introducirá en el mundo de las auditorías y seguridad inalámbrica, y facilitará el acceso a las herramientas que realizarán la ruptura criptográfica del protocolo WEP y del protocolo WPA.

III.8 Seguridad

La seguridad de una red es el proceso por el que los recursos de información digitales son protegidos, los objetivos de la seguridad es mantener la integridad, proteger la confidencialidad y garantizar la disponibilidad. El avance en la tecnología incluyendo la inalámbrica ha generado un cambio en el estilo de vida y de trabajo de las personas y por tanto al usar las redes inalámbricamente el reto de la seguridad es mayor, debido a los riesgos que tienen las redes y muchos de estos se deben al pirateo, teniendo puntos débiles y vulnerabilidades propios de las WLAN que son explotados por personas novatas y también por las que tienen conocimientos en redes y programación. Como se mencionaba anteriormente el reto de la seguridad se vuelve mayor con el crecimiento del mercado móvil y ya un solo dispositivo firewall no siempre es suficiente, es necesario utilizar tecnologías y estrategias adicionales.

Las WLAN son vulnerables a ataques especializados, ya que muchos de estos ataques explotan los puntos débiles de la tecnología por que la seguridad en WLAN es relativamente nueva. Esto sumado a que en muchas ocasiones los dispositivos comercializados vienen con configuración básicas y son usados con estas sin el conocimiento de que en internet se pueden conseguir. Existiendo personas entusiastas, deseosas y cualificadas que se pueden beneficiar de cada una de las nuevas debilidades, en muchos casos y es muy común que estas vulnerabilidades sean compartidas públicamente, como sucede con las herramientas antes mencionadas, de las cuales podemos encontrar infinidad de manuales, videos o tutoriales en línea que muestran como atacar redes, obtener claves de acceso y robar literalmente los servicios de internet.

Como se había mencionado existen clases de ataques:

- Estructuradas
- No estructuradas
- Externas
- Internas

En el presente trabajo, respecto al ataque de redes se enfoco básicamente en el robo de internet que se lleva a cabo en gran cantidad en el ámbito domestico, siendo este tipo de amenazas del tipo no estructurado ya que se lleva a cabo en gran cantidad por individuos inexpertos o de escasos conocimientos, que se basan en los tutoriales, manuales o videos existentes en red. Y obviamente también los hay que tienen conocimientos mayores y motivaciones especificas, algunos por negocio se dedican a "romper" claves. Conocedores más a fondo de las vulnerabilidades pueden obtener mayores beneficios.

La mayoría de los incidentes de seguridad inalámbrica se generan ya que los dueños, administradores de las redes o servicios no implementan medidas o contramedidas disponibles; ya que no es sólo el identificar la vulnerabilidad sino también realizar acciones para contrarrestarlas y monitorear que este funcionando adecuadamente.

Existe algo llamado la rueda de la seguridad WLAN, como nos muestra en la imagen III.8.1 que es el proceso de seguridad de forma continua y eficaz. Este método promueve la aplicación de medidas y se promueve el volver a probar y aplicar una actualización continua.

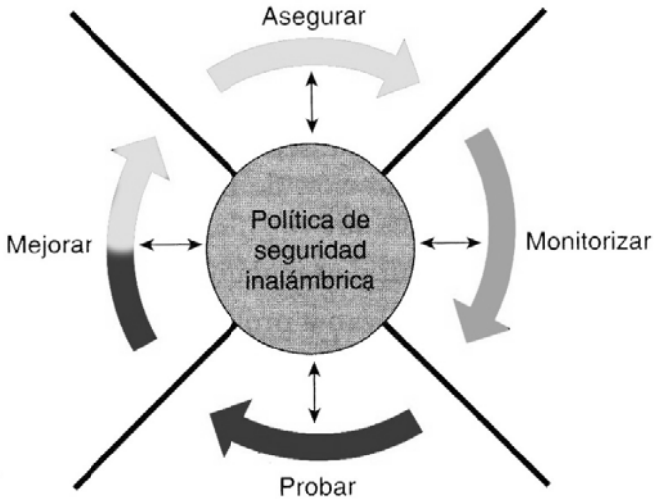

Imagen III.8.1 Rueda de la Seguridad en WLAN

La Rueda de la Seguridad se divide en 4 pasos como lo muestra la figura anterior y son los siguientes:

1. ***Asegurar***. Implementación de soluciones de seguridad para detener o evitar accesos así como también actividades no autorizadas, utilizando lo siguiente:
    - Autenticación.
    - Encriptación o cifrado (WEP, WPA, WPA2).
    - Filtros de tráfico.
    - VLAN y VPN.
    - Deshabilitar o asegurar servicios.
    - Control del área de cobertura de la WLAN.

2. ***Monitorizar.*** En esta etapa implica las siguientes:
    - Detectar violaciones a las políticas de seguridad de la WLAN.
    - Auditar el sistema implicado, anotar registros y detectar intrusiones en tiempo real.
    - Detectar los AP o equipos conectados de forma ilegal.
    - Validar lo implementado en el paso 1.

3. ***Probar.*** Este paso valida la eficacia de la política de seguridad de la WLAN mediante la auditoria de los sistemas y la búsqueda de vulnerabilidades inalámbricas y cableadas.

4. **Mejorar**. Este paso implica utilizar la información obtenida en el punto 3 para mejorar la implementación de WLAN y ajustar la política de seguridad a medida que se identifiquen las vulnerabilidades y riesgos.

La seguridad como se ha mencionado anteriormente con el avance de la tecnología la preocupación a aumentado. Hoy en día con el relativamente bajo costo de los dispositivos ha causado que se deban usar mayores medios de seguridad que ya se han mencionado (protocolos de capa superior), VLAN, VPN, Servidores RADIUS, etc.

Para una red WLAN domestica o de un tamaño relativamente pequeño se puede utilizar el llamado filtrado MAC que a pesar de no estar definido en las especificaciones 802.11, muchos fabricantes tienen esta opción de autentificación implementada. Mediante una lista de las direcciones MAC validas el AP puede controlar el acceso, este control puede ser tedioso ya que debe guardarse un inventario exacto y los usuarios deben informar sobre robos o pérdidas de los adaptadores o de los mismos equipos. LA MAC no es un mecanismo infalible ya que como se mostro anteriormente existen formas de duplicar estas direcciones, aunque se requiere de un proceso para lograrlo, puede suceder que provocando un ataque de negación de servicio se logre detectar una MAC valida y esto una vez hecho se tenga ya una forma de autentificarse al AP de forma "legal" este tipo de ataque es el llamado Spoofing MAC. Este tipo de Filtros se debe utilizar como complemento de otras opciones de seguridad.

Los AP inalámbricos deben ser asegurados, en las redes pequeñas o domesticas pueden ser suficientes la combinación de las siguientes opciones:

- Utiliza sólo la conexión inalámbrica cuando sea necesaria (cableado difícil o inaccesible).
- Evitar la publicación o emisión del ESSID (nombre de la red).
- Utilizar WPA o WPA2
- Utilizar contraseñas robustas.
- Utilizar si el AP lo permite Filtro MAC (utilizado en redes de pocos equipos).
- Utilizar en la medida que sea posible asignación de ip fijas.
- Verificar periódicamente las estadísticas de conexión al AP así como monitorear el funcionamiento de la red para identificar posibles intrusiones.

En nuestra red se utilizan estas medidas de seguridad, siguiendo la rueda de la seguridad.

El router utilizado permite el filtrado MAC, a continuación se muestran las pantallas. En la imagen III.8.2 se muestra la interface del routeador en el área de wireless en la cual nos da las opciones de filtrar a través de MAC.

Imagen III.8.1 Interface de router para configurar filtro MAC.

En esta interface nos da dos opciones en una nos indica que va a permitir el acceso a las direcciones MAC que se encuentren en la lista. En las pruebas realizadas al introducir las MAC permitidas las que no se encontraban en esa lista pero conocían la clave, se lograron autentificar y conectar al AP pero no tuvieron acceso al servicio de internet. En la imagen III.8.2 se muestra un ejemplo de dicha configuración.

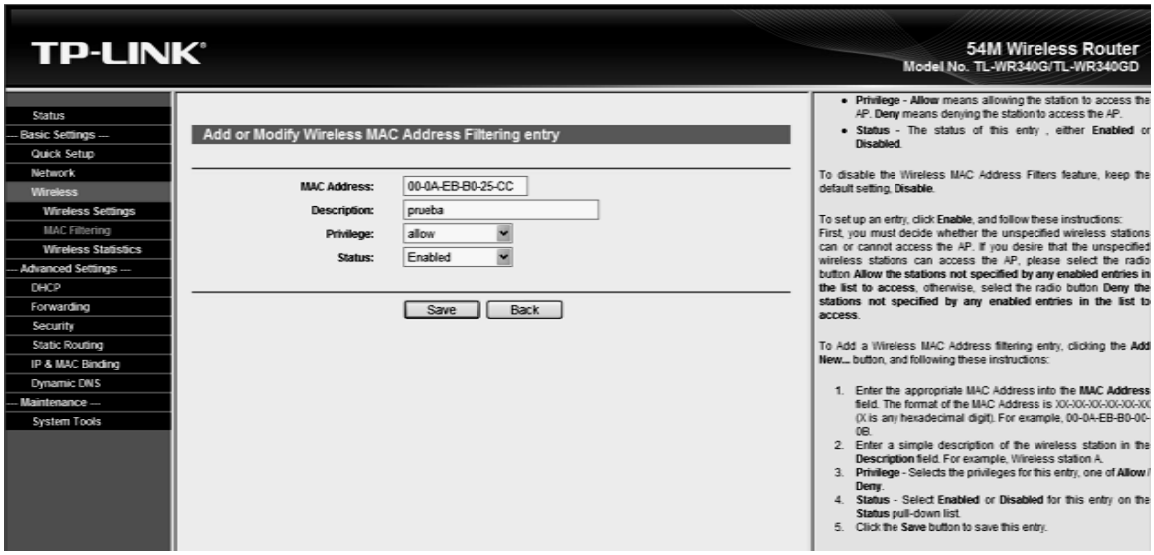

Imagen III.8.2 Configuración de filtro MAC

Este filtro fue útil en la red implementada, sin embargo existen otros tipos de filtro como por ejemplo, filtro de protocolo IP, filtro de puerto; los filtros de protocolo impiden o permiten el uso de protocolos específicos a través del AP. Se pueden configurar filtros de un protocolo individual y activarlos para una o más VLAN.

CONCLUSIONES

En la actualidad la tecnología avanza a pasos enormes y desgraciadamente la inseguridad en las redes WLAN también ya que ésta es relativamente nueva y aún presenta vulnerabilidades por el medio en el que viaja la información, aunque existen opciones de seguridad sobre todo para las redes empresariales o de tamaños grandes, se queda un poco rezagado el tema en cuanto a las redes domesticas también nombradas "SOHO" (Small Office Home Office) que pude tratarse de una oficina pequeña o a una oficina montada en casa. En general, podría considerarse con esta denominación a cualquier conformación de oficina o grupo de profesionales independientes con una capacidad de hasta 10 trabajadores.

En la presente investigación e implementación de una red de este tipo, se pudo comprobar que con software diseñado para auditar redes wireless se logra con los dispositivos adecuados autentificarse y capturar información para almacenarla en un archivo al cual posteriormente se le aplica otra herramienta y comandos adecuados que después de un tiempo nos proporciona la contraseña para poder acceder al servicio de internet.

En la actualidad mediante la web se puede uno documentar y obtener este tipo de software sin ningún costo o asistir a los lugares en los cuales comercian con software y obtener una suite completa de herramientas, también podemos encontrar tutoriales y videos los cuales proporcionan el proceso que se debe seguir.

La real amenaza comienza cuando alguna persona con la inquietud y los ánimos de obtener un servicio "gratuito" y considerando que es un acceso ilegal también podría o debería considerarse un delito; realiza el ataque a AP que debido a la ignorancia o la incorrecta configuración están expuestos a este tipo de ataques.

En la presente investigación se llevo a cabo el "ataque" a un modem 2wire propio con servicio de Prodigy Infinitum instalado en la red WLAN antes implementada y descrita pero también se llevo a cabo las siguientes pruebas con un cable modem Motorola proporcionado con el servicio de cablevisión; llevando la aplicación de la WLAN al ámbito domestico; se comprobó que existen gran número de este tipo de personas, se logró dejando un AP Motorola sin ningún tipo de protección y en minutos había "usuarios" conectados disfrutando del servicio gratuito; al configurar dicho

dispositivo con una clave WEP volvió a ser víctima de un ataque mediante esta vulnerabilidad pero se detecto un número muy limitado de atacantes comparado con los que se autentificaron anteriormente, se identificaron sus MAC de dichos atacantes (siguiendo la rueda de seguridad) y posteriormente se detecto que lograban autentificarse buscando llevar a cabo un ataque más estructurado, en ese momento se opto por cambiar el tipo de protección pasando a WPA, con esta medida se logro disminuir el número de “atacantes” y los existente se pudieron eliminar al conectar el router vía cable Ethernet al cable modem, se elimino el wireless del dispositivo Motorola quedando como único AP el router que se configuro con protocolo WPA/WPA2 y se deshabilito en que se publicara o emitirá el ESSID aun en este paso se pudo detectar un intento de una MAC ya anteriormente identificada, se logro autentificar ya que no se había reiniciado el router, al llevar a cabo este paso, se evito que se autentificara nuevamente.

Finalmente se utilizo el filtro MAC, logrando con esto cerrar aún más el cerco de seguridad en nuestra red Domestica. Se llevo a cabo un nuevo ataque controlado y se intento autentificarse en varias ocasiones con las herramientas utilizadas anteriormente, en ambas se mostraba que el ataque no se pudo llevar a cabo y nos indicaba un listado de posibles causas del error en el ataque.

Finalmente se puede decir que la seguridad en las redes WLAN debe ir siendo más compleja de acuerdo a la misma estructura de la red, y con el avance de la tecnología se presentaran nuevos retos a vencer.

En la actualidad las claves basadas en WEP y las que vienen por default ya son obsoletas ya que como se menciono para este tipo de claves también se pueden descifrar a través de teléfonos celulares. Esto nos muestra que el avance de las técnicas avanzan al mismo paso que la tecnología.

GLOSARIO

- **802.11a.** Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHz.
- **802.11b.**Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2,4 GHz.
- **802.11g.**Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 2,4 GHz y con compatibilidad con versiones anteriores con dispositivos 802.11b.
- **Ad-hoc.** Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.
- **AES (Estándar avanzado de cifrado).** Técnica de cifrado de datos simétrica de bloque de 256 bits.
- **Ancho de banda.** Capacidad de transmisión de un dispositivo o red determinado.
- **Backbone**. El término backbone también se refiere al cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.
- **Banda ancha.** Conexión a Internet de alta velocidad y siempre activa.
- **Banda ISM.** Banda de radio utilizada en las transmisiones de redes inalámbricas.
- **Bit (dígito binario).** La unidad más pequeña de información de una máquina.
- **Byte.** Una unidad de datos que suele ser de ocho bits.
- **Cifrado.** Es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos puedan realizar una interpretación precisa.
- **Conmutador.** Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.
- **CSMA/CA (Acceso múltiple de detección de portadora).** Un método de transferencia de datos que se utiliza para prevenir una posible colisión de datos.

- **CSMA/CD.** Es el acrónimo de Carrier Sense Multiple Acces/Collision Detect. Esto quiere decir que Ethernet censa el medio para saber cuando puede acceder, e igualmente detecta cuando sucede una colisión (p.e. cuando dos equipos trasmiten al mismo tiempo).
- **DDNS (Sistema dinámico de nombres de dominio).** Permite albergar un sitio Web, servidor FTP o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.
- **DHCP (Protocolo de configuración dinámica de host).** Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.
- **Dirección IP dinámica.** Dirección IP temporal que asigna un servidor DHCP.
- **Dirección IP.** Dirección que se utiliza para identificar un equipo o dispositivo en una red.
- **Dirección IP estática.** Dirección fija asignada a un equipo o dispositivo conectado a una red.
- **DNS (Servidor de nombres de dominio).** La dirección IP de su servidor ISP, que traduce los nombres de los sitios Web a direcciones IP.
- **DSL (Línea de suscriptor digital).** Conexión de banda ancha permanente a través de las líneas de teléfono tradicionales.
- **DSSS (Espectro de dispersión de secuencia directa).** Transmisión de la frecuencia con un patrón de bit redundante que se traduce en una menor probabilidad de que la información se pierda durante dicha transmisión.
- **EAP (Protocolo de autenticación extensible).** Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.
- **EAP-PEAP (Protocolo autenticación extensible-Protocolo autenticación extensible protegido).** Método de autenticación mutua que utiliza una combinación de certificados digitales y otros sistemas, como contraseñas.
- **EAP-TLS (Protocolo de autenticación extensible-Seguridad de la capa de transporte).** Método de autenticación mutua que utiliza certificados digitales. Encadenamiento de periféricos Método utilizado para conectar dispositivos en serie, uno tras otro.
- **Enrutador**. Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.
- **Enrutamiento estático.** Reenvío de datos de una red a través de una ruta fija.

- **Ethernet.** Protocolo de red estándar de IEEE que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.
- **Firewall.** Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.
- **Firmware.** El código de la programación que ejecuta un dispositivo de red. Fragmentación Dividir un paquete en unidades menores al transmitirlas a través de un medio de red que no puede admitir el tamaño original del paquete.
- **FTP (Protocolo de transferencia de archivos).** Protocolo estándar de envío de archivos entre equipos a través de redes TCP/IP e Internet.
- **Gateways.** Equipos para interconectar redes.
- **Ghz**. Equivale a 109 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.
- **Hardware.** El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información.
- **HTTP (Protocolo de transferencia de hipertexto).** Protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.
- **Hz (Hercio).** El hertz o hertzio (también se le puede llamar Hercio) es la unidad de frecuencia del Sistema Internacional de Unidades. Existe la división de este término en submúltiplos y múltiplos documentados en un Sistema Internacional de Unidades.
- **IEEE.** Fundado en 1884, es una organización profesional sin fines de lucro, compuesta por más de 380.000 miembros en 150 países, organizados geográficamente en diez Regiones, con más de 340 Secciones y unas 1400 Ramas Estudiantiles. Juega un papel crítico en el desarrollo de estándares, la publicación de trabajos técnicos, el patrocinio de conferencias. El IEEE ha producido muchos estándares ampliamente utilizados, como el grupo 802.x de los estándares LAN y MAN.
- **IPCONFIG (Internet Protocol Configuration).** Utilidad de Windows 2000 y XP que muestra la dirección IP de un dispositivo de red concreto.
- **IPSec (Internet Protocol Security).** Protocolo VPN utilizado para implementar el intercambio seguro de paquetes en la capa IP.
- **Itinerancia**. Capacidad de transportar un dispositivo inalámbrico desde el alcance de un punto de acceso hasta otro sin perder la conexión.
- **Máscara de subred.** Código de dirección que determina el tamaño de la red.

- **Mbps (Megabits por segundo).** Un millón de bits por segundo, unidad de medida de transmisión de datos.
- **Mhz.** Equivale a 106 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.
- **Modelo OSI**. se basa en estructurar el proceso de comunicación en siete áreas independientes a las que llama capas (física, enlace, red, transporte, sesión, presentación y aplicación).
- **Módem de cable.** Un dispositivo que conecta una equipo a la red de la televisión por cable que a su vez se conecta a Internet.
- **Modo infraestructura.** Configuración en la que se realiza un puente entre una red inalámbrica y una red con cable a través de un punto de acceso los equipos móviles se comunican a través del punto de acceso.
- **Nodo**. Unión de red o punto de conexión, habitualmente un equipo o estación de trabajo.
- **Paquete.** Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.
- **Phishing.**Tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial.
- **Ping (Buscador de paquetes de Internet).** Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.
- **Pirata informático.** Un término de jerga para un entusiasta informático. También hace referencia a los individuos que obtienen acceso no autorizado a sistemas informáticos con el fin de robar y corromper datos.
- **PPTP (Protocolo de túnel punto a punto).** Protocolo VPN que permite tunelar el protocolo Punto a punto (PPP) a través de una red IP. Este protocolo se utiliza también como tipo de conexión de banda ancha en Europa.
- **Puente.** Dispositivo que conecta dos tipos diferentes de redes locales, como por ejemplo una red inalámbrica a una red Ethernet con cable.
- **Puerta de enlace.** Un dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles.
- **Puerta de enlace predeterminada.** Dispositivo que redirecciona tráfico de Internet desde su red de área local.
- **Puerto.** Punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.
- **Punto de acceso.** Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red

con cable. También se utiliza para ampliar el alcance de una red inalámbrica.

- **Red Punto a Multipunto.** Aquellas en las que cada canal de datos se puede usar para comunicarse con diversos nodos.
- **Red Punto a Punto.** Aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos.
- **Red.** Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.
- **Red troncal.** Parte de una red que conecta la mayoría de los sistemas y los une en red, así como controla la mayoría de datos.
- **Rendimiento.** Cantidad de datos que se han movido correctamente de un nodo a otro en un periodo de tiempo determinado.
- **Router**. Enrutador, es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.
- **Routing.** El proceso de mover un paquete de datos de fuente a destino, normalmente se usa un "Router".
- **RTP (Protocolo de tiempo real).** Un protocolo que permite especializar aplicaciones tales como llamadas telefónicas, vídeo y audio a través de Internet que están teniendo lugar a tiempo real.
- **RTS (Request To Send).** Método de red para la coordinación de paquetes grandes a través de la configuración Umbral de solicitud de envío (RTS).
- **Sniffer.** Un sniffer es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.
- **SOHO.** (Oficina pequeña/oficina doméstica)
- **SSID (Service Set IDentifier).** Nombre de su red inalámbrica.
- **TCP (Transport Control Protocol).** Un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.
- **TCP/IP (Transport Control Protocol / Internet Protocol).** Protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.
- **Telnet**. Comando de usuario y protocolo TCP/IP que se utiliza para acceder a equipos remotos.
- **TFTP (Trivial File Transfer Protocol).** Versión del protocolo FTP TCP/IP que utiliza UDP y no dispone de capacidades de directorio ni de contraseña.

- **TKIP (Temporal Key Integrity Protocol).** Protocolo de cifrado inalámbrico que cambia periódicamente la clave de cifrado, haciendo más difícil su decodificación.
- **TLS (Transport Layer Security).** Protocolo que garantiza la privacidad y la integridad de los datos entre aplicaciones cliente/servidor que se comunican a través de Internet.
- **Topología**. Distribución física de una red.
- **UDP (User Datagram Protocol).** Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.
- **URL (User Resource Locator).** Dirección de un archivo situado en Internet.
- **VPN (Red privada virtual).** Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet.
- **WAN (Wide Area Network).** Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es Internet.
- **WECCA.** Es una asociación internacional sin fines de lucro formada en 1999. Se formo para certificar la interoperabilidad de los productos WLAN basados en la especificación IEEE 802.11.
- **WEP (Wired Equivalent Privacy)**. Protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro. Para permitir la comunicación entre los equipos y el enrutador se utiliza una clave compartida (similar a una contraseña). WEP ofrece un nivel básico (pero satisfactorio) de seguridad para la transferencia de datos a través de redes inalámbricas.
- **Wireless**. Tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas.
- **WLAN (Wireless Local Area Network).** Grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica.
- **WPA (WiFi Protected Access).** Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. Asegura la transferencia de datos de forma inalámbrica mediante la utilización de una clave similar a WEP. La robustez añadida de WPA es que la clave cambia de forma dinámica. La clave, en continuo cambio, dificulta que un pirata informático pueda conocer la clave y obtener acceso a la red.

- **WPA2 (WiFi Protected Access 2).** WPA2 es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.
- **WPA-Enterprise**. Versión de WPA que utiliza las mismas claves dinámicas que WPA-Personal y también requiere que todo dispositivo inalámbrico esté autorizado según lista maestra, albergada en un servidor de autenticación especial.
- **WPA-Personal.** Versión de WPA que utiliza claves de cifrado en constante cambio y de mayor longitud para complicar el proceso de su decodificación.

BIBLIOGRAFÍA

Academia de Networking de Cisco Systems,
Fundamentos de redes inalámbricas,
trad.José Manuel Diaz,
Pearson 2008.

Wifi Instalación, Seguridad y Aplicaciones.
Carballar, José.
Alfaomega, 2007.

Introducción a las Redes Inalámbricas
Adam Engst, ,
Anaya

Guía de Campo de WiFi
Gómez López, Julio,
Rama, 2008.

Comunicaciones en redes WLAN,
Huidobro Moya, José M, Roldan Martínez David
Limusa 2006.

WiFi, lo que se necesita conocer
Carballar, José Antonio
Alfaomega 2010.

WLAN, Fundamentos y Aplicaciones de seguridad
Andreu,Fernando. Pellejero, Izaskun.
Marcombo,2006

http://www.tp-link.com/es/products/productDetails.asp?pmodel=TL-WR340G

http://wifiway.red-inalambrica.net/

http://es.wikipedia.org/wiki/Slax

http://www.wifislax.com

http://es.wikipedia.org/wiki/WLAN

http://www.informaticamoderna.com/Redes_inalam.htm

http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Vulnerabilidades-de-las-redes-WIFI.php

http://imstrangeandilikeit.blogspot.com/2007/12/mac-spoofing.html

http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf

http://www.cgmenor.compdfredesinalambricas.pdf

http://dns.bdat.net/seguridad_en_redes_inalambricas/c113.html