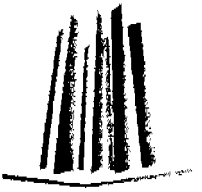


INGENIERIA MECANICA ELECTRICA

INGENIERIA EN COMPUTACIÓN

TESIS

Diseño, Implantación y Puesta a Punto de una Red Inalámbrica basada en el Protocolo 802.11x en el Laboratorio de Comunicaciones L-3 de la Escuela Nacional de Estudios Profesionales "Aragón"; de la Universidad Nacional Autónoma de México.

RAUL VEGA SALOME
CLAUDIA CONTRERAS GUADARRAMA

ABRIL 2005

Claudia Contreras

Guadarrama

8 Abril 2005

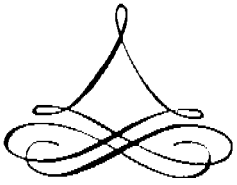
FIRMA

Raul Vega Salame

8 Abril 2005

FIRMA

Es un paso, o tal vez el Final
Puede ser el fin o el inicio de Algo
Aun recuerdo cuando todo Comenzó
Y aun mantengo el mismo gusto por hacer las Cosas
Siempre he preferido el Trabajo, eso lo aprendí de mi Familia
Pero también Aprendí muchas cosas en la Universidad
Aprendes cosas que no sabias que podrías hacer
Pero también aprendes cosas malas, y aprendí a distinguirlas
Mi Papa me lo enseño, también le debo la Paciencia y la Tolerancia
Auque mi Mama me enseño a luchar y mantenerme alegre Siempre
De mi Familia Aprendí la Unión, también los Valores
Lo demás me lo enseño la vida y creo que también es Importante
Siempre estaré agradecido por haber podido Estudiar
De conocer mucha gente y muchos Amigos
Tengo la fortuna de tener verdaderos Amigos
De conocer la amistad, el Amor y muchas cosas mas
Por eso puedo decir que aun no Termino
Que aun tengo la necesidad de seguirme Superando
Y tengo la oportunidad de Hacerlo



Agradecimientos

A Mis Padres: Raul Vega y Maria Salomè.

A Mis Hermanos: Yazmín y Javier.

A Mi Abuelita: Amparo Vázquez.

A Mi Madrina: Maria del Socorro Vega (q.e.p.d ✞).

A Mis Tíos: Pedro, Miguel, Manuel, Joel, Luis, Agripin, Margarito, Rodolfo, Gloria, Rafaela, Marta, Yolanda, León, Francisco, Alfonso, Patricia, Sofía, Silvia, Leonarda, Agustina.

A Mis Primos: Enrique, Abelina, Gema, Rosalin, Amparo, Marisela, Miguel Angel, Mario, Gabriela, Pedro Jr, Sarahi, Diana, Erika, Alejandra, Guadalupe, Maricruz, Cristian, Rafael, Miriam, Johann, Delia y los que faltan.

A Mi Cuñado: Mario.

A Mi Sobrino: Mario Jr.

Al Amor de mi Vida: Claudia.

A mis Amigos: Samuel, Eduardo C, Roberto L, Víctor E, Alejandro Q, Alejandro, Felipe, David, Enrique G, Enrique H, Esteban, Adrián, Juan, Ramón, Narciso, Abundio, Noe, Rodolfo, Manuel, Jorge, Rubén, Ilich, Homero, Roberto G. etc

A mis Amigas: Alejandra, Marcela, Jessica, Andrea, Gabriela, Dulce, Carolina, Juanita, Adela, Elizabeth, Alma, etc

A mi Asesor: David Terán

A todos mis Maestros

A la ENEP Campus Aragón

A La Universidad

A los que olvide.....a los que omití.....a mis enemigos.

Gracias.....

JUSTIFICACIÓN.

Cuando se precisa movilidad en las comunicaciones, el cable se convierte más en un inconveniente que en una ayuda. Depender de un enlace físico como es el hilo, en cualquiera de sus modalidades y naturaleza, supone una seria restricción para conseguir una plena libertad de movimientos.

Para salvar las restricciones impuestas en la utilización del cable, las conexiones inalámbricas se convierten en la alternativa perfecta por su habilidad intrínseca para evitar obstáculos. Dentro del enorme horizonte de las comunicaciones sin hilos las redes inalámbricas van ganando rápidamente adeptos como una tecnología madura y fiable, que permite resolver los inconvenientes derivados de la propia naturaleza del cable como medio físico de enlace en las comunicaciones, muchos de ellos de vital importancia en el entorno de trabajo habitual.

Las instalaciones temporales son un ejemplo de una situación en la que una red inalámbrica tiene sentido o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso del cableado, lo que convierte a las redes inalámbricas en una importante alternativa. La disponibilidad de conexiones y redes LAN inalámbricas puede ampliar la libertad de los usuarios de la red a la hora de resolver varios problemas asociados a las redes con cableado fijo y, en algunos casos, incluso reducir los gastos de implementación, mantenimiento y reestructuración de las redes. Sin embargo, a pesar de esta libertad, las redes LAN inalámbricas traen consigo un nuevo conjunto de desafíos.

Pues bien, estos son solo ejemplos de los supuestos en los que la tecnología WLAN (Wireless LAN) puede ser una solución, pero es muy amplio el abanico de posibilidades que una tecnología como esta nos ofrece, y muy extenso el mercado que ofrece al sector de las telecomunicaciones.

Pero, ¿qué es una red local inalámbrica o WLAN? ¿Qué estructura utiliza? ¿Qué equipos son necesarios y a qué costo? Definiéndola rápidamente, esta tecnología ofrece un acceso a terminales de datos mediante **enlaces punto a punto o bien punto a multipunto a redes LAN** (Local Area Networks), dicho de otro modo, son las redes de datos que hasta ahora se han venido haciendo mediante cableado estructurado pero sin cables, utilizando el aire como medio de transmisión.

Esto es especialmente útil para redes de gran extensión que deban enlazar dos puntos distantes o bien para enlazar dos edificios mediante tecnología IP. Hasta ahora, para realizar enlaces de datos entre diferentes

edificios se ha venido utilizando líneas telefónicas que suponían lamentablemente, un elevado costo para la transmisión de datos.

El estándar más representativo y que marca las características técnicas de la tecnología WLAN es el denominado Wi-Fi (Wireless Fidelity) el cual está redactado por la IEEE en su documento 802.11 y actualmente tiene 3 versiones: 802.11b, 802.11a y 802.11g. Siendo el primero el líder del grupo. Algunos de los puntos que señala el estándar principal son:

Velocidad de transmisión de datos: 11 Mbps a través de DSSS
Frecuencia de transmisión: 2.4 GHz con modulación DBPSK o DQSK.
Seguridad: WEP (Wireless Equivalent Privacy Algorithm) algoritmo de codificación de datos de 128 bits y algoritmo de encriptación RC4.

Esto permite la codificación en el medio RF y evita la intromisión de clientes no deseados. Además se pueden incorporar los mecanismos de seguridad aplicables a cualquier otro tipo de red de datos, como pueda ser un firewall, control de acceso por MAC (dirección física de dispositivo única para cada equipo y marcado por el fabricante), VPN's[1], etcétera.

Se puede observar dos tipologías para este tipo de redes: punto a punto (el caso de enlazar una vivienda con una oficina); y punto – multipunto (proveer acceso a una serie de terminales en un recinto público previo pago de tarjeta de acceso.) La diferencia entre ambas es la capacidad de conexiones que van a tener los dispositivos que se habiliten para tal efecto.

En su vertiente más sencilla, la red punto a punto puede ser la formada por dos terminales equipados con tarjetas de red adaptadoras para WLAN, de modo que pueden poner en marcha una red independiente siempre que estén en el radio de cobertura de las tarjetas. Esto se llama una red de igual a igual *("peer to peer".)*

En el caso que se quiera unir dos redes de área local (LAN), o dos terminales de datos mediante un Enlace de Radio Frecuencia (RF) bastará con los puentes de red que unen dos segmentos de la misma *("Bridges")* y las antenas emisoras/receptoras para realizar el enlace. Estas antenas pueden ser tipo Yagi (normalmente con redomo) o de tipo panel, pueden llegar a cubrir varias decenas de millas dependiendo de la potencia de salida con la que se les equipe, pero es poco usual tener que cubrir distancias mayores a unos pocos kilómetros.

Una red punto a punto entre edificios puede proporcionar la conectividad suficiente para compartir recursos, acceder a servidores, tener salida a Internet a través de enlaces, y en realidad todo aquello que se podría hacer con un equipo

[1] VPN. -Virtual Private Network.

que estuviera físicamente conectado a la red. La tipología punto – multipunto, en cambio presenta una dificultad técnica mayor pero, en contrapartida, toda una gama de funcionalidades que le aportan un mercado mucho más amplio de venta.

Este tipo de redes se diseña a modo de células controladas por los denominados Puntos de Acceso *("Access-Points".)* Éstos son la interfase que separa la red realizada mediante cableado y la red inalámbrica. Las funcionalidades que aportan a la red son básicamente **movilidad** (un dispositivo con tarjeta de red WLAN puede ir cambiando de *Access Point* mientras se mueve por el edificio o recinto servido), **autenticación y seguridad** (el dispositivo que ingresa en la red debe estar autorizado por la misma), y **cobertura suficiente** (el equipo debe tener las características técnicas de transmisión/recepción suficientes para cubrir la celda asignada.)

De este modo, una topología de red típica para este tipo de redes sería como la que muestra la figura:

Donde puede observarse el cambio de medio físico a través del *access point*. Estos dispositivos, además actúan como mediadores en el tráfico de la red con la celda vecina más inmediata, esto es, en los terminales que tienen asignados (del orden de 15 a 50 terminales.) En este sentido, cuando se diseña una red con diferentes celdas, deben solaparse las coberturas de los diferentes AP's (Access Points) de modo que el acceso a red se produzca sin cortes por parte del dispositivo móvil *(roaming.)*

Los puntos de acceso tienen un rango de cobertura finito que va desde los 150 m en lugares cerrados a los 300 metros en lugares abiertos, sin embargo habrá que tener en cuenta la tipología de la edificación a cubrir para diseñar un número determinado de células, como en cualquier sistema de comunicaciones móviles.

¿Qué terminales pueden acceder a este tipo de redes? Pues todos aquellos que dispongan de un adaptador de red con tecnología inalámbrica (por

ejemplo IEEE 802.11b) y que estén dentro del radio de cobertura de una de las celdas.

Así, pueden ser elementos de este tipo de redes, Terminales Informáticos (computadoras convencionales o equipos Macintosh), Asistentes Personales Digitales (PDA), *Data Phones*, Lectores de datos, o cualquier terminal que sea capaz de mandar paquetes IP a través de un adaptador de red, aquí es donde radica la potencia de esta tecnología para desarrollar nuevos productos con tecnología IP y como alternativa a otros protocolos inalámbricos que ya veremos en un futuro (Bluetooth, 3G, GPRS.)

En sus inicios las aplicaciones de las redes inalámbricas fueron confinadas a industrias y grandes almacenes. Hoy en día las redes WLAN pueden establecerse en 3 segmentos básicos:

1. Empresa.

Usado como anexo a la red "fija", dando a los usuarios la libertad de moverse dentro de oficinas, salas de reuniones u otras dependencias de los edificios.

2. SOHO (Small Office Home Office) o PYME.

Las WLAN serán usadas como el mayor "concentrador" de conexiones a Internet dentro de la vivienda o la oficina. Los *Puntos de Acceso* se conectan a un acceso troncal mediante las tecnologías disponibles en el mercado actual (ADSL, RDSI, LMDS, Internet vía satélite, etcétera.)

3. LAN de Acceso Público (PAL.)

Normalmente, se refiere a "puntos calientes" (*hotspots*) públicos donde los usuarios deben esperar o permanecer durante largos periodos de tiempo, como es el caso de estaciones de tren, aeropuertos, centros comerciales, estaciones de servicio, etcétera.

Se pueden establecer así mismo las necesidades de cada uno de los segmentos, de modo que, por ejemplo, en el caso de una empresa será primordial la seguridad y la rapidez de conexión frente a la necesidad de fiabilidad y tarificación (establecer la forma de pago) del servicio que deban tener los usuarios en una cafetería, por ejemplo.

No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de hasta 54 Mbps, las redes cableadas ofrecen velocidades de 10, 100 y 1000 Mbps y en los sistemas de Cable de Fibra Óptica logran

velocidades aún mayores. Pensando en el futuro se piensa que las redes inalámbricas alcancen velocidades de hasta 100 Mbps.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida". Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo. Existen numerosos escenarios en los que este hecho puede ser de interés.

En definitiva, las redes inalámbricas se perfilan como una de las tecnologías más prometedoras de los próximos años. Aunque se ha avanzado mucho en esta ultima década y se están dando pasos importantes en la consolidación de las comunicaciones inalámbricas, esta tecnología se encuentra actualmente en una fase de constante desarrollo e investigación, quedando por resolver varios obstáculos tanto técnicos como de regulación de sus estándares.

OBJETIVO GENERAL.

Establecer las características, fundamentos y principios para el Diseño, Implantación y Puesta a Punto de una Red Inalámbrica basada en el Protocolo 802.11x en el Laboratorio de Comunicaciones L-3 de la Escuela Nacional de Estudios Profesionales "Aragón"; de la Universidad Nacional Autónoma de México.

OBJETIVOS PARTICULARES.

1. - Establecer los conceptos generales sobre Redes Inalámbricas.

2. - Establecer las Especificaciones para el Protocolo 802.11x.

3. - Establecer los parámetros de Seguridad en las Redes Inalámbricas basadas en el Protocolo 802.11x.

4. - Establecerlas Características y Especificaciones de los Productos y Equipos utilizados para Configurar una Red Inalámbrica basada en el Protocolo 802.11x.

5. - Establecer los criterios para la Aplicación de una Red Inalámbrica basada en el protocolo 802.11x, en el Laboratorio de Comunicaciones L-3 de la Universidad Nacional Autónoma de México, Campus *"Aragón"*.

INTRODUCCIÓN.

La expresión **WI-FI** (abreviatura de *Wireless Fidelity*), se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, *Wireless Local Area Networks*).

En un principio, la expresión *Wi-Fi* era utilizada únicamente para los equipos y aparatos con tecnología 802.11b, la Norma (el Estándar) dominante en el desarrollo de las redes inalámbricas de aceptación prácticamente universal, que funciona en una banda de frecuencias de 2.4 GHz y permite la transmisión de datos a una velocidad de hasta 11 Mbps (aunque la velocidad real de transmisión depende en última instancia del número de usuarios conectados a un Punto de Acceso.) Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término *Wi-Fi* se extendió a todos los aparatos provistos con tecnología 802.11 (ya sea 802.11a, 802.11b o 802.11g; los cuales manejan diferentes frecuencias y velocidades de transmisión).

Existe una marca registrada, *Wi-Fi Certified*, que concede la *Wi-Fi Alliance*, una asociación de más de 150 fabricantes y proveedores de aplicaciones, que garantiza que un producto que incorpore este logotipo es interoperable con aparatos de otros fabricantes para trabajar en una red sin cables. Actualmente, existen alrededor de 650 equipos y aparatos que cuentan con este certificado.

Entre las predicciones tecnológicas para el año 2003 y el 2004, todas las grandes consultoras coincidieron en señalar el desarrollo de las tecnologías *Wi-Fi* como una de las principales tendencias. Las ventas de equipos y aparatos con conexión inalámbrica se están incrementando gracias a factores como la extensión de las normas (los estándares), el aumento de la interoperabilidad, la creciente demanda de aparatos portátiles y la aparición de nuevas aplicaciones.

Por el lado de la oferta, la intensa competencia en un mercado en el que todavía no existen claros dominadores conduce a un progresivo abaratamiento de los precios. Según estudios realizados, durante el año 2002 se vendieron 20 millones de circuitos *Wi-Fi* con un crecimiento del 290% con respecto al año 2001. El precio medio del circuito se redujo de $450.00 MN. ($43 dólares en el año 2001), a $230.00M.N. ($20 dólares en el año 2002.) Por su parte, la instalación de una red inalámbrica en el hogar podría abaratarse en un año desde los $2500.00 a $2750.00 que cuesta en la actualidad, hasta los $1200.00.

Por lo que se refiere a la distribución de las aplicaciones *Wi-Fi*, se estima que las computadoras personales (portátiles y de escritorio), serán el principal destino de las mismas pero no se desestima el impacto que tendrán en teléfonos móviles y en los Asistentes Personales Digitales (PDA.)

Como muestra de las grandes expectativas que se generaron en torno al estándar *Wi-Fi*, pueden citarse iniciativas como el *"Proyecto Cometa Networks"* en los Estados Unidos de América, una alianza constituida por las Compañías IBM, Intel y AT&T que tenía el ambicioso propósito de instalar 20.000 hotspots en los principales 50 núcleos metropolitanos de ese país, y que comenzó a ser operativo a finales del 2002. Basándose en la tecnología *Wi-Fi*, el objetivo de *"Cometa Networks"* es posibilitar que empresas de telecomunicaciones, ISP y operadores inalámbricos y de cable puedan ofrecer a sus clientes acceso inalámbrico y de banda ancha a Internet desde su red de Puntos de Acceso (*"Access Point"*). Hasta la fecha este proyecto ha extendido una red de acceso inalámbrico con 400 puntos de acceso solamente pero piensa extenderse en un futuro cercano.

Sin embargo, al día de hoy, *Wi-Fi* es todavía una tecnología novedosa y que se ha empezado a utilizar en hogares y empresas por parte de los adoptadores tempranos (*"early-adopters"*) quienes son las personas y compañías que acogen en forma temprana la tecnología que apenas surge.

Antes de consolidarse definitivamente, esta tecnología deberá resolver una serie de incógnitas que penden en la actualidad sobre su viabilidad:

- **Seguridad:** Una de las mayores tareas pendientes, es la espera de mejoras a normas (estándares) que garanticen la seguridad de las transmisiones inalámbricas.
- **Provecho:** Mejorar la experiencia del usuario final, incidir en las ventajas o aplicaciones para éste, conseguir en definitiva, que la tecnología se convierta en una real comodidad.
- **Flexibilidad:** Dado el gran número de aplicaciones y tecnologías emergentes, el usuario final debe contar con la posibilidad de actualizar ambas, de modo que pueda planear a mediano y largo plazo, más que limitarse a las necesidades inmediatas.
- **Educación:** Actualmente, la *Wi-Fi Alliance* ejerce el papel de principal difusor de las tecnologías inalámbricas y es el gran respaldo de sus ventajas. A medida que el mercado crezca y se segmente, así como las necesidades particulares del usuario final, otros agentes deberán hacerse cargo de este papel o colaborar en la tarea.

La red inalámbrica *Wi-Fi*, transmite una señal de radio de 2.4 GHz o 5 GHz a través de la cual todos los equipos certificados se enlazan inalámbricamente desarrollando un desempeño funcional idéntico al que tendría una red convencional cableada. Por lo tanto, la certificación *Wi-Fi* determina que un equipo es interoperable entre otros aparatos o equipos bajo la misma certificación, sin importar si son manufacturados por distintas marcas. La certificación se otorga a diversos aparatos tales como módulos USB, tarjetas utilizadas en organizadores personales, servidores, computadoras portátiles y otros dispositivos de comunicación o transferencia de datos a través del aire. Usuarios de Internet, así como empresas se ven beneficiadas por esta tecnología inalámbrica que en ocasiones supera la velocidad de las conexiones con cable o DSL.

Los usuarios no necesitan una terminal de conexión ya que por medio del aire a través de las antenas de señal *Wi-Fi* se puede enviar o recibir información desde cualquier parte con la misma facilidad con la que se realiza una llamada telefónica a través de un teléfono celular.

Ahora, esta conectividad a través del aire no significa que la confidencialidad o privacidad de sus comunicaciones esté totalmente expuesta, ya que los estándares manejan un sistema de encriptación llamado WEP[2] el cual asigna una contraseña que identifica equipos y aparatos que forman parte de esa red, impidiendo que aparatos o equipos diferentes a los registrados, tengan acceso sin autorización a la red. Para el caso de empresas que requieren de una seguridad aún mayor, se recomienda utilizar VPN.

Con esto, la lista de opciones para transmisión de datos por medio del aire, crece. Los predecesores de la tecnología *Wi-Fi* comenzaron con la conectividad celular, seguida más delante de la tecnología WIPOP de puntos de presencia inalámbrica.

Finalmente se puede establecer, que en los últimos años se ha presenciado un importante crecimiento tecnológico en todos los ámbitos; sin embargo, uno de los más notables lo constituye el medio informático. Como consecuencia, se sabe que la llegada de un nuevo y moderno equipo de cómputo hoy en día, podría convertirse en una reliquia en unos cuantos meses. Es por eso que las compañías que se pelean el liderazgo en el mundo de los sistemas computacionales deben, además de enfrentar una fuerte competencia, buscar alguna innovación que les dé una leve ventaja tecnológica que mejore velocidad, capacidad de disco, compatibilidad, etcétera. Si dicha ventaja es aprovechada, se traducirá a corto plazo en un notable incremento en las ganancias.

[2] WEP. - Wired Equivalent Privacy.

Partiendo de este hecho, pero desde el punto de vista de las redes, nos encontramos con la misma tendencia, pero obviamente con diferentes factores, tal es el caso de la seguridad, comunicación abierta, escalabilidad, facilidad de operación y de detección de fallas entre muchas otras. Todas estas características han evolucionado enormemente, pero siguen siendo elementales para cualquier operador de red. Es por eso que aunque dicha evolución de las redes ha llegado muy lejos, las bases y necesidades son en esencia las mismas.

RESUMEN.

En la actualidad, las redes cableadas se posicionan como las más utilizadas a nivel mundial; sin embargo, sus similares inalámbricas han crecido rápidamente que hoy en día ya cuentan con un mercado de miles de millones de dólares anuales.

Básicamente, las redes inalámbricas son una tecnología que permite a los usuarios acceder a información y servicios electrónicamente sin importar su posición geográfica. Para lograr esto, en la actualidad existen diversas tecnologías, tal es el caso de las ondas celulares, la luz infrarroja y el espectro disperso, que han evolucionado enormemente con tecnologías como CDMA[3], la cual, además de contar con un alto grado de seguridad, permite soportar varias celdas por medio de una sola, por lo que más usuarios pueden utilizar el sistema inalámbrico con el mismo equipo.

Los servicios soportados por la tecnología inalámbrica van desde voz básica hasta transmisión de datos compleja como ISDN[4]. Gracias a estos avances, las ciudades y poblaciones remotas que no eran capaces de ser comunicadas por medio de un sistema alambrado, y las áreas urbanas con capacidad alambrada insuficiente, pueden ahora contar con nuevos servicios de telefonía y datos. En pocas palabras, las conexiones de red a otras partes del mundo por medio de micro-ondas, satélite, etcétera, son mucho más prácticas económicamente que instalar miles de cables.

[3] CDMA (Code Division Multiple Access.)- Acceso Múltiple por División de Código.
[4] ISDN. (Integrated Services Digital Network.) - Red Digital de Servicios Integrados.

CAPÍTULO I.

CONCEPTOS Y GENERALIDADES DE LAS REDES INALÁMBRICAS

I.1 Introducción

Las redes inalámbricas de área local se diferencian de las redes de área local tradicionales en que los terminales no están interconectados físicamente mediante un cable. El soporte físico del bus ha pasado de ser un cable a ir a través de las ondas. Esto es posible, en gran parte, a que los organismos internacionales que establecen el reparto de las frecuencias del espectro han dejado libres varias franjas para uso personal o privado.

Desde hace poco, existe una nueva tecnología que hace uso de las frecuencias libres de licencia: las redes de área local inalámbricas. Las LAN inalámbricas utilizan básicamente longitudes de onda correspondientes a las microondas (2.4 GHz y 5 GHz) y permiten tener anchos de banda apreciables (desde 1 Mbps en las primeras versiones hasta llegar a los 54 Mbps de los últimos estándares.) Debe mencionarse que aunque la banda alrededor de los 5 GHz es abierta en todo el mundo, el ancho de banda que se puede ocupar depende de la situación particular que haya impuesto cada legislador. Es por ello que en Europa se pueden utilizar hasta 455 MHz, mientras que en Norteamérica el ancho de banda se restringe a 300 MHz y en Japón a 100 MHz.

En muchos sitios, las redes Ethernet de cable tradicional han sido ampliadas con la implantación de redes inalámbricas. La interconexión de varias redes locales (alámbricas e inalámbricas) ha propiciado que algunos visionarios hayan visto la posibilidad de crear una red metropolitana con gran ancho de banda y con la posibilidad de acceso a Internet, de forma que se pudiera acceder a cualquier servicio de los que comúnmente se utilizan en Internet (correo, web, ftp, etcétera) desde cualquier lugar dentro del ámbito metropolitano.

Las redes inalámbricas se perfilan como una de las tecnologías más prometedoras de los próximos años. Aunque se ha avanzado mucho en esta ultima década y se están dando pasos importantes en la consolidación de las comunicaciones inalámbricas, esta tecnología se encuentra actualmente en una fase de constante desarrollo e investigación, quedando por resolver varios obstáculos tanto técnicos como de regulación bajo los mismos estándares existentes.

I.2.- Antecedentes en Redes Inalámbricas

Compartir, agregar o modificar información desde el lugar y a la hora que sea, ahora resulta tarea fácil gracias a las nuevas tecnologías de comunicación. Pero ¿qué fue lo que hizo posible dichas alternativas y como es que ahora se pueden realizar tantas cosas sin necesidad de cables?

La comunicación sin hilos ha estado disponible desde hace ya bastante tiempo con la radiofrecuencia como principal exponente, siendo su principal aplicación las comunicaciones de voz. Hoy en día, millones de personas utilizan los sistemas de radio de dos vías para comunicaciones de voz punto a punto o multipunto, con total normalidad. Sin embargo, en lo que se refiere a la transmisión de datos binarios, aunque ya se conocían las técnicas para modular la señal de radio con la cual conseguir comunicaciones digitales, sólo recientemente se han podido desarrollar y desplegar servicios inalámbricos para datos a gran escala.

En contraste con las LAN's que usan cables de cobre o de fibra-óptica, una red local inalámbrica usa el espacio como su medio de la transmisión. Las redes inalámbricas no transmiten información a través de variaciones en valores de voltaje o pulsos ligeros, sino en forma de ondas electromagnéticas. Como un medio de transmisión, el espacio responde completamente diferente a las características que el cable tiene para la transmisión de señal.

Debido a las circunstancias físicas, el espectro de frecuencia utilizable para la transmisión de ondas electromagnéticas en la Tierra es limitado y además pertenece al dominio público, por lo que su dirección y propiedad están bajo control gubernamental. Cada país tiene una comisión que es responsable de liberar frecuencias para propósitos específicos y coordinar las liberaciones de aprobación internacional. Por ejemplo, en Alemania, la autoridad reguladora para Telecomunicación y Servicio Postal es responsable de establecer reglas tales como la potencia de salida de la señal, ancho de banda, método de modulación y de propagación autorizado para el uso del espectro. .

El crecimiento real de las comunicaciones inalámbricas comenzó a principios de los 80, cuando la gente demostró un interés sustancial en utilizar la telefonía inalámbrica ya que hasta ese entonces el uso principal del espectro era en el área militar y era de tipo "secreto". Es a partir de ese momento cuando al espectro se le da un enfoque comercial ya que los usuarios privados necesitaban comunicaciones seguras parecidas a las militares.

Al ampliar el uso del espectro, se tuvo en consideración que cuando muchos usuarios emitieran comunicaciones de radio en la misma banda de frecuencias, era inevitable la obstrucción no intencional, por lo que debía

regularse también el uso de frecuencias. Por eso la FCC[5] por primera vez en 1985 asignó porciones del espectro de frecuencia de radio que entidades "Industriales, Científicas y Médicas (conocida como banda ISM) podrían usar sin necesidad de una licencia. Estipulo además, los tipos de comunicaciones de radio que estaban permitidos: uno de los esquemas que se puede usar en las bandas ISM es la tecnología de espectro extendido que es la más usada actualmente para las redes inalámbricas.

La banda ISM cubre varios rangos de frecuencia, pero sólo los rangos de alta frecuencia de 860 MHz, 2.4 GHz, y 5.7 GHz son convenientes para la transmisión de los datos. El más alto rango de frecuencia de 24 GHz aun no se ha hecho accesible todavía.

Inicialmente los fabricantes de la tecnología de datos inalámbrica estaban ocupando la banda cercana a los 900 MHz que era la banda licenciada para los celulares analógicos aprovechando así, los componentes inalámbricos existentes para el desarrollo de nuevas tecnologías, pero esto tenía un limitante; esta banda era una infraestructura común para los Estados Unidos. Canadá y Australia pero no estaba asignada para la operación sin licencia en otras partes del mundo, por lo que los fabricantes comenzaron a producir radios que operaban en la parte de 2.4 GHz del espectro de frecuencia que estaba disponible para la operación libre de licencia a lo largo de la mayor parte de Europa y Japón.

La operación en la banda de 2.4 GHz tuvo ventajas importantes respecto a la banda de 900 MHz ya que al operar en una banda abierta que en esencia era común, un fabricante podría construir un solo radio que, mediante algunos ajustes menores podría venderse en todo el mundo con lo que proporcionaría mejores costos de expansión. Actualmente los rangos de baja frecuencia de la banda ISM se usan para control de sistemas de alarma, sistemas de audio, etc., y sólo la frecuencia de rangos de 2.4 GHz y 5.7 GHz son de importancia para la transmisión de los datos.

La banda de 2.4 GHz proporciona un ancho de banda de 83.5 MHz., esta banda ISM es la única banda de frecuencia la cual con pocas limitaciones está disponible en todo el mundo, y actualmente habilita rangos de datos entre 1 Mbps y 54 Mbps. La banda de 5.725 GHz proporciona un ancho de banda mucho mayor permitiendo así un rango de datos arriba de los 54 Mbps. La figura I.1 muestra las frecuencias del espectro utilizadas actualmente para la transmisión de datos.

[5] Comisión Federal de Comunicaciones de Estados Unidos

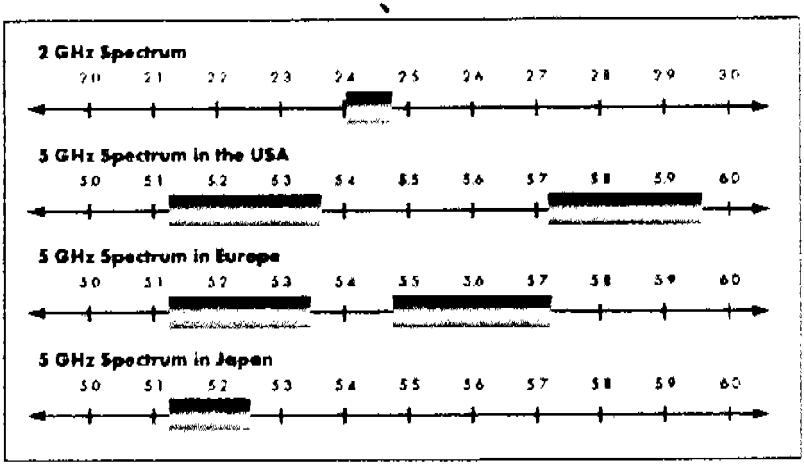


Fig. I.1 Mapa Mundial de Frecuencias WLAN

Para el uso libre de la banda ISM se tenia que cumplir con el requisito previo de que las unidades inalámbricas no excedieran la potencia de salida establecida para la banda-específica (la cual es 100 mW en los 2.4 GHz.) Todos los dispositivos que quieren usar este rango deben examinarse en un laboratorio probando y aprobando su uso para ser compatibles. El objetivo de cumplir este requisito es incrementar el rango de datos usando procedimientos más complejos de modulación.

Por razones históricas y debido a intereses específicos de países, existen todavía diferencias entre los países para el uso de las frecuencias en la banda ISM. Esfuerzos están haciéndose a escala nacional e internacional para terminar estas diferencias en un futuro no distante.

Al notar el beneficio mutuo de definir estándares de la industria para las LAN Inalámbricas, en 1991 varios fabricantes emitieron una Solicitud de Autorización de Proyecto[6] al IEEE a fin de establecer un estándar interoperable para las LAN Inalámbricas el cual fue aprobado en 1997. Este primer estándar fue el 802.11 el cual proporcionaba velocidades de datos de 1 o 2 Mbps, una forma rudimentaria de cifrado de datos así como la transmisión a través de tecnologías de Secuencia Directa y de Salto de Frecuencia sobre una banda de 2.4 GHz además de rayos infrarrojos. Los aspectos relacionados con los rayos infrarrojos de este estándar obtuvieron un pequeño impulso comercial y hoy día representan sólo una pequeña parte en la historia del estándar.

[6] PAR (Project Authorization Request)

Desde entonces se han creado varios estándares con diferente éxito cada uno de ellos, pero igualmente funcionales de acuerdo a las necesidades de las áreas donde han siendo implementados.

I.3 Redes Inalámbricas Locales

Las redes inalámbricas locales conforman una de las tecnologías electrónicas de crecimiento más rápido en toda la historia. Esto es posible gracias a que es una tecnología que cambia totalmente el concepto de la utilización de una computadora, permitiendo tener conectividad a las redes cableadas o a Internet prácticamente sin limitaciones de lugar o tiempo, mejorando así la experiencia de movilidad de cualquier tipo de usuario. ¿Pero que es una Red Local Inalámbrica o WLAN? ¿Qué estructura utiliza? ¿Qué equipos necesita y a que costo?

I.3.1 Definición

El fenómeno asociado al término "inalámbrico", es decir, no tener que instalar más cables además de los de la red telefónica y los de alimentación eléctrica, ha pasado a ser el principal catalizador para las redes en pequeñas y medianas empresas ya que la conexión a Internet o a la red empresarial sin la necesidad del tradicional cableado es una realidad.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles y tarjetas inalámbricas, lo que permite al usuario viajar a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) en un espacio específico sin perder el acceso a los datos de la red.

Sin el acceso inalámbrico, el usuario tendría que llevar consigo pesados cables y disponer de conexiones de red. Las soluciones móviles conceden flexibilidad a la red empresarial, pues le permiten crecer en número de usuarios sin necesidad de recablear para dar acceso a empleados de nuevo ingreso.

Por red de área local (LAN, Local Area Network), entendemos una red de datos privada, que cubre un entorno geográfico limitado. Su aplicación más extendida es la interconexión de equipos de cómputo para compartir recursos e intercambiar datos y aplicaciones. Por red inalámbrica entendemos una red que utiliza ondas electromagnéticas como medio de transmisión de la información que viaja a través del canal inalámbrico enlazado en los diferentes equipos o terminales móviles asociados a la red.

Se puede definir entonces una red inalámbrica de área local (WLAN, Wireless Local Area Network) como: **"Una extensión de la red cableada cuyo fin es proporcionar un servicio de red móvil a todos los usuarios, para cualquier tipo de aplicación que deseen ejecutar, lo mismo si se trata de datos, que de voz o video"**. La siguiente figura muestra el esquema de una WLAN.

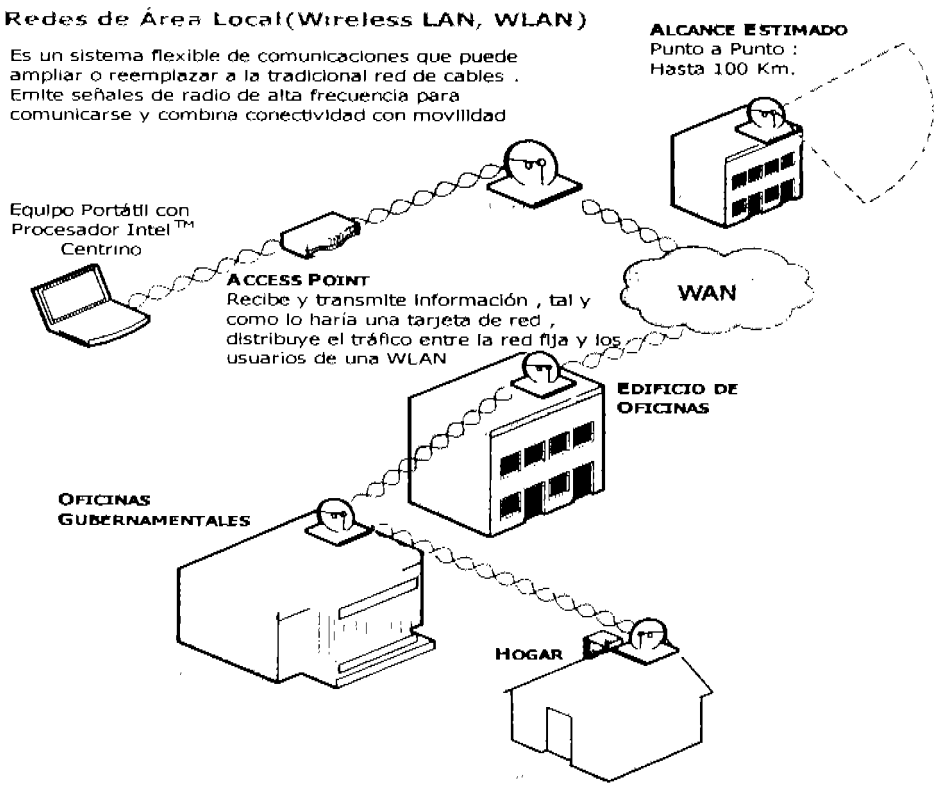


Figura I.2 Esquema de una WLAN

I.3.2 Componentes Esenciales de una WLAN.

Una WLAN (Wireless Local Area Network) es una red inalámbrica en la que una serie de dispositivos (Computadoras, Estaciones de Trabajo ("Workstations"), Impresoras, Servidores, etcétera) se comunican entre sí en zonas geográficas limitadas sin necesidad de tendido de cable entre ellos. La gran ventaja de esta tecnología es que ofrece movilidad al usuario y requiere de una instalación muy sencilla. Entre los componentes que permiten configurar una WLAN se pueden mencionar los siguientes:

Terminales de Usuario.- (Clientes) cuentan con una Tarjeta Interfaz de Red (NIC) que incluye un transceptor radio y la antena.

Puntos de Acceso.- (Access Points o AP), que permiten enviar la información de la red cableada (por ejemplo, Ethernet) hacia los clientes inalámbricos.

Controlador de AP.- Necesario para despliegues que requieren varios AP por razones de cobertura y/o tráfico, Este último suele incorporar funcionalidad de AP, de cliente VPN, de cliente RADIUS para labores de autentificar y autorizar, con un servidor AAA[7] apropiado, de routing y de firewalls.

La existencia en el mercado de dichos dispositivos capaces de interconectarse de forma barata y sencilla ha dado origen a una gran variedad de aplicaciones que sobrepasan ampliamente el ámbito de utilización en entornos empresariales para el que nacieron las WLAN.

I.3.3 Tipos de redes WLAN

Las implementaciones de las WLAN abarcan todas las modalidades posibles de una red:

- **Wireless PAN** (Personal Area Networks; Redes de Area Personal) son redes inalámbricas de corto alcance, permite interconectar dispositivos electrónicos dentro de un rango de pocos metros, para comunicar y sincronizar información. La líder en ésta área es Bluetooth, una tecnología de radio de corto alcance que simplifica las comunicaciones entre dispositivos de red. Facilita la sincronización de los datos entre los dispositivos de red y otras computadoras. Debido a que no fue diseñada para soportar grandes cargas de tráfico, no es una buena alternativa para sustituir a las redes locales.

[7] Servidor de Autentificación, Autorizac Contabilidad

- **Wireless LANs** (Local Area Networks; Redes de Area Local) en general utilizan señales de radio para conectar un conjunto de dispositivos. Soportan tasas de transmisión entre los 11 y 54 Mbps y tienen un rango de entre 30 a 300 metros, con señales capaces de atravesar paredes.

- **Wireless WAN** (Wide Area Networks; Redes de Area Amplia) abarcan áreas geográficas relativamente extensas y permiten a múltiples organismos conectarse en una misma red. Consisten de torres y antenas que transmiten ondas de radio o usan tecnología de microondas para conectar redes de área local, utilizando enlaces punto-punto y punto-multipunto. En la figura I.3 se ilustra los tipos de redes inalámbricas. *(Fuente 3Com México)*

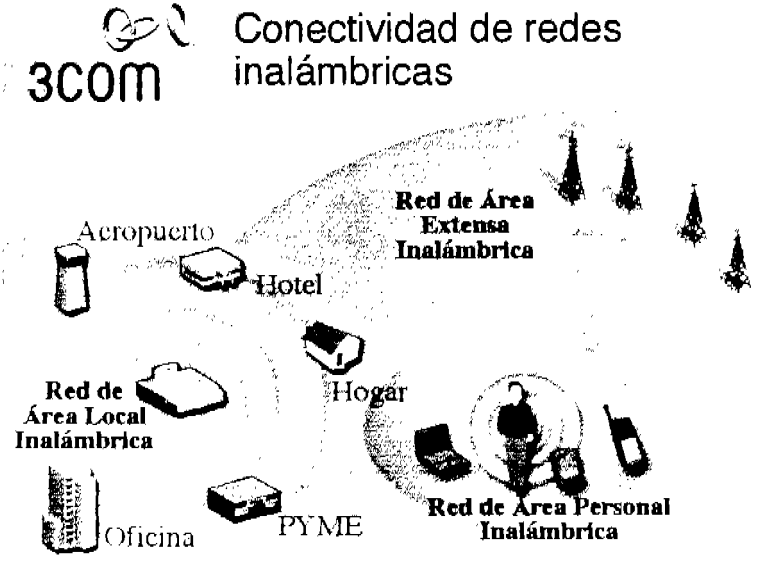


Figura I.3 Conectividad de Redes Inalámbricas

I.4. Topologías en una Red Inalámbrica Local

Las redes LAN inalámbricas se construyeron utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y "ad hoc". Nosotros utilizaremos estos últimos ya que son los más comunes en esta área. Estos

términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

I.4.1. Topología de Infraestructura

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada Punto de Acceso. El Punto de Acceso une a la red LAN inalámbrica y a la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El Punto de Acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura puede haber varios puntos de acceso para dar cobertura a una zona grande o un único Punto de Acceso para una zona pequeña, ya sea un hogar o un edificio pequeño. La figura I.4 muestra este tipo de Topología.

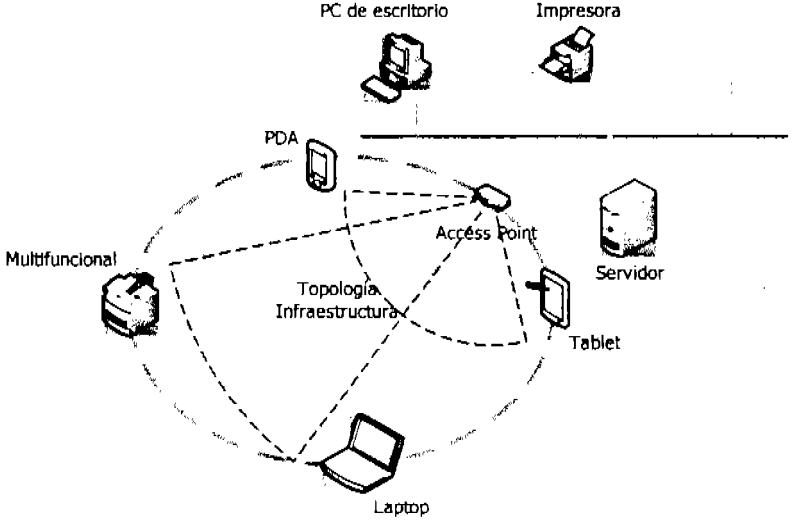


Figura I.4 Esquema de una WLAN con topología de Infraestructura

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a

si mismos o mediante el sondeo activo de una red específica con tramas de sondeo. La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el Punto de Acceso. Una vez que el Punto de Acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el Punto de Acceso y la estación intercambien información y datos de capacidad. El Punto de Acceso puede utilizar esta información y compartirla con otros Puntos de Acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación. En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un Punto de Acceso para poder llegar a su destino en la red LAN inalámbrica o con cable.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras.)

Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red esta despejada. Esta demora, junto con la recepción correcta, representa la parte del protocolo que evita las colisiones. En la modalidad de infraestructura, el emisor o el receptor es siempre el Punto de Acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del Punto de Acceso, se toman medidas especiales para evitar colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el Punto de Acceso y pueda evitar transmitir durante ese intervalo.

El proceso de movilidad de un Punto de Acceso a otro está definido en el estándar. La señalización y el sondeo que se utilizan para buscar un Access Point y un proceso de reasignación que permite a la estación asociarse a un Access Point diferente, junto con protocolos específicos de otros fabricantes entre Access Point, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el Access Point. Estas tramas contienen el valor de reloj del Access Point en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La

sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

I.4.2. Topología Ad Hoc.

En una topología Ad Hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni Access Point. Cada dispositivo se comunica directamente con los demás dispositivos en la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden unirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar datos. La figura I.5 muestra este tipo de Topología.

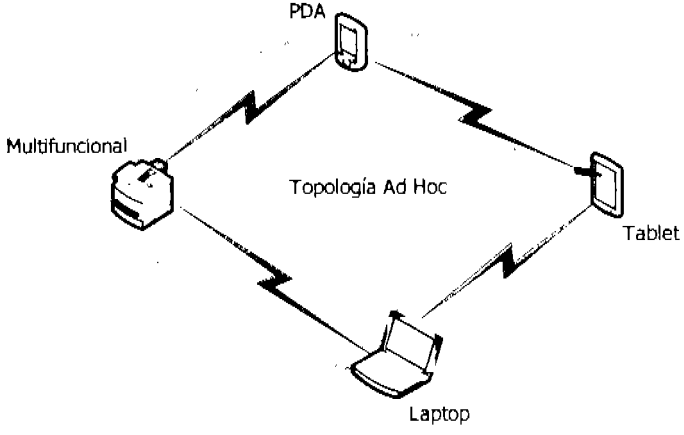


Figura I.5 Esquema de una WLAN con topología Ad Hoc

Las técnicas utilizadas para encaminar paquetes de datos en las redes clásicas cableadas no pueden ser utilizadas en redes Ad Hoc. Los clásicos presuponen que la topología de la red es poco cambiante y, en consecuencia, están basados en complicados algoritmos que tratan de conocer la mejor ruta hacia cualquier destino. En las redes con topología Ad Hoc, debido a la movilidad de los nodos, es inviable esta alternativa.

Además, el ancho de banda y la memoria son reducidos y se saturaría muy pronto la red debido al denso tráfico de control desplegado en este tipo de algoritmos y al rápido crecimiento de las tablas de encaminamiento. Para solucionar este problema se han diseñado distintas técnicas para conseguir encaminar de manera efectiva. Los algoritmos de encaminamiento usados en las redes Ad Hoc se pueden clasificar en tablas de encaminamiento y encaminamiento bajo demanda.

Los algoritmos basados en tablas de encaminamiento tratan de mantener la información necesaria para el encaminamiento continuamente actualizada. Cada nodo mantiene una o más tablas con los datos para encaminar hacia cualquier otro nodo.

Los cambios en la topología de la red proporcionan el envío masivo de paquetes para mantener las tablas actualizadas. Los protocolos difieren en el número de tablas utilizadas y en la política de envío de paquetes para mantener las tablas actualizadas.

En contraste con los algoritmos basados en tablas, en los algoritmos de encaminamiento bajo demanda, las rutas son creadas solo cuando se requieren. Cuando un nodo requiere una ruta hacia un destino concreto se inicia un proceso de descubrimiento de ruta. Este proceso termina cuando se encuentra un camino hacia el destino o cuando se examinan todas las alternativas y ninguna lleva al destino final. Cuando la ruta es descubierta, es necesario mantenerla (mantenimiento de ruta) hasta que el destino se vuelva inalcanzable o la ruta deje de ser necesaria.

I.5. Situación Actual de las Redes Inalámbricas

En los últimos años el crecimiento en la demanda de soluciones inalámbricas para empresas, escuelas, y últimamente también para el hogar, ha crecido de manera espectacular. Las distintas tecnologías inalámbricas permiten dar una cobertura casi en cualquier rincón del planeta. Cientos de millones de personas en todo el mundo se comunican e intercambian información todos los días usando una u otra tecnología inalámbrica, permitiendo el envío de datos con una movilidad sin precedentes.

Las tecnologías inalámbricas más usadas y conocidas hoy día son los teléfonos celulares, sistemas de navegación, los sistemas de búsquedas, servicios de mensajes, el tradicional radio, etc.; pero el gran exponente de la revolución digital y como los bits forman parte de nuestro día a día, proviene del intercambio de datos digitales.

Estos datos no sólo se quedan limitados al ámbito de las computadoras, sino también en una gran cantidad de aplicaciones, pasando desde los grandes

sistemas de datos empresariales y científicos hasta las más pequeñas herramientas personales destinadas a mejorar nuestro día a día. Ya no se esta atado a redes cableadas sino que se puede acceder y compartir datos llevándolos, dondequiera que se vaya.

Desde el principio de los años 70 se han tenido redes, por ejemplo la red Ethernet, que ha supuesto una estandarización a la hora de transmitir datos, con un gran éxito en todo el mundo y aunque no es único, si es el que más ha influenciado el uso habitual de las Redes Área Local (LAN.) Nos hemos acostumbrado a tener redes de computadoras de bajo costo, altas velocidades y una relativa fácil instalación, más que apto para la mayoría de las aplicaciones.

¿Pero cual es el inconveniente de las redes cableadas? El hecho de tener una infraestructura limita a líneas preinstaladas y los costos ante fallos, mantenimiento y/o reestructuración se disparan. La flexibilidad es muy baja e incluso no resulta factible la instalación de éstas soluciones en algunos edificios antiguos de valor histórico o peligrosos con asbestos u otros materiales. Todo esto puede ser solucionado con las nuevas tecnologías inalámbricas, puesto que ya no es necesaria la instalación de cables.

Las redes LAN Inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años. El acceso del usuario normalmente supera los 11 Mbps, de 30 a 100 veces más rápido que las tecnologías de acceso telefónico o de las redes WLAN estándar.

Este ancho de banda es sin duda adecuado para que el usuario obtenga una gran experiencia con varias aplicaciones o servicios a través de dispositivos móviles. Además, los avances en curso de estos estándares inalámbricos continúan aumentando el ancho de banda, con velocidades de hasta 54 Mbps actualmente.

En el actual entorno de negocios, los usuarios móviles que hacen uso de soluciones inalámbricas, pueden transferir archivos, enviar y recibir correo electrónico, tener acceso a la intranet de su empresa además de Internet, recibir información mientras están de viaje e, incluso, utilizar aplicaciones colaborativas como la videoconferencia; todo, como si estuvieran en una red cableada. Los principales beneficios de las tecnologías inalámbricas, son que son flexibles y fáciles de usar, y permiten a los usuarios mantener la comunicación en cualquier momento y lugar, con la misma calidad de servicio que una red cableada a un menor costo.

Las WLAN cuentan con acceso seguro, instantáneo y confiable a la red, que permite conectividad desde cualquier lugar y en cualquier momento, sin comprometer la velocidad o la confiabilidad. La amplia disponibilidad de un acceso móvil a la red habilita el acceso a herramientas adicionales para todos

aquellos usuarios móviles, tales como los servicios Web de impresión. Las interfases intuitivas para usuario final y los sistemas de facturación vuelven conveniente el acceso, ya que los proveedores de servicio que operan con soluciones inalámbricas ofrecen modelos de uso y precios de acceso remoto que se ajustan a las necesidades de cada usuario.

Las redes inalámbricas son más flexibles a la hora de realizar cambios dentro de una organización. Los administradores no tienen que realizar nada para que una persona que esta trabajando en un escritorio se cambie a otro. Esto reduce cambios administrativos y de costos en la organización. El número de dispositivos a administrar es menor, ya que una red inalámbrica se puede componer de un menor número de ellos, permitiendo conocer de una manera más eficiente problemas dentro de la red para su posterior corrección.

En caso de que la organización se desplace a otro sitio, la red inalámbrica se lleva consigo y se pone en funcionamiento de una manera más rápida. Reducen el presupuesto que tienen para implementación de red, al no tener que incluir costos de cableado, los cuales suelen ser costosos.

Este tipo de tecnologías ofrece a los usuarios mayor versatilidad a la hora de acceder a los servicios de red, proporcionando múltiples ventajas en lo que se refiere a mantenimiento de la red, implantación y movilidad de los usuarios. Sin embargo, el uso de un canal compartido y de elementos de acceso a la red cableada directamente accesibles por cualquier persona plantea también ciertos problemas de seguridad que deben ser resueltos, como por ejemplo, el control de acceso a los usuarios a la red, entre otros.

En la gráfica I.6 (*Fuente: Wireless LAN SIMATIC Net de SIEMENS*) se puede ver que los entornos de conectividad "tradicionales" (telefonía de segunda generación y redes de área local alámbricas) han solucionado los problemas a lo largo de los ejes de movilidad en el caso de la telefonía móvil y de gran ancho de banda en el caso de las redes de área local. El futuro se puede entender como la conquista del espacio que engloba las cualidades de gran ancho de banda y movilidad a través de conexiones inalámbricas, o sea, que se busca llegar a espacios que estén lo más alejados de los ejes.

En esta gráfica podemos ver que mientras Bluetooth sólo proporciona cierta libertad al respecto (en realidad ofrece algo más de ancho de banda que la segunda generación de telefonía móvil en espacios muy limitados), las redes locales inalámbricas y la telefonía móvil de tercera generación sí que pretenden conseguir el objetivo de ofrecer gran ancho de banda en cualquier lugar. En esta gráfica podemos ver una de las diferencias que caracterizan estas tecnologías, por ejemplo mientras las redes de telefonía de tercera generación parten de la movilidad y tienden a introducir paulatinamente más ancho de banda, las redes inalámbricas cuentan como punto de partida redes con velocidades de acceso muy altas y tienen como objetivo conseguir que su acceso sea móvil y universal.

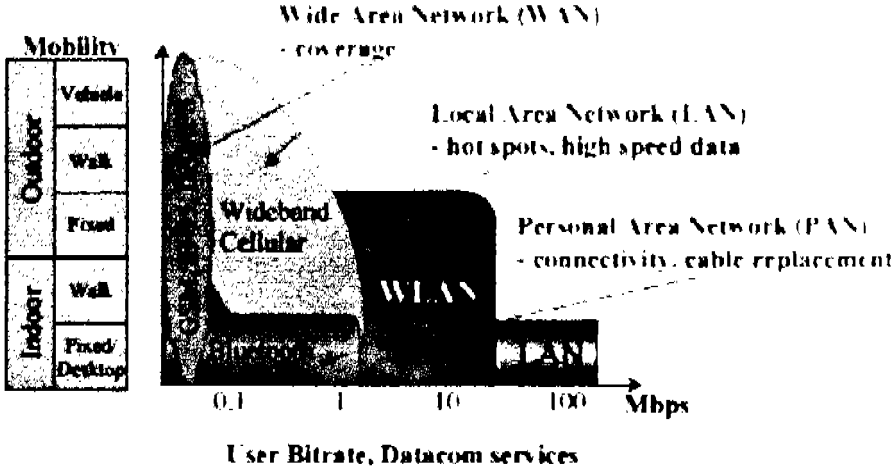


Fig. I.6 Grafica de las Tecnologías de Conectividad Actuales

I.6. Retos de las Redes Inalámbricas de Área Local.

Es impresionante el hecho de que las WLAN sean cada vez mas usadas y vistas no solo como un exótico dispositivo para redes, sino como el vehículo que conducirá a una nueva era de acceso sin controles a Internet de banda ancha para la población en general y a movilidad con conectividad permanente en el entorno de negocios, ya que es una tecnología relativamente económica y sencilla; con un dispositivo pequeño (del tamaño de una pequeña caja de chocolates) se puede tener conectividad de forma inalámbrica de alta velocidad, cubriendo en área abierta (sin obstáculos) el tamaño de una cancha de fútbol.

Pero todavía hay muchos retos que enfrentar, muchas de las barreras que han inhibido el crecimiento de la tecnología inalámbrica están siendo resueltas. Se están superando las cuestiones de estandarización e interoperatividad que eran de las más importantes. Hoy el gran reto está en la entrega de conectividad IP de banda ancha a los usuarios móviles en el sentido de darles a estos usuarios un ambiente computacional similar al disponible en una computadora de escritorio soportada por Ethernet en una oficina convencional. En otras palabras, la meta está en reproducir la experiencia del escritorio para el usuario móvil.

Aún se necesitan grandes mejoras a la actual tecnología inalámbrica en varios aspectos pero los retos más importantes que los ingenieros enfocados al desarrollo de WLAN tienen que afrontar pueden agruparse en cuatro amplias categorías que serán mencionadas a continuación.

I.6.1. Facilidad de Uso.

La simplicidad de operación siempre ha sido una gran preocupación para las redes de área local inalámbrica, diseñada para agregar funcionalidad a las existentes redes locales cableadas sin imponer al usuario nuevos inconvenientes. Mantener la filosofía de operación sin problemas, mientras las capacidades WLAN se siguen extendiendo para soportar a los profesionales móviles, es el principal reto.

Cabe admitir que, aunque aún estamos lejos de una solución satisfactoria, se han logrado avances en materia de facilidad ya que las aplicaciones comerciales están integrando en sus productos las características de tecnología inalámbrica, como por ejemplo Microsoft que, intentando "negociar" con la complejidad de las redes WLAN, ofrece en Windows XP configuración automática de redes inalámbricas, cuyo propósito es establecer de manera automática la conexión con los Puntos de Acceso (AP, Access Point) Wi-Fi más cercanos.

Aunque las configuraciones de estos productos para el acceso a WLAN a veces distan de ser sencillas es un avance el que los productos comerciales integren entre sus características la conectividad inalámbrica.

Debe de mejorarse también la capacidad nativa de seguridad ofrecida por WLAN ya que fue diseñada para simplificar la operación, pero es tan difícil de utilizar que muchas veces no esta implementada del todo en instalaciones inalámbricas incluso, en empresas donde la seguridad es un factor crítico.

Otra capa de complejidad surge cuando el usuario móvil quiere usar un *hotspot* Wi-Fi comercial (por ejemplo en un aeropuerto). El mecanismo de control de acceso del operador del *hotspot* debe servir al doble propósito de autorizar a los suscriptores existentes, al tiempo que también habilita a los usuarios de primera vez para autentificarse y a los usuarios esporádicos a pagar en el sitio. La autenticación basada en navegador, una popular técnica que sirve en ambos extremos, es conveniente y de fácil manejo, pero vulnerable a los relativamente simples ataques de robo de servicio.

Una estrategia más comprensiva, como la especificada en el estándar 802.1x, protege contra éste y algunos otros ataques, pero solo al costo de

complejidad extra; el usuario Wi-Fi en el *hotspot* debe de tener una cuenta de servicio dispuesta de antemano. Esta es una seria, tal vez inaceptable, desventaja en el aún embrionario negocio de los *hotspot*, donde la adquisición de suscriptores es una prioridad sobresaliente.

I.6.2. Seguridad.

Dentro y fuera de las instalaciones de los corporativos, las WLAN representan vulnerabilidades de seguridad potencialmente serias.

La mayoria de las predicciones del crecimiento de WLAN se enfoca en el atractivo del acceso público gratuito, una benigna visión utópica donde los detalles de la seguridad de la red son de importancia secundaria. Hay, sin embargo, otro lado oscuro del cuento de la conectividad inalámbrica, el cual concierne en sus vulnerabilidades a los curiosos y/o *hackers*.

Un escenario comúnmente reportado es aquel donde un *hacker* interviene las comunicaciones WLAN de un establecimiento. Para esto no se necesita una gran habilidad, por aquello de que el protocolo de seguridad WEP suele o no ser habilitado, lo que facilita la captura de información valiosa, como número de tarjetas de crédito.

Consideraciones como esta han levantado una seria preocupación acerca de la viabilidad de WLAN en el entorno comercial, problema que sólo ha sido exacerbado por el descubrimiento de que aún cuando WEP esté operando, la clave de encriptación puede ser recuperada.

En defensa de WEP está el hecho de que nunca se intentó que fuese una solución de seguridad a prueba de balas. Más bien, WEP fue diseñado para ser una técnica simple, fácil de usar para proporcionar una privacidad semejante a las redes cableadas. Esto es, el esfuerzo requerido para romper el código se esperaba que fuera aproximadamente semejante al esfuerzo que un intruso necesita para entrar en una red cableada con Ethernet.

La facilidad y eficiencia del ataque para recuperar la clave, sin embargo mostró que WEP no podía proporcionar ni siquiera ese modesto nivel de seguridad. Reconociendo esto como una gran deficiencia, la comunidad Wi-Fi ha desarrollado dos estrategias que pretenden resolver el problema: retener la metodología de seguridad nativa de WEP pero arreglando sus defectos y/o proporcionar por separado un revestimiento de seguridad, como una red privada virtual (VPN, *Virtual Private Network*) sobre la insegura Wi-Fi.

Estas dos alternativas tienen el potencial de restaurar la fe en la seguridad WEP, pero que alguna de ellas pueda ofrecer el balance de seguridad y facilidad de uso necesario para la amplia aceptación del mercado, todavía esta por verse.

Las mejores propuestas para WEP se enfocan en dos áreas: control de acceso, manejando el estándar 802.1x, y encriptación, que se está desarrollando bajo el 802.11 *Task Group i*. Para proteger contra los ataques, 802.1x proporciona una infraestructura para la mutua autentificación; esto es, un proceso que permite a la red autenticarse con el usuario y viceversa. Se apoya en una base de datos de usuarios autorizados y permite el acceso a la WLAN sólo a aquellos que se han autenticado apropiadamente a sí mismos.

Una segunda ventaja de 802.1x es su soporte para el intercambio frecuente de claves entre los extremos de una conexión aérea Wi-Fi. Este mecanismo permite el uso del protocolo de integridad de claves temporales (TKIP), un procedimiento de encriptación mejorado capaz de frustrar el ataque de recuperación de claves que fue tan dañino para el WEP original. TKIP es considerado altamente promisorio como la cura para los problemas de seguridad de Wi-Fi.

Hay dos desafíos enfrentando la estrategia 802.1x/802.11i. El primero tiene que ver con el tiempo al mercado. El entusiasmo por Wi-Fi, que ha sido fuerte en los años recientes, se debilitó por un período debido a preocupaciones por la seguridad. Entre más tiempo tome desarrollar un sistema de seguridad confiable para enfrentar los problemas actuales, más difícil será reconstruir el dinamismo de Wi-Fi. El segundo reto es convencer a los escépticos administradores de sistemas de que pueden confiar con seguridad las comunicaciones privadas de sus empresas a una sola solución que sólo ha sido limitada al escrutinio público.

La metodología VPN para la seguridad Wi-Fi asume que las LAN inalámbricas (incluyendo las conexiones inalámbricas y las redes cableadas que dan soporte a los Access Point) son inseguras, no importando si WEP está habilitado o no. La protección es proporcionada por un mecanismo de seguridad por separado, típicamente un túnel IPsec, ejecutándose encima de la conexión inalámbrica y extendiéndose de la computadora del usuario a la puerta de enlace (*gateway*) detrás de los Access Point. Esto proporciona protección de extremo a extremo, independientemente de las vulnerabilidades de la red subyacente. Una extensión directa de esta arquitectura, por supuesto, puede también proteger las comunicaciones de un usuario usando una WLAN fuera de su oficina, escuela, hogar, como, por ejemplo, un *hotspot*.

La tecnología VPN ha estado disponible comercialmente durante varios años, y generalmente se considera capaz de proporcionar una fuerte seguridad,

pero el costo – especialmente para las WLAN corporativas -, es significativo por eso no representa la solución más rápida al problema de seguridad.

I.6.3. Movilidad

Habilitar la movilidad WLAN dentro de un solo edificio es relativamente simple, pero extenderla a los *hotspots* públicos con conexiones permanentes seguras no lo es tanto. La movilidad, por supuesto, es una ventaja central de las redes inalámbricas. Incluso las implantaciones más rudimentarias permiten, por lo menos, deambular (hacer *roaming*) por la red dentro de la cercanía de un Access Point, a lo cual (por analogía con la telefonía) podría llamársele *"roaming"* inalámbrico. Sin embargo, lo que se necesita para dar soporte al usuario móvil es algo más similar a la capacidad de *roaming* global de los sistemas celulares.

En materia de tecnología, el primer paso en el camino a la movilidad es la interoperabilidad de varios vendedores a nivel de dispositivos, lo que asegura que el adaptador de la LAN inalámbrica (típicamente una tarjeta que comúnmente se inserta) utilizado por un usuario pueda establecer comunicación con los Access Point, aún cuando hayan sido manufacturados por diferentes fabricantes. Esta interoperabilidad "confiable", que no pudo ser garantizada simplemente por conformidad con los primeros estándares, se consiguió a través de la iniciativa Wi-Fi, bajo la Alianza para la Compatibilidad Ethernet inalámbrica (WECA, *Wireless Ethernet Compatibility Alliance*, por sus siglas en ingles).

Los esfuerzos por un progreso hacia el *roaming* con nivel de servicio a gran escala son dirigidos por una iniciativa de la WECA, conocida como *Roaming* de Proveedores de Servicio de Internet (WISPr, *Wireless Internet Service Provider roaming*, por sus siglas en ingles).

Aunque no se han hecho públicos los detalles de WISPr, el objetivo es construir un consenso sobre las mejores prácticas comunes para el *roaming* inalámbrico. Tal capacidad debe permitir al suscriptor de un WISP hacer *roaming* en otro territorio, autenticarse él mismo y obtener acceso a esa red.

La propuesta WISPr proveería un mecanismo uniforme para manejar las funciones de Autenticación, Autorización y Contabilidad (AAA, *Authentication, Authorization and Accounting*, por sus siglas en ingles), necesarias para esto. Una estrategia más adecuada para el *roaming* a través de múltiples WISPr es agregarlos bajo la sombrilla de una organización y revender sus servicios por medio de una sola suscripción. Mientras que las capacidades de WISPr pueden formar las bases para el acceso WLAN difundido, no son suficientes para habilitar el tipo de movilidad que requiere un usuario viajero, el cual requiere

conectividad IP de banda ancha para obtener un ambiente computacional similar al disponible en una PC soportada por Ethernet en una oficina convencional.

El componente faltante sería la movilidad siempre activa, la cual requiere de una infraestructura capaz de proporcionar una conexión inalámbrica segura y bajo solicitud, es decir, que permita maniobrar en el estilo de cerrar el equipo, moverse, abrir el equipo y continuar con el trabajo, donde se dejo antes. En dicho modelo, el sistema debe mantener suspendidas las sesiones de cómputo y proporcionar instantáneamente una conexión segura, siempre que se necesite. Esta ventaja sería algo más que sólo contar con un adorno extra. La respuesta del usuario sobre el acceso a Internet de banda ancha por cable y DSL sugiere que la conveniencia de estar siempre conectado es tan importante para el suscriptor como la capacidad de banda ancha para la información por sí misma.

La movilidad continua puede ser implementada por medio de una metodología MIP[8] o algunas otras. Típicamente, los elementos necesarios son: un Administrador Central de Movilidad (el agente de casa de la MIP), para seguirle la pista al usuario móvil y guiar la ruta convencional de IP; y un cliente móvil (el agente externo en la MIP, que puede ser desplegado como un componente independiente en una red externa o construido en el sistema operativo de la computadora portátil), para manejar los detalles de la conexión en las cercanías del usuario. Juntos, el administrador y el cliente crean y mueven las rutas del MIP, según las necesidades del usuario, y aseguran que las sesiones no se interrumpan cuando aquél suspende la operación o pasa de una subred a otra.

La IP móvil, junto con una solución de seguridad de extremo a extremo con la VPN, proporcionan una metodología conceptualmente satisfactoria a la conectividad permanente que necesitan los ejecutivos móviles. Desafortunadamente, esta capacidad no es todavía una característica estándar en los sistemas operativos más populares como Windows o MacOS, y su implantación en plataformas tan cerradas representa un reto trascendental.

El problema parte del hecho de que tanto el MIP como la VPN están superponiendo tres metodologías, mejor implantadas en la pila IP de los sistemas operativos. En los sistemas operativos cerrados, sin embargo, esta avenida esta bloqueada; el único recurso es esperar por una versión de sistema operativo que ofrezca esta ventaja o recurrir a los rodeos. De todas formas, ya sea por medio de una versión de sistema operativo o sacándole la vuelta, una solución de uso sencillo para movilidad permanente y segura es un requerimiento clave para extender el soporte WLAN a los usuarios móviles corporativos.

[8] IP Móvil o Móvil IP, por sus siglas en ingles

I.6.4. Administración de la Red.

Las redes Wi-Fi, especialmente aquellas que contienen *hotspots*, presentan retos de administración desalentadores. El servicio debe ser prestado a pesar del comportamiento egoísta de algunos usuarios, los ataques de *hackers* y la interferencia de otros sistemas. Tecnología inalámbrica innovadora y un plan de negocios bien estructurado y meditado de nada servirán si la red inalámbrica está pobremente administrada.

Además de las tareas usuales asociadas con la administración de las LAN cableadas (como el monitoreo del buen estado del equipo y la carga del tráfico), las WLAN presentan desafíos adicionales debido a que el desempeño de la red es muy dependiente de características variables e impredecibles en la capa física (por ejemplo, la conexión aérea).

Administrar la red para asegurar un desempeño parejo de la capa física (entrega de señal con fuerza adecuada con un aceptable nivel de interferencia) es un problema primordial. Los sistemas celulares enfrentan una situación parecida, pero tienen la ventaja de que, en su mayor parte, están diseñados, como sistemas completos, con herramientas adecuadas de administración integradas desde el principio. Las WLAN, en cambio, son más frecuentemente sobrepuestas en las capas existentes de la infraestructura cableada, únicamente con herramientas rudimentarias para administrar la fuerza de la señal y las interferencias.

En una red cableada, los problemas con la fuerza de la señal casi siempre provienen de una fuerte falla en algunos de los componentes, como un cable roto o una tarjeta de interfaz descompuesta. El desempeño de la capa física es esencialmente binario: funciona o no funciona. La situación es completamente diferente en el mundo inalámbrico, donde los cambios rutinarios de la ubicación de un usuario pueden causar variaciones en la fuerza de la señal de hasta 30 decibeles o más. El administrador de la red debe ser capaz de distinguir entre variaciones causadas por la operación normal y aquellas que indican fallas latentes, causadas, por ejemplo, por reconfiguración de las divisiones de la oficina.

En el manejo de interferencias, la tarea de la administración es similar a la que se enfrentan los operadores celulares, pero con una diferencia crucial, los sistemas celulares operan en bandas de frecuencia concesionadas, mientras que las redes WLAN, operan en las bandas no concesionadas. El operador celular, al menos en principio, puede administrar el espectro radial a través del área de servicio para optimizar el desempeño del sistema; el operador WLAN, en contraste, debe enfrentarse con múltiples fuentes de interferencia, muchas de la cuales no están bajo su control. En un ambiente como ese, toda la noción de la administración de redes puede ser vista como una paradoja.

Pero la situación, aunque desafiante, no debe representar que no existe esperanza. Por medio de una combinación cuidadosamente trabajada de técnicas de capas MAC y canalización de frecuencias, las redes WLAN pueden llevar, al menos, una administración rudimentaria de la interfase mutua entre usuarios. Si vamos más lejos, el Grupo de Tarea del estándar 802.11 probablemente recomiende herramientas adicionales para habilitar diferentes grados de servicio (presumiblemente a diferentes precios) para ser ofrecidos a distintos grupos de usuarios.

A pesar de estos avances, las redes inalámbricas permanecerán vulnerables a otras fuentes de interferencia, como un horno de microondas operando en la misma banda de frecuencia que una red WLAN cercana bajo la administración de otra empresa. Este último problema no es serio todavía porque la densidad de las instalaciones WLAN aún es relativamente baja, pero se irá haciendo más severo a medida que proliferen este tipo de redes. Es imperativo desarrollar herramientas que permitan a los administradores de sistemas monitorear la interferencia, identificar la fuente y tomar la acción correctiva.

La gran facilidad con que un Access Point puede ser añadido a una LAN cableada es, en sí misma, fuente de un serio problema de administración de la red. El llamado Punto de Acceso malintencionado (AP Rogue, por sus siglas en ingles), que resulta ser una calamidad para los administradores de la red, se trata de un Punto de Acceso no autorizado conectado a la Intranet de la corporación, quizá dentro de las instalaciones de la compañía o posiblemente en la casa de un empleado a distancia.

Cabe aclarar que el AP Rogue es un problema trascendental de vulnerabilidad. Independientemente de que la corporación utilice WEP o VPN, un Punto de Acceso malintencionado con WEP deshabilitado puede exponer las comunicaciones internas de la corporación al mundo exterior. Aun cuando WEP esté habilitado en el Punto de Acceso no autorizado, los corporativos que utilizan la VPN para asegurar sus WLAN se vuelven vulnerables a ataques que, de otro modo, serían inofensivos.

La detección de este tipo de Access Point dentro de las fronteras de la corporación (tal vez por medio de técnicas de *sniffing* y *pinging*), representa una carga de trabajo adicional, pero probablemente manejable, para los administradores de redes; en todo caso, es mucho más difícil detectarlos en las residencias de los empleados.

Para que las WLAN sigan expandiéndose en el ambiente de los negocios, deben desarrollarse herramientas y técnicas que den a los administradores confianza en que la seguridad no está siendo comprometida por puntos de acceso malintencionados dentro y fuera de los límites de una empresa.

CAPÍTULO II.

LAS ESPECIFICACIONES PARA EL PROTOCOLO 802.11x.

II.1 Introducción

Ante la existencia de dispositivos WLAN de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidad.

Las redes WLAN cumplen con los estándares genéricos aplicables al mundo de las LAN cableadas (i.e IEEE 802.3 o equivalentes) pero necesitan una normativa específica adicional que defina el uso de los recursos radioeléctricos. Estas normativas específicas definen de forma detallada los protocolos de la capa física (PHY) y de la capa de Control de Acceso al Medio (MAC) que regulan la conexión vía radio.

El primer estándar de WLAN lo generó el organismo IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) en 1997 y se denomina IEEE 802.11.

Desde entonces varios organismos internacionales han desarrollado una amplia estandarización normativa de WLAN y han generado un abanico de nuevos estándares. En los Estados Unidos de América, el grueso de la actividad lo mantiene el organismo IEEE con los estándares 802.11 y sus variantes (b, g, a) y en Europa el organismo relacionado es el ETSI con sus actividades en HiperLan2 o HomeRF.

II.2 Estándares de Redes de Área Local Inalámbrica.

En los últimos años han ido apareciendo una serie de estándares o especificaciones que tratan de cubrir distintas áreas en la tecnología inalámbrica, todos ellos con distintos niveles de estandarización e interoperabilidad. El más ampliamente extendido es el estándar IEEE 802.11, aunque también existen otras propuestas alternativas e incompatibles entre sí, como HomeRF o Bluetooth®, este último más enfocado a las redes de área personal. En este apartado se pretenden introducir los estándares más populares, mostrando sus características y requisitos técnicos. Se resumirán los aspectos más relevantes de cada uno de ellos en la Tabla II.1 tras haber sido presentados.

II.2.1. Redes IEEE 802.11

Las redes IEEE 802.11 suponen la apuesta del IEEE por las redes inalámbricas. Toda ellas se basan en una red tipo Ethernet y, aunque su filosofía es la misma, difieren en la banda de frecuencia utilizada, el ancho de banda que ofrecen, etcétera. Se verá que mientras las redes *Bluetooth®* se han implantado en componentes electrónicos de la gama baja, las redes 802.11 están siendo mayormente utilizadas a la hora de interconectar portátiles y PDA.

La especificación original de 802.11 preveía conexiones a velocidades de 1 ó 2 Mbps en la banda de los 2.4 GHz utilizando secuencia directa (DSSS) como método de transmisión en el espectro expandido *("Spread Spectrum)"*. En sus últimos estándares se utiliza la banda de los 5 GHz y puede llegar a ofrecer el nada despreciable ancho de banda de hasta 54 Mbps. Para evitar interferencias este último estándar utiliza otro método de transmisión conocido como OFDM, (Multiplexación por División en Frecuencia Ortogonal), que además proporciona una dificultad añadida a la hora de espiar la red.

Una de las características comunes en las diferentes implementaciones del estándar 802.11 es el uso del Protocolo de Seguridad WEP, *Wireless Equivalent Privacy*. WEP tiene como objetivo conseguir una seguridad equivalente a la de las redes convencionales (de cable); el problema reside en que las redes tradicionales basan gran parte de su seguridad en que es difícil comprometer el cable, mientras que la comunicación de las redes inalámbricas va por el aire. WEP es un protocolo razonablemente fuerte y computacionalmente eficiente, sin embargo, su uso no deja de ser opcional y se descubrió que no es del todo seguro, por lo que recientemente para mejorar estas debilidades se ha usado el Protocolo WAP (Wi-Fi Protected Access).

Dentro de la familia del 802.11, el estándar más extendido a día de hoy es el **802.11b**, también conocido como Wi-Fi (Wireless Fidelity). Wi-Fi es un término registrado auspiciado por la WECA, cuya finalidad es certificar productos de diferentes fabricantes basados en 802.11 y capaces de interoperar entre sí.

802.11b utiliza la banda de los 2.4 GHz y proporciona anchos de banda de hasta 11 Mbps. En espacios de interior es capaz de comunicar nodos separados 50 metros entre sí, mientras que llega a los 100 metros en el exterior.

La siguiente generación del 802.11 viene de mano de **802.11a**, también denominado WLAN. Esta implementación utiliza la banda de los 5 GHz y puede llegar a ofrecer el nada despreciable ancho de banda de hasta 54 Mbps. Para evitar interferencias se transmite en OFDM (Multiplexación por División en Frecuencia Ortogonal) y probablemente aún no se ha extendido su uso por su alto precio y porque no es compatible con los otros estándares 802.11.

Para terminar con las redes 802.11, cabe mencionar que también existe el estándar **802.11g**. Esta versión proporciona entre 20 y 54 Mbps usando DSSS y OFDM. La característica que lo hace especialmente interesante es su compatibilidad con las 802.11b y que tienen mayor alcance y menor consumo que las 802.11a.

II.2.2. Redes Bluetooth

La tecnología inalámbrica Bluetooth permite conectar a la perfección teléfonos móviles a distintos dispositivos como auriculares, computadoras portátiles y agendas personales sin preocuparse de cables o de la posición de los dispositivos.

Diseñado por un consorcio de importantes multinacionales, Nokia, Ericsson, IBM, Intel, y Toshiba. Bluetooth es capaz de operar en entornos ruidosos, utilizando un esquema de saltos de frecuencia y enlaces rápidos que contribuyen a hacer las conexiones más robustas. Sus módulos de radio actúan en la banda ISM de los 2.4GHz, y distribuye su espectro en 79 saltos o canales, con un desplazamiento de 1MHz cada uno, empezando en los 2.402GHz y acabando en los 2.480GHz. En algunos países este rango de frecuencias se ha visto temporalmente reducido, al haber tenido que adaptarse a sus regulaciones particulares respecto a la asignación del espectro radioeléctrico; así, España y Francia, por ejemplo, utilizarán en principio un sistema reducido a 23 canales.

Cada uno de los canales RF de la banda Bluetooth es, a su vez, dividido en fragmentos de tiempo numerados, teniendo cada fragmento una duración de 625 milisegundos. Cuando dos dispositivos Bluetooth establecen una comunicación, se designa a uno de ellos como maestro y al otro como esclavo, y transmiten la información alternativamente. El dispositivo maestro sólo puede iniciar su transmisión en uno de los segmentos de tiempo pares, mientras el esclavo sólo puede hacerlo en los impares. Además, el inicio de los paquetes de información debe alinearse con el inicio de los segmentos. Para evitar las interferencias, se salta a una nueva frecuencia cada vez que se transmite o se recibe uno de los paquetes. No es la primera vez que se usa este procedimiento pero, comparado con otros sistemas en la misma banda de frecuencias. Bluetooth salta más rápido y usa paquetes más cortos, con lo que se minimizan más, si cabe las oportunidades para el error.

Con respecto a su potencia, cada dispositivo Bluetooth puede clasificarse en tres grupos: Clase 1, 2 y 3. Los dispositivos de Clase 1 son los más potentes, diseñados para conexiones de largo alcance (en torno a los 100 metros) con una potencia máxima de salida de 20 dBm; los dispositivos de Clase 2 son los más comunes, con un alcance de 10 metros y una potencia máxima de 4 dBm;

finalmente, los dispositivos de Clase 3 tendrán un alcance de tan sólo 10 centímetros, y carecen de potencia de salida.

Las limitantes de este estándar son: usa la misma banda que los estándares 802.11 b y g además que no es compatible con otros estándares.

II.2.3. Otros Estándares WLAN

Existen otro tipo de redes, que aún no habiendo alcanzado la popularidad de los casos descritos con anterioridad, merecen que sean presentadas brevemente. Estas propuestas alternativas tienen en ocasiones el apoyo de grandes corporaciones, como por ejemplo, HomeRF el cual cuenta con el respaldo de Intel.

Una tecnología que no es estrictamente competidora de Bluetooth, pero que tiene ciertas similitudes con ella es la denominada **HomeRF** (Home Radio Frequency), las principales aplicaciones en que se encuentra éste estándar es la interconexión inalámbrica de un PC a otros dispositivos electrónicos de consumo, como son videos, electrodomésticos, juguetes avanzados, impresoras, centralitas, teléfonos inalámbricos, etc., con un rango de distancia que alcanza hasta los 45 metros. Al igual que Bluetooth, HomeRF utiliza el salto de frecuencia FHSS (que en este caso es de 50 por segundo) como método de transmisión para evitar interferencias; admite la comunicación de datos de 10Mbps, 5Mbps, 1.6Mbps, 0.8Mbps y en sus planes futuros esta el alcanzar los 20Mbps. Permite conectar hasta un total de 127 dispositivos y utiliza, también, la misma banda de 2.4 GHz.

Soporta comunicación de voz y datos, permitiendo hasta 6 conversaciones. El grupo de trabajo HRFWG, formado en marzo de 1998 por compañías como Compaq, Ericsson, Hewlett- Packard, IBM, Intel, Microsoft, Motorola, entre más de 100 son los que apoyan este estándar y han desarrollado el protocolo SWAP (Shared Wireless Access Protocol), basado en el estándar IEEE 802.11 para datos y el protocolo DECT para voz. Información adicional se encuentra en http://www.homerf.org.

A pesar de que 802.11a ha sido criticado negativamente, al menos por una parte, como la analogía inalámbrica de ATM, la tecnología que representa la mejor analogía es **HiperLan2**. Este estándar inalámbrico de alta velocidad que opera en los 5 GHz del espectro gozó del apoyo de compañías líder de tecnologías como Nokia, Panasonic y Sony. El regulador europeo ETSI creo regulaciones específicamente diseñadas para tomar en cuenta HiperLan2 y dejar a lado 802.11, pero sin importar esto, como tecnología LAN Inalámbrica, HiperLan2 prácticamente ha muerto. Algunos fabricantes aun tratan de colocar esta tecnología en el mercado de consumidores pero este hecho goza de poco

apoyo por parte de la comunidad inalámbrica ya que su implementación es complicada. Con esta tecnología se podían tener ancho de banda de datos de 6, 9, 12, 18, 27, 36 y 54Mbps como medidas de seguridad utiliza un esquema de cifrado-descifrado de uso opcional.

Tabla II.1 Estándares más importantes en WLAN

Estándar	Velocidad Máxima	Método de Propagación	Ancho de banda de canal	Frecuencia	Alcance	Numero de dispositivos	Medidas de Seguridad	Potencia de Transmisión máxima
802.11b	11 Mbps	DSSS	25 MHz	2.4 GHz	100m	Hasta 256	WEP	800 mW
802.11a	54 Mbps	OFDM	25 MHz	5 GHz	100 m	Hasta 256	WEP	800 mW
802.11g	54 Mbps	OFDM DSSS	25 MHz	2.4 GHz	125 m	Hasta 256	WEP	800 mW
HomeRF2	10 Mbps	FHSS	5 MHz	2.4 GHz	40-45 m	Hasta 127	Cifrado	100 mW
HiperLan2	54 Mbps	OFDM	25 MHz	5 GHz	150 m	Hasta 127	Cifrado	800 mW
Bluetooth	10 Mbps	FHSS AFH		2.4 GHz	100 m	Hasta 127	Cifrado	800 mW

II.3 El Estándar de facto: IEEE 802.11

El sector inalámbrico estableció, en 1999, el estándar 802.11b (o Wi-Fi) como el estándar predominante, lo que fomentó una baja en los precios de ésta tecnología a medida que iba aumentando la demanda. Hoy día, el equipo de red Wi-Fi para el uso empresarial y doméstico se vende a precios muy competitivos con las redes cableadas, y es muy fácil de comprar e instalar. En

esta parte hablaremos de manera general de los distintos estándares que existen para las redes Wi-Fi.

La denominación WI-Fi (Wireless-Fidelity) aplicada al protocolo inalámbrico IEEE 802.11b significa que, vía radio, mantiene con fidelidad las características de un enlace Ethernet cableado.

El estándar 802.11 IEEE debe ser observado con mayor detalle debido a que tiene un conjunto de variantes que ofrecen diferentes alternativas de conexión inalámbrica por lo que ha capturado la atención de los proveedores principales de esta tecnología y no es de extrañar que las expectativas del desarrollo inalámbrico sean muy positivas.

Las extensiones al estándar original se reconocen con la adición de una letra al estándar original como por ejemplo 802.11a, 802.11b y 802.11g.

II.3.1 Características del estándar 802.11b

Comúnmente denominado Wi-Fi, 802.11b describe el estándar IEEE para una red local inalámbrica que opera en la banda de radio a 2.4 GHz, que también es la frecuencia para hornos de microondas, teléfonos inalámbricos y dispositivos Bluetooth. Las redes locales inalámbricas basadas en el estándar 802.11b se utilizan con mucho más frecuencia que las redes 802.11a u 802.11g, y pueden alcanzar una transferencia de datos máxima de 11 Mbps a distancias aproximadas de 100 metros. 802.11b fue la primera tecnología de red local inalámbrica que se ofreció a los consumidores y que permitió la creación de redes inalámbricas en la oficina y en el hogar, así como puntos de conexión públicos, por eso es el estándar que lidera los desarrollos actuales de WLAN.

Emplea solamente DSSS como método de propagación y utiliza modulación en forma de onda CCK (Complementary Code Keying) lo que permite alcanzar su velocidad de 11 Mbps. Cada red local que se instale, emplea para transmitir 25 MHz del total de 80 MHz que típicamente se tiene en esa banda como disponible lo que implica que en una misma área de cobertura más de tres redes operando pueden ser un problema.

Es importante considerar si se está pensando en implementar una red inalámbrica o a un acceso a Internet inalámbrico que la gran mayoría de puntos de acceso inalámbricos de hoy día son 802.11b. En la siguiente tabla se resumen sus principales características.

802.11b (Wi-Fi)

Frecuencia
2.400 - 2.4835 GHz
ISM Band (Industry, Science, and Medicine)

Tecnología
DSSS (Direct Sequenced Spread Spectrum)
- Modulación
  - CCK (Complementary Code Keying) 5.5 / 11 Mbps
  - QPSK (Quadrature Shift Keying) 2 Mbps
  - BPSK (Binary Phase Shift Keying) 1 Mbps
- 14 canales, 11 con regulación FCC
  - 3 non-overlapping
- 20 MHz

Ancho de Banda
- 11 Mbps transmisión / 5.5 Mbps efectivos
- Fall back 5.5, 2 and 1 Mbps

Seguridad
- WEP 64 bit, 128 bit encripción
- SSID (Service Set Identifier)
- 802.1x
- MAC Filtering

Media access protocol
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Distancia
- Hasta 100 metros

Aprobación Julio 1999

Tabla II.2 Características del estándar 802.11b

II.3.2 Características del estándar 802.11a

También conocido como WLAN, describe el estándar inalámbrico para una red que opera en la banda de radio de 5 GHz, la cual es de 300 MHz (frente a los 83.5 de la banda de 2.4 GHz) y se puede disponer en 2 bloques de frecuencia uno de 200 MHz y el otro de 100.

Las redes locales inalámbricas basadas en el estándar 802.11a, pueden tener una velocidad máxima de transmisión de 54 Mbps, en distancias que alcanzan unos 100 metros, lo que proporciona una velocidad de datos de red hasta cinco veces superior que 802.11b y pueden gestionar más tráfico que las redes basadas en ese estándar. La ventaja de operar en una frecuencia más alta es que se tienen 12 canales disponibles. Esto hace que la norma "a" sea más adecuada para instalaciones empresariales a gran escala: más canales ofrecen soporte para mayor densidad de usuarios por Punto de Acceso en un espacio determinado.

Los productos Wi-Fi "a" y "g" comparten la misma técnica de modulación OFDM, lo que da a ambos estándares un caudal de procesamiento más alto pero contra esta ventaja, no es compatible con 802.11b, por lo que se necesitara un nuevo equipo inalámbrico si se cambia de estándar.

802.11a permite que coexistan en el mismo espacio de cobertura hasta ocho redes, tiene mayor consumo de energía; hecho que representa un problema en el uso de equipos móviles y requiere de actualización de hardware.

Sin embargo, lo más destacado de este estándar 802.11a, es que a pesar de que en el mercado estadounidense ya existen multitud de productos que lo utilizan, su operatividad no ha sido posible en forma considerable dentro de los países europeos como España, Italia, Portugal y Alemania, porque la banda en la que opera, los 5GHz, es de uso restringido militar y en los países en los cuales su uso es de licencia libre solo tiene asignados 150MHz de banda. Según comenta Antonio Gracia, responsable de producto final de 3Com en España, "los países afectados estamos a la espera de que se liberalice esta frecuencia, pero lo cierto es que hoy por hoy, todavia no se ha movido nada". La siguiente tabla resume las principales características del estándar.

802.11a (Wi-Fi)

Frecuencia
5 GHz
UNII Band (Unlicensed National Information Infrastructure)

Tecnología
OFDM (Orthogonal Frequency Division Multiplexing)
- Modulación
  - 64-QAM (64-level quadrature amplitude modulation) 48/54 Mbps
  - 16-QAM (16-level quadrature amplitude modulation) 24/36 Mbps
  - QPSK (Quadraphase-shift Keying) 12/18 Mbps
  - BPSK (Binary Phase Shift Keying) 6/ 9 Mbps
- Canales
  - 12 non-overlapping
- 20 MHz

Ancho de Banda
- 54 Mbps transmisión / ~30 Mbps efectivos
- Fall back 48, 36, 24, 18, 12, 9, 6 Mbps

Seguridad
- WPA (Wi-Fi Protected Access)
- WEP 64 bit, 128 bit encripción
- SSID (Service Set Identifier)
- 802.1x
- MAC Filtering

Media access protocol
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Distancia
- Hasta 100 metros

Aprobación Julio 1999

Tabla II.3 Características del estándar 802.11a

II.3.3 Características del estándar 802.11g

Es el estándar ratificado más recientemente como norma Wi-Fi que describe un método de red inalámbrica que opera en tres canales del espectro de los 2.4 GHz. Al utilizar la tecnología OFDM (Modulación por División Octogonal en Frecuencia), las redes locales inalámbricas basadas en el estándar 802.11g pueden alcanzar una velocidad de transferencia de datos de 54 Mbps.

Funciona en la misma banda de radio que el estándar 802.11b y sus productos son compatibles por lo que los clientes "b" y "g" pueden compartir la misma red inalámbrica pero en esta situación el Punto de Acceso debe manejar los 2 tipos de transmisiones: OFDM y DSSS; el resultado del exceso de carga es una baja del desempeño para los clientes "g".

Al operar en la banda de 2.4 mantiene la característica de tener problemas con más de tres redes operando a la vez. En la siguiente tabla se resumen las principales características de este estándar.

802.11g (Wi-Fi)

Frecuencia
2.412 - 2.4835 GHz
ISM Band (Industry, Science, and Medicine)

Tecnología
- DSSS (Direct Sequenced Spread Spectrum)
- OFDM (Orthogonal Frequency Division Multiplexing
- Modulación DSSS
  - CCK (Complementary Code Keying) 5.5 / 11 Mbps
  - QPSK (Quadraphase-shift Keying) 2 Mbps
  - BPSK (Binary Phase Shift Keying) 1 Mbps
- Modulación OFDM
  - 64-QAM (64-level quadrature amplitude modulation) 48/54 Mbps
  - 16-QAM (16-level quadrature amplitude modulation) 24/36 Mbps
  - QPSK (Quadraphase-shift Keying) 12/18 Mbps
  - BPSK (Binary Phase Shift Keying) 6/ 9 Mbps

- 14 canales, 11 con regulación FCC
  - 3 non-overlapping
- 20 MHz

Ancho de Banda
- 54 Mbps transmisión / ~30 Mbps efectivos
- Fall back 48, 36, 24, 18, 12, 9, 6 Mbps

Seguridad
- WPA (Wi-Fi Protected Access)
- WEP 64 bit, 128 bit encripción
- SSID (Service Set Identifier)
- 802.1x
- MAC Filtering

Media access protocol
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Distancia
- Hasta 125 metros

Aprobación Junio 2003

Tabla II.4 Características del estándar 802.11g

II.3.4 Otras Especificaciones IEEE

Una de las principales virtudes de este estándar es que posee diferentes variantes que potencian su capacidad de transporte y seguridad. Aquí explicamos brevemente los desarrollos que se están realizando en el IEEE para mejorar los actuales sistemas inalámbricos.

- **802.11c** Es un esquema pensado para introducir en las WLAN el esquema de calidad de servicio y el manejo de direcciones MAC para puentes entre redes.

- **802.11d** Define requerimientos físicos de operación para diferentes paises.

- **802.11e** Está dirigido a los requerimientos de Calidad de Servicio (QoS) para todas las interfases IEEE WLAN de radio. Diseñada para soporte de aplicaciones de voz y video.

- **802.11f** Define la comunicación entre puntos de acceso (roaming) para facilitar redes WLAN de diferentes proveedores.

- **802.11h** Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia-Pacífico. La norma IEEE 802.11h es una evolución de 802.11a que permite la asignación dinámica de canales y control automático de potencia para minimizar los efectos interferentes.

- **802.11i** Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Llaves Íntegras-Seguras Temporales) y AES (Estándar de Encriptación Avanzado).

- **802.11j** Define la coexistencia entre 802.11a e HyperLan2.

- **802.11n** Que se propone proveer velocidades mayores a 100 Mbps.

II.3.5 ¿Qué estándar es la mejor opción?

Aunque no es un cuestionamiento fácil de responder y, actualmente, la búsqueda de la respuesta está en boca de especialistas y analistas de todo el mundo, se debe tener en cuenta lo siguiente: aunque la velocidad ideal del 802.11g es de 54 Mbps, en un entorno real (fuera de un laboratorio de pruebas) y según diferentes fabricantes de equipos, la velocidad sería de 6 Mbps (debido a que la interferencia de dispositivos a la misma frecuencia puede afectar su desempeño). En cambio, el 802.11a, en pruebas reales, tiene un desempeño de hasta 20 Mbps. Por otro lado, las pruebas con 802.11b llevan a tener una velocidad efectiva de 4 Mbps hoy día. Así que el usuario deberá evaluar, de acuerdo a sus necesidades y costos en que tecnología se va a invertir.

La siguiente tabla contiene las especificaciones del estándar 802.11 que actualmente están en el mercado.

Estándar	802.11b	802.11a	802.11g
Velocidad	11 Mbps / 5.5 Mbps	54 Mbps / 30 Mbps	54 Mbps / 30 Mbps
Frecuencia	2.4 GHz	5.8 GHz	2.4 GHz
Precio	Económico	Alto	Accesible
Distancia máxima	50 - 100 m	50 -100 m	50 - 125
Popularidad	Amplia	Nuevo	Nuevo
Compatibilidad	Comunmente usado	No compatible	802.11b

Tabla II.5 Especificaciones Actuales del estándar 802.11

II.4.- Las Capas OSI en el estándar IEEE802.

La Norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del Sistema OSI: la capa física y la capa de enlace. De hecho, a la capa de enlace se le divide en dos; por lo que, el resultado son tres capas:

- **PHY** (*Physical Layer*, "Capa Física"), es la capa que se ocupa de definir los métodos por los que se difunde la señal.
- **MAC** (*Médium Access Control*, "Control de Acceso al Medio"), es la capa que se ocupa del control de acceso al medio físico. En el caso de Wi-Fi 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.
- **LLC** *(Logical Link Control)*, es la capa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

La capa física (PHY) del estándar IEEE 802.11 se diseñó para cumplir con la regulación de radio frecuencia del FCC (Organismo Federal en USA). Las mismas bandas de frecuencia, con algunas variantes, se utilizan en el resto del mundo. La Figura II.6 muestra el espectro de la banda de 2.4 GHz. Los canales (de 22 MHz cada uno) utilizados por 802.11b son los impares (canales 1, 3, 5, 7, 9, 11 y 13).

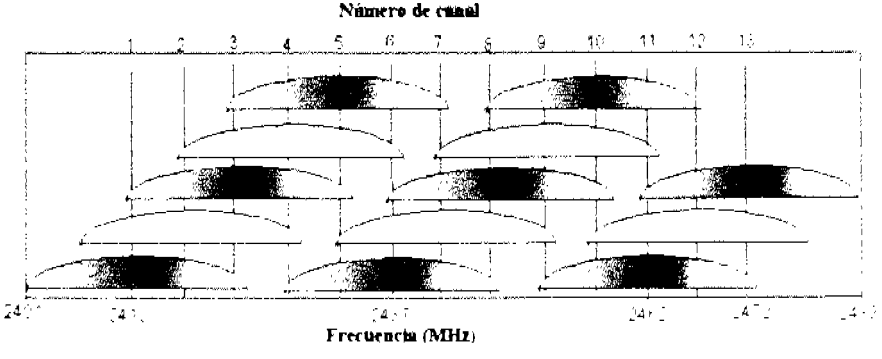


Figura II.6.- Frecuencias asignadas en la Banda 2.4 GHz.

II.4.1.- La Capa Física

Como se ha visto, la capa física se ocupa de definir los métodos por lo que se difunde la señal. Para hacer esto, la capa física de IEEE 802.11 se divide en dos subcapas: lo que se conoce como PLCP (*Physical Layer Convergence* Procedure, "Procedimiento de Convergencia de la Capa Física") y PMD (*Physical Médium Dependent*, "Dependiente del Medio Físico").

PLCP se encarga de convertir los datos a un formato compatible con el medio físico. Por ejemplo, este formato es distinto si se trata de un medio físico de infrarrojos o de radio, mientras que PMD es el que se encarga de la difusión de la señal. Por cierto, aunque las especificaciones de IEEE 802.11 proyectan la opción de utilizar infrarrojos como medio de transmisión, no se llego a desarrollar de manera considerable este sistema debido principalmente al corto alcance que ofrece y a que no es utilizable en el exterior debido a interferencias producidas por agentes naturales como la lluvia y la niebla.

En cuanto a la utilización del medio radioeléctrico, la tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como "Espectro Expandido" *(Spread Spectrum)*. Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario para la transmisión de la información. Lo que se consigue con esto es un sistema muy resistente a las interferencias de otras fuentes de radio, resistente a los efectos de eco *(multipath)* y puede coexistir con otros sistemas de radiofrecuencia sin verse afectado y sin influir en su actividad. Estas ventajas, hacen que la tecnología de espectro expandido sea la más adecuada en las bandas de frecuencia para las que no se necesita licencia.

Existen distintas técnicas de espectro expandido, entre las que se encuentran la tecnología CDMA utilizada en la tercera generación de telefonía móvil y las 3 técnicas que el estándar IEEE 802.11 utiliza como métodos de propagación.

- ✓ FHSS (*Frequency Hopping Spread Spectrum*, "Espectro Expandido por Salto de Frecuencia"), con la que se consiguen velocidades de transmisión de 1 Mbps.

- ✓ DSSS (*Direct Sequence Spread Spectrum*, "Espectro Expandido por Secuencia Directa"), con la que se consiguen velocidades de transmisión de 2 Mbps. En versiones posteriores de este sistema, se ha conseguido, velocidades superiores.

- ✓ OFDM (Orthogonal Frecuency Division Multiplexing, "Multiplexación Ortogonal por División de Frecuencias"), con la que se consigue velocidades de transmisión de hasta 54 y 100 Mbps.

Dependiendo de la velocidad a la que se van a transmitir los datos, la Norma IEEE 802.11 utiliza una técnica u otra.

En 1999, el IEEE sacó una nueva versión de DSSS que permite transmitir datos a 11 Mbps. Esta nueva versión DSSS es usada en la Norma IEEE 802.11b. Por esta razón, al 802.11b también se le conoce como 802.11 DSSS ó 802.11 HR (*High Rate*, "Alta Velocidad").

Por otro lado, la mayoría de las tarjetas inalámbricas de las estaciones de trabajo son semidúplex (sólo tienen un equipamiento de radio), por lo que pueden transmitir o recibir, pero no ambas cosas simultáneamente.

II.4.1.1- FHSS.

La técnica FHSS (*Frequency Hopping Spread Spectrum*, "Espectro Expandido por Salto de Frecuencia"), consiste en dividir la banda de frecuencias en una serie de canales e ir transmitiendo la información saltando de un canal a otro de acuerdo con un patrón de saltos *(Spreading Code or Hopping Code)*, conocido tanto por el emisor como por el receptor. El tiempo máximo que se debe permanecer en cada frecuencia está regulado en 400 mseg. El inconveniente de FHSS es que tenía la necesidad de sincronizar el emisor y el receptor en la frecuencia a utilizar en cada momento. Este problema fue resuelto por los ingenieros de *Sylvania Electronics Systems®* desde hace ya muchos años.

El Estándar (Norma) IEEE 802 definió en 1997 que cada canal de FHSS tuviera un ancho de banda de 1 MHz dentro de la banda de frecuencias de 2.4 GHz. El ancho de banda total disponible y, por tanto, el número total de canales disponibles varía de acuerdo con el marco regulatorio de cada país o área geográfica, pero en cualquier caso, siempre existen tres juegos de secuencia de saltos.

La técnica FHSS reduce las interferencias porque, en el peor de los casos, la interferencia afectará exclusivamente a uno de los saltos de frecuencia, y la señal se libera de ésta al saltar a una frecuencia distinta. El resultado es que el número de bits erróneos es extremadamente bajo. Otra de las ventajas de FHSS, es que permite que coexistan varias comunicaciones en la misma banda de frecuencias. Para ello, cada comunicación debe tener un patrón de saltos con distinta secuencia.

A pesar que la Norma original IEEE 802.11 incluía el sistema FHSS, no existe actualmente, ninguna especificación IEEE que utilice esta técnica. La razón es que la velocidad máxima que se consigue con la técnica FHSS es de

pocos Mbps. No obstante, es posible que en un futuro se consigan velocidades superiores; se habla de hasta 15 Mbps.

II.4.1.2.- DSSS.

La técnica DSSS se basa en sustituir cada bit de información por una secuencia de bits conocida como *chip* o *código de chips (Chipping Code)*. Estos códigos de chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits. Entre las señales que son eliminadas se encuentra el ruido y las interferencias.

El *código de chips* permite al receptor identificar los datos como pertenecientes a un emisor determinado. El emisor genera el *código de chips* y, sólo los receptores que conocen dicho código pueden descifrar los datos. Por tanto, en teoría, DSSS permite que varios sistemas puedan funcionar en paralelo; cada receptor filtrará exclusivamente los datos que corresponden con su *código de chips*. Por otro lado, cuanto más largo es el *código de chips*, más resistente será el sistema a las interferencias y mayor número de sistemas podrán coexistir simultáneamente. La Norma IEEE 802.11 establece que la longitud mínima del *código de chips* debe ser de 11.

En la práctica, la coexistencia de sistemas no se consigue por el uso de distintos *códigos de chips*, sino por el uso de distintas bandas de frecuencias. Un sistema DSSS de 11 Mbps (IEEE 802.11b), necesita un ancho de banda de 22 MHz, siendo la distancia mínima entre portadoras de 30 MHz. Como el ancho de banda disponible en la banda de 2.4 GHz (en el área regulada por el FCC) es de 83.5 MHz, sólo es posible la coexistencia de tres sistemas DSSS en el mismo lugar.

II.4.1.3.- OFDM.

Es la técnica de gestión de frecuencias utilizada por el IEEE 802.11a y 802.11g. Esta técnica divide el ancho de banda en subcanales más pequeños que operan en paralelo. De esta forma, se consigue llegar a velocidades de transmisión de hasta 54 Mbps (100 Mbps con soluciones propietarias).

La técnica OFDM fue patentada por *Bell Labs*® en 1970, y está basada en un proceso matemático llamado FFT (*Fast Fourier Transform*, "Transformada Rápida de Fourier"). OFMD divide la frecuencia portadora en 52 subportadoras solapadas, 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor. Este sistema consigue un uso muy eficiente del espectro radioeléctrico.

OFMD puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite OFMD son 6, 9, 12, 18, 24. 36, 48 y 54 Mbps.

Una de las ventajas de OFDM, es que consigue una alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno (eco). Estas ondas llegan al receptor con distinta amplitud y a distinto tiempo que la señal principal, produciendo interferencias. Estas interferencias son un problema a velocidades superiores a 4 Mbps; por este motivo, se utilizan técnicas (como OFDM) que mitiguen este efecto. En la siguiente tabla se muestran las principales caracteristicas de estas técnicas.

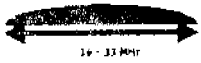
FHSS	DSSS	OFDM
Transmite los datos en portadoras que cambian o saltan de frecuencia en función del tiempo	Banda angosta dispersa sobre un amplio espectro Baja amplitud	Transmite señales simultáneas de alta velocidad Divide el espectro en varios sub-portadoras
Ventajas Alta tolerancia a interferencia Alta seguridad contra intercepción de la señal	**Ventajas** Alta velocidad Más resistente contra interferencia que banda angosta	**Ventajas** Alta eficiencia espectral Alta velocidad de transmisión No requiere retransmisión de datos
Desventajas Baja/Media velocidad Dificultad en P-MP Difícil de sincronizar en Larga distancia	**Desventajas** Ciertas afectaciones por ruido y multitrayectoria Próximo a su límite de velocidad	**Desventajas** Costo Requiere mayor capacidad de procesamiento
		

Tabla II.7 Características de los métodos de Propagación en el Espectro

II.4.2 La Capa MAC en IEEE802.

Respecto a la capa MAC (Control de Acceso al Medio) se puede mencionar que los estándares IEEE 802.11 utilizan dos posibles mecanismos de acceso:

1.- CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) en el que cada estación escucha a otros usuarios (Carrier Sense) y si el control esta sin usar la estación está autorizada a transmitir (Collision Avoidance). Pero si está ocupada, cada estación espera hasta que la transmisión presente, finalice, y después entre en un procedimiento de "Random Back". Esto previene que múltiples estaciones intenten obtener el medio inmediatamente después de completarse la transmisión precedente.

El proceso de transmisión es el siguiente, si el medio ha estado libre durante un intervalo de tiempo (DIFS) entonces se transmite el paquete de datos. Una vez recibido, el receptor enviará una conformación de recepción (ACK). La Figura II.8 presenta el comportamiento de este protocolo.

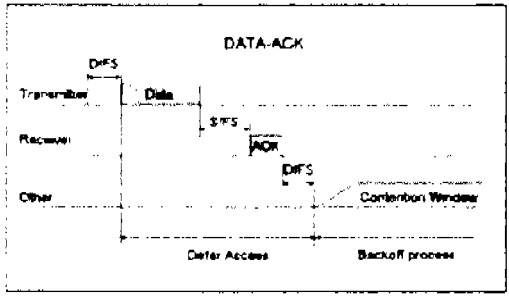


Figura II.8.- Protocolo CSMA/CA.

Si el transmisor ha encontrado el medio ocupado, espera a que se acabe la transmisión actual, y cuando vuelva a intentar transmitir tendrá que esperar el tiempo DIFS, más un tiempo de contención (Back-Off) seudoaleatorio.

2.- RTS/CTS: Es un procedimiento opcional en el que la terminal que quiera transmitir tiene que enviar al Punto de Acceso, una solicitud de envio (Request To Send) a la que el Punto de Acceso accede (Clear To Send) a la transmisión. De esta manera se soluciona el problema del nodo oculto en el que dos transmisores separados no detectan las transmisiones de terminales distantes y los paquetes llegan degradados al Punto de Acceso. En este caso el Punto de Acceso coordina el tráfico WLAN al ser el encargado de dar los permisos de transmisión.

II.5- Mecanismos de Seguridad usados en IEEE802.11.

Como se sabe, la Seguridad en Redes tipo Inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el Aire. Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el Punto de Acceso y los clientes inalámbricos, proteger al sistema de administración de acceso no autorizado y la protección de los datos mismos.

En los inicios de la Tecnología Inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN privadas desde la calle. En la actualidad, existen técnicas más complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos a este tipo de redes.

El estándar inalámbrico 802.11 original incorpora encriptación y autenticación *WEP* (Privacidad Equivalente a Cable). Sin embargo, en el año 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo ya que la clave *WEP* puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica, por lo que dentro de los estándares de seguridad del Grupo 802.1x, se propuso utilizar mecanismos que permitan ligar una WLAN a sistemas como RADIUS para la validación de usuarios. El método para ligar los puntos de acceso, las llaves de usuario y los sistemas de RADIUS en una red inalámbrica, se conoce como EAP (Extensible Authentication Protocol), y tiene una diversidad de variantes como: EAP-MD5-Cisco Wireless (también conocido como LEAP o Lightweight EAP), EAP-TLS, y EAP-TTLS.

Otra propuesta para resolver el problema de debilidad de WEP es utilizar el protocolo TKIP (Temporal KEY Integrity Protocol) como parte de los estándares de 802.11i. Se presenta también como solución usar un nuevo estándar que la Alianza de Wi-Fi llama WPA (Wi-Fi Protected Access), pero esto representa un cambio en la creciente ola de interfaces instaladas en el mercado.

Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquellos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

La seguridad es uno de los aspectos esenciales para la aceptación de las WLAN por usuarios empresariales o para aplicaciones públicas. Como todas las tecnologías radio, las WLAN no se pueden confinar dentro de los muros de un

edificio por lo que deben extremarse las medidas de seguridad, ya que en caso contrario se abriría la red LAN a todo aquel que con una tarjeta WLAN y una antena direccional quiera conectarse.

II.6 Extendiendo la WLAN: Intercomunicación entre Puntos de Acceso

Los estándares mencionados hasta ahora permiten la conexión de los clientes dentro de una misma sub-red IP o entre varias. Actualmente si se quiere mover un cliente sobre diferentes sub-redes IP se pueden utilizar soluciones de varios fabricantes situación que no se podía realizar antes. El IEEE desarrollo un nuevo estándar que define la intercomunicación entre puntos de Acceso de distintos fabricantes (facilitando el "Roaming") y que estuvo disponible a partir de finales del 2003. Entre otros temas este estándar define el registro de un Punto de Acceso dentro de una red y el intercambio de información cuando un usuario se mueve por una zona cubierta por AP de diferentes fabricantes. Esta norma es conocida como IEEE 802.11f.

¿Pero cuando se necesita más de un AP? El caudal eficaz real en una transmisión (conocido como *Throughput)* promedio de una red WLAN es sensiblemente inferior a la cantidad indicada como velocidad máxima de la tecnología. Esto es debido a que parte de la información transmitida se consume en cabeceras radio o en funciones de codificación de canal. Adicional a la distancia existente entre el terminal y el Punto de Acceso, la existencia de interferencias disminuirán aún más la capacidad práctica transmitida. En una red WLAN la capacidad se configura, por defecto, en modo automático para que se regule en función de la calidad del enlace radio.

Además, la capacidad resultante debe ser compartida por los distintos usuarios que comparten un mismo Punto de Acceso. Cuando la capacidad resultante para cada usuario no es suficiente para la aplicación requerida es necesario incrementar el número de Puntos de Acceso en una misma celda (utilizando diferentes canales radio) y así permitir mayores densidades de tráfico.

Para evitar solapamiento entre canales, cuando dos equipos transmiten en el mismo emplazamiento, la norma IEEE 802.11 indica que se debe dejar una separación entre las frecuencias centrales de los canales mayor de 22 MHz. Esta condición significa que, en la banda de 2.4 GHz, hasta tres Puntos de Acceso pueden coexistir en una misma celda (se suelen emplear los canales 1, 6 y 11 de la banda 2.4 ver Figura II.6). La banda de 5 GHz (IEEE 802.11a) permite la utilización de hasta ocho Puntos de Acceso coexistiendo en la misma celda. La utilización de dispositivos de banda dual 802.11 a + 802.11 b permitiría la instalación de hasta once Puntos de Acceso en la misma celda sin solape de frecuencia.

El dimensionado del número de Puntos de Acceso de una red debe garantizar el tráfico en el área considerada pero también la cobertura radioeléctrica. En muchas ocasiones la presencia de obstáculos obliga al despliegue de entornos multi-celda para garantizar la cobertura del área deseada. El enlace de estas tecnologías está íntimamente relacionado con las antenas utilizadas y con el entorno de propagación (interior, exterior, obstáculos, etcètera).

Dependiendo de la frecuencia y del número de obstáculos se considera que en aplicaciones de interior (potencia 20 dBm) el enlace típico del 802.11 varía entre 45 y 100 m, sin embargo en aplicaciones de exterior (potencia 30 dBm) y en función de la ganancia de las antenas terminales este enlace puede ser superado ampliamente.

II.7 Más allá del Uso en Redes Empresariales.

Originalmente las redes WLAN fueron diseñados para su empleo en redes empresariales. En este tipo de aplicaciones una sub-red WLAN, compuesta por varios Puntos de Acceso inalámbricos, se conecta a una red cableada que permite acceder a todos los servicios disponibles en la empresa.

Pero en la actualidad las redes WLAN han encontrado una gran variedad de nuevos escenarios de aplicaciones tanto en el ámbito residencial como en entornos públicos, a continuación se listan los usos más frecuentes.

- Escenario Residencial: Una línea telefónica terminada en un router ADSL al cual se conecta un AP para formar una red WLAN que ofrece cobertura a varias computadoras en el hogar.
- Redes Corporativas: Una serie de Puntos de Acceso distribuidos en varias áreas de la empresa conforman una red WLAN autónoma o complementan a una LAN cableada. Son aplicaciones de alta densidad de tráfico con altas exigencias de seguridad.
- Acceso público a Internet desde cafeterías, tiendas,... En estos establecimientos se ofrece a los clientes una tarjeta inalámbrica (NIC) que permite acceso a Internet desde sus propios portátiles. Es un escenario de acceso involucrando un bajo número de Puntos de Acceso, parecido al residencial, pero que necesita mayores funcionalidades en el núcleo de red (servidor AAA, billing, etcétera).
- Acceso público en banda ancha de pequeños pueblos, hoteles, Campus Universitarios,... En general este escenario necesita múltiples Puntos de Acceso para garantizar la cobertura del área considerada.

Es necesario distinguir entre las redes sin ánimo de lucro (redes libres) que ofrecen un servicio gratuito a una comunidad y las redes que ofrecen servicios de pago a clientes que residen o transitan por la zona de cobertura.

- WLAN para cobertura de "Hotspots" Es un escenario público donde estas redes cubren áreas donde se concentra un gran número de usuarios de alto tráfico como son aeropuertos, estaciones de ferrocarril, centros de congresos, etc. La red a instalar requiere un elevado número de Puntos de Acceso así como importantes exigencias de seguridad, gestión de red, facilidades de facturación, etcétera.

- Acceso a Internet desde medios públicos de transporte. En los últimos meses se esta convirtiendo en un tema de actualidad el hecho de que compañías ferroviarias quieran ofrecer acceso de banda ancha desde sus trenes en movimiento, o compañías aéreas (como Lufhtansa) que ofrecen acceso a Internet desde sus vuelos Intercontinentales; en varias ciudades del mundo se disponen de taxis que incorporan una pantalla integrada en el asiento que permite acceder a Internet de banda ancha. En el caso de Lufhtansa la solución está basada en un acceso Wi-Fi en el interior del avión que termina un enlace vía satélite con la red Internet. En las otras dos aplicaciones Wi-Fi forma parte tanto de la red de acceso (en el interior del vehículo) como de la solución de transporte hacia la red fija.

Pero, ¿qué se necesita para la conexión a ese tipo de redes? En la mayoría de los casos, este acceso a Internet no es gratis. Se debe contar con un Proveedor de Servicios de Internet inalámbrico, igual que se tiene un proveedor de acceso a Internet vía telefónica. Además, se requiere de una computadora que soporte esta tecnología. Se puede hacer por medio de una tarjeta externa o, bien, teniendo una computadora con soporte de conectividad inalámbrica 802.11b integrada.

La Figura II.9 muestra la infraestructura de red necesaria para un Operador que quiera ofrecer todo este tipo de aplicaciones.

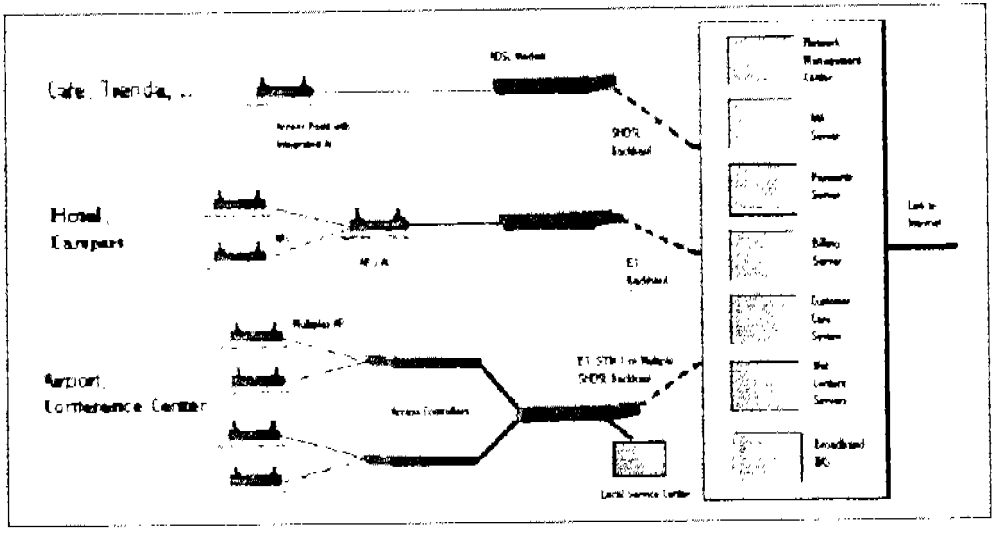


Figura II.9.- Arquitectura de Red para Oferta de Distintos Tipos de Aplicaciones.

Como las redes públicas son del tipo de pago por servicios siempre hay un operador de telecomunicaciones detrás de su gestión. Como se deduce en la Figura II.9 un Operador establecido (especialmente si es móvil) dispone de gran parte de la infraestructura necesaria para ofrecer un servicio de amplia cobertura. Actualmente existen varios tipos de operadores actuando en el sector WLAN:

- Operadores "Wireless ISP" que ofrecen cobertura local de banda ancha en pueblos o en pequeñas ciudades utilizando WLAN. Este servicio está bastante extendido en USA.
- Operadores "Wireless SP" que ofrecen cobertura nacional en los puntos de alta densidad de tráfico conocidos como "hotspots" (aeropuertos, estaciones, hoteles, etcétera) utilizando WLAN.
- Operadores móviles que complementan su oferta de movilidad global con cobertura WLAN en "hotspots". Esta actuación es debido a dos factores: de un lado evitar que los operadores WLAN anteriores, que ofrecen la cobertura de "Hotspots" a nivel nacional, capten un porcentaje importante de mercado de servicios de UMTS. De otro lado capitalizar su infraestructura de red dado que ya poseen muchos activos necesarios para las redes WLAN tales como plataformas de autentificación, de gestión de red, de servicios, de facturación, etcétera.

Como ejemplos de operadores que ofrecen este tipo de servicios públicos en la actualidad se pueden mencionar los siguientes:

- Wayport (USA) que cubra una tarifa de $4.95 a $7.95 por día y localidad. Este proyecto tiene 542 hotspots en lugares de tránsito denso, como aeropuertos u hoteles, además de un acuerdo con McDonald's para instalar Wi-Fi en buena parte de los restaurantes de comida rápida de EE UU.
- Mobilestar (USA) ofrece tarifas de suscripción mensual que van desde pago por minuto o un solo pago por acceso sin límite.
- En Europa, Telia HomeRun ofrece servicios similares en Suecia y en Noruega pero con tarifas más altas.
- T-Mobile (rama móvil de DT) anunció en Diciembre 2002 que se haría cargo de la red Wi-Fi de 1200 Starbucks Cafes en USA. Gran parte de la infraestructura Wi-Fi de dichos cafés pertenecía a MobileStar que se desliga de dichos nodos de acceso.
- France Telecom en Febrero 2003 hizo el lanzamiento del servicio WLAN.
- El Proyecto Cometa Project anuncia 20.000 hotspots en USA en un futuro cercano.
- En España se tiene los ejemplos de Afitel con despliegue en la Ciudad de Zamora o la oferta de NeoSky para llevar servicios de banda ancha a aldeas remotas por medio de una red WLAN conectada vía satélite con la red Internet.
- En México Telmex y Multivisión ofrecen el servicio de conectividad móvil.

Strategy Analytics Research[9] sobre un estudio de mercado realizado sobre el uso de WLAN, estima que en Europa habrá en el año 2006 más de 20 millones de usuarios de redes WLAN públicas generando más de 3000 millones de dólares de ingresos para sus operadores.

Se considera que el 10% de los usuarios de redes móviles serán también usuarios de redes WLAN y que los operadores móviles perderán más del 10% de sus ingresos por la competencia de esta tecnología por lo que les recomienda que complementen sus redes con tecnología WLAN.

La Figura II.10 muestra la estimación del mercado mundial para las aplicaciones públicas de las WLAN realizada por Strategy Analytics.

[9] Strategy Analytics es una firma de Consulta e Investigación de Mercado Global en áreas de Comunicación, Informática y de Entretenimiento

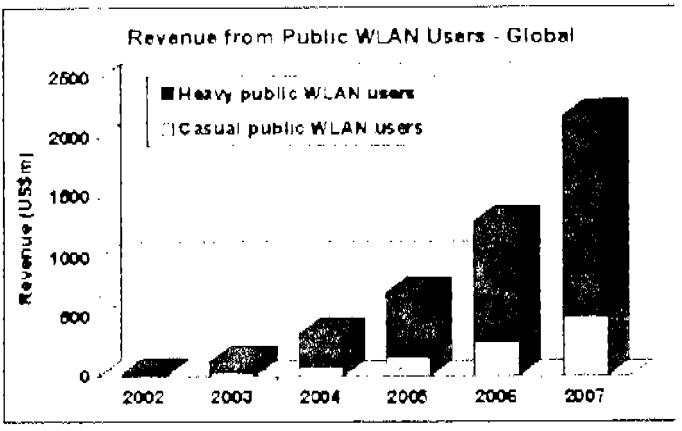


Figura II.10 Mercado Mundial para Aplicaciones Públicas WLAN (Strategy Analytics)

El estudio de Strategy Analytics considera que actualmente se está llegando a un proceso de consolidación de los operadores WLAN del que sobrevivirá un pequeño número final de operadores con acuerdos de "Roaming" entre ellos. Esta fase también añadirá servicios WLAN a la oferta de la mayoría de los operadores móviles produciéndose un complemento ideal de conectividad global a nivel nacional. Con cobertura de banda ancha en todos los puntos de alta densidad de tráfico (hotspots).

Pero ¿qué ha hecho que haya crecido tan rápidamente esta tecnologia?

• Primero, es una tecnología que cambia totalmente el concepto de la utilización de una computadora, permitiendo tener conectividad a Internet prácticamente sin limitaciones de lugar o de tiempo, mejorando así la experiencia de movilidad de cualquier tipo de usuario.

• Segundo, es una tecnología relativamente barata: con un dispositivo del tamaño de una pequeña caja de chocolates se puede dar acceso wireless a Internet de alta velocidad, cubriendo en área abierta (sin obstáculos) el tamaño de una cancha de fútbol; todo esto, incluyendo una tarjeta inalámbrica para una computadora (si la computadora no la tiene integrada), cuesta menos de 300 dólares.

Otro factor clave para el éxito de esta nueva tecnología es el desarrollo de puntos públicos de conexión inalámbrica, conocidos como Hotspots, los cuales están inundando los centros comerciales, hoteles, aeropuertos, restaurantes, cafés, bibliotecas, parques y todos los sitios públicos que se pueda imaginar. Y México no es la excepción. Hoy hay en el país más de 400 sitios públicos

habilitados con conexión inalámbrica a Internet, y este número seguirá en aumento.

II.7.1 El uso más conocido de una WLAN: El HotSpot

El uso del Internet desde su nacimiento ha crecido exponencialmente y ese éxito se basa en lo accesible que se ha vuelto con el pasar de los años. Sin embargo, a medida que más gente lo utiliza, crece más el número de aplicaciones que lo aprovechan así como su sofisticación. Hoy día tenemos aplicaciones que nunca nos habríamos imaginado, como los chat, intercambio de música y video, radio, mensajeros instantáneos, videoconferencia, salones de clase virtuales, etc.

Estas aplicaciones por su rico contenido y gráficos demandan mejores computadoras y una capacidad mayor de comunicación en lugar de los enlaces por teléfono, esta nueva y mayor línea de comunicación se conoce como "banda ancha" como el ADSL (e-go, infinitum, etc.)

Por otro lado, la gente quiere tener siempre a la mano todos los servicios que usa a través de la tecnología; así tenemos que hoy día hay mas teléfonos celulares que teléfonos tradicionales, las agendas electrónicas desplazan a las agendas de escritorio, el crecimiento de ventas de computadoras portátiles son de dos dígitos y el de las computadoras de escritorio es casi nulo. En el caso de Internet, la gente ya no se conforma con tener acceso en su oficina y en su casa, quiere tener a la mano el Internet para ver su correo electrónico, mensajes instantáneos, información que se encuentra en el servidor de su oficina, o buscar el horario de la película que quiere ver en la página de su cine favorito, sin tener que ir a su oficina, casa ni estar atado a un cable telefónico o de red local.

Así tenemos que el Internet, los accesos de banda ancha y las redes inalámbricas se conjugan para solucionar esta necesidad, en un mercado creciente a nivel mundial bajo el nombre de Internet inalámbrico o "Hotspot" como se les llama en Estados Unidos.

Un Hotspot es una zona de cobertura donde se puede accesar al Internet inalámbrico de alta velocidad. El acceso a Internet en lugares públicos ha unido la necesidad de conexión con una interesante oportunidad de negocio para aquellas empresas capaces de proporcionar dichos accesos en lugares como Aeropuertos, Estaciones de Tren, Puertos, Centros de Convenciones, Hoteles, Cafeterías, Hospitales, etc.

Pero ¿A Quien le interesa usar Internet en lugares públicos? La respuesta se tiene agrupada de la siguiente manera:

- **Corporativos**: Los viajeros de negocios en todo el mundo, gente que labora en grandes y medianas empresas en México a nivel ejecutivo y en los departamentos de ventas, mercadotecnia y distribución, son usuarios frecuentes de computadoras portátiles, agendas electrónicas como Palm y PowerPC y redes inalámbricas. Equipo que les proporciona generalmente la empresa donde trabajan para realizar trabajo de campo y estar comunicados con clientes, proveedores y compañeros de trabajo. Hoy día están limitados para comunicarse en las oficinas que visitan y algunos hoteles y restaurantes. Es un nicho de mercado que está en constante búsqueda de lugares adicionales para conectarse.

- **Instituciones Educativas**: Casi la totalidad de las universidades privadas y muchas preparatorias en el país cuentan ya con el servicio de Internet inalámbrico para sus maestros y alumnos, donde intercambian información como tareas, trabajos en equipo, clases por videoconferencia, calificaciones, investigación, etc... por lo que los alumnos son requeridos a adquirir computadoras portátiles desde el primer semestre. Este grupo de usuarios son ávidos usuarios del Internet y gustan de usar aplicaciones de entretenimiento como correo electrónico, chats, mensajería instantánea, jugar en línea con gente de todo el mundo en sitios específicos por Internet, bajar música y archivos MP3, comprar boletos de conciertos, buscar información de viajes, antros y horarios de películas en su cine favorito, etc.

- **Publico en General**: de clase media y clase alta, ya sean pequeños empresarios, profesionistas independientes, empleados en un corporativo o amas de casa, este grupo de gente utiliza la computadora y el Internet para el trabajo y entretenimiento, pero también suele utilizar la computadora portátil y/o la agenda electrónica como un símbolo de status y gusta de convivir con sus conocidos en restaurantes, cafés, centros comerciales, cines, gimnasios y eventos deportivos.

Por otro lado, la oferta de computadoras portátiles en México desde hace mas de un año ya incluye la tarjeta de red inalámbrica en casi todos los modelos de diferentes marcas y la tendencia es que la totalidad la incluya en corto plazo. Sus dueños no importando la edad, actividad o grupo socioeconómico buscaran sacarle todo el provecho a su capacidad de red inalámbrica y buscaran lugares públicos para conectarse a Internet.

Hoy día es muy limitado el número de lugares que ofrecen este servicio, y casi el 100% de ellos pertenecen a una cadena de tiendas/restaurante de conveniencia que da un servicio caro pues esta ligado a una conexión DSL para casa o pequeña empresa y limita al usuario a estar conectado en las tiendas o

en su casa, nunca en los dos al mismo tiempo. El resto de lugares dan un servicio gratuito e inestable porque carece de administración del uso, del que los usuarios rara vez se enteran de que existe el servicio pues no tiene nombre, marca ni publicidad. Mucho menos un retorno sobre la inversión para el negocio y además incrementa el costo de operación, pues sus empleados tienen que dar soporte técnico e información de uso a sus clientes.

De acuerdo a su tamaño los HotSpots tienen diferentes clasificaciones:

- Pequeños (Hoteles, Cafeterías, etc.) manejados por un gateway con un sistema Wi-Fi 802.11b de 22 Mbps integrado Ofrecen acceso hasta a 100 usuarios simultáneos, incluyen un switch VLAN de 4 puertos y permiten la validación y control de usuarios mediante sistemas propietarios o mediante un Servidor RADIUS externo.

- Medianos (Grandes Hoteles, Aeropuertos, Centros Comerciales, etc.) manejados por un equipo que soporta el acceso simultáneo de hasta 250 usuarios. Permiten la validación y control de usuarios tanto mediante sistemas propietarios como mediante un Servidor RADIUS externo.

- Grandes (Redes Metropolitanas) utiliza un gateway que permite el acceso simultáneo de hasta 1024 usuarios. Este tipo de equipo incluye un switch VLAN de 4 puertos y permiten la validación y control de usuarios tanto mediante sistemas propietarios como mediante un Servidor RADIUS externo.

Los Hotspots implementados en México por tipo de servicios son:

		
Aeropuerto	**Escuela/Universidad**	**Otros**
CD de México		**Centro Com. Pabellón Polanco**
Acapulco	**Universidad Panamericana**	**Centro Comercial Plaza Inbursa**
Cancún (área Nacional)	**IPADE**	**Centro Comercial Plaza Loreto**
Monterrey	**IPN**	**Centro Comercial Plaza Masarik**
Guadalajara	**ITAM**	**Centro Com. Pabellón Altavista**
Ixtapa	**Universidad del Valle de México**	**Cinemex**
Tijuana		**Papalote Museo del niño**
Los Cabos		
Puerto Vallarta		

Café / Restaurant

Sanborns
VIPS
Café Caffe
Beer Factory
Toks
Fishers
Fonda de Santa Clara
Giornale Caffe
Gloria Jean's
Hard Rock Café
Konditori
Lynis
El Péndulo
Grupo Orraca
California
RainForest
Santa Fe Cafe

Hotel

Fiesta Inn
Flamingos Plaza
Calinda
Fiesta Americana
Ritz
Sheraton
Hilton

Hospital

Grupo Angeles
Español

Libreria

Ghandi
Porrúa

Empresas reconocidas que proporcionan este servicio:

Banamex

MEXICANA

AmericanAirlines

II.8- Entorno Regulatorio

Uno de los principales atractivos de Wi-Fi es que no se requiere de una licencia para operar los dispositivos en la banda de 2.4 o 5 GHz. Sin embargo, libre de licencia no significa "sin regulación". De hecho, en distintos grados dependiendo de cada país, Wi-Fi esta sujeto a una variedad de regulaciones que impactan el rango, escalabilidad, portabilidad, protección del producto y una variedad de factores adicionales que impactan la capacidad de uso en general de la tecnología.

Hoy en día existen aproximadamente 200 países en el mundo. Como estados soberanos, cada uno de ellos tiene la autoridad de crear e implementar regulaciones que sean únicas para su país. De hecho, unos cuantos países (pocos afortunadamente) han impulsado regulaciones sobre Wi-Fi que sólo son específicas para esos países. La gran mayoría de países opta por acoger un conjunto común de regulaciones de otro país (normalmente más grande). Un conjunto de países que por lo regular son colindantes y comparten un conjunto común de regulaciones se conoce dentro de la especificación 802.11 como un *dominio regulador*. Los dominios reguladores son:

- **FCC** que significa Comisión Federal de Comunicaciones del gobierno de Estados Unidos de América.
- **ETSI** el Instituto Europeo de Estándares de Comunicaciones.
- **Otros** cada uno de ellos sólo cubren a su país natal.

Los reguladores de los distintos países están revisando frecuentemente el proceso de asignación de bandas de frecuencias para aplicaciones WLAN. Cada país tiene una estrategia diferente en este tema y por lo tanto es conveniente que los usuarios potenciales de WLAN comprueben localmente si solamente pueden desplegar Puntos de Acceso (AP) en aplicaciones de interior o si también pueden desplegarlos en entornos de exterior y cuales son las frecuencias que deben utilizar.

Actualmente en Europa gran parte de la banda de 5 GHz está reservada para aplicaciones de HiperLan2 o de tecnologías con asignación dinámica de frecuencias (como 802.11h). Tecnologías como 802.11a estarán limitadas a usar solamente 150MHz del total de la banda disponible. Sin embargo estos temas están en revisión permanente y pueden cambiar en un futuro ya que continuamente se esta proponiendo a los reguladores consideren la posibilidad de nuevas asignaciones en la banda 5150-5725 MHz. La Figura II 11 resume la situación regulatoria para uso de WLAN públicas en los países más significativos en donde se ha implementado esta tecnología. (*Fuente Tribuna Tecnológica de Alcatel España).*

Country	[illegible]	Commercial use of spectrum for PWLAN services 5 GHz	[illegible]
[illegible]	Yes	Conditional Yes	No
Belgium	Yes	Yes	Yes
[illegible]	Conditional No	[illegible]	Unknown
Denmark	Yes	Yes	No
[illegible]	Yes	Yes	No
France	Conditional No	[illegible]	Unknown
[illegible]	Yes	[illegible]	Yes
[illegible]	[illegible]	Conditional No	Not Applicable
[illegible]	Yes	Conditional Yes	Yes
[illegible]	[illegible]	Conditional No	
[illegible]	Conditional No	Conditional Yes	
Luxembourg	Conditional No	Conditional No	
[illegible]	Yes	Under consultation	No
Portugal	Yes	[illegible]	No
[illegible]	Yes	[illegible]	
Sweden	Yes	Conditional Yes	No
UK	Yes	Under consultation	Yes at 31 July 200
United States	Yes	Yes	Unknown

PWLAN: Public Wireless LAN

Figura II.11 Regulación de Bandas de Frecuencias en Países Significativos (2004).

II.9 Organizaciones de Certificaciones

En 1999 se creó una organización internacional sin ánimo de lucro denominada Alianza para la Compatibilidad de Redes Ethernet Inalámbricas (WECA), cuya misión consiste en certificar la interoperabilidad de productos de distintos fabricantes basados en la especificación 802.11. Después de su fundación, ésta organización cambio su nombre debido a la variedad de nombres que se fueron manejando en esta tecnología, como Airport, Wireless Ethernet, etc. y decidió para evitar confusiones, definir a la organización como la **Alianza Wi-Fi** (Wi-Fi Alliance) la cual actualmente tiene afiliadas más de 150 compañías y ya han recibido la certificación Wi-Fi® cerca de 650 productos diferentes desde que se inicio el proceso en Marzo 2000.

Esta certificación garantiza que productos de distintos fabricantes son capaces de comunicarse entre sí y gran parte de ellos ya están disponibles comercialmente. El amplio interés del sector para que exista interoperabilidad y compatibilidad entre los productos ha permitido resolver algunas de las cuestiones relacionadas con la implementación de las redes LAN inalámbricas.

Existen en el mercado una gran variedad de dispositivos inalámbricos: Puntos de Acceso (AP), NIC inalámbricos, portátiles con Wi-Fi integrado, Pocket PCs Wi-Fi, Servidores inalámbricos, etc.

Para relacionar productos compatibles Wi-Fi se creo un Logo que certifica al usuario que se está utilizando un dispositivo que sigue el estándar 802.11. Recientemente, de acuerdo al estándar que maneje el producto, el logo Wi-Fi va acompañado de la una letra y color.

Para mayor información consultar las páginas Web:

www.wi-fi.org
www.wi-fizone.org

CAPÍTULO III.

LA SEGURIDAD EN LAS REDES INALÁMBRICAS BASADAS EN EL PROTOCOLO 802.11x.

III.1 Introducción

En los años recientes, la proliferación de computadoras personales portátiles y Asistentes Digitales Personales (PDA) ha provocado la expansión de los entornos en los que las personas utilizan las computadoras. Simultáneamente, la conectividad se está convirtiendo en una parte integral de los entornos de trabajo y como resultado, los diferentes tipos de redes inalámbricas han ganado una gran popularidad. Sin embargo, con la conveniencia de los accesos inalámbricos han llegado también nuevos peligros, la mayoría relacionados con la Seguridad. Cuando los datos son transmitidos a través de ondas de radio, la intercepción y enmascaramiento se convierte en algo trivial para cualquiera en disposición de un equipo de radio. Es por este motivo, que existe la necesidad de emplear técnicas adicionales para proteger las comunicaciones.

El estándar 802.11 para redes inalámbricas incluyo desde su aparición, protocolos de seguridad, usados para proteger comunicaciones a nivel de enlace contra escuchas indeseadas y ataques de otra naturaleza, pero en sus primeras versiones éstos protocolos no dieron buenos resultados. Poco después de la aparición del protocolo 802.11b, expertos en seguridad descubrieron varios defectos serios de seguridad en el protocolo WEP (Wired Equivalent Privacy) que acompañaba a este estándar, defectos que tenían su origen en la aplicación errónea de primitivas criptografías. Estas debilidades condujeron a un número de ataques prácticos que demostraron que ése primer estándar no alcanzó sus metas de seguridad.

Ante esta amenaza, tanto el IEEE como los fabricantes se pusieron manos a la obra para solucionar este agujero y han desarrollado nuevos estándares de encriptación y autenticación que tratan de minimizar la exposición a potenciales peligros. La siguiente norma desarrollada por IEEE es la 802.1x, la cual se trata de un mecanismo estándar para autentificar centralmente estaciones y usuarios, simplificando así el soporte de cientos o miles de puestos ya que es lo suficientemente flexible para soportar distintos algoritmos de autentificación y facilita a los fabricantes el desarrollo de mejoras complementarias. 802.1x se basa en el protocolo de autentificación EAP (Extensible Authentication Protocol.) Los mensajes EAP son encapsulados en mensajes 802.1x, por lo que se conocen como EAP over LAN. Este estándar mejoró la parte de autenticación pero descuido la parte de encriptación; detalle que mejoraría con el siguiente estándar: WPA.

El grupo de trabajo enfocado a la parte de seguridad del IEEE es el 802.11i el cual esta encargado de hacer y mejorar estándares que fortalezcan la tecnología Wi-Fi en sus actuales debilidades.

La WECA (Wireless Ethernet Compabilty Alliance) recomienda a los usuarios del sector empresarial seguir utilizando los sistemas de seguridad propios de los estándares, ya que éstos son mejorados continuamente, sin embargo, de ser necesario considerarse otros mecanismos de seguridad como Redes Privadas Virtuales, IPSec (IP Security) o firewalls.

III.2 Generalidades de Seguridad Informática

Garantizar que los recursos informáticos de un dispositivo estén disponibles para cumplir sus propósitos, es decir, que no estén alterados o dañados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática.

La seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo pérdida o daño ya sea de manera personal, grupal o empresarial. En este sentido es la información el elemento principal a proteger, resguardar y recuperar dentro de una red.

La Administración de la Seguridad en una red se basa en la identificación de los activos de información, así como en el desarrollo de documentación e implantación de políticas, estándares, procedimientos y guías que permitan mantener la confidencialidad, integridad y disponibilidad de la información.

Herramientas de administración tales como la clasificación de datos y el análisis de riesgos, son utilizadas para identificar amenazas, clasificar activos y evaluar vulnerabilidades para que en conclusión, se puedan implantar los controles de seguridad que sean efectivos. En pocas palabras, la Seguridad de la Información es una combinación de:

1.- Medidas Preventivas.- Se basan en el control de riesgos, con el fin de evitar o disminuir la ocurrencia de un evento no deseable: contraseñas, tarjetas de identificación, planes de contingencia, herramientas de alerta, políticas, Firewalls y encriptación; son tan sólo algunos ejemplos de estas medidas preventivas.

2.- Controles de Detección.- Permiten identificar la actividad normal o anormal dentro de una situación particular. Ejemplos de este tipo de vigilancia son los registros de visitas, los sensores de movimiento, los sistemas de localización de intrusos y los antivirus. Los mecanismos de detección deben

proveer los elementos para el reporteo y seguimiento de la ocurrencia de los eventos.

3.- Medidas de Recuperación.- Son utilizadas para restaurar la integridad, disponibilidad y confidencialidad de los activos de información hacia su estado esperado. Los sistemas para tolerancia a fallas, los respaldos y los planes de recuperación ante desastres son ejemplos claros de este tipo de medidas.

Hoy en día, el modelo de seguridad más cercano a cubrir los puntos anteriormente mencionados se basa en una clasificación de cuatro puntos fundamentales:

- ✓ Alerta continua de amenazas.- Busca proporcionar la información con el tiempo suficiente para que la toma de decisiones sea efectiva.
- ✓ Protección.- Mantiene los mecanismos de identificación y prevención de las vulnerabilidades, así como la garantía de la confidencialidad de la información.
- ✓ Respuesta a incidentes.- Busca el aspecto completo, tanto de los mecanismos internos como de los externos, para la reacción ante un evento de seguridad.
- ✓ Administración bajo un control proactivo de todos los elementos.- Se enfoca en los procesos de políticas, además de mantener la simplicidad del modelo de seguridad.

Además del prototipo arriba descrito, en un Modelo de Seguridad de Información, se debe prever un proceso de educación y transferencia de conocimientos que ahonde sobre los principios y prácticas de un uso aceptable de la tecnología dentro de la Organización. Estos principios deben estar construidos en la estrategia de seguridad y, pueden agruparse en 3 tipos básicos de principios:

- **Los Principios de Persistencia,** de naturaleza fundamental y que rara vez cambian. Se enfocan en el mantenimiento de la confidencialidad, integridad y disponibilidad de la Información; que son los fundamentos de la Tecnología de la Información (TI). Ejemplos de principios de persistencia son la responsabilidad, el reconocimiento, la ética, la heterogeneidad, la proporcionalidad, el tiempo, la integración, el análisis y la equidad.

- **Los Principios de Funcionalidad**. Los principios de funcionalidad se modifican cuando existen cambios importantes en el desarrollo de tecnología. Se relacionan con las diferentes categorizaciones de procesos existentes dentro de la infraestructura de seguridad y permiten, precisamente, ajustarse a estándares internacionales, los cuales manejan las mejores prácticas en los diferentes ramos de tecnología de la Información (TI) para ajustarse de la mejor manera posible a una

estrategia efectiva de seguridad. Un ejemplo del principio de funcionalidad, puede ser el control de accesos.

- **Los Principios de Detalle de Seguridad**. Éstos cambian de manera constante y son más detallados. En este caso, con el fin de proporcionar los elementos necesarios para actuar según las políticas y la forma de reaccionar ante un evento de seguridad, se definen todos los procedimientos y actividades requeridas en cada uno de los principios de funcionalidad establecidos.

Como paso inicial en un Modelo de protección de Seguridad, se debe saber cuáles son las amenazas y vulnerabilidades relacionadas con la tecnología con que se trabaja dentro de la organización. Por un lado, están los riesgos asociados con el ámbito de participación de la Empresa, aunque tampoco hay que olvidar la probabilidad de ataque varia de acuerdo a la tecnología utilizada.

Pero la relación de amenazas y vulnerabilidades es un tema más complejo que sólo estadísticas. En general, es necesario enfrentarse a situaciones particulares de acuerdo a cada modelo de negocio, el cual es distinto en todas las organizaciones, no importando el sector.

El riesgo es resultado de la combinación de amenazas, vulnerabilidades y valores de los activos de la Tecnología en Información. Con el fin de mitigarlo, se puede realizar un análisis de riesgo o de vulnerabilidades, con el propósito de aplicar, de manera eficiente, los controles de seguridad requeridos. Las diferencias básicas entre ambos es el alcance buscado.

En el análisis de vulnerabilidades sólo se muestra la información relevante a la tecnología, sin profundizar en la función de negocio de dicho activo, mientras que un análisis de riesgo se ubica también su función dentro del modelo de negocio.

III.3 Mecanismos de seguridad en el 802.11

Cuando se discuten los sistemas de seguridad WLAN, las dos áreas principales son Autenticación y Cifrado. Aunque estas áreas están interrelacionadas, deben ser consideradas en forma separada debido a que constituyen aspectos diferentes de una arquitectura general de seguridad.

III.3.1 Autenticación

Autenticación es el proceso en que se determina que un individuo, o cualquier objeto, como por ejemplo un dispositivo, es quien dice ser. El concepto de autenticación no esta limitado al área de Tecnología de Información sino que se aplica en muchos aspectos de nuestra vida cotidiana. Existe una gran diversidad de tipos de credenciales diferentes, como contraseñas, certificados, tarjetas de identificación, placas, etc., y en algunos casos se usa más de una credencial a la vez.

En las redes inalámbricas se puede configurar el uso de varios tipos de credenciales los cuales son:

- **SSID** (*Service Set Identifier*, "Identificador del Conjunto de Servicios"), es un código alfanumérico que se configura en cada cliente y punto de acceso que forma parte de la red WLAN. En las WLAN los puntos de acceso normalmente se distribuyen con un SSID predeterminado que es específico del fabricante (normalmente esta compuesto de una sola palabra) que se emite como parte de las balizas a los puntos de acceso. En la parte del cliente generalmente se tiene configurado un "SSID nulo", al dejar el SSID en blanco o usar un nombre comodín como "cualquiera" o "ninguno" en la utilidad de cliente, será capaz de asociarse al punto de acceso de la red asociada.

  Este código puede ser utilizado como una simple contraseña entre la estación y el punto de acceso o como un identificador de emplazamiento del emisor en una Red Pública. Lo cierto es que este sistema no garantiza excesivamente la Seguridad, ya que los códigos SSID son emitidos en forma de texto sin codificar. Cualquier receptor con los Paquete(s) y Programa(s) *("Software")* adecuado(s) puede averiguar estos datos.

  Las herramientas administrativas como, por ejemplo, NetStumbler e incluso Windows XP de Microsoft, proporcionan la capacidad de registrar todos los SSID "que se puedan percibir" en un cliente y luego permitir que el cliente se asocie al punto de acceso seleccionado, esto es una característica agradable para las áreas publicas, por ejemplo, en donde es posible que este instalada mas de una WLAN. Algunos fabricantes proporcionan la capacidad de eliminar el SSID de las balizas de emisión a los puntos de acceso; por un lado, esto resuelve el problema de seguridad, pero por el otro, deshabilita la capacidad de que un cliente pueda encontrar la red adecuada con la cual quiere conectarse. Mas aun, es común que las personas configuren incorrectamente los puntos de acceso, dejando los SSID en las balizas y emitiendo la contraseña.

Un SSID debe considerarse mas como un nombre de red que como una contraseña, debe actuar como un medio de identificación del punto de acceso o, cuando el mismo SSID se añade a múltiples puntos de acceso de una LAN Wi-Fi entera. Es muy normal que una empresa use el mismo SSID en todos los puntos de acceso sin importar su ubicación.

- ***Manejo de direcciones MAC***: Muchos fabricantes Wi-Fi proporcionan la capacidad de restringir el acceso a la LAN basándose en la tabla de direcciones MAC. La programación de direcciones MAC son los únicos identificadores numéricos que usan los fabricantes para los dispositivos LAN como, por ejemplo, las tarjetas de interfaz de red (NIC) que usan cable y las inalámbricas, al igual que los interruptores, direccionadores, concentradores y Puntos de Acceso. Los números de direcciones MAC son similares a los números de identificación. Mediante esta característica, puede introducir un número de direcciones MAC o un rango de direcciones MAC dentro de un punto de acceso o varios puntos de acceso, y por lo tanto solo permitir que los dispositivos que tienen estas direcciones se asocien, o puedan acceder a la LAN. A pesar de que esto proporciona algún nivel de seguridad, el enfoque tiene dos problemas importantes:

  1.- Las direcciones MAC pueden ser "falsificadas". Algunos adaptadores de cliente usan la Dirección de Administración Universal (Universally Administered Address, UAA, por sus siglas en ingles) que definen los fabricantes de tal forma que sobrescribe una Dirección Administrada Localmente (Locally Administered Address, LAA, por sus siglas ingles). Un pirata informático puede usar un analizador de protocolo inalámbrico para husmear el tráfico inalámbrico y encontrar una dirección MAC valida y luego simplemente copiarla en un adaptador de cliente compatible con LAA y, por lo tanto, hacerse pasar por el cliente legitimo.

  2.- Las bases de datos separadas crean problemas administrativos. Cada tabla de direcciones MAC que se ubica en puntos de acceso individuales representa una base de datos separada. A pesar de que algunos fabricantes proporcionan medios para replicar estas tablas a lo largo de un grupo de puntos de acceso, esta solución rompe la sincronización y crea problemas de actualización.

- **Certificados**: este tipo de credencial en las redes inalámbricas es una especie de "boleto" que se entrega a un dispositivo especifico que es valido para un periodo definido. Cuando el usuario del dispositivo intenta obtener el acceso a la red, el dispositivo despliega su certificado a un servidor de autenticación a través de la red. Los dispositivos que contienen certificados validos obtienen el acceso a la red.

Los nombres de usuario y contraseñas son medios de autenticación sensibles al tiempo. Cualquier persona que use una LAN empresarial, ya sea cableada o inalámbrica, esta familiarizada con los nombres de usuario y contraseñas para la autenticación. Cuando se autentican en una LAN cableada, los nombres de usuario y contraseñas normalmente se usan para obtener el acceso a dominios del servidor mediante la capa de aplicación, el acceso mismo a la red cableada normalmente no esta restringido.

Los nombres de usuario y contraseñas también se pueden usar para el acceso a la WLAN y representan un segundo tipo de autenticación que incluyen los sistemas de seguridad empresariales. La autenticación no se lleva a cabo en la capa de aplicación sino en la capa física misma, lo cual significa que el usuario que no este autenticado no podría obtener ningún tipo de acceso a la red.

Las contraseñas pueden ser permanentes o semipermanentes; es decir, son validas durante un periodo relativamente largo, por ejemplo, semanas o meses. Otras contraseñas pueden ser validas para un solo uso y se conocen como contraseñas de un solo uso (One Time Passwords, OTP, por sus siglas en ingles). Estas contraseñas, que también se conocen como tokens flexibles, se generan al escribir un número de identificación personal permanente en una aplicación que entonces genera una contraseña de un solo uso que se aplica normalmente mediante un rango de combinaciones alfanuméricas que pueden ser reconocidas por el servidor de autenticación. Las organizaciones que se preocupan más por la seguridad insisten en el uso de OTP para los accesos remotos y, actualmente, también solicitan el soporte OTP para la autenticación WLAN.

Por ultimo, muchas de estas credenciales de autenticación no se excluyen unas a las otras. Los distintos medios de autenticación se pueden usar en combinación para añadir capas de seguridad. El uso de un número de identificación personal para obtener un OTP es un ejemplo simple de esto. Usar un certificado además del nombre de usuario y contraseña representa otro ejemplo. En los escenarios de acceso publico, es posible que los usuarios tengan que conectar un SIM GSM (el chip de autenticación que se encuentra en muchos teléfonos celulares) dentro de sus computadoras portátiles, y luego proporcionar un nombre de usuario y contraseña para obtener el acceso a la red.

III.3.2 Cifrado

De forma muy parecida en la que la industria WLAN ha adoptado el concepto de autenticación de una variedad de fuentes, también ha imitado el proceso de cifrado. La noción de usar un código para ocultar el significado de un mensaje que se envía a personas no intencionadas, o entrometidas, es casi tan vieja como la noción de enviar mensajes. El cifrado es la práctica de cambiar la información de forma que este tan cerca como sea posible de ser imposible de leer sin la información necesaria para descifrarla. Esta información puede ser una clave, secreto o código, además puede tomar la forma de un anillo decodificador de secretos o un libro de códigos. Generalmente, mientras más complicado sea el código, será mas difícil descifrarlo. Además, mientras más complicado sea el código, codificar o decodificar la información normalmente consumirá mas tiempo del uso de procesador.

El tema del cifrado es bastante complicado, sin embargo, existen algunos conceptos importantes que deben conocer los profesionales IS que despliegan una LAN Wi-Fi.

Un cifrado o algoritmo es una formula que se usa para generar un flujo de datos cifrados basados en una clave de cifrado. Estas claves de cifrado se pueden medir en términos de longitud: en general, mientras más grande sea la clave, será más complicado y robusto el código. En el mundo digital, la unidad de medida que se usa para las longitudes de claves son los bits. Por lo tanto, por ejemplo, una clave de 40 bits es menos robusta que una de 128 bits. Una clave de cifrado de 40 bits da como resultado 2^{40} (mas de un billón) de combinaciones posibles. Una clave de 128 bits ofrece 2^{128} combinaciones. Suponiendo que se usa el mismo algoritmo, una clave de 128 bits es 2^{88} veces mas difícil de romper que una clave de 40 bits.

Para crear el mensaje codificado, denominado texto codificado, se combina la clave de cifrado con el mensaje original, o texto simple. Existen dos tipos principales de cifrado: *el cifrado de flujo* que codifica el texto simple usando 1 bit a la vez, y el *cifrado de bloque* que fragmenta el texto simple en bloques y luego los cifra bloque por bloque. Los cifrados de flujo se consideran más eficientes y rápidos, debido a que los cifrados de bloque introducen un paso extra al proceso, el cual impacta el desempeño pero incrementa la robustez. La combinación de la clave del cifrado y el texto simple se conoce como una función OR exclusiva (o, con mayor frecuencia, XOR) como muestra la figura III.1. Entonces, el texto de cifrado que se obtiene queda, en teoría, tan fuertemente cifrado como el número posible de combinaciones que la longitud de la clave supone.

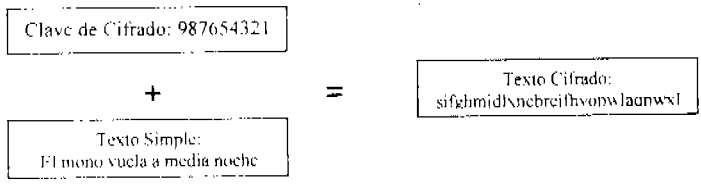


Fig. III.1 Ejemplo del uso de la clave de cifrado.

Es razonable pensar que si el mismo mensaje se codifica con el mismo código, se obtendrá el mismo mensaje secreto (el mismo texto simple pasa a través de la función XOR con la misma clave que da como resultado el mismo texto cifrado). En términos de redes, este texto simple es un solo paquete, el cual a menudo se repite debido a los errores en la transmisión y a los envíos que esto implica. Esta repetición frecuente de paquetes y la repetición resultante de texto cifrado proporcionan a los piratas informáticos mejores oportunidades de descubrir el código.

Una manera de resolver este problema es mediante el uso de un vector de inicialización el cual es un valor numérico de una longitud en bits determinada que se adjunta a la clave de cifrado (como muestra la figura III.2). A diferencia de la clave de cifrado, el vector de inicialización sufre modificaciones frecuentemente (tan a menudo como el envío de cada paquete) y se envía en forma de texto simple de forma tal que pueda ser reconocido tanto en las estaciones emisoras como las receptoras. La modificación en el vector de inicialización produce los cambios en el flujo cifrado, lo cual da como resultado un texto cifrado distinto aun cuando el texto simple, o el paquete, sea exactamente el mismo.

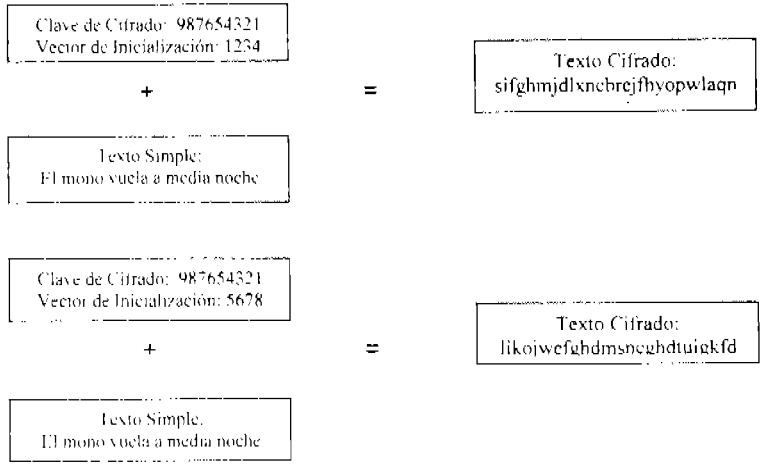


Fig. III.2 Ejemplo del uso del vector de inicialización.

III.4 WEP: La Primera Norma de Seguridad en el estándar 802.11

La seguridad ha sido parte de los estándares WLAN desde que apareció el estándar 802.11 con velocidades de 1 y 2 Mbps en 1997. Es importante recordar el estado de la industria en ese momento. Debido a las velocidades de datos relativamente bajas y precios altos de esos tiempos, las WLAN eran simplemente un nicho tecnológico, apelando casi exclusivamente a los mercados verticales como el de ventas y manufactura. Estos mercados están caracterizados por una cantidad relativamente pequeña de dispositivos de cliente específicos para las aplicaciones, por ejemplo, los lectores de código de barras y las terminales POS, por ubicación. Normalmente, estos dispositivos no salían de las instalaciones donde estaban implementados.

En 1997, las WLAN representaban una tecnología relativamente obscura, la cual solo era importante para una cantidad pequeña de industrias e individuos; no eran el fenómeno Wi-Fi actual y las personas no tenían como diversión conducir sus automóviles en los vecindarios, centros comerciales y parques industriales buscando redes inalámbricas que pudieran piratear.

Dada la manera drástica en que la industria WLAN ha cambiado a lo largo de este periodo tan corto, no es sorprendente que el estándar de seguridad que acompañaba a los estándares WLAN originales haya quedado tan tremendamente obsoleto. El estándar inicial se conoce como Privacidad Equivalente al Cableado (WEP), que en ese tiempo tenía la tarea de proporcionar la seguridad a las personas que enviaban información como, por ejemplo, los números de tarjeta de crédito desde terminales POS a través de la RF. Desafortunadamente, a medida que el estándar se volvió cada día más obsoleto debido al rápido desarrollo del mercado, este término de seguridad comenzó a verse como a un alardeo vacío.

El estándar WEP proporciona el cifrado de paquetes usando claves de cifrado estáticas que comparten todos los dispositivos en la WLAN, inclusive los puntos de acceso y los clientes. Cuando se aplica a las redes relativamente pequeñas, que son típicas en las aplicaciones como, por ejemplo, las de venta al publico e instalaciones de almacenes, la instalación manual de la claves WEP en cada dispositivo de cliente es una tarea abrumadora. De hecho, se puede decir que configurar algunos medios centralizados para generar y distribuir las claves de cifrado es una tarea mortal. Una preocupación muy valida acerca de almacenar las claves de cifrado comunes en los dispositivos cliente es que si un solo dispositivo es descifrado (cuando el dispositivo de cliente cae en las manos de un pirata-informático) ese dispositivo se puede usar para descifrar todo el tráfico de la LAN. Mediante las claves de cifrado compartidas, la implicación de una ruptura en la seguridad significa que todas las claves de cifrado y los dispositivos restantes deben ser cambiados.

Sin embargo, la posibilidad de que los dispositivos de cliente específicos para aplicaciones, junto con sus claves WEP almacenadas, se pierdan o sean robadas, es muy remota. Incluso cuando se pierde un dispositivo, el cambio en las claves de cifrado en una docena de lectores del código de barras puede arruinar solo una tarde, no una carrera. En pocas palabras, la arquitectura de clave compartida y estática de WEP se ajusta bien a los requerimientos de seguridad de algunas aplicaciones, las cuales alguna vez constituyeron la gran mayoría de los despliegues WLAN pero que ahora representan aplicaciones pequeñas y cada vez menos usadas.

La opción de la clave de cifrado estática y compartida en una LAN Wi-Fi empresarial no puede ni siquiera imaginarse actualmente, ya que las redes dan servicio a cientos o miles de usuarios. Solo la instalación de claves de cifrado de manera manual en esta cantidad de dispositivos requiere casi de un empleo de tiempo completo. A diferencia de los dispositivos específicos para aplicaciones, las computadoras portátiles y PDA normalmente salen de los edificios de las empresas, atraviesan aeropuertos y se dejan en automóviles y hogares. En otras palabras, no sólo existen probabilidades de que uno de estos dispositivos sea robado, sino que es inevitable el hecho de que exista la posibilidad de que los dispositivos sean robados, lo cual daría como resultado tener que cambiar todas las claves en toda la red. La arquitectura de clave de cifrado estática y compartida que se ajusta relativamente bien a las aplicaciones específicas es, fundamentalmente, incompatible con las redes del tamaño de despliegues empresariales.

Además de los problemas de escalabilidad asociados con la arquitectura WEP, la robustez de las claves de cifrado mismas han sido cuestionadas por distintas partes. Las claves de cifrado que usa WEP están basadas en el algoritmo de cifrado RC4, un cifrado de flujo diseñado por Ron Rivest (quien representa a la R en el acrónimo Seguridad RSA, una compañía de seguridad de datos con buena reputación y muy respetada). RC4 (cifrado 4 de Rivest) es un cifrado de flujo y se puede implementar usando varias longitudes de clave. Además de usarse en WEP, RC4 se emplea en los productos de seguridad RSA y es el algoritmo base de la Capa de Conexión Segura (Secure Sockets Layer, SSL, por sus siglas en ingles) un protocolo de reconocimiento para proteger el tráfico a través de Internet. RC4 es el cifrado de flujo que se usa más ampliamente y el algoritmo que se seleccionó para WEP debido, en parte, a su velocidad relativamente alta y su robustez. El punto es que el algoritmo RC4 se usa en forma extensa y es relativamente robusto, los problemas que aparecen en WEP no se deben atribuir al algoritmo base.

La implementación en WEP del algoritmo RC4 ofrece claves de cifrado que son de 40 bits de largo y tienen un vector de inicialización de 24 bits, lo cual da como resultado una clave de 64 bits de longitud en total. Muchos fabricantes han ido mas allá del estándar para proporcionar claves que sean de 104 bits de longitud, lo que da como resultado una longitud de clave total de 128 bits cuando

se añade el vector de inicialización. Para generar una clave WEP, se debe introducir una cadena alfanumérica, para los productos de algunos vendedores, en formato hexadecimal (número del cero al nueve, además de las letras de la A a la F), mientras que otros pueden usar cualquier cadena alfanumérica.

Observe que con un vector de inicialización de solo 24 bits de longitud, un valor especifico que se usa para generar el flujo de una clave será repetido cada 2^{24} o 16777216 veces. A pesar de que esto a simple vista parece poco frecuente, recuerde que un vector de inicialización se usa en cada paquete enviado. En una WLAN empresarial bastante normal, fácilmente podrían existir 16 millones de paquetes en el curso de un solo dia. En otras palabras, la cantidad relativamente pequeña de vectores de inicialización disponibles limita la capacidad de la arquitectura WEP para resolver el problema de la repetición de claves, lo atenúa un poco mediante la disminución de la repetición, pero no lo elimina. Peor aun, en agosto del 2001, algunos investigadores respetados en el campo descubrieron errores en el algoritmo de programación de claves que usa WEP y afirmaron que tanto las claves de 40 como las de 128 bits de WEP pueden ser descubiertas con tan solo la captura de 4 millones de paquetes (los cuales puede transmitir una LAN empresarial en cuestión de horas.) La idea de que existan piratas informáticos entrando fácilmente a una red "protegida" con WEP, razonablemente ocasiono una ola de paralización en Wi-Fi.

III.5 Mejorando WEP con la Norma 802.1x

802.1x IEEE es un estándar ratificado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para el control de acceso a la red basado en puertos; pertenece al grupo de trabajo 802.1 y es parte de un conjunto de estándares de nivel básico que se aplican a una amplia variedad de estándares de red. 802.1x fue diseñado originalmente para usarse con tecnologías cableadas como, por ejemplo, Ethernet.

Un tema que aparece en la historia de las WLAN es que copia tecnologías de áreas distintas con el fin de resolver problemas más rápidamente. Por esta razón, 802.1x fue, adoptado por la industria inalámbrica como el medio principal de autenticar usuarios en la LAN. La arquitectura 802.1x esta compuesta de tres partes principales: un solicitante, un autenticador y un servidor de autenticación. Cuando se aplica a Wi-Fi, el solicitante reside en los dispositivos de cliente y el punto de acceso sirve como el autenticador. El solicitante normalmente es un fragmento pequeño de software que se ubica en el sistema operativo o el controlador de dispositivo que proporciona el fabricante del adaptador de cliente. El punto de acceso actúa como el portero de la LAN, permitiendo que el dispositivo de cliente obtenga el acceso a la LAN sólo después de que el cliente ha sido autenticado. Los servidores de Servicio de Autenticación Remota de usuario por medio del acceso telefónico (Remote Authentication Dial-In User

Service, RADIUS, por sus siglas en ingles), que inicialmente fueron desarrollados para la autenticación de usuarios de red remotos que usaban una conexión telefónica hacia la red a través del sistema telefónico publico inseguro, fueron mejorados para autenticar usuarios accediendo a la LAN a través de un medio igualmente inseguro: ondas de radio.

El proceso de autenticación de 802.1x cuando se aplica a las WLAN funciona de la manera siguiente:

1. El cliente obtiene el acceso al medio inalámbrico a través de CSMA/CA y crea una asociación con un punto de acceso.

2. El punto de acceso compatible con 802.1x acepta la asociación pero ubica al cliente en una "área de espera" sin estar autenticado. Para el cliente sin autenticación, el puerto virtual, es decir, la puerta de enlace, hacia la LAN esta bloqueado. El punto de acceso envía una solicitud de identificación al cliente.

3. El cliente proporciona una respuesta de identificación que tiene el nombre de usuario o un identificador especifico similar que no es secreto. Al recibir la respuesta de identificación, el punto de acceso reenvía esta respuesta a través del enlace cableado hacia el servidor RADIUS. Si un punto de acceso esta configurado de manera que sólo acepte clientes compatibles con 802.1x y la respuesta de identificación del cliente no ha llegado, el cliente continua asociado con el punto de acceso pero dentro del área de espera de manera indefinida sin ser autenticado (sin obtener acceso a la red).

4. El servidor RADIUS busca el ID de usuario en la base de datos. Es importante observar que los servidores RADIUS mismos no siempre incorporan una base de datos con ID de usuario y credenciales de autenticación, sino que acceden a estas credenciales que están en una base de datos separadas como, por ejemplo, Active Directory de Windows 2000 o la base de datos de los Servicios de dominio de NT. La ventaja de este enfoque es que una base de datos común, y a menudo preexistente, se puede habilitar de manera que soporte la autenticación inalámbrica además de la cableada. Esto permite la centralización de la autenticación de credenciales, y por lo mismo, la disminución de la carga administrativa.

5. Una vez que el ID de usuario ha sido identificado por el servidor RADIUS, comienza un proceso de interrogación al cliente (en donde el punto de acceso pasa las preguntas del servidor RADIUS al cliente). El cliente responde a estas preguntas hasta que llega el momento de que el servidor RADIUS determina que el cliente es en realidad legitimo. Debido a que 802.1x no especifica los tipos de autenticación, dejando este aspecto a los fabricantes individuales, pueden variar los medios a través

de los cuales el cliente es interrogado, responde y la forma en que finalmente es autenticado en la LAN.

6. En las WLAN, no solo el cliente debe estar autenticado en la LAN, la LAN también debe estar autenticada en el cliente. Es decir, existe la posibilidad de que un cliente se pueda asociar con un punto de acceso que no sea parte de la infraestructura de la empresa. De hecho, los puntos de acceso ocultos pueden estar instalados por el pirata informático con el propósito de interceptar la información de autenticación del cliente. Por lo tanto, cuando se aplica la autenticación 802.1x en las WLAN, proporciona una autenticacion mutua, el cliente en la red y la red en el cliente. Por lo tanto, el cliente inicia lo que es esencialmente el proceso inverso de interrogación y respuestas con el servidor RADIUS.

7. Una vez que el cliente ha sido autenticado en la red a través del punto de acceso y el servidor RADIUS, y la red ha sido autenticada en el cliente, se abre el puerto virtual en el punto de acceso y el cliente puede comenzar a acceder a la red inalámbrica y cableada.

A pesar de que la autenticación 802.1x resuelve las capacidades de autenticación relativamente débiles del estándar 802.11 original, no resuelve de manera directa el problema de las claves de cifrado. Es decir, no resuelve los aspectos de escalabilidad o administración asociados con las claves estáticas de cifrado, las cuales son comunes a lo largo de toda la red y se almacenan en todos los dispositivos de cliente. Lo que resuelve este problema es la incorporación de un servidor de autenticación a la arquitectura. Un servidor RADIUS, o posiblemente, un servidor Kerberos (un servidor de autenticación altemativo), proporciona no solo las capacidades de autenticación, sino también la capacidad de generar claves de cifrado que son especificas para ese cliente en particular. La generación de claves centralizada es igual cuando se administran usuarios remotos de acceso telefónico que cuando se administran usuarios Wi-Fi, haciendo que los servidores RADIUS sean la opción lógica para este rol.

Cuando el cliente ha sido autenticado por el servidor RADIUS después de haber comparado las credenciales del cliente con las credenciales almacenadas en la base de datos, el servidor RADIUS también inicia el proceso de la generación de claves dinámicas. Como se ilustra en la figura III.3, este proceso de intercambio de claves se lleva a cabo durante la autenticación del cliente en la red. Debe observarse que estas claves especificas del cliente son claves unidifusion, que sólo se usan cuando el trafico esta dirigido a un cliente en particular. Las claves multidifusion se usan cuando el tráfico se emite a una variedad de clientes, son compartidas y tienen algunas de las mismas desventajas de las claves WEP compartidas.

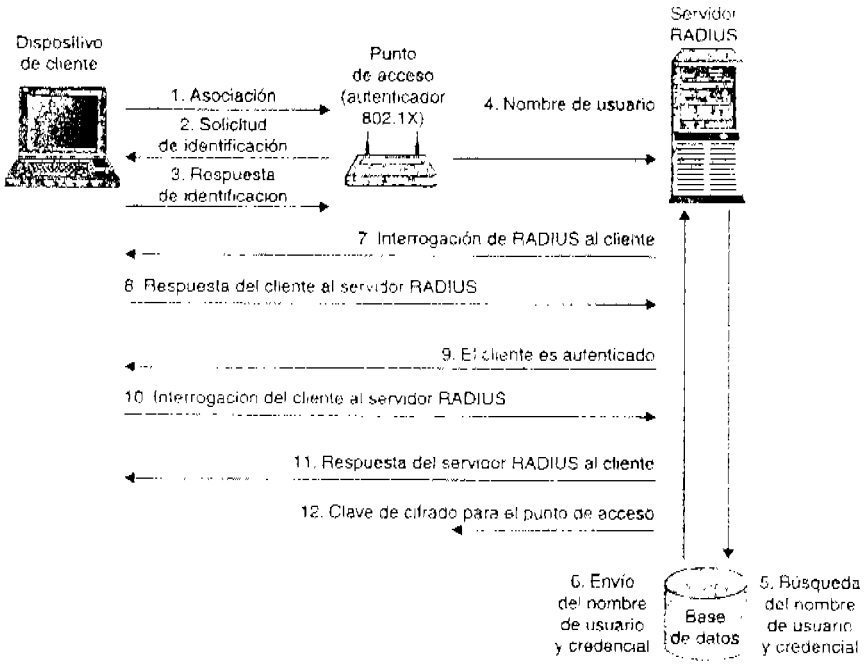


Figura III.3 Autenticación 802.1x con servidor RADIUS y una Base de Datos.

Las claves específicas de cliente no sólo son particulares para el cliente, sino también son específicas para una sesión de cliente. La mayoría de los servidores RADIUS proporcionan la capacidad de ajustar la duración de la sesión, y los profesionales IS tienden a establecer los tiempos de sesión según convenga. Mientras mas corta sea la duración de la sesión, será menor el número de paquetes que se enviaran con una clave de cifrado en particular. Esto significa que los piratas informáticos tendrán menos paquetes con los cuales podrán trabajar, lo cual hace que el trabajo de descubrir una clave sea mucho mas difícil. Por otro lado, mientras mas corta sea la duración de la sesión, será mayor el número de autenticaciones necesarias durante un periodo determinado. Dependiendo de la arquitectura y carga de la red, esto puede dar como resultado problemas en el desempeño debido a que el servidor RADIUS debe funcionar con un grado mayor de intensidad. Desde el punto de vista de un usuario, estos tiempos de sesión deben tener un impacto leve; el proceso de volverse a autenticar que se lleva a cabo al inicio de cada sesión nueva, normalmente ocurre en el fondo en donde, como ejemplo, la contraseña del usuario se envía desde el cache de memoria en el dispositivo de cliente del usuario y no es necesario que se tenga que crear la clave de manera manual.

Al crear claves unidifusion que sean especificas para una sola sesión y un solo usuario, la severidad de que se rompa la seguridad en el caso de que una clave sea pirateada, queda enormemente mitigada. La ruptura en la seguridad resultaría en la desprotección de los datos de solo ese usuario y sólo para esa sesión en particular. Esto contrasta con la perdida de las claves de cifrado estáticas y compartidas, las cuales permiten que el pirata informático descifre paquetes de todos los usuarios y todas las sesiones tanto en el pasado como en el futuro. Estas claves dinámicas de cifrado "desaparecen" del dispositivo de cliente al final de una sesión o cuando el dispositivo de cliente es apagado, la perdida de una computadora portátil ya no provocara un desastre en la seguridad.

III.6 El estándar 802.11i

Reconociendo la necesidad de una arquitectura de seguridad mucho mas robusta y escalable para las LAN Wi-Fi, el comité 802.11 del IEEE decidió designar un grupo de trabajo dedicado especialmente para la seguridad. El grupo de trabajo 802.11i (TGi en términos del IEEE) se formo en el año 2001 y, a pesar de que hasta la fecha no han entregado un estándar ratificado ha hecho mucho para proporcionar una seguridad empresarial que ofrezca interoperabilidad.

802.11i especifica a 802.11x, junto con el Protocolo de autenticación extensible (EAP), como los medios mediante los cuales los clientes Wi-Fi y las redes se pueden autenticar mutuamente. Lo que es notable acerca del EAP es que el aspecto extensible del protocolo proporciona la flexibilidad de autenticar usando una variedad de maneras. Esto les ofrece a los fabricantes la libertad de ofrecer diferentes tipos de autenticación o métodos de autenticación usando tipos distintos de credenciales. 802.11i especifica RC4, el mismo algoritmo de cifrado que se usa para las claves WEP estáticas, como el algoritmo de cifrado para las claves dinámicas de cifrado de una sola sesión y un solo usuario.

Los fabricantes han aprovechado la flexibilidad del esbozo del estándar 802.11i para ofrecer una variedad de tipos o métodos de autenticación. Para que una arquitectura 802.11i pueda funcionar, los tipos de autenticación que se usan en el lado del cliente deben ser soportados por el servidor RADIUS debido a que los puntos de acceso están, principalmente, simplemente pasando el trafico de la autenticación de un lado hacia el otro entre el cliente y el servidor RADIUS, un solo punto de acceso compatible con 802.11i es capaz de funcionar con los dispositivos de cliente que usan varios tipos distintos de autenticación, suponiendo que estos tipos de autenticación son soportados por el servidor RADIUS. Los servidores RADIUS de algunos fabricantes tienen soporte integrado para múltiples tipos de autenticación, lo cual permite tener un solo servidor RADIUS que soporte múltiples tipos de autenticación del lado del

cliente. Con la creación de la primera arquitectura de seguridad empresarial (antes del estándar) de la industria, a principios del año 2001, Cisco Systems ofreció el primer tipo de autenticación, que se llegó a conocer como LEAP (lo cual significaba EAP Ligero, sin embargo desde entonces ha estado inevitablemente en las tinieblas). Con LEAP, las contraseñas son las credenciales de autenticación, habilitando las pantallas de inicio de sesión a la red en el lado del cliente y desplazando a las bases de datos de los dominios de la red.

Debido a que Cisco es un fabricante de hardware del lado del cliente, originalmente LEAP solo estaba disponible con los adaptadores de cliente Cisco, pero hoy en día, otros fabricantes tienen la licencia para ofrecerlo, incluyendo a Apple Computer Corporation. LEAP es compatible con el esbozo del estándar 802.11i, como parte de uno de los distintos tipos de autenticación que están disponible actualmente.

Como parte del sistema operativo Windows XP, Microsoft añadió un segundo tipo de autenticación alternativo al conjunto 802.11i. El tipo de Autenticación Protocolo de Autenticación Extensible con Seguridad en la Capa de Transporte (Extensible Authentication Protocol with Transport Layer Security, EAP/TLS, por sus siglas en ingles) se basa en certificados en lugar de contraseñas como credencial de autenticación; la ventaja de un certificado en comparación con una contraseña es que no requiere de la intervención del usuario y se puede decir que incluye un grado mas alto de seguridad debido a que las credenciales son mucho mas aleatorias que las contraseñas seleccionadas por los usuarios. Por otro lado, la autenticación basada en certificados se lleva a cabo en el dispositivo, no a nivel del usuario. Un ladrón se puede autenticar en la red si roba el dispositivo sin necesitar ningún conocimiento especial. Debido a que EAP/TLS proviene de una compañía de software y reside en el sistema operativo, prácticamente funciona con cualquier adaptador de cliente compatible con 802.11 de cualquier fabricante. Esta es una ventaja para los grupos IS que tienen poco, o ningún, control sobre los tipos de hardware de cliente en la LAN lo cual es típico en las instalaciones universitarias y también son comunes en otras empresas.

Originalmente, EAP/TLS tenia como fin estar disponible solo en Windows XP (se pueden sacar propias conclusiones acerca de si la decisión se hizo por motivos técnicos o de ventas.) Para ser justos, Microsoft ha reconsiderado esto y, a mediados del 2002, ha comenzado el proceso de ofrecer EAP/TLS para otros sistemas operativos (incluyendo a Windows 98, Windows 2000 y varias formas de Windows CE) como parte de paquetes de servicio que se pueden descargar. Otros fabricantes han ofrecido tipos de autenticación alternativas, incluyendo el método de autenticación EAP con Capa Segura de Transporte de Túnel (Extensible Authentication Protocol with Tunneling Transport Layer Security, EAP/TTLS, por sus siglas en ingles) que está integrada a la utilidad de seguridad de cliente Odyssey de Funk Software. Meetinghouse Software ha

ofrecido un tipo de autenticación EAP/TTLS similar integrado en la utilidad de cliente Aegis. En EAP/TTLS, se configura un túnel seguro de autenticación en la Capa 2 entre el cliente y el punto de acceso usando TLS. Una vez que se establece el túnel seguro, entonces EAP/TTLS funciona a través de él, permitiendo que se envíen y reciban una variedad de credenciales de autenticación, incluyendo contraseñas y certificados, a través del túnel seguro. EAP/TTLS es un subconjunto de EAP/TLS debido a que solo usa TLS en el lado del servidor pero no en el del cliente. Sin embargo, al proporcionar la autenticación de contraseñas además de certificados, EAP/TTLS es una especie de EAP/TLS mejorado.

Una alternativa más reciente a EAP/TTLS es el Protocolo de Autenticación Protegida Extensible (Protected Extensible Authentication Protocol, PEAP, por sus siglas en ingles), el cual es similar a EAP/TTLS en el sentido de que también establece un túnel para la autenticación, permitiendo el uso de una variedad de credenciales de autenticación. Una implementación inicial de PEAP en los productos de Cisco Systems proporciona soporte para OTP con el fin de obtener una versión aun más robusta de la autenticación a nivel de usuario. Microsoft ha declarado que proporcionara soporte para PEAP además de EAP/TLS en algunos sistemas operativos, proporcionando, por lo tanto, no solo el uso de credenciales basadas en certificados sino que también en contraseñas. Muchos expertos en seguridad consideran que PEAP proporcionara una seguridad mas alta que el método anterior EAP/TTLS.

Para soportar estos tipos de autenticación en el lado del cliente, se requiere, desde luego, el soporte del servidor RADIUS. El Servidor de control de acceso de Cisco proporciona soporte para los tipos de autenticación LEAP y EAP/TLS. El servidor Windows XP de Microsoft soporta EAP/TLS, mientras que el servidor RADIUS Steel Belted de Funk Software puede utilizar LEAP y EAP/TTLS, mientras que el servidor RADIUS Merit de Interlink proporciona soporte para LEAP. Muchos servidores RADIUS proporcionan capacidades de recuperación de fallas, lo cual significa que si se recibe un tipo no soportado de autenticación, pasara la autenticación a otro servidor RADIUS, cuando esta disponible. De esta forma, puede tener un solo servidor RADIUS o incluso múltiples servidores RADIUS para proporcionar soporte de respaldo a todos los tipos de autenticación del lado del cliente. Como se muestra en la figura III.4 esto ofrece una variedad de opciones para desplegar una arquitectura de seguridad que proporciona interoperabilidad.

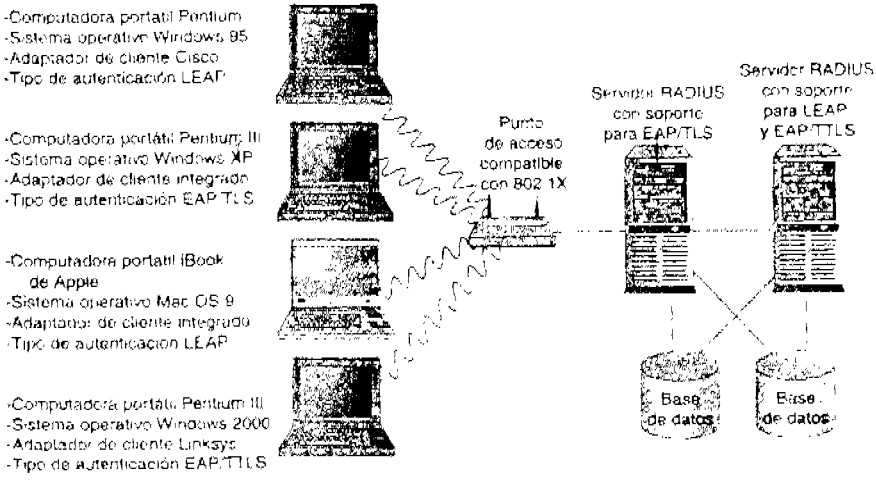


Fig. III.4 El esbozo del estándar 802.11i.

III.7 Solución al Problema de Cifrado: el Estándar WAP

Los distintos tipos de autenticación que se describieron anteriormente representan una gran parte de la necesidad de proporcionar los métodos de autenticación que proporcionen la interoperabilidad que se requiere para escalar la seguridad a niveles empresariales. Sin embargo, no resuelven todas las limitaciones de la implementación 802.11 del algoritmo RC4. Esta deficiencia en la seguridad basada en los estándares para la LAN Wi-Fi no se ha ignorado.

El Protocolo de Integridad de Clave Temporal (Temporal Key Integrity Protocol, TKIP, por sus siglas en ingles) es un medio parcial para "disminuir" las deficiencias de la implementación de RC4 en 802.11 para las claves de cifrado estáticas y, aun más importante, dinámicas. A finales del 2002, TKIP permaneció como un elemento definido de manera general en el esbozo del estándar 802.1 Ii. TKIP también se basa en RC4 y esta formado esencialmente de tres mejoras importantes en relación a la implementación inicial del algoritmo:

- Combinación de clave por paquete: La clave de cifrado se combina con la dirección MAC de la estación emisora y un numero de paquete secuencial para complicar aun más la clave básica, haciéndola mas difícil de romper.
- Un vector de inicialización de 48 bits: el doble de la longitud del vector de inicialización de 24 bits original que se especifico en el estándar

WEP inicial. Recuerde que las longitudes de la clave tienen un efecto exponencial mientras que una clave de 24 bits tiene aproximadamente 16 millones de combinaciones, una clave de 48 bits proporciona cerca de 280 billones de combinaciones. La longitud mas larga de esta clave, junto con la combinación de clave por paquete, hace que las claves de cifrado sean varias órdenes de magnitud más robustas que las implementaciones de generaciones anteriores.

- Comprobación de integridad de mensaje (Message Integrity Checks, MIC, por sus siglas en ingles), la cual esta diseñada para frustrar los ataques inductivos o de hombre en el medio. La implementación MIC en TKIP es una versión de la siguiente generación llamada (de forma suspicaz) "Michael". Mediante un MIC, las direcciones de envio y recepción además de otra información única, se integra en la carga cifrada. Los cambios en esta información, que están asociados a la intercepción de un paquete, dan como resultado el rechazo del paquete y una alerta que indica que un ataque puede estar fraguándose.

A pesar de todas las mejoras que ofrecen TKIP y WPA, las arquitecturas basadas en RC4 siguen siendo consideradas por muchas personas como métodos fundamentalmente insuficientes para organizaciones que están preocupadas especialmente por la seguridad. Por ejemplo, los distintos Estándares de Procesamiento de Información Federal (FIPS), que son aplicables para muchas aplicaciones del gobierno federal incluyendo el ejército, excluyen el algoritmo RC4 en las comunicaciones sensibles que no son secretas.

El estándar FIPS-197, publicado en noviembre del 2001, define el Estándar de Cifrado Avanzado (AES), un estándar de cifrado de la siguiente generación que se basa en las claves de 128 bits de longitud (como mínimo) generadas por el algoritmo Rijndael. Este desarrollo se mantiene en tendencias de la industria mas amplias: los fabricantes de redes privadas virtuales (VPN) quienes durante un largo tiempo han usado el mandato federal del Estándar de Cifrado de Datos (Data Encryption Standard, DES, y el posterior 3DES o "DES triple") están migrando a AES como un estándar de cifrado de la generación siguiente.

Existe un acuerdo general entre estos fabricantes que se enfocan a las ofertas Wi-Fi empresariales de que AES es el estándar de cifrado de la siguiente generación para la transmisión WLAN. Dado que RC4 es menos robusto que DES o 3DES, y que DES y 3DES son menos robustos que AES, significa que mediante la adopción AES, la industria Wi-Fi prácticamente esta avanzando hacia una nueva generación de seguridad.

Es posible que la migración a AES no sea tan sencilla como parece a primera vista, y es posible que en realidad no sea una migración completa. El cifrado tiene un impacto significativo en el desempeño de la red, en especial cuando se implementa en el software y se procesa en el anfitrión. Cuando el algoritmo RC4 relativamente "ligero" se implementa en el software, el impacto en el desempeño puede exceder 25%. Un algoritmo Rijndael implementado de la misma forma produce un impacto en el desempeño de 50%. Por tanto, el escenario más probable es que el algoritmo RC4 (con las mejoras TKIP y WPA asociadas) coexistirá con el estándar AES. Los fabricantes están planeando mejoras a las balizas 802.11 que ofrecerán las capacidades de seguridad del dispositivo lo que permite que los dispositivos asociados negocien el nivel más alto de seguridad que es mutuamente posible. Los fabricantes están, además, desarrollando implementaciones AES basadas en hardware. De forma muy parecida en que los mecanismos de cifrado basados en hardware proporcionan un desempeño mejor para el WEP basado en RC4, éstos métodos de cifrado de la siguiente generación proporcionarán la ayuda aún más necesaria de EAS basado en Rijndael, proporcionando un nivel más alto de seguridad con un impacto mínimo en el desempeño.

III.8 Tipos de Ataques en WLAN

Después de que el primer ataque hacia una red Wi-Fi fue publicado, aparecieron medios mas sofisticados de atacar las redes inalámbricas protegidas mediante WEP. Mientras que los primeros ataques fueron pasivos (se basa en la obtención de información de la LAN), hay otra clase de ataques activos que representan incluso mas problemas para WEP. Entre estos ataques que se conocen como inductivos o ataques de hombre en el medio, están los siguientes:

- ✓ **Los ataques de repetición** construyen de manera incremental copias de la clave usando un bit a la vez mediante el análisis estadístico de las respuestas predecibles a los mensajes de texto simple que envía el pirata informático.

- ✓ **Los ataques de modificación de bits** son similares a los ataques de repetición en el sentido de que se basan en las respuestas predecibles de las estaciones receptoras. El pirata informático modifica un mensaje (cambia los bits) para provocar un mensaje de error cifrado en una estación receptora, el cual entonces se puede comparar con la respuesta predecible para derivar la clave a través de múltiples iteraciones.

Existen otras formas de ataques a la seguridad de la red, ya sean redes inalámbricas o cableadas. Estos ataques y las maneras en las que se podrían aplicar en las WLAN son los siguientes:

- **Los ataques de denegación de servicio (DOS)** están diseñados para obligar que la red salga de linea (no para obtener información). En Internet, un ataque DOS se puede llevar a cabo mediante la inundación de un servidor usando una tormenta de datos como, por ejemplo, las solicitudes de inicio fingidas. El servidor es incapaz de controlar y rechazar el volumen de solicitudes y por lo tanto se satura o es incapaz de responder a las solicitudes legítimas. El giro inalámbrico de este tipo de ataques es saturar la banda de frecuencia aplicable con ruido.

- **Los ataques de diccionario** se basan en el hecho de que mediante algunos modelos de autenticación, una contraseña se mantiene en secreto pero el nombre de usuario se envía en forma de texto simple y se puede interceptar fácilmente. Por lo tanto, un pirata informático puede obtener distintos nombres de usuario y luego comenzar el proceso (generado por una computadora) de adivinar las contraseñas que usan palabras que se encuentran en los diccionarios de idiomas. Este conocido ataque de fuerza bruta puede ser exitoso debido a la capacidad que tiene el poder de procesamiento poco costoso y la realidad de que la mayoria de los usuarios son poco creativos cuando seleccionan las contraseñas. Los ataques de cumpleaños son similares a los ataques de fuerza bruta y han aparecido debido a la frecuencia con la cual los usuarios seleccionan las fechas de sus cumpleaños como contraseñas. Cuando el pirata informático tiene un nombre de usuario y la contraseña asociada valida, entonces podrá entrar a la red, inalámbrica o cableada, haciéndose pasar por un usuario legitimo.

III.9 Asegurando una WLAN

Un Administrador de Red, dispone de opciones de configuración que puede reducir la viabilidad de los ataques descritos. El cliente típico de una red inalámbrica es una computadora portátil (móvil por naturaleza), y empleará con frecuencia soluciones VPN para acceder a las computadoras que se encuentren dentro del firewall cuando lo haga a través de conexiones telefónicas. Proponer que la misma VPN sea también utilizada para las conexiones sobre 802.11 elimina la necesidad de procurar seguridad a nivel de enlace.

III.9.1 Firewalls

Las reglas de las que dependen los filtros de los Firewalls se basan en distintos factores, condiciones o características de los paquetes de datos. Las características comunes son las siguientes:

Dirección IP.- Tanto la dirección IP origen como destino pueden ser utilizadas para controlar los paquetes. Este tipo de filtros se utiliza habitualmente para bloquear la comunicación con ciertos servidores externos o para bloquear el acceso a Internet de ciertos usuarios.

Nombres de Dominio.- Esta característica se utiliza de la misma forma que el filtrado de direcciones IP, pero basadas en los nombres de dominio en vez de en los números IP. Ya se sabe que los números IP de un servidor pueden cambiarse fácilmente, mientras que los nombres de dominio suelen ser más estables.

Protocolos.- Los protocolos son también una característica interesante a filtrar. Por ejemplo, se puede dejar pasar el protocolo *http* para permitir el acceso a páginas *web*, pero no permitir el protocolo *telnet*, para impedir ejecutar comandos en computadoras remotos, el protocolo *ftp* para impedir la bajada de archivos potencialmente infectados de virus o el protocolo *smtp* para impedir que desde la computadora de un usuario se pueda crear un servidor de correo desde donde enviar correos ilegales (*"spam"*).

Puertos.- Mientras las direcciones IP se utilizan para identificar los equipos origen y destino de la comunicación, los puertos son unos números que sirven para identificar cada una de las aplicaciones con comunicaciones simultáneas que puede tener un mismo equipo. Generalmente, cada número de puerto se utiliza para una aplicación distinta; por ejemplo, el servicio *web* suele utilizar el puerto 80, Telnet el 23, o el correo electrónico POP03 el 110. Por tanto, filtrar los números de puerto es una forma de "filtrar" los servicios a los que se puede acceder o ser accedidos.

Contenido.- Los Firewalls pueden filtrar también los datos que contienen determinadas palabras o frases. En este caso, el Firewall analiza todo el contenido de los paquetes en busca de las palabras o frases prohibidas.

III.9.2 La Alternativa VPN

Muchos de los problemas inherentes a la transmisión de datos seguros a través de un medio inalámbrico que es fundamentalmente inseguro, son muy similares a los problemas inherentes a la transmisión de datos seguros a través

de Internet que también es fundamentalmente inseguro. Esto conduce a la pregunta: ¿por que no simplemente usar la tecnología VPN existente para 'resolver el problema de la seguridad inalámbrica? Muchas organizaciones han optado por ignorar los desarrollos que se han realizado en la seguridad específica para Wi-Fi y simplemente despliegan una VPN sobre la capa física Wi-Fi que es relativamente insegura. Existe una variedad de ventajas en este enfoque ya que la tecnología VPN es relativamente madura. Mediante años de experiencia en la protección de datos importantes a través de Internet, los fabricantes VPN han encontrado y mitigado la mayoría, sino es que todos los tipos de ataques que se han hecho en contra de las WLAN. Actualmente, las VPN proporcionan una variedad de métodos de autenticación que integran los cifrados DES, 3DES y AES.

El enfoque VPN aprovecha la infraestructura de seguridad existente y el conocimiento del personal. Muchas organizaciones empresariales se han basado en las VPN para ofrecer acceso en lugar de líneas contratadas costosas y que no son escalables o circuitos privados. A un nivel conceptual, sino es que técnico, estos esfuerzos se pueden aprovechar para resolver también los problemas de los clientes inalámbricos.

Con las VPN, existe cierta capacidad de interoperabilidad. A pesar de que es cierto que no existe un estándar que realmente incluya interoperabilidad en las VPN, los fabricantes han, hasta cierto grado, solucionado esto mediante soluciones técnicas y de mercadotecnia. Las soluciones VPN están formadas por una aplicación del lado del cliente y un concentrador hardware en el otro extremo, o una aplicación de servidor basada en software. La mayoría de las aplicaciones VPN del lado del cliente operan en un rango muy amplio de sistemas operativos del lado del cliente y están disponibles por un costo muy bajo, o gratuitamente Al hacer esto, los fabricantes VPN pueden resolver el problema principal de las tecnologías que aun no cuentan con un estándar de interoperabilidad.

Sin embargo, existen algunas desventajas cuando se usa una solución VPN para resolver la seguridad WLAN:

Las VPN están principalmente diseñadas sin tomar en cuenta demasiado el acceso a la red. Desde la perspectiva del usuario, normalmente la invocación del cliente VPN requiere de pasos adicionales, una inconveniencia que no es consistente con la libertad que ofrecen las WLAN. En el lado administrativo, a pesar de que es posible que el equipo especifico VPN o hardware dedicado para las VPN este instalado previamente para ofrecer el acceso remoto, es poco probable que sea capaz de controlar el trafico asociado con las LAN Wi-Fi una

tecnología que principalmente es de acceso local. El hardware de concentradores VPN soporta un número fijo de clientes, sin duda existe un costo asociado con cada cliente adicional que se soporta. Es posible que los servidores VPN basados en software también tengan una "cantidad de lugares" finita. Aprovechar la tecnología VPN para dar soporte a las WLAN requerirá, como mínimo, de una actualización significativa a la infraestructura.

Las ventajas de "interoperabilidad" de las VPN son su desventaja. Es decir, debido a que los clientes VPN residen en el software y usan el procesador del anfitrión, su operación implicara un impacto en el desempeño mucho mayor al que ocasionan las soluciones que implementan el cifrado en el hardware. A pesar de que esto es cierto en el lado del cliente, es mucho mas visible en el software de servidor VPN dentro de la infraestructura.

Las VPN están limitadas en el sentido que no proporcionan la capacidad de priorizar el flujo de paquetes que se requiere para el tráfico sensible al tiempo, como el de voz y video. Las VPN solo proporcionan soporte para el trafico unidifusión IP y no soportan otros protocolos, por ejemplo, IPX y AppleTalk.

En pocas palabras, debe considerar tanto las ventajas como las desventajas de desplegar o aprovechar una VPN para satisfacer los requerimientos de seguridad de las WLAN. Se debe observar también que una VPN y las soluciones de seguridad específicas para las WLAN no se excluyen mutuamente. Para aplicaciones que incluso están dentro de la misma organización, las VPN pueden representar una solución mejor que WEP, TKIP Y WPA y viceversa.

Los siguientes son los 10 puntos que siempre hay que tener en cuenta a la hora de pensar en la Seguridad de una Red Wi-Fi:

1.- Cambiar los parámetros de seguridad que vienen configurados por defecto en el equipo Wi-Fi. Sobre todo, se debe cambiar la clave de acceso a las propiedades de configuración de los puntos de acceso. También es importante cambiar el nombre de red (ESSID).

2.- Deshabilitar la configuración remota del punto de acceso. Muchos puntos de acceso permiten que se acceda a sus características de configuración desde una red remota (por ejemplo, Internet). Un intruso puede utilizar esta propiedad para averiguar la forma de acceder localmente a la red o para cambiar la configuración de acuerdo con sus intereses (por ejemplo, añadiendo a la red un punto de acceso falso desde donde actuar impunemente).

3.- Activar siempre el cifrado WEP. Se ha visto que el cifrado WEP tiene muchas debilidades, pero, no cabe duda de que es mucho mejor que no tener activado ningún cifrado. Por otro lado, al configurar las claves WEP, no hay que elegir claves que sean extremadamente fáciles. Además, es recomendable cambiar estas claves periódicamente.

4.- Configurar los puntos de acceso para que no envíen el ESSID (nombre de red). Generalmente, los puntos de acceso publican el nombre de la red para que sus usuarios puedan conectarse a ella con toda facilidad Esta característica es muy interesante en redes de acceso público, pero no tienen gran interés en las redes privadas. Impedir que el punto de acceso publique su nombre de red (ESSID), complica el acceso indebido.

5.- Utilizar las características de Firewall del punto de acceso o, en su defecto, instalar un equipo o programa(s) Firewall. Una característica de Firewall que suelen incluir la mayoría de los puntos de acceso es la posibilidad de controlar el acceso comprobando las direcciones MAC de las tarjetas adaptadoras de red de sus usuarios. Es buena idea habilitar esta opción. Ya se sabe que este sistema no es absolutamente infalible, pero una muy buena barrera para la mayoría de los intrusos.

6.- Si es posible, deshabilitar la asignación dinámica de números IP (DHCP). Esto complicará un poco la configuración de las computadoras de los usuarios, pero aumentará su seguridad.

7.- Cuando se trata de compartir archivos e impresoras, compartir sólo lo necesario. No compartir nunca todo el disco duro de un computadora, sino solamente el directorio o archivo que se necesite compartir. Además, si es posible, protegerlos con claves.

8.- No dejar grabados en los equipos los datos de acceso a la red. Ni tampoco dejas esos datos escritos en papeles que están permanentemente con el equipo.

9.- Si es posible, configurar una Red Privada Virtual, (VPN).

10.- La seguridad es tan débil como el más débil de sus eslabones. A veces, el eslabón más débil de esta cadena son sus propios usuarios. Por tanto, es importante informar a los usuarios de aquellas medidas mínimas de seguridad que deben tener en cuenta y recordárselas periódicamente.

CAPÍTULO IV.

PRODUCTOS Y EQUIPOS UTILIZADOS PARA CONFIGURAR UNA RED INALÁMBRICA BASADA EN EL PROTOCOLO 802.11x.

IV.1.- Introducción.

La mayoría de las redes inalámbricas que hay en el mercado (sean Wi-Fi o de otro tipo), funcionan de una manera similar: tienen unas estaciones base (puntos de acceso) que coordinan las comunicaciones, y unas tarjetas de red (adaptadores de red) que se instalan en las computadoras y que les permite formar parte de la red.

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

Las características y propiedades de cada uno de los elementos de la red WLAN sean AP's, Tarjetas de Red, Antenas, etc. son muy parecidas (dentro de su propia categoría) aún cuando son de diferentes fabricantes. Se expondrá en este capitulo, como ejemplo, en forma detallada un solo dispositivo de cada categoría, pero se mostraran imágenes con los diferentes diseños que de ese dispositivo puede encontrarse en el mercado.

IV.2.- El Punto de Acceso.

El Punto de Acceso *("Access Point")* es el centro de las comunicaciones de la mayoría de las redes inalámbricas. El Punto de Acceso no sólo es el medio de intercomunicación de todas las terminales inalámbricas, sino que también es el Puente de Interconexión con la red fija y/o Internet. Existen dos categorías de Puntos de Acceso:

- **Puntos de Acceso Profesionales.-** Diseñados para crear redes corporativas de tamaño mediano y grande. Éstos suelen ser los más caros; pero, incluyen mejores características (aunque sean particulares del fabricante), como son mejoras en la seguridad y, una más perfecta integración con el resto del equipo. Los líderes de este tipo de equipamiento son: Cisco®, 3Com®, Agere/Orinoco® (antiguamente conocida 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. La diferencia se nota cuando se dispone de un gran número de usuarios. En estos casos, los puntos de acceso profesionales ofrecen mejores resultados, eso sí, multiplicando el precio por cuatro o cinco. Los que más puntos de acceso de tipo económicos venden son: Intel®, 3Com®, D-Link®, Agere/Orinoco®, NetGear Proxim® y Linksys®.

Además de lo anterior, cada equipo tiene sus propias características externas, por ejemplo, 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.

Por otro lado, es habitual que los Puntos de Acceso se utilicen también como pasarela de conexión con otras redes (por ejemplo, con Internet). Desde este punto de vista, es importante que se tengan en cuenta dos cosas: la primera es que se fije en las características de *router* del Punto de Acceso: DHCP, NAT o propiedades de firewalls son características 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 dar movilidad a los usuarios que la necesitan), junto con una red cableada, para darle conectividad al resto de los usuarios. Generalmente, las redes corporativas utilizan el Protocolo TCP/IP; no obstante, hay que tener en cuenta que en el mercado existen otros protocolos como SPX/IPX, NetBIOS, LANtastic, etcétera. 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.

Por último, los equipos Wi-Fi tienen la ventaja de que tienen la garantía de interfuncionar sin problemas de acuerdo con la Norma IEEE 802.11b, g o a. Esto es así, sin duda, en relación con los adaptadores de red; sin embargo, existe cierta incompatibilidad en relación con los puntos de acceso. La incompatibilidad aparece a la hora de mantener en servicio una comunicación cuando un usuario para del área de cobertura de un punto de acceso al de otro (a esto se le llama *"roaming"*). En este caso, si los Puntos de Acceso son de diferentes fabricantes, es muy posible que se corte la comunicación. La comunicación se podrá volver a establecer con el nuevo punto de acceso, pero no se habrá producido una transferencia sin interrupciones, que es de lo que se trata finalmente. Para evitar este problema, es recomendable que los puntos de acceso vecinos sean del mismo fabricante. Además, cuando todos los dispositivos sean del mismo fabricante, es posible utilizar alguna característica adicional propietaria del fabricante. Se puede valorar si esto merece la pena. En cualquier caso, el IEEE

está trabajando para solucionar este problema (Grupo de Trabajo IEEE 802.11f). Por cierto, esto no tiene nada que ver con las tarjetas inalámbricas que se conectan a las computadoras; estas últimas, sí pueden proceder de fabricantes distintos y no habrá problema en su utilización.

IV.2.1.- Características de los Puntos de Acceso.

Los Puntos de Acceso son realmente unas pequeñas cajas de las que sobresalen una ó dos antenas. Algunos fabricantes se han preocupado incluso, de darles una forma estilizada que se salga de la típica forma de una simple caja. Aunque la estética exterior de la caja pueda parecer un hecho sin importancia, en las redes para el hogar puede ser un punto a valorar. Por otro lado, a veces la estética es algo más que las apariencias. Unos puntos de acceso incluyen útiles opciones para poderlos soportar en la pared o en el techo, mientras que otros carecen de este tipo de accesorios. En cualquier caso, en su interior se encontrará lo mismo:

- Un equipo de radio (de 2.4 GHz en el caso de 802.11b y 802.11g ó 5 GHz en el caso de 802.11a).
- Una o dos antenas (que pueden o no, apreciarse exteriormente).
- Un programa de gestión de las comunicaciones.
- Puertos para conectar el punto de acceso a Internet o a la red cableada.

IV.2.1.1.- La Radio.

El objetivo principal de los puntos de acceso es comunicarse con las terminales vía radio. Por tanto, lo principal de los puntos de acceso es su equipamiento de radio. Este equipamiento viene integrado en un conjunto de *chips* electrónicos conocidos como *chipsets*. Aunque en el mercado existen muchos fabricantes de puntos de acceso, son muchos menos los que fabrican *chipsets*. Dos de los principales fabricantes de *chipsets* Wi-Fi son: Lucent® e Intersil®.

Desde el punto de vista del usuario, el funcionamiento de los distintos dispositivos *chipsets* es idéntico. Además, entre ellos deben ser compatibles. No obstante, la Teoría de la Compatibilidad trae sorpresas a veces, por lo que resulta recomendable comprar equipos (puntos de acceso y tarjetas inalámbricas) que utilicen *chipsets* del mismo fabricante. La única forma de estar seguros de esto es comprar todo el equipamiento del mismo fabricante.

Esto puede ser un contrasentido desde el punto de vista de la compatibilidad de la marca Wi-Fi, pero tiene sus ventajas prácticas.

IV.2.1.2.- Los Puertos.

Los puntos de acceso necesitan disponer de puertos para poderse conectar con una red local cableada y con Internet. Para conseguir esto, los puntos de acceso suelen traer uno o más puertos 10/100Base-T (RJ-45). No obstante, las posibilidades de conectividad de los puntos de acceso no acaban aquí; dependiendo del modelo, se pueden encontrar los siguientes puertos:

- Un puerto especial para conectarse a un concentrador (*"Hub"*) o interruptor (*"Switch"*) de red de área local Ethernet (*"uplink port"*).

- Disponer internamente de un concentrador, 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 concentrador o un interruptor independiente. En cualquier caso, si se necesitase de más de cuatro puertos, siempre se puede comprar otro concentrador y conectarlo al punto de acceso para extender la red.

- 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 ó 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 módem).

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

- 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.

IV.2.1.3.- Gestión del Punto de Acceso.

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 interfase basada en páginas *web*. Para hacer uso de esto, sólo se necesita instalar el programa que incluye el punto de acceso.

No obstante, es importante saber que algunos puntos de acceso no utilizan una interfase *web*, sino que requieren de la introducción directa de líneas de comandos (lo que se conoce como CLI, *"Command Line Interface"*, Interfase de Línea de Comandos) o, incluso, requieren de un sistema operativo particular. Por ejemplo, *Airport Base Station de Apple®* requiere disponer de una computadora con sistema operativo *Mac®*. En cualquier caso, siempre es buena idea asegurarse de que el punto de acceso es compatible con el sistema operativo instalado originalmente en los equipos.

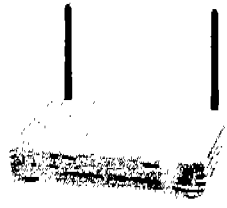
En la siguiente Tabla y Figura se indican las características de un Punto de Acceso marca Linksys.

Figura IV.1 Punto de Acceso de Banda Dual A y G Marca Linksys

Standards compatibles • IEEE 802.11a • IEEE 802.11b • IEEE 802.11g • IEEE 802.3 • IEEE 802.u	**Metodos de Seguridad** • 64-, 128- 152 bits WEP • MAC Address Filtering	**Metodos de Propagacion** Orthogonal Frequency Division Multiplexing (OFDM) • Complementary Code Keying (CCK)	**Transmitter Output Power** • 802.11a 16 dBm • 802.11g 14 dBm • 802.11b 16 dBm
Power • 5 V DC • 2.5 A	**Rango de Frecuencia** 2.4GHz to 2.462GHz	**Puerto** • Un Puerto 10/100 RJ-45	
Humedad • En Operacion : 10% al 85% (no-condensado) • Almacenado : 5% al 90% (no-condensado)	**Temperatura** • En Operacion: 32°F to 104°F (0°C to 40°C) • Almacenado: -4°F to 158°F (-20°C to 70°C)	**Dimensiones** • Largo = 186 mm • Ancho = 175mm • Altura= 48mm	**Peso** 14.11oz (0.4 Kg)

Tabla IV.2 Especificaciones del Punto de Acceso de Banda Dual A y G Marca Linksys

Otros ejemplos de Puntos de acceso son:



Access Point 3Com

Access Point 3Com

Access Point Zyxel

IV.3.- Adaptadores Inalámbricos de Red.

Los adaptadores de red son las tarjetas o dispositivos que se conectan a las computadoras para que puedan funcionar dentro de una red inalámbrica. Estos equipos pueden recibir también el nombre de tarjetas de red o interfases de red. De hecho, se conoce como NIC (*Network Interface Cards*, "Tarjetas de Interfase de Red") a cualquier tarjeta que se instala o conecta a una computadora que sirve para integrarlo en una red, sea ésta cableada o inalámbrica.

Los adaptadores de red 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) para mantener a la computadora a la que están conectados dentro de la red inalámbrica a la que se asocie.

Como todos los equipos de radio, los adaptadores de red necesitan una antena. Ésta suele venir integrada dentro del propio adaptador sin que externamente se note. Algunos adaptadores; sin embargo, permiten identificar claramente su antena. En cualquier caso, la mayoría de los adaptadores incluyen un conector para poder disponer una antena externa. Este tipo de antenas aumentan considerablemente el alcance del adaptador.

IV.3.1.- Tipos de Adaptadores de Red.

Al igual que desde hace tiempo viene siendo normal encontrar computadoras que incluyen de fábrica un puerto Ethernet RJ-45, recientemente están apareciendo en el mercado algunas computadoras portátiles que ya tienen integrado un adaptador de red Wi-Fi. No obstante, éstos son todavía

excepciones, lo normal es que el adaptador de red sea un equipo independiente que haya que instalar o conectar a la computadora o PDA. Actualmente, existen los siguientes tipos de adaptadores inalámbricos de red:

- **Unidades USB.-** Se trata de unidades inalámbricas que se conectan a la computadora (portátil o de escritorio) mediante un puerto USB. Estas unidades son más propias de las computadoras de escritorio, ya que evitan tener que instalar en su interior un adaptador de tarjeta PCMCIA. No obstante, son válidas para todo tipo de computadoras. Si la computadora ya tiene ocupados todos sus puertos USB (por ejemplo, porque se está utilizando para el teclado, la impresora, etcétera), en el mercado existen multiplicadores de puertos USB que permiten sacar cuatro puertos de donde había uno (cuestan unos 40 dolares).

- **Tarjetas PCMCIA.-** Éstas son tarjetas que tienen un tamaño similar al de una tarjeta de crédito y que se intersectan en los puertos PCMCIA (*PC Card*) de tipo II que suelen incorporar la mayoría de las computadoras portátiles. Se pueden encontrar tarjetas PCMCIA de Wi-Fi desde 40 dólares (y el precio sigue bajando). Las computadoras de escritorio no suelen contar con puertos PCMCIA.

- **Tarjetas PCI o ISA.-** Las computadoras de escritorio no suelen disponer de ranuras PCMCIA. De lo que sí disponen son de ranuras PCI o ISA donde se pueden instalar todo tipo de tarjetas de periféricos, entre las que están las tarjetas Wi-Fi. No obstante, lo cierto es que no es fácil encontrar en el mercado este tipo de tarjetas Wi-Fi. La solución alternativa consiste en instalar tarjetas conversoras de PCI o ISA a PCMCIA. Estos conversores son tarjetas PCI o ISA que se insertan en una ranura interna de la computadora y que ofrecen un puerto PCMCIA al exterior.

El precio de estos adaptadores es de unos 40 dólares. Evidentemente, de forma adicional, haría falta disponer de la tarjeta PCMCIA.Se explicara a continuación con mayor detalle cada una de ellas.

IV.3.1.1.- Adaptadores USB.

USB (*Universal Serial Bus*, "Bus Serie Universal"), es un nuevo puerto de comunicaciones que se diseñó para poder mejorar la forma en cómo los periféricos se conectaban a las computadoras. Hasta que apareció USB en 1993, las únicas posibilidades de conectar un periférico a una computadora era mediante el puerto serie o el puerto paralelo (además del puerto del

teclado/ratón y el puerto de juegos). El inconveniente mayor con estos puertos es que sólo se podían conseguir velocidades de transmisión de 115 Kbps. Adicionalmente, las computadoras sólo disponían de un puerto paralelo y dos seriales, con lo que el número de dispositivos a conectar se reducía a tres; además, son puertos que no le permiten a la computadora reconocer automáticamente el dispositivo que tienen conectado, ni alimentarlos a través del propio puerto. USB vino a traer las siguientes ventajas:

- No hace falta apagar la computadora para conectar o desconectar un periférico USB.
- La computadora reconoce automáticamente los periféricos que se conecten mediante USB. Si es preciso, instalan automáticamente los controladores necesarios para hacerlo funcionar adecuadamente.
- Ofrecen una alta velocidad de transferencia de datos: 2 Mbps.
- Permite conectar hasta 127 dispositivos USB. Incluso, aunque la computadora disponga de un solo puerto, basta con instalar un multiplicador de puertos (un concentrador), para disponer de más puertos USB.
- Ofrece alimentación eléctrica a los periféricos a través del propio conector 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 la computadora.

Todo lo anterior ha hecho que los periféricos USB hayan ido desplazando poco a poco al resto de periféricos del mercado, hasta el punto de que ya existen computadoras que no disponen de puertos serie ni paralelo, sino sólo puertos USB. Hoy en día, prácticamente todos los tipos de periféricos ofrecen la posibilidad de ser conectados a la computadora a través de un puerto USB: impresoras, módem, digitalizadores, cámaras, discos duros, etcétera. El caso de los adaptadores de red inalámbricos no iba a ser menos.

Desde el punto de vista de los adaptadores de red inalámbrica, USB ofrece la ventaja de poder compartir el adaptador entre diferentes computadoras según se necesite. Como instalar el adaptador es tan fácil como conectarlo al puerto USB, si una computadora necesita conectarse a la red, se le enchufa el adaptador y listo. Cuando no lo necesite, con sólo desenchufarlo del puerto USB se tiene bastante. Otra de las ventajas es que el adaptador puede reorientarse con respecto al Punto de Acceso para buscar una mejor cobertura, sin tener que

mover la computadora. El único inconveniente de los adaptadores USB es que son dispositivos externos a la computadora. No quedan integrados dentro de él como lo hacen los adaptadores PCMCIA o ISA.

En la siguiente Tabla y Figura se indican las características de una tarjeta de red tipo USB marca Dlink.

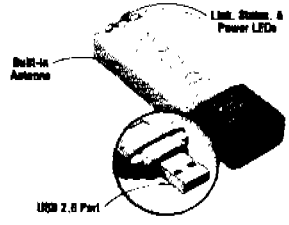
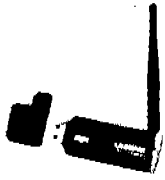


Figura IV.3 Tarjeta de Red tipo USB Marca Dlink

Standards compatibles • IEEE 802.11g • IEEE 802.11b	**Metodos de Seguridad** • 64-, 128-WEP • WPA (WI-Fi Protected Access)	**Metodos de Propagacion** Orthogonal Frequency Division Multiplexing (OFDM) • Complementary Code Keying (CCK)	**Rangos de Distancia** • Interiores: hasta 328 pies (100 metros) • Exteriores: hasta1.312 pies (400 metros)
Media Access Control CSMA/CA with ACK	**Rango de Frecuencia** 2.4GHz to 2.462GHz	**Transmitter Output Power** 14Bm ± 2dB	**Tipo de Antena** Omni Direccional
Humedad 80% maximo (no-condensado)	**Temperatura** En Operacion: 32°F to 104°F (0°C to 40°C) Almacenado: 4°F to 167°F (-20°C to 75°C)	**Dimensiones** • Largo = 2.95 pulgadas (75mm) • Ancho = 0.91 pulgadas (23mm) • Altura= 0.7 pulgadas (6.3mm)	**Peso** 0.021 lb (4.4g)
Signal Rates: **With Automatic Fallback** • 54Mbps • 48Mbps • 36Mbps • 24Mbps • 18Mbps • 12Mbps • 11Mbps • 9Mbps • 6Mbps • 5.5Mbps • 2Mbps • 1Mbps	**Receiver Sensitivity** • 54Mbps OFDM • 48Mbps OFDM • 36Mbps OFDM • 24Mbps OFDM • 18Mbps OFDM • 12Mbps OFDM • 11Mbps CCK • 9Mbps OFDM • 6Mbps OFDM • 5.5Mbps CCK • 2Mbps QPSK • 1Mbps BPSK		

Tabla IV.4 Especificaciones de la Tarjeta de Red tipo USB Marca Dlink

Otros diseños de tarjetas USB son:



Tarjeta de Red
Tipo USB
Marca Linksys

Tarjeta de Red
Tipo USB
Marca SMC

Tarjeta de Red
Tipo USB
Marca Microsoft

IV.3.1.2.- Tarjetas PCMCIA.

Uno de los problemas que tenían antiguamente las computadoras portátiles era que difícilmente podían ampliarse en sus prestaciones. Para instalarle una tarjeta de red o un módem a una computadora de escritorio, basta con añadir en su interior la tarjeta correspondiente (ISA, PCI, etcétera). El interior de las computadoras portátiles, sin embargo, estuvo completamente cerrado hasta que aparecieron unos puertos especiales conocidos como PCMCIA (*Personal Computer Memory Card International Association*, "Asociación Internacional de Tarjetas de memoria para computadoras portátiles").

Los puertos PCMCIA son una especie de ranura en la que se pueden insertar unas tarjetas del tamaño de una "tarjeta de crédito". Estas tarjetas quedan insertadas en el interior de la ranura, por lo que la computadora portátil no pierde su integridad y fácil portabilidad. En el mercado existen muchos tipos de tarjetas PCMCIA: módem, tarjetas de red Ethernet, discos duros, etcétera.

Las tarjetas PCMCIA fueron creadas en 1989 por una Asociación de Fabricantes de equipos con el propósito inicial de desarrollar una Norma de Arquitectura de Sistemas y de Paquetes y Programas para tarjetas de memoria intercambiables (de ahí su nombre). No obstante, la idea fue tan buena que se ha utilizado para todo tipo de periféricos.

Todas las tarjetas PCMCIA 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 conector, 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 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).

Por una razón exclusivamente de espacio, cada tarjeta requiere su propio tipo de ranura en la computadora. Esto quiere decir que una ranura Tipo III admite cualquier tipo de tarjeta, mientras que una ranura Tipo I sólo admite tarjetas de este tipo. El tamaño más habitual de las tarjetas es el de Tipo II. Aparte del tamaño y del peso, 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. Por cierto, los adaptadores Wi- Fi PCMCIA suelen ser de Tipo II (con un bus de 32 bits tipo *CardBus*), y la mayoría de las computadoras portátiles incluyen una o dos ranuras PCMCIA para este tipo. Si se tiene una computadora muy antigua, será mejor comprobar si admite este tipo de tarjetas antes de comprar el adaptador.

En la siguiente Tabla y Figura se indican las características de una Tarjeta de Red tipo PCMCIA marca SMC

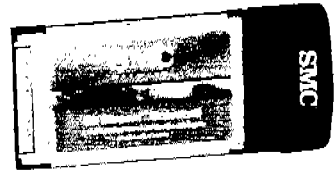


Figura IV.5 Tarjeta de Red tipo PCMCIA Marca SMC

Otros Modelos de tarjetas de este tipo son:

Tarjeta de Red
Tipo PCMCIA
Marca Buffalo

Tarjeta de Red
Tipo PCMCIA
Marca Belkin

Standards compatibles • IEEE 802.11b • IEEE 802.11g • IEEE 802.11a	**Metodos de Seguridad** • 64-, 128-WEP • WPA (Wi-Fi Protected Access) • AES • 802.1x Authentication	**Tranamittar Output Power** 16 dBm max	**Canales de Operación** • 11Canales (USA y Canadá) • 13 Canales (ETSI) • 14 Canales (Japón)
Signal Rates: With Automatic Fallback •802.11b • 11Mbps • 5.5Mbps • 2Mbps • 1Mbps •802.11g • 54Mbps • 48Mbps • 36Mbps • 24Mbps • 18Mbps • 12Mbps • 11Mbps • 9Mbps • 6Mbps • 5.5Mbps • 2Mbps • 1Mbps •802.11a • 54Mbps • 48Mbps • 36Mbps • 24Mbps • 18Mbps • 12Mbps • 9Mbps • 6Mbps •802.11* (Turbo) •108Mbps • 72Mbps • 48Mbps • 36Mbps • 24Mbps • 18Mbps • 12Mbps	**Tipo de Modulación** • 802.11a 16-QAM 64-QAM CCK QPSK BPSK • 802.11b CCK DQPSK DBPSK	**Metodos de Propagacion** • Direct Sequence Spread Spectrum DSSS • Orthogonal Frequency Division Multiplexing (OFDM)	

Tabla IV.6 Especificaciones de la Tarjeta de Red tipo PCMCIA Marca SMC

IV.3.1.3.- Adaptadores PCI e ISA.

Las computadoras de escritorio no suelen incluir ranuras PCMCIA. Estas computadoras suelen disponer de suficiente espacio interior como parar admitir la instalación de nuevos periféricos a base de tarjetas Tipo PCI (*Peripheral Components Interconnect*, "Interconexión de Componentes Periféricos") o ISA (*Industry Standard Architecture*, "Arquitectura Normalizada de la Industria"). Este tipo de tarjetas es más barata que las tarjetas PCMCIA, aunque también son mayores en tamaño y de instalación algo más compleja (entre otras cosas, hay que abrir la computadora). Lo curioso en este caso es que difícilmente se encuentran en el mercado adaptadores inalámbricos de red de tipo PCI o ISA. El motivo quizás sea que las mayores prestaciones de las redes inalámbricas se consiguen con una computadora portátil (por aquello de la movilidad), así que el mayor mercado de adaptadores de red está hoy por hoy en el de las tarjetas PCMCIA, siendo relativamente pequeño el de las tarjetas PCI e ISA.

¿Cómo se conectan entonces las computadoras de escritorio a las redes inalámbricas? Pues con adaptadores USB o utilizando una tarjeta convertidora de PCI o ISA a PCMCIA. Una tarjeta convertidora de PCI o ISA a PCMCIA es una tarjeta que se instala en el interior de la computadora en una de las ranuras PCI o ISA disponibles y que ofrece al exterior una ranura PCMCIA (generalmente de Tipo II ó III). Dicho de otra manera, este convertidor le añade una ranura PCMCIA a la computadora.

Las tarjetas convertidoras de este tipo suelen ser baratas, pero a este precio hay que añadirle el precio de la propia tarjeta PCMCIA, por lo que la conexión a la red inalámbrica de la computadora de escritorio pasa a ser algo más cara que la de la computadora portátil.

El mayor inconveniente que presentan los dispositivos PCI e ISA es que requieren ser instalados en el interior de la computadora. Por otro lado, hay que abrir la computadora. Adicionalmente, incluso los que anuncian ser del Tipo *"Conectar y Funciona"* (Plug&Play), finalmente requieren que se les instale el programa de los controladores.

Por cierto, si se tiene una computadora que dispone tanto de ranuras PCI como ISA, siempre es más aconsejable utilizar las tarjetas del tipo PCI. Éstas suelen dar menos problemas de instalación y requieren menos recursos del sistema (una sola IRQ frente a las dos que requiere ISA). No hay más que pensar que ISA es una Norma de principios de los años 80; mientras que PCI es de principio de los años 90 (en 1993, exactamente). PCI fue desarrollado por *Intel®* como competidor al que poco antes se había convertido en el primer estándar de bus local, el estándar VESA (*Video Electronics Standard Association*, "Asociación para la Normalización de la Electrónica de Vídeo"). La principal novedad que trajo PCI fue el ser, el primer sistema que permitía lo que vino a ser posteriormente la tecnología de *"Conectar y Funciona"*, (Plug&Play). Finalmente, ISA, también conocido como *Bus AT*, puede transmitir información a una velocidad máxima de 16 Mbps, mientras que PCI puede llegar a 528 Mbps.

En la siguiente Tabla y Figura se indican las características de una tarjeta de red tipo PCI marca Belkin

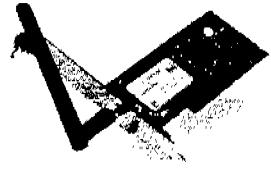
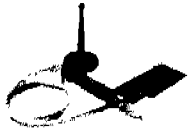


Figura IV.7 Tarjeta de Red tipo PCI Marca Belkin

Standards compatibles • IEEE 802.11b • IEEE 802.11g	**Metodos de Seguridad** • 64-, 128 bits WEP	**Metodos de Propagacion** • Complementary Code Keying (CCK)	**Modo de Red** • Ad hoc • Infraestructura
Antena • Exterior	**Rango de Frecuencia** 2.4GHz to 2.462GHz	**Consumo de Voltaje** • Tx/Rx 550/350 mA • 3.3 VDC	**Temperatura** • En Operacion: 32 to 185 °F (0 to 85°C) • Almacenado: -40 to 194°F (-40°C to 90°C) **Humedad** • 95% (no-condensado)

Tabla IV.8 Especificaciones de la Tarjeta de Red tipo PCI Marca Belkin

Otros Modelos de tarjetas de este tipo son:



Tarjeta de Red
Tipo PCI
Marca SMC

Tarjeta de Red
Tipo PCI
Marca Belkin

Tarjeta de Red
Tipo ISA
Marca Linksys

IV.3.1.4.- Adaptadores para PDA.

Un PDA es un pequeña computadora que cabe en la palma de la mano; de hecho, el dispositivo más vendido es el *"Palm Pilot de 3Com"* ®. Es cierto que también se les conoce como *Pocket PC* (PC de bolsillo) o como *HandHeldPC* (PC de mano).

Debido a su pequeño tamaño, los PDA pueden llevarse siempre encima, por lo que suelen incluir aplicaciones, que de alguna manera, son asistentes personales de su usuario: agenda de direcciones, agenda de actividades, lista de tareas, juegos, etcétera. No obstante, un PDA (Asistente Personal Digital) puede utilizarse como herramienta de comunicación: permite acceder a Internet, ver páginas *web*, gestionar correos electrónicos, etcétera. De hecho, los nuevos PDA incluyen versiones reducidas de programas de gestión conocidos como

Microsoft Word®, Microsoft Excel®, Microsoft PowerPoint®, etcétera. En definitiva, un PDA es una pequeña computadora de gran utilidad debido precisamente a su tamaño.

Habitualmente, un PDA se conecta a Internet a través de una computadora personal. Los correos se escriben en el PDA, pero no se transmiten (reciben) hasta que no se conectan mediante un cable (o infrarrojos) a la computadora personal con el que se ha asociado previamente.

También existe la posibilidad de conectarle un módem especial al PDA y acceder directamente a Internet a través de un proveedor de acceso (vía llamada telefónica). En este sentido, han aparecido más recientemente en el mercado equipos PDA que incluyen en su interior una terminal móvil, o teléfonos móviles que incluyen en su interior las capacidades de los PDA.

Cualquiera de las soluciones anteriores tiene un inconveniente, y es que no permite que el PDA esté conectado a Internet permanentemente, al menos, sin pagar unas altas tarifas por las llamadas telefónicas (del móvil o del fijo). Por otro lado, salvo en el caso del PDA con móvil (con alto costo en llamadas), el PDA siempre estará conectado por cable para intercambiar sus datos con la computadora asociada o conectarse a Internet. Pues bien, las redes inalámbricas le ofrecen al PDA la posibilidad de liberarse de las ataduras del cable.

En el mercado, existen módulos adaptadores de red inalámbrica para los principales modelos de PDA: *3Com®, Compaq®, HP®, Casio®*, etcétera. A la hora de comprar uno de estos dispositivos, es conveniente asegurarse de que es el adecuado para el modelo concreto de PDA de que se dispone. Estos módulos suelen ser tarjetas de tipo *"Compact Flash"* con una pequeña antena exterior. En la siguiente Tabla y Figura se indican las características de una tarjeta adaptadora para PDA marca Belkin.

Figura IV.9 Tarjetas Adaptadoras para PDA Marca Belkin y Linksys

Standards compatibles	Metodos de Seguridad	Metodos de Propagacion
• IEEE 802.11b	• 64-, 128-WEP	• Direct Sequence Spread Spectrum DSSS

Tabla IV.10 Especificaciones de la Tarjeta Adaptadora para PDA Marca Belkin

IV.4.- Compatibilidad entre los Sistemas Operativos y los componentes Wi-Fi

Los adaptadores de red, como el resto de los periféricos, para su correcto funcionamiento necesitan instalar un pequeño programa que se conoce como *"Controlador del Dispositivo"*. Este programa es específico de cada sistema operativo y se instala, de forma automática o manual, cuando se instala el adaptador o cuando se conecta a la computadora por primera vez.

Los sistemas operativos suelen disponer de los controladores de dispositivos de los periféricos más comunes del mercado. En muchos casos, es suficiente conectar el adaptador a la computadora y automáticamente se instala todo lo necesario. Sin embargo, en otras ocasiones, el sistema operativo no dispone del controlador adecuado. Para estos casos, el fabricante suele incluir un Disco Compacto con el adaptador que contiene los controladores para los principales sistemas operativos. Incluso, puede incluir un programa instalador del controlador. Si no se dispone de dicho Disco Compacto, también se puede acceder a la página *web* del fabricante del equipo para intentar obtenerlo. El inconveniente es que no todos los adaptadores disponen del controlador necesario para todos los sistemas operativos. La mayoría incluyen un controlador para *Windows®*, pero son muchos menos los que lo incluyen para *Linux®* o *Macintosh OS®*. Esto quiere decir, que es importante asegurarse de que el controlador que se va a comprar es compatible con el sistema operativo de la computadora en el que se va a instalar. Esto es más importante aún si se dispone de *Linux®* o *Macintosh OS®*. Los que lo tienen más complicado son los usuarios de *Macintos OS®*, éstos últimos, pueden buscar en las marcas *Agere/Orinoco®* o *Proxium®*.

IV.5.- Puentes.

Un Puente *("Bridge")* 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 red como si todos formaran parte de la misma red. La mayoría de los puntos de acceso hacen las funciones de puentes al poder interconectar una red local cableada con la red inalámbrica. Esto hace posible que las computadoras de la red inalámbrica utilicen las impresoras de la red cableada o accedan a los archivos de cualquiera de sus computadoras.

No obstante, existe un equipo conocido como Puente Inalámbrico que es algo distinto de un Punto de Acceso. Un Puente Inalámbrico interconecta dos redes remotas (cableadas o no), mediante una conexión inalámbrica. Estas dos redes pueden ser interconectadas también mediante cable, pero los puentes inalámbricos evitan la necesidad de tener que instalar el cable.

La solución inalámbrica requiere de dos equipos puentes inalámbricos, uno en cada extremo. En cualquier caso, estos equipos pueden ser utilizados para extender el área de cobertura de una red inalámbrica, sobre todo cuando se trata de interconectar zonas localizadas en edificios distintos o que no tienen una visibilidad directa para poder utilizar antenas externas direccionales. En la siguiente Tabla y Figura se indican las características de un Puente marca Linksys.

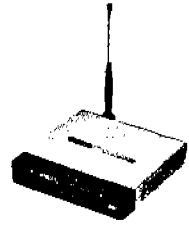
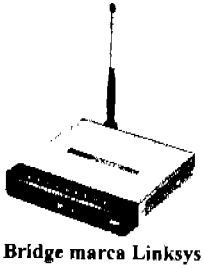


Figura IV.11 Bridge Marca Linksys

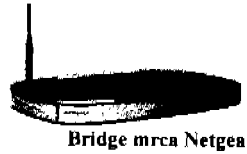
Standards compatibles • IEEE 802.11b • IEEE 802.11g • IEEE 802.1Q • IEEE 802.1d • IEEE 802.3 • IEEE 802.u	**Metodos de Seguridad** • 64-, 128 WEP • PSK-TKIP • RADIUS (solo para el bridge y no APRA clientes)	**Metodos de Propagacion** Orthogonal Frequency Division Multiplexing (OFDM) • Complementary Code Keying (CCK)	**Transmitter Output Power** • 802.11g 12 dBm • 802.11b 16 dBm
Power • 5 V DC • 2 A	**Rango de Frecuencia** •2.4GHz to 2.462GHz	**Puerto** • 5 Puertos 10/100 RJ-45 con soporte a Auto MDI/MDIX	**Tipo de Cable** • Categoria 5
Humedad • En Operacion : 10% al 85% (no-condensado) • Amacenado : 5% al 90% (no-condensado)	**Temperatura** • En Operacion: 32°F to 104°F (0°C to 40°C) • Almacenado: -4°F to 158°F (-20°C to 70°C)	**Dimensiones** • Largo = 130 mm • Ancho = 132mm • Altura= 29mm	**Peso** 13.6oz (0.39 Kg)

Tabla IV.12 Especificaciones del Bridge Marca Linksys

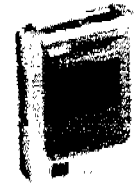
Otros Modelos de Bridges son:



Bridge marca Linksys



Bridge mrca Netgear



Bridge marca SMC

Bridge Zyxel

IV.6.- Antenas

¿Para que sirven las antenas? La mayoría de los usuarios de LAN inalámbricas no piensa ni sabe mucho sobre la función de las antenas, solo percibe que la fuerza de la señal y su caudal se degradan en su conexión; pero escalar a antenas es una forma fácil y efectiva en costos de ampliar el alcance de una WLAN.

Las antenas se pueden clasificar atendiendo a 2 características: Direccionalidad y Ganancia. La direccionalidad significa que envía y lo recibe mejor en una dirección que en otra. La ganancia dice cuánto mejor es en esa dirección. Lógicamente, cuanto más alta es la ganancia, mejora el rango (en la dirección en la cual la antena irradia.)

Las antenas no dan más señal que la de origen (para aumentar esta señal están los amplificadores), lo que hacen es "enfocar" la señal en una dirección particular.

La mayor parte de los Puntos de Acceso de WLAN vienen con *antenas bipolares omnidireccionales* de 4 o 6 dBi que transmiten en todas direcciones alrededor de su eje. Los clientes ubicados en dirección horizontal a las antenas reciben la señal más fuerte, y los clientes que queden verticales reciben una señal más débil. Antes de agregar una antena, debe verificarse si el cambio de posición del Access Point o el cliente mejora la fuerza de la señal.

Una *antena direccional* concentra las señales en los planos horizontal y vertical para producir una cobertura hemisférica de aproximadamente 30 grados. Esta es típica de la variedad plana o de panel, que se montan en las paredes o en el techo, y es adecuada en áreas donde varios clientes tienen acceso a la WLAN desde la misma dirección, como una sala de conferencias o una fila de cubículos.

Una *antena parabólica* es un panel cóncavo que casi siempre produce una señal muy alta con muchos grados de direccionalidad. Las antenas pueden ser sólidas o estar hechas de malla (se recomienda para lugares donde el viento sopla muy fuerte). Una antena parabólica ofrece mayor valor por el dinero que representa su adquisición, pero algunos la consideran de aspecto desagradable. Este tipo de antena es adecuada para aplicaciones de largo alcance, de punto a punto, como conectar dos edificios que están a mas de una milla de distancia.

Al considerar una antena, primero debe verificarse si el adaptador de Cardbus inalámbrico o Punto de Acceso le permite conectar una. Si es así debe decidirse que tipo de conector necesita. Por lo general, los Puntos de Acceso usan un conector SMA, y las tarjetas cliente usan gran variedad de conectores, por lo que podría requerirse un cable o adaptador personalizado. En la siguiente

Tabla y Figura se indican las características de una antena Omnidireccional marca SMC.

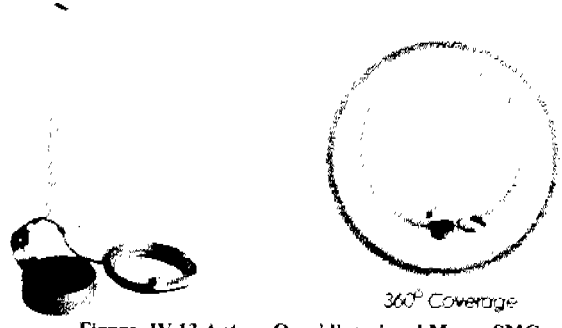


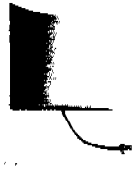
Figura IV.13 Antena Omnidireccional Marca SMC

Standards compatibles • IEEE 802.11g • IEEE 802.11b	**Rango de Frecuencia** • 2.4GHz to 2.5 Hz	**Ganancia** • 4 dBi	**Tipo de Antena** Omni Direccional 360°
Polarizacion • Linea Vertical	**Plano Horizontal** • 360° **Plano Vertical** • 40°	**Conector** • SMA Tipo de cable • ULA - 316	**Impedancia** • 50 ohms
Humedad 95% en 25° C	**Temperatura** • En Operacion: -10°C to 55°C	**Dimensiones** • Largo = 2.95 pulgadas (75mm) • Ancho = 0.91 pulgadas (23mm) • Altura= 0.7 pulgadas (6.3mm)	**Peso** 6.34 oz (180 gr.)

Tabla IV.14 Especificaciones de una Antena Omnidireccional Marca SMC

Otros Modelos de Antenas en la gama de frecuencia de 2.4 GHz son:

Antena Portable
Marca Linksys
Tipo USB



Antena Omnidireccional
Marca Dlink
14 dBi

Antena de Escritorio
Marca US Robotics
4 dBi

Antena Direccional
Marca SMC
6 dBi

IV.7.- Otros Dispositivos Inalámbricos

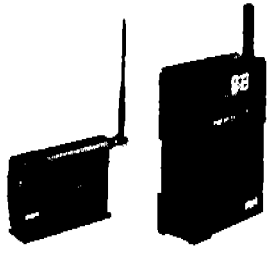
Si bien Wi-Fi tenía como función, originalmente, el permitir la movilidad sin cables de terminales conectadas a Internet en un área limitada, hoy esta tecnología está cruzando nuevas fronteras, y se está enfocando hacia aparatos que, tradicionalmente, no se conectaban a Internet. Ejemplos de esto son Prismiq y Sound Blaster Wireless Music, que permiten al usuario descargar los archivos de música MP3 y WAV de sus PC y reproducirlos, en tiempo real, en cualquier equipo en la casa. O el Streamium MC-i250, de Philips, equipo de música que, además de permitir lo mismo, sintoniza estaciones de radio tomándolas del espectro aéreo y de Internet.

Por su parte, Gateway ofrece su Connected DVD Player, un reproductor de DVD con acceso inalámbrico a las imágenes, archivos de música y video almacenados en la computadora. Por su lado, Sharp estará ofreciendo, muy pronto, su Wireless Aquos, un televisor con pantalla de LCD que también se conecta por vía inalámbrica a las computadoras. Así, el entretenimiento es motor de la expansión de Wi-Fi hacia otros terrenos. El Wireless-B Game Adapter, de Linksys (empresa del grupo Cisco), permite conectarse vía Wi-Fi a equipos de videojuegos como PlayStation 2, Xbox y GameCube, y Hitachi, por su parte, ha desarrollado un sistema de localización basado en Wi-Fi, entre tres y diez veces más preciso que el GPS, con un alcance de hasta 450 metros.

Esta expansión no termina aquí, Ya se está trabajando en desarrollos que permitirán incluir el Wi-Fi en automóviles, cámaras de video y los video juegos portátiles, además de que se busca la manera de reducir el consumo de energía de los chips Wi-Fi para adaptarlos a los teléfonos celulares. Por ejemplo, el gigante del software se monta en este boom con su tecnología Microsoft .NET Compact Framework, ideada para construir "de manera sencilla" aplicaciones para todo tipo de dispositivos móviles, desde PDAs y teléfonos móviles hasta XDAs (soluciones híbridas que reúnen las principales características de estas máquinas) y equipos empotrados diseñados para el mundo automotriz.

Intel por su parte ha presentado una nueva familia de procesadores y aceleradores multimedia para potenciar las capacidades de los dispositivos inalámbricos de bolsillo más avanzados. Estos procesadores (Intel PXA27x) se han diseñado para gestionar múltiples modos de acceso de banda ancha inalámbrica y proporcionar la potencia informática necesaria para las videoconferencias con movimiento completo en teléfonos móviles. A esto Intel añade su nuevo chip complementario del acelerador multimedia Intel 2700G, el procesador Intel PXA27x, que permite la reproducción de vídeo de calidad DVD en las PDA, todo esto con un bajo consumo para una mayor movilidad. Otro ejemplo es el de PalmOne. Los usuarios de las venerables Palm recibieron

recientemente la noticia de que palmOne ahora añade la conectividad Wi-Fi a sus dispositivos, al liberar una nueva tarjeta Wi-Fi para los modelos Tungsten T3 y Zire 72, que ya contaban con la tecnología Bluetooth. Ahora también podrán conectarse a Internet rápidamente, siempre que se encuentren dentro de la zona de cobertura de un punto de acceso Wi-Fi o "hotspot". A continuación se muestran las imágenes de los dispositivos más conocidos de éste tipo.



Game Adapter Linksys 802.11g y 802.11b

Consola para integrar un Xbox a una red inalambrica 802.11g marca Microsoft

Sistemas de Música Linksys 802.11b

Sistema de Música Netgear 802.11 b y g

Internet Video Camera Linksys 802.11g

CAPÍTULO V.

APLICACIÓN DE UNA RED INALÁMBRICA BASADA EN EL PROTOCOLO 802.11 x EN EL LABORATORIO DE COMUNICACIONES L-3 DE LA ENEP *"ARAGÓN"* DE LA UNAM.

V.1.- Introducción

La popularización de la tecnología inalámbrica está suponiendo un creciente interés por parte de los usuarios y de las empresas proveedoras en buscar soluciones alternativas más fáciles de implantar a las necesidades de comunicaciones existentes o a las nuevas necesidades que puedan surgir. Se puede decir que las aplicaciones de las redes inalámbricas se pueden dividir en tres campos:

- Aplicaciones relacionadas con la facilidad de comunicar dispositivos portátiles.- Si se dispone de una computadora portátil o PDA, éstos pueden disponer de conexión con el resto de la red local o a Internet sin necesidad de tener que estar atados a un conector de red. Es más, se puede disfrutar de estos servicios aunque se permanezca en movimiento.

- Aplicaciones relacionadas con la facilidad de configuración y reorganización.- Las redes de área local cableadas son complicadas de instalar por la necesidad que tienen de disponer de un conector al lado de cada computadora. Incluso reorganizar una red cableada puede ser todo un problema si la nueva disposición no coincide con los lugares donde hay red. Las redes inalámbricas son fáciles de instalar y, no tienen necesidad de modificación cuando las computadoras se cambian de sitio.

- Aplicaciones relacionadas con la facilidad de establecer comunicación punto a punto vía radio.- Cablear una red local dentro de un edificio puede ser una tarea abordable; pero, interconectar las redes de dos edificios o comunicar dos computadoras distantes es muy complicado de hacer por los propios medios vía cable. Resolver esto vía inalámbrica no supone mucho problema. La única limitación es que, si la distancia es grande, se debe contar con la visibilidad directa entre los extremos.

Aparte de lo anterior, la existencia de los servicios de acceso a Internet con banda ancha y la popularización de las redes inalámbricas está llevando a un creciente interés por parte de las empresas proveedoras en ofrecer servicios y aplicaciones basados en el hecho de que los usuarios pueden disponer de un dispositivo inalámbrico en cualquier lugar y con una alta velocidad de acceso hacia y desde Internet.

Esto le da un valor añadido importante a los servicios de banda ancha como juegos multimedia, videoconferencias, televigilancia, visitas virtuales. telerreunión, teleinformación, retransmisión de actividades, recepción de televisión, radio, acceso a disco duro virtual, interconexión de redes, teleasistencia, teletrabajo, trabajo en grupo, etcétera.

Un campo de aplicación que todavía no está muy extendido es el del control de los dispositivos del hogar desde la computadora. Programar la calefacción, controlar el dispositivo de riego o poner en marcha el horno de micro-ondas desde la computadora no es abordable si hay que llenar la casa de agujeros por donde se van a instalar los cables; sin embargo, es mucho más asimilable si lo único que hay que hacer es conectar unos dispositivos inalámbricos a cada aparato, para, a continuación, poder controlarlos tanto desde la computadora de casa como desde cualquier parte del mundo a través de Internet. Desde este punto de vista, hacer televigilancia del hogar o poner en marcha o apagar cualquier aparato puede que se convierta en habitual dentro de un tiempo.

V.2.- Aplicaciones en la Empresa.

Las redes inalámbricas son aplicables en cualquier campo de la industria donde exista la necesidad de utilizar un dispositivo informático, tener movilidad y permanecer en contacto en tiempo real con recursos informáticos dentro o fuera de la empresa. Las redes inalámbricas son especialmente útiles cuando los empleados necesitan acceder a la información desde distintos sitios o mantener una cierta movilidad. Éste seria el caso, por ejemplo, de médicos, enfermeras, inspectores, agentes, vendedores, personal de mantenimiento, personal de almacén, atención al cliente, personal de exposición, etcétera.

Para ver las ventajas de las redes inalámbricas, simplemente hay que pensar en la alternativa actual: utilizar formularios en papel. copias del papel a la computadora, manejar información impresa no actualizada, tener que moverse para conseguir acceder a la información de la empresa, etcétera. Esto trae consigo, la duplicación del trabajo, aumentar los tiempos de respuesta, introducir errores de interpretación de la escritura manual. Manejar información no actualizada, perder tiempo en desplazamientos innecesarios, etcétera. Una computadora portátil o PDA con conexión inalámbrica puede mejorar grandemente el rendimiento y eficacia de muchos puestos de trabajo; facilita la movilidad, elimina el papeleo, disminuye los errores, reduce los costos de gestión, acerca la empresa al trabajador, aumenta la eficiencia.

V.3.- Comunidades Inalámbricas.

Una de las ventajas de las redes Wi-Fi es que permite que cualquier usuario pueda fácilmente conectarse a una red inalámbrica con tan sólo entrar en su área de cobertura. Esta particularidad hace posible disponer de redes inalámbricas públicas a las que puede acceder cualquier usuario para conectarse a Internet o hacer uso de cualquier otro servicio que ofrezca (uso de impresoras, uso de programas en red, juegos, almacenamiento de información, etcétera).

V.3.1.- Organización de las Comunidades Inalámbricas.

Técnicamente, una comunidad inalámbrica es una red de redes inalámbricas interconectadas entre sí, para crear una red única con cobertura, generalmente, metropolitana o regional, pero que podría llegar a tener alcance nacional o internacional.

Cada red está gestionada por un administrador de red y está formada por las computadoras o dispositivos Wi-Fi de los usuarios, uno o más puntos de acceso y los equipos y enlaces necesarios para hacer funcionar la red y las interconexiones de la red con el resto de la comunidad. A cada punto de acceso se le conoce con el nombre general de nodo.

Para que toda la comunidad funcione de forma interconectada, es imprescindible que exista un acuerdo en el uso de las direcciones IP. Cada red inalámbrica, cada administrador, necesita su propio rango de direcciones IP para poder asignar direcciones a sus usuarios. Por otro lado, la comunidad necesita determinadas direcciones IP para los elementos de red (servidores DNS, ruteadores, etcétera). Además, no puede haber dos direcciones repetidas. La gran ventaja es que no se utilizan IP públicas de Internet, sino IP privadas. Las direcciones IP privadas pueden ser utilizadas por los administradores de red con toda libertad, sin que las instituciones que gestionan la numeración de Internet tengan que intervenir.

Para organizar todo esto, varios grupos internacionales de comunidades Wi-Fi han desarrollado unos reglamentos internos de direccionamiento. Por ejemplo en España la asociación *Redlibre* ha planteado el uso de direcciones IP en todo ese país utilizando el rango de direcciones privadas 10.0.0.0 para usuarios y el rango 172.16.0.0 para las direcciones necesarias de red (*www.redlibre.net/direccionamiento.php*).

De acuerdo con el plan de direccionamiento de *Redlibre*, cada nodo tendrá como mínimo un rango de 32 direcciones. De todas éstas, 29 son para usuarios (de la 10.x.x 2 a 10.x.x.30), una es para el Punto de Acceso (10.x.x.31).

otra para el ruteador (10.x.x.1) y otra para la red (10.x.x.0). La máscara de red a utilizar sería la 255.255.255.224. Esto quiere decir que la dirección de cada red termina en .0, .32, .64, .96, .128, .160, .192 y .224. En cualquier caso, si una red necesitase de más direcciones, siempre puede ocupar más de un rango de 32 direcciones.

Para el enrutamiento del tráfico entre nodos, se utiliza un Protocolo de Enrutamiento Dinámico del tipo IGP (*Interior Gateway Protolols*). Los más conocidos son RIP (*Routing Information Protocol*) y OSPF (*Open Shortest Path First*). Por otro lado, para interconectar distintas comunidades inalámbricas, deben utilizarse protocolos del tipo EGP (*Exterior Gateway Protocol*) como, por ejemplo; BGP (*Border Gateway Protocol*).

V.4.- Redes Comerciales de Acceso Público Inalámbrico.

Una comunidad inalámbrica puede convertirse, con la configuración adecuada, en una red inalámbrica de acceso público que ofrezca una serie de servicios comerciales. Quizá el principal de los servicios sea el acceso a Internet desde lugares públicos (cafeterías, aeropuertos, bibliotecas, etcétera), pero este servicio se puede complementar con otros como uso de impresoras, uso de programas en red, juegos, almacenamiento de información, etcétera.

A las redes inalámbricas que ofrecen sus servicios al público se las conoce como redes inalámbricas de acceso público, PWLAN (*Public Wireless Local Area Network*, "Red Pública Inalámbrica de Área Local") o, simplemente, *hotspot*.

Las redes comerciales de acceso público inalámbrico sitúan sus puntos de acceso en aquellos lugares donde existe una gran asistencia de público con tiempo suficiente para conectarse a Internet para realizar cualquier tarea profesional o personal. Estos lugares suelen ser hoteles, centros de convenciones, aeropuertos, campus universitarios, centros comerciales, cafeterías, restaurantes, bibliotecas, etcétera. En estos lugares les ofrecen a sus usuarios la facilidad de acceder a Internet desde su propia computadora (previamente dotada con una tarjeta Wi-Fi). Los proveedores de este servicio suelen cobrar una cuota mensual fija, una tarifa por uso o ambas cosas, ofreciendo la posibilidad de hacer uso de su servicio desde cualquier punto de su red.

Los usuarios principales de este tipo de servicios son dos: personas de negocios que se desplazan continuamente y tienen necesidad de mantener acceso a Internet (desde hoteles, aeropuertos, restaurantes, etcétera), y en general el gran público que aprovecha su estancia en un lugar público (cafeteria, centro comercial, biblioteca, etcétera), para pasar un tiempo de ocio.

Los servicios de acceso público inalámbrico son vistos como una oportunidad de negocio, tanto por los operadores de telecomunicaciones de red fija y móvil, como por las empresas independientes. Al proveedor de este tipo de servicio se le conoce por el término general de WISO (*Wireless Internet Service Provider*, "Proveedores de Acceso Inalámbrico a Internet").

V.5.- Enlace Punto a Punto.

Aunque el estándar Wi-Fi es utilizado habitualmente para crear redes locales inalámbricas, también puede utilizarse para crear un enlace de comunicación entre dos puntos. Esta facilidad sirve, por ejemplo, para interconectar dos edificios de una forma fácil, rápida y barata. Tradicionalmente, para establecer una comunicación entre dos puntos que no estuviesen situados en un mismo entorno privado, sólo existía la alternativa de recurrir a un operador de telecomunicaciones. Esto supone pagar una cuota alta y una tarifa mensual más o menos elevada. Con Wi-Fi se puede establecer esta misma conexión (hasta 11 Mbps) con un único costo de compra de los equipos (e instalaciones si es el caso). Posteriormente, no hay que hacer ningún pago mensual, salvo los posibles trabajos de mantenimiento, si los hubiera.

Aunque se puede establecer una comunicación punto a punto utilizando puntos de acceso o tarjetas de red, en el mercado existen unos equipos Wi-Fi especialmente pensados para este trabajo. A estos equipos se les conoce con el nombre de *wireless bridge* ("Puente Inalámbrico"). Un Puente Inalámbrico interconecta dos computadoras o dos redes remotas (cableadas o no) mediante una conexión inalámbrica. Una conexión inalámbrica requiere de dos equipos de Puentes Inalámbricos, uno en cada extremo.

Una aplicación en la que se utilizan habitualmente los equipos Puente es en la interconexión de puntos de acceso para crear una red extensa inalámbrica que cubra todo un Campus universitario, una zona empresarial y/o industrial, un vecindario o una ciudad. Los equipos Puente pueden establecer enlaces punto a punto o punto a multipunto.

Un par de equipos puente completados con antenas direccionales, y una buena instalación, puede llegar a establecer enlaces de más de 10 kilómetros. En algún caso, para eliminar al máximo las pérdidas del cable y conectores, se instala el Puente en una caja pegada a la antena. Hay que tener en cuenta que cada 3 dB de pérdida, supone disminuir la potencia a la mitad.

V.6.- Televigilancia.

La televigilancia consiste en poder ver desde un lugar lo que está ocurriendo en otro lugar mediante la transmisión de vídeo y audio. Tradicionalmente, la televigilancia se ha llevado a cabo mediante la instalación de caros circuitos dedicados. Internet y las soluciones de Acceso de Banda Ancha (DSL o módem-cable) permiten establecer soluciones de televigilancia a un costo muy bajo. Además, la tecnología inalámbrica permite situar los dispositivos de televigilancia (las cámaras) de una forma fácil y rápida, sin depender de costosas instalaciones cableadas. Por otro lado, Internet ofrece la ventaja de que las imágenes pueden ser vistas desde cualquier parte del mundo.

En el mercado existen cámaras inalámbricas Wi-Fi que permiten situar la cámara en cualquier lugar, con la sola necesidad de disponer un enchufe de alimentación eléctrica o, en su defecto, de una batería. La señal de vídeo se transmite vía Wi-Fi hasta la red local o Internet.

Hay que tener claro que estas soluciones de televigilancia sólo ofrecen la posibilidad de ver imágenes de forma remota. En ningún caso, esta simple retransmisión de imágenes sustituye a los múltiples servicios de vigilancia y asistencia de las empresas profesionales de este sector.

Las cámaras inalámbricas suelen disponer de un Servidor *web* interno al que se puede acceder tanto para la configuración de la cámara como para ver su imagen. La cámara se configura como cualquier otro dispositivo inalámbrico (excepción de las propiedades de vídeo que son propias de este dispositivo). Si se dispone de varias cámaras, existen aplicaciones (como *IPview*) que permiten gestionarlas simultáneamente e, incluso, realizar grabaciones de las imágenes.

Para determinar aplicaciones resulta más conveniente llevar la imagen de la cámara a un Servidor desde donde se ofrece al público. También existen empresas en Internet que, por un módico precio, colocan en sus servidores las imágenes de vídeo recogidas por las cámaras *web* de sus clientes.

En cualquier caso, la televigilancia a través de Internet resulta una buena solución de supervisión de instalaciones y dependencias tanto para el uso particular (supervisión de los niños, vigilancia de la casa, etcétera), como para la pequeña empresa y profesionales (supervisión de instalaciones, tiendas, almacén, despacho, teletrabajadores, etcétera). Además, estos sistemas permiten ser combinados con el envío de mensaje de correo electrónico o llamadas al teléfono móvil en el caso de dispersarse alguna alarma. Como conclusión, se puede ver a continuación algunas de las aplicaciones de los sistemas de televigilancia por Internet:

- **Residencial.-** Permite supervisar el estado del hogar o de la alguna residencia u oficina.
- **Guarderías.-** Los padres autorizados, pueden ver a sus hijos en la guardería.
- **Personas mayores.-** Permite estar en contacto directo con personas mayores que viven solas.
- **Comunidad.-** Permite que cualquier vecino pueda ver las instalaciones comunes para supervisar el juego de los niños o el aparcamiento de los automóviles.
- **Industrial.-** Control de almacenes solitarios, verificación de alarmas, etcétera.
- **Construcción y proyectos.-** Permite que los clientes puedan ver el estado de la construcción o el proyecto, sin tener que desplazarse.
- **Vigilancia.-** Para ver y vigilar a distancia distintos centros desde una oficina "central".

Por último, las cámaras inalámbricas tienen la posibilidad de ser instaladas sobre personas o equipos en movimiento. Esto las hace ideales para cámaras subjetivas en la retransmisión o grabación de imágenes deportivas o de aventura.

V.7.- Wi-Fi en el Automóvil

En la "Muestra de Electrónica de Consumo" *(Consumer Electronics Show)* que tuvo lugar en Las Vegas, Nevada, Estados Unidos de América en Enero del Año 2003, las empresas Linksys y Zadiant Technologies presentaron una serie de aplicaciones de redes inalámbricas para el automóvil. La aplicación que más llamó la atención fue la posibilidad de cargar el equipo de música del automóvil con la música en formato MP3 que se tiene en la computadora de casa sin necesidad de cables. El auto dispone de una unidad Wi-Fi que le permite conectarse con la computadora de casa y hacer la transferencia de música de una forma rápida, segura y fácil.

Otra de las aplicaciones que tiene Wi-Fi para el automóvil es la que se ha venido a llamar "Maleta Digital" *(Digital Briefcase)*. Una Maleta Digital consiste en que se lleva un servidor en el coche con toda la información y aplicaciones que se necesita para la vida diaria. Cuando se está en casa, se puede acceder al servidor del automóvil desde la computadora del hogar y cuando se está en la oficina, desde la computadora del trabajo. Es algo así como pensar que el automóvil es una herramienta informática personal, más personal aún que la computadora portátil, y con la ventaja que no se tiene que cargar con él. Obviamente, el inconveniente de este tipo de aplicaciones es que se necesitaría

estar siempre a una distancia del automóvil inferior a los 100 metros. En las grandes ciudades esto no es posible muchas veces ni en la casa.

Por otro lado, el disponer de Wi-Fi en el automóvil hace posible que se pueda acceder a Internet desde él. Bastaría con acercarse a un punto Wi-Fi público (conocidos como *hotspot*) para poder leer el correo electrónico, acceder a las noticias o bajarse la música o vídeo para el resto del trayecto. Uno de los sitios propicios para este tipo de actividades son por ejemplo, las gasolineras, las áreas de descanso de las autopistas y los estacionamientos públicos.

Yendo un poco más allá, hay quien habla de aprovechar este enlace entre el automóvil e Internet para poder tener el vehículo vigilado y localizado. Una cámara en el interior y un sistema GPS pueden complementar el equipamiento para permitir un sistema de vigilancia y localización del automóvil.

V.8.- Telefonía Wi-Fi.

La telefonía Wi-Fi permite establecer y mantener conversaciones telefónicas utilizando sus facilidades de movilidad. En definitiva, la telefonía Wi-Fi viene a ser la unión de las redes inalámbricas y de la telefonía IP.

La telefonía Wi-Fi puede tener su campo principal en las empresas y sectores como la Educación, salud, fabricación o almacenamiento, donde la movilidad de los trabajadores es un factor importante. La ventaja que ofrece la telefonía Wi-Fi frente a las comunicaciones inalámbricas de voz actuales, es que permite integrar la facilidad de transmisión de voz con la de datos y vídeo. Adicionalmente, la existencia de lugares de acceso público Wi-Fi permite disponer de un servicio telefónico inalámbrico de bajo costo desde lugares públicos.

Para poder hacer uso de esta tecnología, se espera disponer tanto de terminales telefónicas especificas, como de terminales multipropósitos: PDA y computadoras portátiles. Las terminales basadas en PDA pueden resultar muy interesantes, ya que permiten integrar las funciones de telefonía, vídeo y datos en una sola terminal de reducido tamaño.

Los retos que tienen que vencerse en la actualidad para la introducción de este servicio son tres fundamentalmente: la calidad de audio en una red abierta llena de interferencias y retardos; actualmente no está garantizada la continuidad del servicio cuando se desplaza el usuario, y la falta de seguridad de las comunicaciones Wi-Fi. A pesar de lo anterior, para los problemas anteriormente señalados, existen soluciones que harán que este servicio sea posible con todas las garantías a corto o mediano plazo.

En cualquier caso, salvo que se disponga de una red Wi-Fi muy congestionada, siempre se puede establecer una comunicación de voz utilizando los servicios de las empresas de telefonía por Internet. Estas empresas hacen de intermediarios entre Internet y la red telefónica permitiendo establecer una comunicación telefónica desde una computadora a cualquier número telefónico del mundo.

Las tarifas de estas empresas suelen ser algo más altas que las de una llamada local en el lugar de destino. En el mundo existen muchas empresas de telefonía por Internet. Generalmente, suelen utilizar el sistema de prepago, de forma que el usuario sólo tiene que recargar su cuenta con la cantidad que estime oportuna y podrá hablar hasta que se le agote el saldo.

V.8.1.- Recibir Llamadas en la Terminal Wi-Fi.

Cuando se dispone de una terminal inalámbrica Wi-Fi desde donde se pretende realizar las comunicaciones telefónicas, esto implica disponer de la posibilidad tanto de realizar llamadas como de recibirlas. Ya se ha visto que, para realizar las llamadas, se necesita disponer de los servicios de una empresa intermediaria que transfiera la llamada de Internet a la red telefónica, pero qué pasa cuando lo que se pretende es recibir las llamadas telefónicas en la terminal inalámbrica. Para solucionar este problema, algunos fabricantes han desarrollado un sistema que convierte las llamadas telefónicas en datos IP que pueden ser remitidos a la computadora del usuario (o al teléfono IP) por un proveedor de servicio. Para que esto funcione, el usuario tiene que desviar previamente sus llamadas telefónicas a un número de teléfono de su proveedor de servicio. Si este servicio lo presta el propio operador telefónico, este reencaminamiento podría realizarse de forma automática. También se puede contar con un número telefónico independiente para las llamadas a la computadora o teléfono IP. Cuando el usuario recibe la llamada en su terminal inalámbrico (computadora portátil o PDA), verá un icono en la pantalla que le indica que tiene una llamada telefónica en espera. El usuario puede aceptar o no dicha llamada. De hecho, el usuario podría, incluso, navegar y hablar por teléfono simultáneamente.

V.8.2.- Teléfonos Wi-Fi.

La tecnología Wi-Fi está en continua evolución. Lo que surgió como una solución para crear redes locales inalámbricas que permitieran la comunicación de datos está evolucionando hacia un sistema inalámbrico que da soporte a cualquier necesidad de comunicación: datos, voz, imagen, etcétera.

En ese sentido, fue anunciada la aparición en el año 2003, de terminales telefónicos inalámbricos de tecnología Wi-Fi. Estos terminales permiten recibir y realizar llamadas telefónicas de voz siempre que se esté dentro del área de cobertura de una red Wi-Fi (dentro de la empresa, en la casa o conectado a alguna red Wi-Fi pública). Para evitar tener que llevar encima dos terminales distintas (uno Wi-Fi y otro de telefonía móvil), algunos fabricantes ya han prometido que ofrecerán terminales multimodos (GSM, Wi-Fi y PCS). Esto posibilitará que, con una sola terminal, se pueda utilizar Wi-Fi cuando se esté dentro del área de cobertura Wi-Fi y GSM o PCS cuando se esté fuera del área de cobertura Wi-Fi.

Los teléfonos Wi.-Fi, al igual que los teléfonos IP o la telefonía por computadora, necesitan que se contrate los servicios de una empresa de telefonía por Internet. Estas empresas pueden ofrecer incluso, un número telefónico exclusivo para las comunicaciones de voz sobre IP (VoIP).

V.9.- El Hogar Digital.

Desde hace algunos años se viene hablando insistentemente de la Domótica, o lo que es lo mismo, de la automatización del hogar. Cada nuevo desarrollo tecnológico produce inmediatamente que se desarrolle la imaginación para verle una aplicación al hogar. No obstante, su implantación real siempre se ha visto frenada por toda una serie de limitaciones, entre las que se encuentran las siguientes:

- Necesidad de nuevo cableado por todo el hogar.
- Complicación en su instalación.
- Alto costo.
- Baja velocidad de transmisión.
- Capacidad de crecimiento limitada.
- Compatibilidad.

Pues bien, la tecnología Wi-Fi viene a eliminar prácticamente todas las barreras anteriores. De hecho, con la tecnología Wi-Fi se puede ir más allá de la Domótica y crear lo que se está viniendo en llamar "Vivienda Inteligente". Ésta consta de tres tipos de redes interconectados:

- **Red Domótica o de Automatización.-** Interconecta los dispositivos eléctricos del hogar, puntos de luz, calefacción, riego, conmutadores, sistemas de seguridad, etcétera.
- **Red de Entretenimiento.-** Interconecta la recepción de televisión, películas, radio, juegos, etcétera.
- **Red de Datos.-** Interconecta computadoras y dispositivos informáticos (impresoras, digitalizadores, graficadotes, etcétera).

El mercado está avanzando en esta idea. De hecho, ya se tiene desarrollado lo que se conoce como pasarela residencial. Éste es un dispositivo único que hace de interfase entre el exterior y cada una de las subredes del hogar (domótica, entretenimiento y datos). Los organismos de normalización están realizando un gran esfuerzo con el objeto de conseguir un estándar común de trabajo que permita desarrollar esta industria.

Una de las iniciativas de normalización más relevante es la que se conoce como OSGi (*Open Gateway Initiative*, "Iniciativa de Pasarela de Servicios Abierta"). Ésta es una alianza, establecida en 1999, de las empresas más importantes del sector de las telecomunicaciones, microelectrónica y fabricantes de equipo de consumo con el objetivo de conseguir un estándar capaz de comunicarse con prácticamente cualquier tipo de aparato eléctrico o electrónico del hogar. Por otro lado, en relación con el entretenimiento, en el mercado ya existen soluciones que permiten recibir música, películas o canales de televisión por Internet. Este tipo de recepción garantiza una buena calidad de recepción al no verse sometidas a las limitaciones de las recepciones tradicionales de radiofrecuencias.

V.10.- Descripción del Proyecto de Red Inalámbrica para el Laboratorio de Comunicaciones (L-3) de la Escuela Nacional de Estudios Profesionales "Aragón," de la Universidad Nacional Autónoma de México.

V.10.1.- Propuesta del Proyecto.

El siguiente documento fue llevado a cabo por Claudia Contreras Guadarrama y Raúl Vega Salomé, siendo el presente, de carácter confidencial y exclusivo para la Universidad Nacional Autónoma de México en la Escuela Nacional de Estudios Profesionales en el Campus *"Aragón"*, Laboratorio L-3 del Área Eléctrica y Electrónica.

El Laboratorio L-3 es un edificio de 3 niveles que se encuentra ubicado dentro de la ENEP Campus *"Aragón"*, en el cual se imparten diversos laboratorios de las Carreras de Ingeniería Mecánica Eléctrica e Ingeniería en Computación. Este edificio se encuentra ubicado dentro del Campus Universitario en el Área de Laboratorios.

Se propone un Sistema Inalámbrico de Red de Área Local (WLAN) para que proporcione cobertura a todo el laboratorio y tal vez a áreas adjuntas.

V.10.2.- Introducción al Proyecto de la Creación de una Red Inalámbrica.

Este proyecto tiene como objetivo principal acercar las nuevas tecnologías de comunicación inalámbrica a los profesores y alumnos de la ENEP *"Aragón"*, demostrando el funcionamiento de una red de este tipo. Esto se realizará implementando una WLAN (*"Wireless Local Area Network"*, Red de Área Local) de banda ancha, vía radio.

El proyecto se propone para el L-3 inicialmente; pero en un futuro, se puede extender a más laboratorios (L-1, L-2, y L-4) y a otras áreas como la Biblioteca, el Edificio de Gobierno, el CAE, el Departamento de Servicios Escolares, etcétera. Esto permitiría a los profesores y alumnos verificar información electrónica en todo momento. Además, esto los acercaría a las nuevas tecnologías de la información y a nuevos medios de comunicación.

El proyecto para la creación de una red inalámbrica en el L-3, permite no sólo que los usuarios accedan a Internet, sino que al disponer de una red local que interconecte a todos los usuarios a alta velocidad, será posible la incorporación de distintos servicios en dicha red. Así, serán fácilmente utilizables servicios de carácter general, como: intercambio de archivos, verificación de su historial académico, y ayudará en la forma de inscribirse a las materias y los laboratorios.

Para la realización de este proyecto, se extenderá una red local mediante una tecnología de interconexión vía radio, definida en la Norma (Estándar) IEEE 802.11g, la cual permite no sólo reducir los costos de implantación; sino que también ofrece una movilidad total a los usuarios de dicha red, ya que al utilizar ondas de radio, el acceso a la red es posible mediante dispositivos móviles desde cualquier localización que tenga cobertura.

Esta tecnología de creación de redes locales vía radio, lleva varios años utilizándose por empresas, plazas, particulares y centros educativos, y ha sido una opción barata y muy viable.

Las empresas públicas y privadas son los principales beneficiarios de esta tecnología, ya que con un único punto de acceso es posible tener a una serie de usuarios conectados dentro de un mismo edificio, aprovechando la movilidad típica de este tipo de redes, la reducción inicial de gastos de cableado y de cambios de infraestructura (para modificaciones posteriores en la ubicación de otras áreas) propios de un medio físico como el de Ethernet IEEE 802.3. Además, es posible la interconexión entre varios edificios sin tener que recurrir a obra civil, lo que permite el ahorro de todos los costos que ello representa.

Este proyecto se basa en el estándar IEEE 802.11g (o Wi-Fi), definido y protegido por la Norma vigente. Dicha Norma, crea un acceso al medio sin

cables, eliminando el problema de la poca o nula movilidad que una red LAN cableada convencional. Este proyecto pretende la creación de una red alternativa a la existente, que permita intercambiar información y recursos entre sus distintos usuarios para su propio beneficio y el de toda la comunidad del Laboratorio.

Esta tecnología hará uso de un sistema de difusión de las señales radioeléctricas denominado "Spread Spectrum Radio", éste sistema utiliza un ancho de banda mayor al estrictamente necesario a cambio de conseguir reducir la vulnerabilidad a las interferencias y garantizar la coexistencia con otras transmisiones. Utiliza varias bandas de frecuencias (ISM Band) que antes estaban reservadas solo para uso Industrial, Científico y Medico. Las frecuencias destinadas para datos son:

- 902 - 928 MHz
- 2.4 – 2.4835 GHz (banda que utilizará nuestro proyecto).
- 5.725 – 5.850 GHz

Una característica básica que hace especialmente interesantes este tipo de redes, es la altísima velocidad de transmisión de datos que pueden alcanzar, comparándola con otras posibilidades existentes. Otra característica importante es la completa compatibilidad de este tipo de redes con cualquier red ya existente.

Esto permite trabajar con computadoras remotos, como si estuvieran conectados en la Red de Área Local, encargándose el Protocolo, de negociar automáticamente las velocidades de transmisión entre las máquinas; dependiendo de la calidad de la conexión: 54Mbps, 11Mbps, 5.5Mbps, 2Mbps ó 1Mbps.

La implantación de una red de estas características, presenta algunos detalles relativos a la seguridad que son necesarios cuidar puesto que el medio de transmisión físico es el aire, por lo tanto; no se puede evitar que un tercero pueda recibir determinada información. Pero implantando una política de seguridad, se puede lograr una adecuada privacidad de los datos, que permita asegurar las transmisiones con la misma seguridad que ofrece una red local, ya que este tipo de red permite la implantación de sistemas de seguridad basados en la encriptación de paquetes sin ningún tipo de límites con respecto a la longitud de las claves empleadas, lo que permite asegurar las transmisiones y evitar que la información recibida sea descifrada por personal no autorizado.

Este proyecto está sustentado por la experiencia obtenida, tanto en la implantación de redes particulares para empresas y para los denominados *"Café-Internet"*; así como, para negocios pequeños.

V.10.3.- Topología de la Red Inalámbrica en el Campus "Aragón".

Este tipo de red local, al estar basada en transmisiones de radio, presenta la gran ventaja de que extender la red por el Campus se limita a situar en lugares estratégicos lo que se conoce como Puntos de Acceso, que son los dispositivos autónomos que, vía radio, van a interconectar los distintos dispositivos móviles que se unan a la red, así mismo, las diferentes ampliaciones necesarias se limitan a situar más puntos de acceso en las zonas que por sus características necesiten de una cobertura especial, ya sea por el número de clientes a conectar, por la dificultad del acceso (distancia) o por otras necesidades específicas.

V.10.3 .1 Arquitectura de Sistemas.

Los componentes que se utilizarán para implantar esta red son:

- Tarjetas inalámbricas del tipo PCMCIA, USB y PCI.
- Punto de acceso.
- Antenas omnidireccionales de alta ganancia.

El punto de acceso que se propone es un equipo *LINKSYS*™, Modelo WRT54G el cual se ilustra en el Anexo 2. Se optó por este equipo por su bajo costo y por su confiabilidad, así como por la fácil operación, configuración y mantenimiento.

Además del equipo (el cual consiste en un Ruteador Access Point), también se agregó un par de antenas que servirán para reforzar la señal del equipo de WI-FI.

Por la parte de clientes, se tendrán equipos portátiles: Dell®, Sony® y un PDA Sony®.

V.10.3.2.- Paquetes y Programas.

En clientes el sistema operativo es Windows XP®, Windows 2000® y Windows Milenium® de Microsoft™. En Punto de Acceso se maneja en el software de instalación y administración propio de Linksys™.

V.10.3.3.- Usuarios Permitidos a la Red del L-3.

Cualquier perfil de usuario es válido para acceder a la red inalámbrica (WLAN). Sólo hay que disponer de una tarjeta de red inalámbrica apropiada y estar ubicado en una zona de cobertura. Desde el punto de vista del usuario final, la configuración necesaria para acceder a esta red es similar a la configuración necesaria para conectarse a una red de cable convencional, con la ventaja de que sólo es necesaria una configuración inicial para conectarse (independientemente de su ubicación física) dentro del área de cobertura. No se requieren configuraciones especiales para realizar el acceso ya que éste es transparente al usuario.

Cada usuario contará con una contraseña, así como una autorización previa por parte del administrador de la red (tal vez sea necesario una autorización determinada por una autoridad especial).

La seguridad en la red se hará por medio del Protocolo WEP encriptado a 64 bits, si es necesario se aumentará a 128 bits.

La autentificación de cada equipo inalámbrico, se verificará por medio el direccionamiento MAC (*"Massive Access Control"*), la cual es única por cada tarjeta de red y solo será dada de alta si se obtiene el permiso adecuado.

V.10.4.- Puntos Importantes antes de Implantar la Red.

V.10.4.1.- Definir Áreas.

Este punto es importante ya que aquí se considera el alcance y las áreas que podrían ser beneficiadas por este proyecto. Las áreas involucradas y beneficiadas son:

Todas las secciones del Laboratorio L-3 (Eléctrica y Electrónica) que incluye:

- Laboratorio de Electricidad y Magnetismo.
- Laboratorio de Potencia.
- Laboratorio de Electrónica.
- Laboratorio de Medición e Instrumentación.
- Laboratorio de Control.
- Laboratorio de Comunicaciones.

V.10.4.2.- Definir Usuarios.

La definición de usuarios es un punto que puede causar polémica ya que en un momento dado, se podría estar en desacuerdo en la asignación; sin embargo, recuérdese que es una lista de usuarios sugerida, y que puede ser modificada si no se está de acuerdo por diversos motivos. Los usuarios que se considera podrían ser aceptados sin ningún problema son:

- El Jefe del Laboratorio.
- Profesores de Asignatura que tiene asignadas labores en el laboratorio.
- Profesores de Carrera que tiene asignadas labores en el laboratorio.
- Instructores del Laboratorio que impartan laboratorios.
- Prestadores de Servicio Social asignado a los diferentes laboratorios.
- Ayudantes de Profesor de los diferentes laboratorios.
- Técnicos Académicos de todos los laboratorios.
- Algunos alumnos destacados que por su desempeño académico, demuestren que accederán a la red para investigar sus tareas, trabajos y proyectos. (Es necesario en este caso, que el alumno cuente con su propio equipo: por ejemplo, un Ordenador Portátil, un Asistente Digital Personal (PDA), etcétera).

V.10.4.3.- Definir Servicios.

Aquí se proponen algunos de los servicios que pueden ser activados desde el equipo en el cual se van a conectar todos los usuarios, estos servicios se pueden definir y bloquear a disposición del Administrador; además, se pueden definir por horario y por bloques de IP, por jerarquía, etcétera.

Los servicios que son considerados necesarios implican desde revisar un correo electrónico personal con un cliente WEB, revisar horarios, verificar las prácticas en línea, realizar inscripciones, verificar manuales en línea, buscar información que se publique en general en Internet, así como verificar alguna información de carácter educativo.

Lo ideal sería que cada persona cuente con un acceso controlado por tiempo el cual se puede configurar en el equipo *Linksys*™. Los servicios que serían necesarios son los siguientes:

- Correo Electrónico.
- FTP.
- Navegador WEB.
- Telnet.

V.10.4.4.- Área de Cobertura.

La cobertura estará limitada al área del Laboratorio, debido a que por las restricciones del equipo, sólo puede abarcar unos 100 metros en el interior del mismo (con equipo adicional se puede aumentar la cobertura), pero por cuestiones de infraestructura esta cobertura estará limitada. El equipo de radio estará puesto en el primer piso del Laboratorio, ya que por su zona estratégica dará cobertura a la mayoría de las áreas del Laboratorio. El lugar que se propone es el cubículo donde actualmente se encuentra el Concentrador (HUB) de la Red Local del Laboratorio L-3. (Se denomina Cubículo del Servidor).

V.10.4.5.- Implantar Tácticas de Seguridad.

El programa de instalación del equipo cuenta además con una utilería que permite reconfigurar el equipo y permite verificar el estatus del mismo; así como, definir los servicios, tiempo de acceso, y verificación de intrusos en la red, los cuales pueden desconectarse en cualquier momento, además esta utilería puede configurar la contraseña para que no pueda ser modificada esta información. Es casi imposible que alguien acceda a la Red y que no pueda ser detectado.

V.10.5.- Preguntas y Respuestas de esta Tecnología.

¿Qué costo de implantación tiene una red de estas características?

Implementar una red de estas características tiene un costo inferior o tal vez igual que implementar una red cableada en un edificio, pero presenta la gran ventaja de que si hay que cambiar la disposición de los distintos elementos se puede hacer de una manera sencilla, sin ningún costo adicional. Además, en muchos casos, será más sencillo y barato utilizar una red sin cables al no tener que poner físicamente el cable por zonas de difícil acceso, y si se trata de interconectar edificios, este tipo de red resulta mucho más rentable económicamente al no requerir de obra civil para realizar la interconexión de ellos.

A nivel metropolitano, presenta un número elevado de ventajas, ya que no es necesario realizar obras en las áreas para interconectar los edificios, se permite, por otro lado el acceso a la red desde cualquier punto del área de cobertura, sin la necesidad de tener un cable que conecte a la red, todo ello con una velocidad de hasta 54 Mbps.

¿Qué costo de mantenimiento presenta este tipo de red?

Una vez instalada la red, el mantenimiento que presenta es menor al de instalaciones de cable, ya que tiene la ventaja de que al no utilizar elementos mecánicos, se evitan los posibles problemas que puedan surgir del deterioro sufrido por cables, como pueden ser roturas accidentales.

¿Por qué se debe apoyar este tipo de redes?

Las sociedades mejor comunicadas en la actualidad, son las que mayores oportunidades de crecimiento tienen; en realidad, estas redes son en la actualidad la infraestructura que permite un mayor desarrollo de la sociedad, al igual que los transportes lo fueron en los momentos de mayor desarrollo industrial. El uso de las comunicaciones inalámbricas puede mejorar la calidad de vida, la facilidad de acceso a la información para autoformarse, la facilidad de comunicación para desarrollar nuevas actividades o mejorar las existentes y muchas cosas más de la vida cotidiana.

Es por esto que el principal objetivo de la red inalámbrica en un Campus *"Aragón"*, es ofrecer un acceso libre a servicios de la propia red. Con esto se consigue que se expanda todavía más el uso de las nuevas tecnologías y que la Institución tenga un mayor avance tecnológico en la comunidad estudiantil.

BIBLIOGRAFÍA.

Inteligencia, B. (2003). **Wi-Fi: El Estándar Inalámbrico.** En línea o [URL]. http://www.baquia.com.es/Wi-Fi/ el estándar inalámbrico/htm

LAN/MAN Standards Committee of the IEEE Society (1999). **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard 802.11.**

Dawson, E. and Nielsen, L. (1996). **Automated Cryptanalysis of XOR Plaintext Strings.** *Cryptologia*, (2): 165-181, April, 1996.

Singh, S. (1999). **The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography.** New York: Doubleday Editors.

Tutte, W. T. and Fish, I. (1998). **A Transcript of Tutte's**. June 19. 1998 Lecture al the University of Waterloo.

Schneier, B. and Mudge, W. (1998). **Cryptoanalysis of Microsoft's Point-toPoint Tunneling Protocol (PPTP).** *In 5TH ACM Conference on Computer and Communicatios Security*, pages 132-140. San Francisco California, Novembre 1998. ACM Press.

Wagner, D. and Schneier, B. (1996). **Analysis of the SSL 3.0 Protocol.** *In Procedings of the 2nd USENIX Workshop on Electronic Commerce (EC-96).* pages 29-40, Berkeley, November 18-21, 1996, USENIX Association.

Krawczyk, H., Bellare, M. and Canetti, R. (1997). **HMAC:Keyed-Hashing for Message Authentication.** February 1997. Status: INFORMATIONAL

Braden, B., Borman, D. and Partridge, C. (1988). **Computing the Internet Checksum.** *Internet Request for Comments RFC 1071, Internet Engineering Task Force*, September 1988.

Mallory, T. and Kullberg, A. (1990). **Incremental Updating of the Internet Checksum.** *Internet Request for Comments RFC 1141, Internet Engineering Task Force*, January 1990.

Kocher, P. (1995). **Cryptoanalysis of Diffie-Hellman, RSA, DSS and other Cryptosystems using Timming Attacks.** *In Don Coppersmith, editor, Advances in Cryptology, CRYPTO'95: 15TH Annual International Cryptology Conference, Santa Barbara, California, USA*, August 27-31, 1995: *Proceedings*, pages 171-183. Springer-Verlag, 1995.

Kent, S. and Randall A. (1998). **Security Architecture for the Internet Protocol.** *Internet Request for Comment RFC 2401, Internet Engineering Task Force*, November 1998.

Bellovin, S. (1996). **Problem Areas for the IP Security Protocols.** *In 6TH USENIX Security Symposium*, San Jose, California, July 1996. USENIX.

Stugglebine S. G. and Gligor, V. D. (1992). **On Message Integrity in Cryptographic Protocols.** *In Proc. IEEE Symposium on Research in Security and Privacy*, pages 85-105, 1992.

Carballar, José A. (2004). **Wi-Fi. Cómo Construir una Red Inalámbrica.** México: Alfaomega, serie Ra-Ma.

Rey, E. (2002). **Comunicaciones Móviles.** Madrid: Marcombó.

Hernández Rábanos, J. (1998). **Comunicaciones Móviles de Tercera Generación.** Madrid Paraninfo.

Stallings, W. (2002). **Wireless Communications and Networks.** New York: Prentice-Hall.

ANEXO 1.

GLOSARIO DE TÉRMINOS PARA REDES INALÁMBRICAS.

10BASET.- Es el estándar de la red Ethernet que permite velocidades de transmisión de 10 Mbps. 10BaseT se basa en la Norma IEEE 802.3.

100baseT.- Es el Estándar de la red Ethernet que permite velocidades de transmisión de 100 Mbps. Este estándar es también compatible con el estándar anterior 10BaseT. 100BaseT se basa en la Norma IEEE 802.11u y se le conoce comúnmente como *Fast Ethernet* o Ethernet Rápido.

802.11.- Conjunto de estándares de red de área local inalámbrica definidos por el IEEE (*Institute of Electrical and Electronics Engeneers*, "Instituto de Ingenieros Eléctricos y Electrónicos"). Entre estos estándares se encuentra 802.11b, que es en el que se basa Wi-Fi.

ACCESO TELEFÓNICO.- Establece una comunicación via módem utilizando una línea telefónica básica. También se le conoce por el término inglés "*Dial-Up*".

ACTIVE X.- Tecnología desarrollada por Microsoft® para incluir aplicaciones en las páginas HTML.

ADMINISTRADOR.- Persona responsable del mantenimiento y/o gestión de una red corporativa, red de área local (cableada o inalámbrica) o de un servidor de red.

ADLS (*Asymmetric Digital Subscriber Line*, "Línea de Abonado Digital Asimétrica").- Tecnología pensada para poder transmitir datos a alta velocidad a través del bucle de abonado de la linea telefónica. El bucle de abonado es el cable de cobre que va desde la casa del usuario hasta la central telefónica.

ANCHO DE BANDA.- Es la cantidad de datos que puede circular en un medio por unidad de tiempo. Generalmente, se mide en bits por segundos. También puede hacer referencia a un rango de frecuencias.

API (*Applicaction Program Interface*, "Interfase entre Programas").- Interfase que permite la comunicación entre programas, redes y bases de datos.

ARP (*Address Resolution Protocol*, "Protocolo de Resolución de Direcciones").- Se trata de un Protocolo usado para averiguar la dirección del enlace correspondiente

ASCII (*American Standard Code for Information Exchange*, "Código Normalizado Americano para el Intercambio de Información").- Se trata de un código que le asigna a cada letra, número o signo empleado por los ordenadores, una determinada combinación de ceros y unos. Este es el código más ampliamente utilizado por todos los ordenadores a escala internacional.

ASP (*Active Server Pages*, "Páginas de Servidor Activo").- Lenguaje de Programación creado por Microsoft® para permitir aumentar la interactividad en las páginas *web*.

ATM (*Asynchronous Transfer Mode*, "Modo de Transmisión Asíncrono").- Es una tecnología de transmisión de Datos a alta velocidad, la cual posee la característica de poder transmitir diferentes tipos de información, incluyendo: voz, datos, fax, vídeo, audio e imágenes.

AUP (*Acceptable Use Policy*, "Política de Uso Aceptable").- Se refiere a las normas que deben cumplir todos los usuarios que hacen uso de la red.

BANDA ANCHA.- Hace referencia a las comunicaciones que transmiten datos a alta velocidad. Éste es un término relativo; sin embargo, se suele considerar banda ancha a cualquier comunicación con velocidad superior a 64 Kbps.

BANDA DE FRECUENCIAS.- Es un rango de frecuencias del espectro radioeléctrico. Éste, está dividido en bandas de frecuencias que regulatoriamente son utilizadas para distintas finalidades.

BLUETOOTH®.- Es una tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de 10 metros). Al contrario que otras tecnologías como Wi-Fi, la tecnología *"Bluetooth"* no está pensada para soportar redes de ordenadores, sino más bien, para comunicar un ordenador o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, un PDA con su ordenador, un ordenador con su impresora, etcétera.

BSS (*Basic Service Set*, "Conjunto de Servicios Básicos").- Es una de las modalidades de comunicación en las que se puede configurar las terminales de una red Wi-Fi. En este caso, la red inalámbrica dispone de un equipo (punto de acceso) que se encarga de gestionar las comunicaciones (internas y externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como "Modo Infraestructura".

CANAL.- La banda de frecuencia en la que trabaja una red inalámbrica, se divide en canales. Por cada canal se puede establecer una comunicación.

CCK (*Complementary Code Keying*, "Salto de Código Complementario").- Es una técnica de modulación utilizada en Wi-Fi junto con las técnicas de espectro distribuido.

CGI (*Common Gateway Interface*, "Interfase de Pasarela Común").- Es un estándar que describe cómo un navegador *web* intercambia información con un servidor *web*. Esto le permite al servidor leer información introducida por el usuario en una página *web*, procesarla y mostrarle los resultados posteriormente.

CLIENTE.- Es un programa que trabaja en el ordenador local para poder hacer uso de algún servicio del ordenador remoto. El programa del ordenador remoto que permite ese uso recibe el nombre de "Servidor". También puede hacer referencia al propio ordenador o dispositivo local que depende del ordenador o dispositivo remoto (llamado "Servidor"). En las redes Wi-Fi, cliente puede hacer referencia a los dispositivos (ordenadores, PDA, etcétera) conectados a la red a través de un Punto de Acceso.

CLIENTE/SERVIDOR.- Es un sistema mediante el cual las aplicaciones quedan divididas en dos partes: la parte residente en el ordenador del usuario, el cliente, y la parte residente en un ordenador central compartido, el servidor. El cliente se encarga de hacer de interfase con el usuario. El servidor se encarga de gestionar la compartición de las aplicaciones, información y periféricos entre los distintos clientes. El Sistema Cliente/Servidor es utilizado tanto en las redes de área local como en servicios en línea *(on-line)*.

CORTAFUEGOS O FIREWALLS.- Es un dispositivo de seguridad (Arquitectura de Sistemas o Programa), que controla los accesos a una red local desde el exterior (típicamente, Internet).

CRC (*Cyclic Redundancy Check*, "Comprobación Cíclica de Redundancia").- Son unos datos adicionales que se adjuntan al final de la información para poder comprobar fácilmente que no ha habido errores en la transmisión. Los datos CRC son el resultado de hacer determinadas operaciones matemáticas con la información original. Como las operaciones son las mismas en origen y en destino, si el resultado no es el mismo, es que hay un error en la transmisión.

CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*, "Acceso Múltiple por detección de Portadora con Evidencia de Colisión").- Es el sistema que emplea Wi-Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos puedan intentar hacer uso del medio simultáneamente (evita la colisión).

DHCP (*Dynamic Host Configuration Protocol*, "Protocolo de Configuración Dinámica del *"Host"*).- Es un protocolo que permite que un servidor asigne dinámicamente las direcciones IP a los ordenadores "clientes", conforme éstos las van necesitando. La mayoría de los ruteadores (incluso los incluidos en los puntos de acceso) incluyen la función de servidor DHCP.

DIRECCIÓN MAC.- Es un número único que asignan los fabricantes a los dispositivos de red (adaptadores de red y puntos de acceso). Este número es permanente y viene grabado en el propio dispositivo, para permitir identificarlo de forma inequívoca. Las direcciones MAC están formadas por 12 caracteres alfanuméricos (por ejemplo; 12-AB-56-78-90-FE).

DSL (*Digital Subscriber Line*, "Línea Digital de Abonado").- Es el término genérico que hace referencia a la familia de tecnologías que utilizan la línea telefónica para transmitir datos a alta velocidad. ADSL, SDSL o HDLS son algunas de estas tecnologías. También se utiliza el término xDSL, para hacer referencia a esta familia de tecnologías.

DSSS (*Direct Sequence Spread Spectrum*, "Espectro Expandido por Secuencia Directa").- Es la técnica de modulación utilizada por los sistemas IEEE 802.11b (Wi-Fi) para transmitir datos a alta velocidad (11 Mbps).

ESTACIÓN BASE.- Es el nombre general que reciben los equipos de una red inalámbrica que se encargan de gestionar (administrar) las comunicaciones de los dispositivos que forman la red.

ETSI (*European Telecommunications Standards Institute*, "Instituto Europeo de Normas de Telecomunicaciones").- Creado en Marzo de 1989 y con sede cerca de Nice, Francia.

ESPECTRO EXPANDIDO.- Es un sistema de difusión de las señales radioeléctricas. Este sistema utiliza un ancho de banda mayor al estrictamente necesario a cambio de conseguir reducir la vulnerabilidad a las interferencias y garantizar la coexistencia con otras transmisiones.

ESS (*Extended Service Set*, "Conjunto de Servicios Extendido").- Es una de las modalidades en las que se puede configurar una red local inalámbrica Wi-Fi. Reciben este nombre las redes inalámbricas que están formadas por más de un punto de acceso.

FHSS (*Frequency Hopping Spread Spectrum*, "Espectro Expandido por Salto de Frecuencia").- Es una técnica de modulación utilizada tanto por los sistemas IEEE 802.11 como por *Bluetooth*®. Transmite datos abaja velocidad (1 Mbps) por lo que en la versión 802.11b se sustituyó por el sistema DSSS para poder transmitir datos a alta velocidad (11 Mbps).

GATEWAY.- Es una Pasarela. Es un sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí. La Pasarela adapta el formato de los datos de una aplicación a otra o de una red a otra. Se utiliza generalmente, para interconectar dos redes distintas o para hacer que una aplicación entienda los datos generados por otra aplicación distinta

HOMEPNA (*Home Phoneline Networking Alliance*, "Alianza de Red Doméstica sobre Líneas Telefónicas").- Es el nombre que recibe el grupo que creó las especificaciones que permiten crear una red local de datos utilizando la infraestructura telefónica del hogar. La red de datos utiliza los mismos cables telefónicos que los teléfonos, fax o los módems DSL.

HOMERF (*Home Radio Frecuency*, "Radio Frecuencia del Hogar").- Es una tecnología de red de área local inalámbrica que en su día fue promovida por Intel. Existen tres versiones en el mercado que alcanzan los 1.6, 10 y 40 Mbp, respectivamente. En cualquier caso, Homero ha quedado hoy en día en el olvido debido al auge de Wi.Fi.

IBSS (*Independent Basic Service Set*, "Conjunto de Servicios Básicos Independientes").- Es una de las modalidades de comunicación en las que se pueden configurar las terminales de una red Wi-Fi. En este caso, la red inalámbrica no dispone de punto de acceso, llevándose a cabo las comunicaciones de forma directa entre las distintas terminales que forman la red. Este modo de conexión también es conocido como *ad hoc*, modo independiente o de igual a igual.

ISM (*Industrial Scientific and Medecine*, "Industrial, Científica y Médica").- Estas siglas hacen referencia a la banda de frecuencias radioeléctricas reservadas a aplicaciones de este tipo. Ésta es la banda de frecuencias en las que actúa Wi-Fi.

MAC (*Medium Access Control*, "Control de Acceso al Medio").- Es un conjunto de protocolos de las redes inalámbricas que controla cómo los distintos dispositivos se comparten el uso del espectro radioeléctrico.

MODO AD HOC.- Se refiere a las redes inalámbricas Wi-Fi que disponen de un equipo central, conocido como Punto de Acceso, que se encarga de gestionar las comunicaciones (internas y Externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como Modo BSS.

OFDM (*Orthogonal Frecuency Division Multiplexing*, "Multiplexado Ortogonal por División de Frecuencia").- Es una técnica de modulación utilizada por las redes de área local inalámbrica de alta velocidad (IEEE 802.11a e HiperLAN2). Permite transmitir datos de hasta 54 Mbps.

PUNTO DE ACCESO.- Es el equipo de la red inalámbrica que se encarga de gestionar las comunicaciones de todos los dispositivos que forman la red. El punto de acceso no sólo se utiliza para controlar las comunicaciones internas de la red, sino que también hace de puente en las comunicaciones con las redes externas (redes cableadas o Internet).

ROAMING.- Se conoce por este nombre a la posibilidad que tienen los equipos inalámbricos de desplazarse dentro del área de cobertura de una red inalámbrica sin perder la conexión.

RUTEADOR (*Router*).- Es un sistema utilizado para transferir entre dos redes que utilizan un mismo Protocolo. Un Ruteador puede ser un dispositivo *software, hardware* o una combinación de ambos. Los puntos de acceso, generalmente, hacen las funciones de Ruteador. A este equipo también se le conoce como enrutador.

SSID (*Service Set Identifier*, "Identificador del Conjunto de Servicios").- Es el parámetro que identifica la red inalámbrica. También se le conoce como nombre de red.

VPN (*Virtual Private Network*, "Red Privada Virtual").- Hace referencia a las soluciones que permite crear redes completamente privadas, en cuanto a seguridad y confidencialidad utilizando para ello infraestructuras no seguras (como Internet o redes inalámbricas).

WECA (*Wireless Ethernet Compatibility Alliance*, "Alianza de Compatibilidad Ethernet Inalámbrica").- Es una asociación de fabricantes de equipos de red creada en 1999 con el objetivo de fomentar la tecnología inalámbrica, y asegurarse la compatibilidad de equipos. WECA es la creadora de la marca Wi-Fi y, es quien se encarga de certificar los equipos de esta marca.

WEP (*Wireless Equivalency Protocol*, "Protocolo de Equivalencia con Red Cableada").- Es el sistema cifrado de datos que incorporan las redes Wi-Fi. El sistema WEP surgió con la idea de ofrecerle a las redes inalámbricas un estado de seguridad similar al que tienen las redes cableadas.

WI-FI (*Wireless Fidelity*, "Fidelidad Inalámbrica").- Es una marca creada por la Asociación WECA con el objetivo de fomentar la tecnología inalámbrica y asegurarse la compatibilidad de equipos. Todos los equipos con la Marca WI-Fi, son compatibles entre sí, y utilizan la tecnología inalámbrica definida por IEEE en su Norma (Estándar) 802.11b.

WLAN (*Wireless Local Area Network*, "Red de Área Local Inalámbrica").- Es el acrónimo con el que se hace referencia a las redes de área local inalámbricas. Las redes Wi-Fi son un ejemplo de este tipo de redes.

WPA (*Wi-Fi Protected Access*, "Acceso Wi-Fi Protegido").- Son unas especificaciones de seguridad basadas en la Norma IEEE 802.11i que incrementa fuertemente el nivel de protección de datos y de control de acceso a las redes Wi-Fi. Las facilidades de seguridad ofrecidas por WPA pueden implantarse en las redes Wi-Fi existentes mediante una instalación de programa(s) y paquete(s).

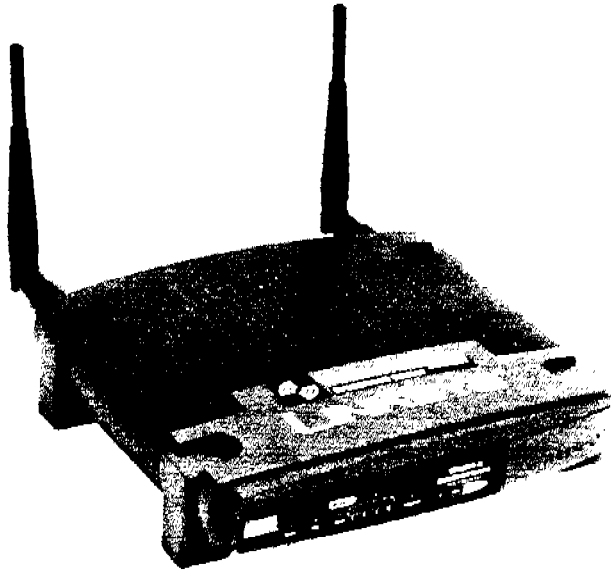
ANEXO 2.

PLANOS DE DESCRIPCIÓN DEL PROYECTO DE RED INALÁMBRICA PARA EL LABORATORIO DE COMUNICACIONES (L-3), DE LA ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES "ARAGÓN", DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

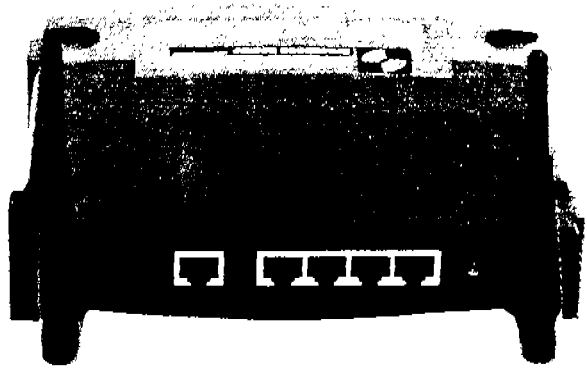
Los componentes utilizados en este proyecto se describen en éste anexo. Primero se mostraran las especificaciones de los productos utilizados y posteriormente los planos e imágenes de la cobertura de la red.

Componentes de la Red

El Punto de Acceso es un equipo Linksys el cual se ilustra abajo y se dan mas detalles del mismo.



Vista Frontal del Wireless-G Broadband Router WRT54G



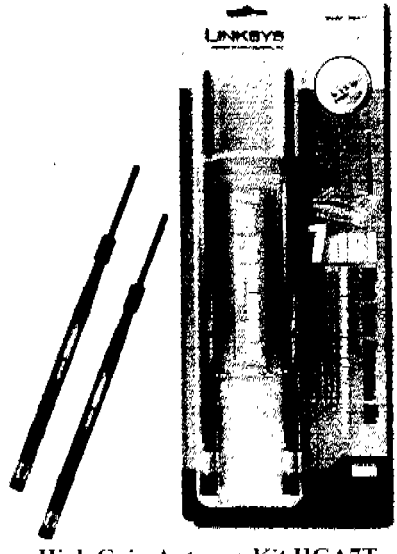
Vista Posterior del Wireless-G Broadband Router WRT54G

Detailed Specifications

Model	**WRT54G**
Key Features	**- Compatibility with Draft 802.11g and 802.11b (2.4GHz) Standards - Setup Wizard for Easy Installation - Access Your Corporate Network Remotely through Virtual Private Networking (VPN)?Supports IPSec and PPTP Pass- Through - Supports Dynamic Domain Name System (DDNS) Service, Static and Dynamic Routing (RIP1 and 2), DMZ Hosting - Web-based Utility for Easy Configuration from Any Web Browser - DHCP Server Capability to Assign IP Addresses Automatically - All Ethernet Ports Support Auto-Crossover (MDI/MDI-X)?No Need for Crossover Cables**
Standards	**IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g**
Network Protocols	**TCP/IP, IPX/SPX, NetBEUI**
Device Management	**Web-Based**
Security	**- Enhanced Internet Security Management Functions: Internet Access Policies with Time Schedules, Website Blocking, IP and MAC Address Filtering; Port Filtering; Wireless MAC Address Filtering; Stateful Packet Inspection (SPI) Firewall; and NAT Technology - Wireless Security with up to 128-bit WEP Encryption**
Ports	**Internet: One 10/100 RJ-45 Port for Cable/DSL Modem LAN: Four 10/100 RJ-45 Switched Ports One Power Port**
LEDs	**Power, DMZ, Diag**

	WLAN: Act, Link LAN: Link/Act, Full/Col, 100 Internet: Link/Act, Full/Col, 100
Data rate	Up to 54Mbps (Wireless), 10/100Mbps (Ethernet)
Wireless Operating Range	Not specified
Modulation Technology	CCK, DQPSK, DBPSK, OFDM
Frequency Band	2.4GHz
Antenna	15 dBm
VPN Support	IPSec and PPTP Pass- Through
Humidity	10% to 85%, Non-Condensing
Operating Temperature	32°F to 104°F (0°C to 40°C)
Weight	17 oz. (0.482 kg)
Dimensions	7.32" x 6.89" x 1.89" (186 mm x 175 mm x 48 mm)

Las especificaciones de las antenas se muestran a continuación:



High Gain Antenna Kit HGA7T

Detailed Specifications	
Manufacturer Part Number	HGA7T
Product Name	HGA7T Omni-directional Antenna
Marketing Information	Increase the range of your Wireless network! Attach these high gain antennas to your Linksys Wireless Broadband Router or Access Point, and increase both the effective strength of the outgoing signals, and the receive sensitivity for incoming signals
Manufacturer Website Address	www.linksys.com
Technical Information	
Antenna Type	Omni-directional
Antenna Frequency	2.4 to 2.5GHz
Gain	7 dBi
Impedance	50 ohm Nominal
Polarization	Linear Vertical
Connectors	RP-TNC
VSWR	1.92 Maximum
Miscellaneous	
Additional Information	Works with both Wireless-G and Wireless-B devices
Package Contents	Two High Gain Antenna for TNC Connectors One Antenna Stabilizer
Compatibility	WRT54GS WRT54G WAP54G BEFW11S4 WAP11 AS2TNC (Antenna Stand)
Environmental Conditions	
Temperature	-20 to 65°C (-4 to 149°F) Operating -30 to 75°C (-22 to 167°F) Storage
Humidity	0 to 85% Non-condensing Operating
Physical Characteristics	
Dimensions	11.22" Height x 0.55" Width
Weight	1.48 oz – Unit Weight
Warranty & Support	
Standard Warranty	3 Year(s) Limited

Esquema de la Red.

El lugar en donde se implantará este servicio es un edificio de sólo 3 Niveles, los cuales se ilustran adelante.

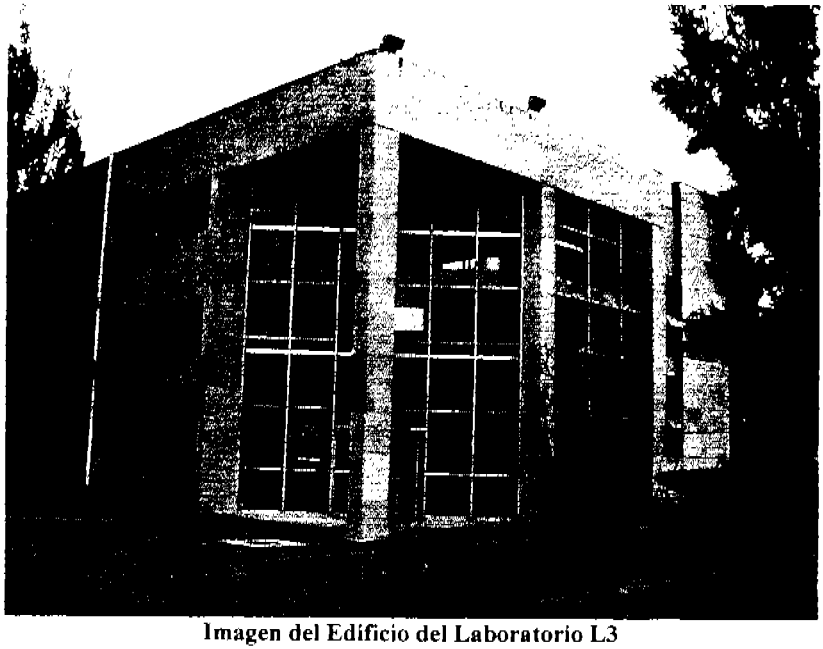


Imagen del Edificio del Laboratorio L3

Planta Baja

Laboratorio de Potencia

Laboratorio de Electricidad y Magnetismo

1er Piso

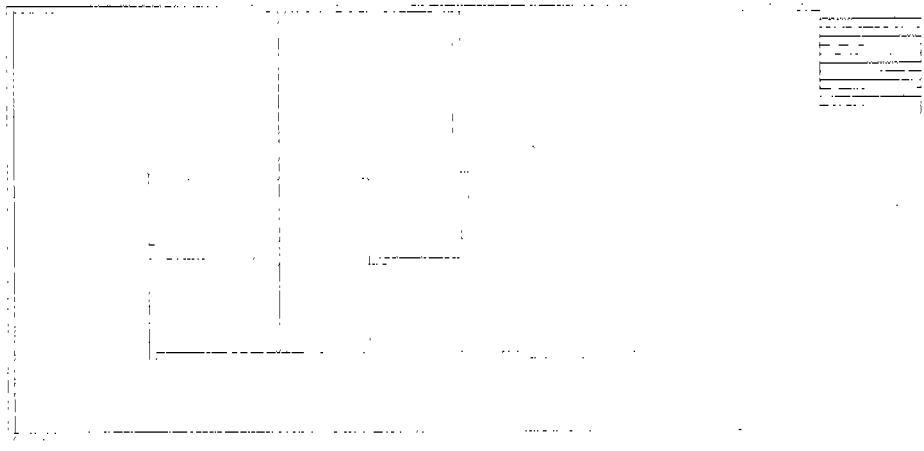
Laboratorio de
Medición

Laboratorio de
Electrónica

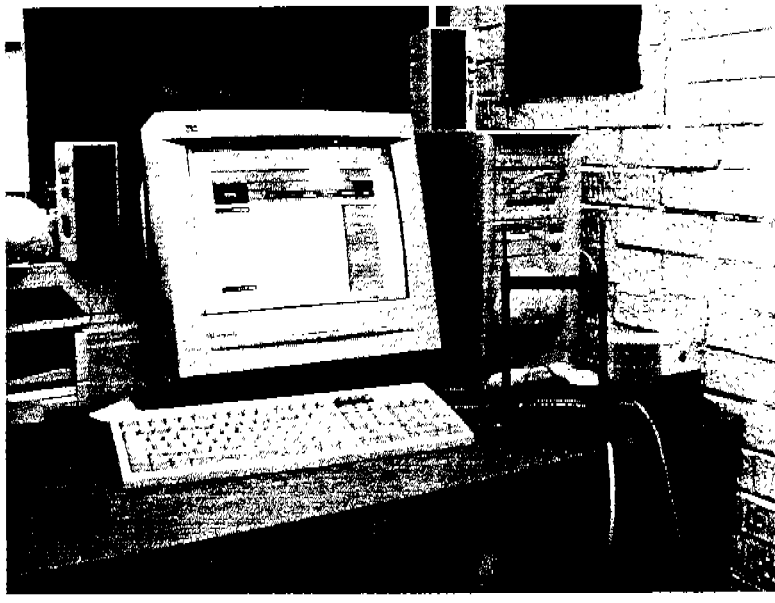
Laboratorio de
Comunicaciones

Laboratorio de
Control

2do Piso



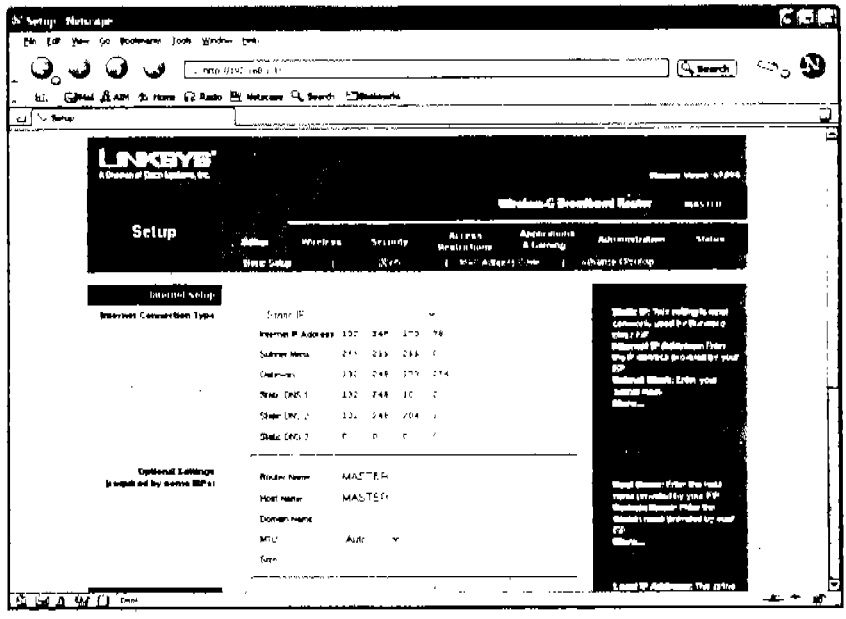
El equipo Central estará ubicado en un cubículo del edificio L3.



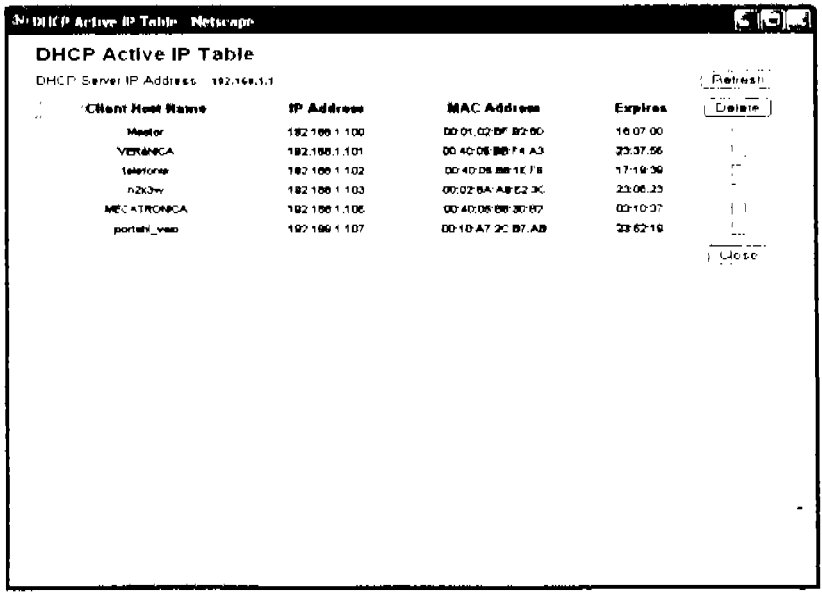
A continuación se muestran las ventanas del programa de administración del Punto de Acceso Linksys.

La configuración del Punto de Acceso es mediante una IP Estática, los parámetros mas importantes son los siguientes:

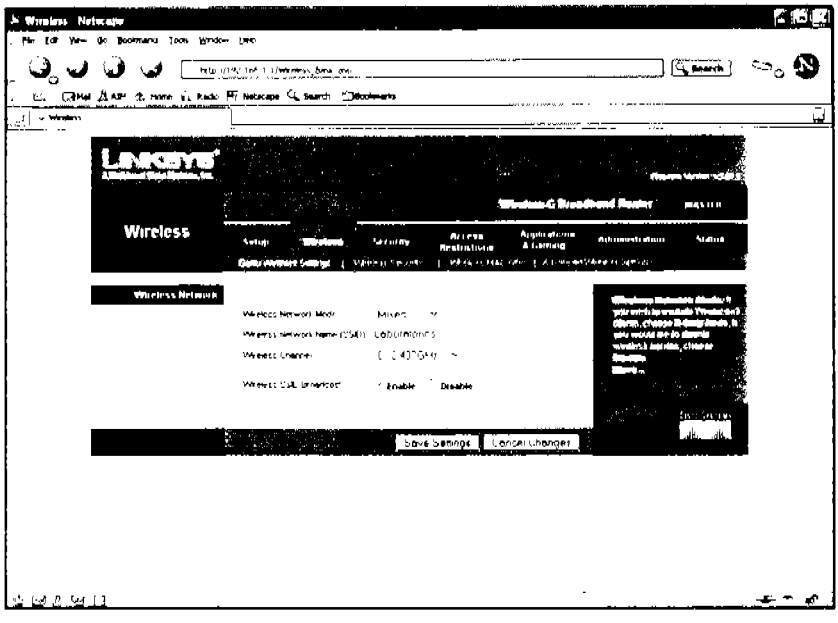
IP 132.248.173.78
Subnet Mask: 255.255.255.0
Gateway: 132.248.173.254
DNS1: 132.248.10.2
DNS2: 132.248.204.1
Wireless Network Name (SSID): Laboratorios
Wireless Chanel: 6
Security Mode: WEP



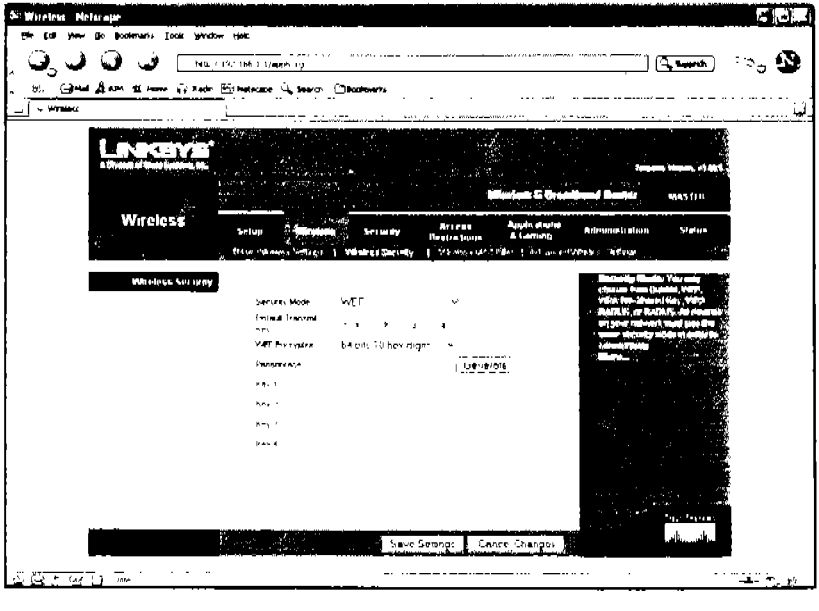
Ventana de Configuración Principal



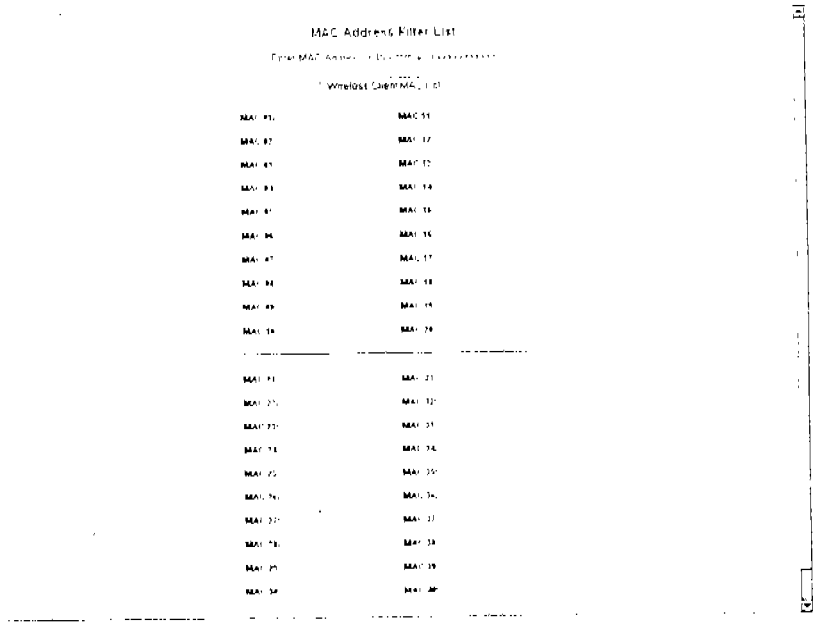
Lista de Clientes Aceptados



Configuración de Red Inalámbrica



Configuración de la Seguridad de la Red Inalámbrica



Lista de Clientes que se autorizan Mediante su MAC

ÍNDICE.

Justificación 1
Objetivo General 6
Objetivos Particulares 6
Introducción 7
Resumen 11

CAPÍTULO I.- CONCEPTOS Y GENERALIDADES DE LAS REDES INALÁMBRICAS 12

I.1.- Introducción 12
I.2.- Antecedentes en Redes Inalámbricas 13
I.3.- Redes Inalámbricas Locales 16
I.3.1.- Definición 16
I.3.2.- Componentes Esenciales de una WLAN 18
I.3.3.- Tipos de Redes WLAN 18
I.4.- Topologías de una Red Inalámbrica Local 19
I.4.1.- Topología de Infraestructura 20
I.4.2.- Topología *Ad-Hoc* 22
I.5.- Situación Actual de las Redes Inalámbricas 23
I.6.- Retos de las Redes Inalámbricas de Área Local 26
I.6.1.- Facilidad de Uso 27
I.6.2.- Seguridad 28
I.6.3.- Movilidad 30
I.6.4.- Administración de la Red 32

CAPÍTULO II.- LAS ESPECIFICACIONES PARA EL PROTOCOLO 802.11x 34

II.1.- Introducción 34
II.2.- Estándares de Redes de Área Local Inalámbrica 35
II.2.1.- Redes IEEE 802.11 35
II.2.2.- Redes Bluetooth... 36
II.2.3.- Otros Estándares WLAN 37
II.3.- El Estándar de Facto: IEEE 802.11 38
II.3.1.- Características del Estándar 802.11b 39
II.3.2.- Características del Estándar 802.11a 40
II.3.3.- Características del Estándar 802.11g 42
II.3.4.- Otras Especificaciones IEEE 43
II.3.5.- ¿Qué Estándar es la mejor Opción? 44
II.4.- Las Capas OSI en el Estándar IEEE 802 45
II.4.1.- La Capa Física 46

II.4.1.1.- FHSS 47
II.4.1.2.- DSSS 48
II.4.1.3.- OFDM 48
II.4.2.- La Capa MAC en IEEE 802 50
II.5.- Mecanismos de Seguridad usados en IEEE 802.11 51
II.6.- Extendiendo la WLAN: Intercomunicación entre Puntos de Acceso 52
II.7.- Más allá del Uso en Redes Empresariales 53
II.7.1.- El Uso más conocido de una WLAN: El Hot Spot 58
II.8.- Entorno Regulatorio 61
II.9.- Organizaciones de Certificaciones 63

CAPÍTULO III.- LA SEGURIDAD EN LAS REDES INALÁMBRICAS BASADAS EN EL PROTOCOLO 802.11x 65

III.1.- Introducción 65
III.2.- Generalidades de Seguridad Informática 66
III.3.- Mecanismos de Seguridad en el 802.11 68
III.3.1.- Autenticación 69
III.3.2.- Cifrado 72
III.4.- WEP: La Primera Norma de Seguridad en el Estándar 802.11 74
III.5.- Mejorando WEP con la Norma 802.1x 76
III.6.- El Estándar 802.11i 80
III.7.- Solución al Problema de Cifrado: el Estándar WAP 83
III.8.- Tipos de Ataques en WLAN 85
III.9.- Asegurando una WLAN 86
III.9.1.- Firewalls 87
III.9.2.- La Alternativa VPN 87

CAPÍTULO IV.- PRODUCTOS Y EQUIPOS UTILIZADOS PARA CONFIGURAR UNA RED INALÁMBRICA BASADA EN EL PROTOCOLO 802.11x 91

IV.1.- Introducción 91
IV.2.- El Punto de Acceso 91
IV.2.1.- Características de los Puntos de Acceso 93
IV.2.1.1.- La Radio 93
IV.2.1.2.- Los Puertos 94
IV.2.1.3.- Gestión del Punto de Acceso 95
IV.3.- Adaptadores Inalámbricos de Red 96
IV.3.1.- Tipos de Adaptadores de Red 96
IV.3.1.1.- Adaptadores USB 97
IV.3.1.2.- Tarjetas PCMCIA 100
IV.3.1.3.- Adaptadores PCI e ISA 102
IV.3.1.4.- Adaptadores para PDA 104

IV.4.- Compatibilidad entre los Sistemas Operativo y los Componentes Wi-Fi 106

IV.5.- Puentes 106
IV.6.- Antenas 108
IV.7.- Otros Dispositivos Inalámbricos 110

CAPÍTULO V.- APLICACIÓN DE UNA RED INALÁMBRICA BASADA EN EL PROTOCOLO 802.11x EN EL LABORATORIO DE COMUNICACIONES (L-3), DE LA ENEP *"ARAGÓN"* DE LA UNAM 112

V.1.- Introducción 112
V.2.- Aplicaciones en la Empresa 113
V.3.- Comunidades Inalámbricas 114
V.3.1.- Organización de las Comunidades Inalámbricas 114
V.4.- Redes Comerciales de Acceso Público Inalámbrico 115
V.5.- Enlace Punto a Punto 116
V.6.- Televigilancia 117
V.7.- Wi-Fi en el Automóvil 118
V.8.- Telefonía Wi-Fi 119
V.8.1.- Recibir Llamadas en la Terminal Wi-Fi 120
V.8.2.- Teléfonos Wi-Fi 120
V.9.- El Hogar Digital 121
V.10.- Descripción del Proyecto de Red Inalámbrica para el Laboratorio de Comunicaciones (L-3), de la Escuela Nacional de Estudios Profesionales *"Aragón"*, de la Universidad Nacional Autónoma de México 122
V.10.1.- Propuesta del Proyecto 122
V.10.2.- Introducción al Proyecto de la Creación de una Red Inalámbrica 123
V.10.3.- Topología de la Red Inalámbrica en el Campus *"Aragón"* 125
V.10.3.1.- Arquitectura de Sistemas 125
V.10.3.2.- Paquetes y Programas 125
V.10.3.3.- Usuarios permitidos en la Red del L-3 126
V.10.4.- Puntos Importantes antes de Implantar la Red 126
V.10.4.1.- Definir Areas 126
V.10.4.2.- Definir Usuarios 127
V.10.4.1.- Definir Servicios 127
V.10.4.1.- Definir Area de Cobertura 128
V.10.4.1.- Implantar Tàcticas de Seguridad 128

V.10.5.- Preguntas y Respuestas de esta Tecnologìa 128

Conclusiones 130
Bibliografía 132

Anexo 1.- Glosario de Términos para Redes Inalámbricas 134
Anexo 2.- Planos de Descripción del Proyecto de Red Inalámbrica para el Laboratorio de Comunicaciones (L-3), de la Escuela Nacional de Estudios Profesionales *"Aragón"*, de la Universidad Nacional Autónoma de México 140
Índice 151