UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
"ARAGÓN"

"REDES INALÁMBRICAS WLAN; ASPECTOS BÁSICOS DEL IEEE 802.11b PARA LA COMUNICACIÓN DE DATOS ENTRE COMPUTADORAS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE :

INGENIERO MECÁNICO ELÉCTRICO

(ÁREA: ELÉCTRICA – ELECTRÓNICA)

P R E S E N T A :

LUIS CESAR ZENDEJAS GONZÁLEZ

ASESOR :
ING. ADRIAN PAREDES ROMERO

MÉXICO 2005

AGRADECIMIENTOS

Principalmente a DIOS por la oportunidad que me dio de estudiar, y por las constantes muestras de Amor y Seguridad; reafirmando su confianza en mí y los que me rodean.

A mis Padres Rossy y José Luís, por respaldar y solventar mis estudios.
Mamá: ... por tus cuidados y pendientes en estos años... Gracias
Papá: ... cuando sea grande quiero ser como tú.... Gracias

A mis hermanos, Dulce Roció; eres muy inteligente y la mejor hermana, échale ganas. ¡¡¡
A Erick: es un orgullo ser tu hermano ¡¡¡....

A ti Araceli por tus porras, ánimos y sacrificos compartidos, mi reconocimiento por tu esfuerzo y dedicación; felicidades Arquitecta .... Te Amo

A la UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO por la oportunidad de ser Universitario, desde el CCH Azcapo hasta la FES ARAGON.
A los Profesores de la carrera de IME, por los conocimientos y experiencias compartidas.

A los compañeros de IME: Arturo, por tu amistad, Luís Daniel, Alejandro, Isaac, Carlos y Clara por la amistad brindada, y a toda la generación (IME 2000 -2004)

A mi asesor el Ing. Adrián Paredes por su colaboración en este trabajo, y a mis sinodales por su dedicación:
M en I Ulises Mercado Valenzuela
Ing. José Luís García
Ing. Sergio Galicia Rangel
Ing. Esteban Arellano

Y a toda la familia y amigos, que confiaron y estuvieron pendientes de mi...GRACIAS

Luis Zesar

" Todo lo Puedo en Cristo que me Fortalece ..."
San. Pablo (Fil. 4:13)

INDICE

REDES INALAMBRICAS WLAN: ASPECTOS BASICOS DEL IEEE 802.11b PARA LA COMUNICACION DE DATOS ENTRE COMPUTADORAS

INTRODUCCION A LAS REDES WLAN

En la actualidad hablar de Tecnología Inalámbrica ya sea en artículos para el hogar, en la industria o aplicaciones experimentales, es muy cotidiano. Y es que hoy la palabra Wireless (sin cables) es muy escuchada. Pues cuando se consideran las múltiples ventajas y beneficios que proporciona esta tecnología, es fácil optar por esta alternativa. El término Redes Inalámbricas (Wireless Networking) se refiere a la tecnología que permite a dos o más computadoras comunicarse a través de protocolos de red estándar, llámese TCP/IP (Transmisión Control Protocol and the Internet Protocol), FTP (File Transfer Protocol), pero sin el uso de un cable (IEEE 802.11b). En la que cualquier red que no utilice un cable para comunicarse, podría ser considerada una red inalámbrica, pero en general se refiere más al termino de LAN; las redes celulares también son redes inalámbricas, aunque por el momento se clasifican como medios de comunicación de voz más que de datos, mientras que la transmisión vía satélite entra dentro de las llamadas redes WAN.

El formar parte de una comunidad Wireless trae múltiples beneficios tan grandes como estar conectado a Internet, y es que: Internet no es muy diferente de una red de campus muy desarrollada. Internet solo es: como su nombre indica, una red de redes. En una red WLAN de tu comunidad se pueden encontrar el mismo tipo de recursos que en Internet o en una LAN casera e incluso un acceso a Internet o a tu LAN casera.

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

Actualmente, existen varias soluciones de redes LAN inalámbricas, con distintos niveles de estandardización e interoperabilidad. Dos soluciones que hoy por hoy lideran el sector son Home RF®, Wi-Fi® (IEEE 802.11b). De estas dos, las tecnologías 802.11 disponen de una mayor aceptación en el mercado y están destinadas a solucionar las necesidades de las redes LAN inalámbricas para zonas activas empresariales, domésticas y públicas. La alianza Wireless Ethernet Compatibility Alliance; WECA®, trabaja para proporcionar certificados de compatibilidad con los estándares 802.11, lo que ayuda a garantizar la interoperabilidad entre los distintos fabricantes.

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, se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlando el ingreso a esta red, y protegiendo al sistema de administración de acceso no autorizado.

En este documento, se ofrece una descripción de las tecnologías para Redes de Área Local Inalámbricas (WLAN) que se implementan hoy en día. Se incluye información general sobre las Topologías de las Redes Inalámbricas y terminología necesaria para comprender algunos aspectos de las mismas. Así como un análisis sobre sus ventajas y desventajas cuando se quiere emplear este tipo de Redes. En una sección posterior se describen los distintos retos asociados a la implementación de tecnologías para redes LAN Inalámbricas.

CAPITULO 1

REDES WLAN

CAPITULO 1

1. REDES WIRELESS

Wireless es una tecnología basada en el uso de radiofrecuencias para la comunicación de equipos de cómputo. Normalmente denominada como IEEE 802.11b, Wireless permite deshacerse del cableado tradicional.

La tecnología 802.11b conocida también como: Wi-Fi ® (estándar de Fidelidad Inalámbrica) es capaz de unir a computadoras que se encuentren dentro de un área de cobertura a las ondas que emite un radio, sin necesidad de un cable de conexión entre ellos. De esta forma, se puede navegar por Internet desde la oficina, la terraza de un café, un cuarto de hotel, jardines o pasillos de una universidad o un aeropuerto, de la misma forma que se escucha la radio.

Gracias a la tecnología utilizada, Wireless puede brindar beneficios como:

Menor costo de implementación en comparación al cableado tradicional, ya que no existen cables que tender, ni lo que ello implica (rosetas de red, tubería, canaletas, etc). Además el tiempo de implementación de una red Wireless es de unas horas, en comparación con el cableado que puede llevar días enteros.

Movilidad, ya que al no tener cables, usted puede moverse de un lugar a otro con su computadora inalámbrica o reubicar una PC, sin necesidad de preocuparse por tender cable nuevo. Para usuarios con equipos móviles, esta movilidad permite la libertad de trabajar con su computadora desde una sala de juntas, oficina, cafetería, etc.

Velocidad, las redes tradicionales por cable operan a una velocidad de 10 Mbps (Megabits por segundo) o 100 Mbps. En un ambiente de trabajo normal, estas velocidades no son reales, por lo que la inversión en equipos de estas velocidades no es justificable. Una red Wireless trabaja a velocidades desde 1 Mbps (que es la velocidad normal a la que trabaja su red cableada) hasta velocidades de 5, 11 o 22 Mbps reales, lo que le brinda mejor aprovechamiento de su red interna, a un menor costo.

Los siguientes imagines nos presentan una Red Cableada Ethernet contra una Red Wireless:

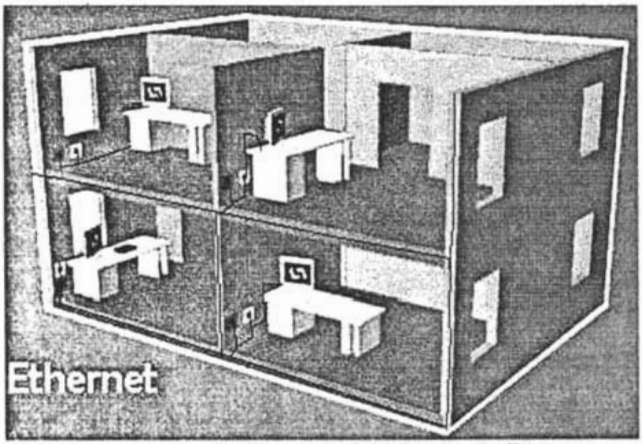


Fig. 1.1 Red Cableada Ethernet

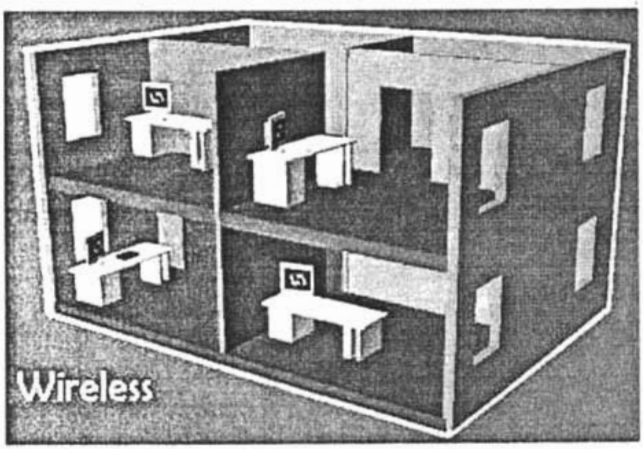


Fig. 1.2 Red Wireless

1.1 CONCEPTO DE RED

Una Red es un conjunto de computadoras independientes (host) capaces de comunicarse electrónicamente. Los orígenes de las redes de computadoras se remontan a los primeros sistemas de tiempo compartido, al principio de los años sesenta, cuando una computadora era un recurso caro y escaso. La idea que encierra el tiempo compartido es simple. Puesto que muchas tareas requieren solo una pequeña fracción de la capacidad de una gran computadora, se sacara mayor rendimiento de esta, si presta servicios a mas de un usuario al mismo tiempo. Del tiempo compartido a las redes hay solo un pequeño escalón.

Una vez demostrado que un grupo de usuarios mas o menos reducido podía compartir una misma computadora, era natural preguntarse si muchas personas muy distantes podrían compartir los recursos disponibles (discos, terminales, impresoras, e incluso programas especializados y bases de datos) en sus respectivas computadoras de tiempo compartido.

Las redes tradicionales están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información. La Red de Área Local, es un ejemplo de la configuración utilizada en muchas oficinas y empresas. Las diferentes computadoras se denominan estaciones de trabajo y se comunican entre sí a través de un cable o línea telefónica conectada a los servidores. Éstos son computadoras como las estaciones de trabajo, pero poseen funciones administrativas y están dedicados en exclusiva a supervisar y controlar el acceso de las estaciones de trabajo a la red y a los recursos compartidos (como las impresoras).

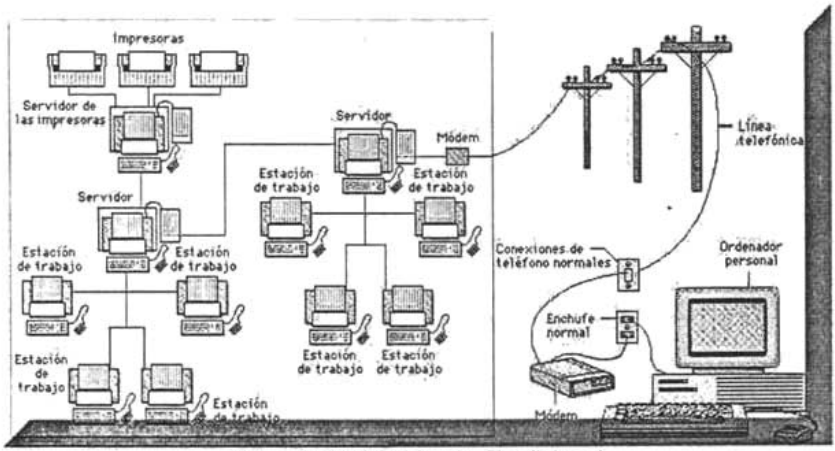


Fig. 1.3 Red Cableada Tradicional

La figura 1.3 representa una conexión principal entre servidores de red; la línea de unión entre estaciones de trabajo muestra las conexiones locales. Un módem (modulador/demodulador) permite a las computadoras transferir información a través de las líneas telefónicas normales. El módem convierte las señales digitales a analógicas y viceversa, y permite la comunicación entre computadoras muy distantes entre sí.

1.1.1 CONEXIONES FÍSICAS

Una red tiene dos tipos de conexiones: conexiones físicas, que permiten a los ordenadores transmitir y recibir señales directamente. Y conexiones lógicas, o virtuales, que permiten intercambiar información a las aplicaciones informáticas, por ejemplo a un procesador de textos.

Las conexiones físicas están definidas por el medio empleado para transmitir la señal, por la disposición geométrica de los ordenadores (topología) y por el método usado para compartir información.

1.1.2 CONEXIONES LOGICAS

Las conexiones lógicas son creadas por los protocolos de red y permiten compartir datos a través de la red entre aplicaciones correspondientes a ordenadores de distinto tipo

1.1.3 CONEXIONES INTERNAS

Una LAN suele estar formada por un grupo de ordenadores, pero también puede incluir impresoras o dispositivos de almacenamiento de datos como unidades de disco duro. La conexión material entre los dispositivos de una LAN puede ser un cable coaxial, un cable de dos hilos de cobre o una fibra óptica. O las conexiones inalámbricas empleando transmisiones de infrarrojos o radiofrecuencia.

Las redes emplean protocolos, o reglas, para intercambiar información a través de una única conexión compartida. Estos protocolos impiden una colisión de datos provocada por la transmisión simultánea entre dos o más computadoras. En la mayoría de las LAN, los ordenadores emplean protocolos conocidos como Ethernet o Token Ring. Las computadoras conectadas por Ethernet comprueban si la conexión compartida está en uso; si no es así, la computadora transmite los datos. Como los ordenadores pueden detectar si la conexión está ocupada al mismo tiempo que envían datos, continúan controlando la conexión compartida y dejan de transmitir si se produce una colisión. Los protocolos Token Ring transmiten a través de la red un mensaje especial (*token* en inglés).

El ordenador que recibe la contraseña obtiene permiso para enviar un paquete de información; si el ordenador no tiene ningún paquete que enviar, pasa la contraseña al siguiente ordenador.

1.1.4 CONEXIONES EXTERNAS

Las conexiones que unen las WLAN con recursos externos, como otra WLAN o una base de datos remota, se denominan puentes, reencaminadores y pasarelas (*gateways*). Un puente crea una LAN extendida transmitiendo información entre dos o más WLAN. Un camino es un dispositivo intermedio que conecta una WLAN con otra WLAN mayor o con una WAN, interpretando la información del protocolo y enviando selectivamente paquetes de datos a distintas conexiones de LAN o WAN a través de la vía más eficiente disponible. Una puerta conecta redes que emplean distintos protocolos de comunicaciones y traduce entre los mismos.

Los computadores de una LAN emplean puertas o caminos para conectarse con una WAN como Internet. Estas conexiones suponen un riesgo para la seguridad porque la WLAN no tiene control sobre los usuarios de Internet. Las aplicaciones transferidas desde Internet a la WLAN pueden contener virus informáticos capaces de dañar los componentes de la WLAN; por otra parte, un usuario externo no autorizado puede obtener acceso a ficheros sensibles o borrar o alterar ficheros. Un tipo de puerta especial denominado cortafuegos impide a los usuarios externos acceder a recursos de la WLAN permitiendo a los usuarios de la WLAN acceder a la información externa.

1.2 CLASIFICACION DE REDES TRADICIONALES

Podemos clasificar las redes tradicionales en cinco tipos, según el área geográfica que abarquen. Estas son:

- LAN - Red de Área Local (Local Area Network) Red formada por computadoras que se encuentran en un mismo edificio, fabrica o campus universitario, es decir en un radio de unos pocos kilómetros cuadrados.

- MAN - Red de Área Metropolitana (Metropolitan Area Network) Red que abarca el área de una ciudad.

- WAN - Red de Área Amplia (World Area Network) Red que abarca países enteros y hasta todo el mundo.

- WLAN - Red de Área Local Inalámbrica (Wireless Local Area Network) Red de área local (LAN) que utiliza ondas electromagnéticas para comunicar equipos conectados a una red en vez de cables, como coaxial,

par trenzado o fibra óptica, por ejemplo. Si bien la conexión inalámbrica puede establecerse a través de diferentes tipos de ondas electromagnéticas el estándar ya mencionado. se centra en la tecnología de radiofrecuencias.

- WPAN – Red Personal de Area Local Inalámbrica con un alcance muy limitado. Las redes PAN se utilizan para conectar dispositivos, como asistentes personales digitales (PDA).

Las redes Wi-Fi no sólo tienen su nicho de introducción en entornos en los que es mandatario una solución inalámbrica. Contrariamente a lo que se piensa, una de sus grandes ventajas radica en su empleo como red fija, pues son múltiples los beneficios que ofrecen frente a la instalación de cableado estructurado convencional. Es esta una faceta todavía relativamente desconocida pero que puede reportar un fuerte impulso a su introducción en el ambiente empresarial y residencial. Se puede aplicar tanto a redes de área local (LANs) dentro de la empresa como en la interconexión de redes de edificios próximos, en la que la solución cableada requiere complejas tramitaciones o es obligada la contratación de la línea de datos a un operador de red con licencia para operar públicamente.

1.3 TRANSMISION DE DATOS

Varias redes pueden conectarse entre si formando una red lógica de área mayor. Para que la transmisión entre todas ellas sea posible se emplean los Routers, que son los sistemas que conectando físicamente varias redes se encargan de dirigir la información por el camino adecuado. Cuando las redes que se conectan son de diferente tipo y con protocolos distintos se hace necesario el uso de los Gateways, los cuales además de encaminar la información también son capaces de convertir los datos de un protocolo a otro. Generalmente los términos Router y Gateway se emplean indistintamente para referirse de forma general a los sistemas encargados del encaminamiento de datos en Internet.

Lo que se conoce como Internet es en realidad una red de redes, la interconexión de otras redes independientes de manera que puedan compartir información entre ellas a lo largo de todo el planeta. Para ello es necesario el uso de un protocolo de comunicaciones común. El protocolo que proporciona la compatibilidad necesaria para la comunicación en Internet es el TCP/IP.

Los protocolos de comunicaciones definen las normas que posibilitan que se establezca una comunicación entre varios equipos o dispositivos, ya que estos equipos pueden ser diferentes entre si.

1.4 REDES CONMUTADAS

a) CONMUTADAS POR CIRCUITOS

Redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.

b) CONMUTADAS POR MENSAJE

En este tipo de redes el conmutador suele ser un computador que se encarga de aceptar tráfico de los computadores y terminales conectados a él. El computador examina la dirección que aparece en la cabecera del mensaje hacia el DTE (Estación Terminal de Datos), que debe recibirlo. Esta tecnología permite grabar la información para atenderla después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.

c) CONMUTADAS POR PAQUETES

En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, estás insertados dentro de informaciones del protocolo y recorren la red como entidades independientes

d) REDES ORIENTADAS A CONEXIÓN

En estas redes existe el concepto de multiplexión de canales y puertos conocido como circuito o canal virtual, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.

e) REDES NO ORIENTADAS A CONEXIÓN

Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es INTERNET

f) RED PUBLICA DE CONMUTACIÓN TELEFÓNICA (PSTN)

Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo

acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino.

1.5 TECNOLOGÍA WLAN

Según el diseño requerido se tienen distintas tecnologías aplicables:

1.5.1 BANDA ESTRECHA

Se transmite y recibe en una específica banda de frecuencia lo más estrecha posible para el paso de información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias. Así mismo un filtro en el receptor de radio se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada.

1.5.2 BANDA ANCHA

Es el usado por la mayor parte de los sistemas sin cable. Fue desarrollado por los militares para una comunicación segura, fiable y en misiones críticas. Se consume más ancho de banda pero la señal es más fácil de detectar. El receptor conoce los parámetros de la señal que se ha difundido. En caso de no estar en la correcta frecuencia el receptor, la señal aparece como ruido de fondo. Hay dos tipos de tecnología en banda ancha:

1.5.2.1 SALTO DE FRECUENCIA (FHSS)

El Espectro Expandido por Salto de Frecuencia (Frecuency-Hopping Spread Spectrum): Utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado es como tener un único canal lógico. Para un receptor no sincronizado FHSS es como un ruido de impulsos de corta duración.

1.5.2.2 SECUENCIA DIRECTA (DSSS)

La señal de Espectro Expandido por Secuencia Directa (Direct-Sequence Spread Spectrum): se genera un bit redundante por cada bit transmitido. Estos bits redundantes son llamados "chipping code". Cuanto mayor sea esta secuencia mayor es la probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda). Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado.

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto.

En una configuración típica de LAN sin cable, los Puntos de Acceso (AP´s) conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

Fig. 1.4 Punto de Acceso de 3com®

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

1.6 INTERCONEXIÓN DE REDES

Una de las características mas notables en le evolución de la tecnología de las computadoras es la tendencia a la modularidad. Los elementos básicos de una computadora se conciben, cada vez mas, como unidades dotadas de autonomía, con posibilidad de comunicación con otras computadoras o con bancos de datos.

La comunicación entre dos computadoras puede efectuarse mediante los tres tipos de conexión:

1.6.1 CONEXIÓN DIRECTA

A este tipo de conexión se le llama transferencia de datos on–line. Las informaciones digitales codificadas fluyen directamente desde una computadora hacia otra, sin ser transferidas a ningún soporte intermedio.
Los datos pueden viajar a través de una interfaz serie o paralelo, formada simplemente por una conexión física adecuada, como por ejemplo un cable, o en este caso el espacio libre.

1.6.2 CONEXIÓN A MEDIA DISTANCIA

Es conocida como conexión off-line. La información digital codificada se graba en un soporte magnético o en una ficha perforada y se envía al centro de proceso de datos, donde será tratada por una unidad central u host., con velocidades del orden de 280 Kbps hasta los 2 Mbps.

1.6.3 CONEXIÓN A GRAN DISTANCIA

Con redes de transferencia de datos, de interfaces serie y módems se consiguen transferencia de información a grandes distancias.
La tecnología electrónica, con sus microprocesadores, memorias de capacidad cada vez más elevada y circuitos integrados, hace que los cambios en el sector de las comunicaciones puedan asociarse a los de las computadoras, porque forma parte de ambos. Hace ya algún tiempo que se están empleando redes telefónicas para las comunicaciones de textos, imágenes y sonidos. Por otro lado existen redes telefónicas, públicas y privadas, dedicadas solamente a la transmisión de datos.

Mediante el teléfono de nuestra casa se puede establecer comunicación con cualquier lugar del mundo, marcando las claves correctas. Si se dispone de la ayuda de una computadora, conectada a la línea telefónica mediante un modulador / demodulador (MODEM), se puede comunicar con otras computadoras que dispongan de los mismos elementos.

Cada día existe más demanda de servicios de telecomunicación entre computadoras, y terminales conectados en lugares alejados de ellas, lo cual abre más el abanico de posibilidades de la conjunción entre las comunicaciones y la computación o informática, conjunción a la que se da el nombre de *telemática.* Sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps. Existe otro tipo de conexión respectiva para las WLAN.

1.6.4 ARQUITECTURA CLIENTE-SERVIDOR.

La arquitectura cliente-servidor es una forma específica de diseño de aplicaciones, aunque también se conoce con este nombre a los ordenadores en los que se estas aplicaciones son ejecutadas. Por un lado, el cliente es el ordenador que se encarga de efectuar una petición o solicitar un servicio. El cliente no posee control sobre los recursos, sino que es el servidor el encargado de manejarlos. Por otro lado, el ordenador remoto que actúa como servidor evalúa la petición del cliente y decide aceptarla o rechazarla consecuentemente.

Una vez que el servidor acepta el pedido la información requerida es suministrada al cliente que efectuó la petición, siendo este último el responsable de proporcionar los datos al usuario con el formato adecuado. Finalmente debemos precisar que cliente y servidor no tienen que estar necesariamente en ordenadores separados, sino que pueden ser programas diferentes que se ejecuten en el mismo ordenador.

1.7 TOPOLOGÍA DE UNA RED WIRELESS

Se llama topología de una Red al patrón de conexión entre sus nodos, es decir, a la forma en que están interconectados los distintos nodos que la forman los criterios a la hora de elegir una topología, en general, buscan que eviten el coste del encaminamiento, dejando en segundo plano factores como la renta mínima, el coste mínimo, etc. Otro criterio determinante es la tolerancia a fallos o facilidad de localización de éstos. También tenemos que tener en cuenta la facilidad de instalación y reconfiguración de la Red.

1.7.1 RED PUNTO A PUNTO

Puede ser simple o compleja. La más básica se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual.

Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o pre-configuración.

Fig. 1.5 Red Punto a Punto

1.7.2 CLIENTE Y PUNTO DE ACCESO

Instalando un Punto de Acceso (APs) como ya se menciono, se puede doblar el rango al cuál los dispositivos pueden comunicarse, pues actúan como repetidores. Desde que el punto de acceso se conecta a la red cableada cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso.

Fig. 1.6 Cliente y Punto de Acceso

Los puntos de acceso tienen un rango finito, del orden maximo de 150m en lugares cerrados y 300m en zonas abiertas.

1.7.3 MULTIPLES PUNTOS DE ACCSESO

En zonas grandes como por ejemplo un Campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Esto es llamado "Roaming".

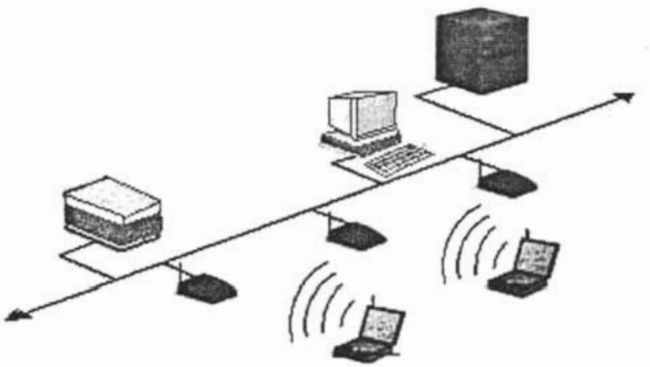


Fig. 1.7 Múltiples puntos de acceso y "Roaming"

1.7.4 PUNTO DE EXTENSION

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso. Los puntos de extensión funcionan como su nombre indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión.

Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

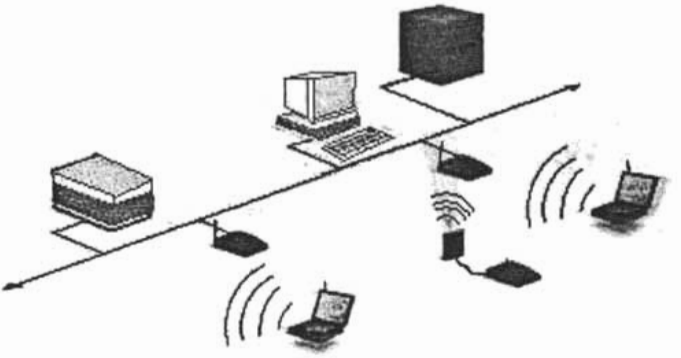


Fig. 1.8. Uso de un Punto de Extensión.

1.7.5 ANTENA DIRECCIONAL

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: se quiere una Lan sin cable a otro edificio a 1Km de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cuál permite una conexión sin cable en esta aplicación.

Fig. 1.9 Utilización de antenas direccionales.

1.8 MODELO DE REFERENCIA DE INTERCONEXIÓN DE SISTEMAS ABIERTO (OSI)

En 1978, la Organización Internacional de Estándares (ISO) publicó un conjunto de especificaciones que describía una arquitectura de conectar distintos dispositivos. y consiste en siete niveles o capas donde cada una de ellas define las funciones que deben proporcionar los protocolos con el propósito de intercambiar información entre varios sistemas. Esta clasificación permite que cada protocolo se desarrolle con una finalidad determinada, lo cual simplifica el proceso de desarrollo e implementación. Cada nivel depende de los que están por debajo de él, y a su vez proporciona alguna funcionalidad a los niveles superiores.

En 1984, la ISO publicó una revisión de este modelo y lo llamó modelos de referencia de Interconexión de Sistemas Abiertos (OSI – Open System Interconection).

Se consideró que los protocolos y modelos de la OSI llegarían a dominar las comunicaciones entre computadores, reemplazando eventualmente las Implementaciones particulares de protocolos así como a modelos rivales tales como TCP/IP, el Protocolo de Control de Transmisión y Protocolo Internet.

El modelo consta de 7 niveles o capas: Física, Enlace, Red, Transporte, Sesión, Presentación y Aplicación.

1.8.1 DETALLE TÉCNICO DE LAS CAPAS DEL MODELO OSI.

1.8.1.1 CAPA FÍSICA

La capa física abarca el conjunto físico propiamente dicho del que consta toda comunicación y también abarca las reglas por las cuales pasan los bits de uno a otro. Sus principales características son las siguientes:

1.8.1.1.1 CARACTERÍSTICAS MECÁNICAS

Relaciona las propiedades físicas de la interfaz con el medio de transmisión. A veces, incluye la especificación de un conector que une una o más señales del conductor, llamadas circuitos.

1.8.1.1.2 CARACTERÍSTICAS ELÉCTRICAS

Relaciona la representación de los bits por ejemplo, en términos de niveles de tensión y la tasa de transmisi6n de datos. Maneja voltajes y pulsos eléctricos.

1.8.1.1.3 FUNCIONAL

Especifica las funciones realizadas por los circuitos individuales del interfaz físico entre un sistema y el medio de transmisión.

1.8.1.1.4 DE PROCEDIMIENTO

Especifica la secuencia de eventos por los que se intercambia un flujo de bits a través del medio físico.

1.8.1.2 CAPA DE ENLACE DE DATOS

Mientras la capa física proporciona solamente un servicio bruto de flujo de datos, la de enlace de datos intenta hacer el enlace físico seguro y proporciona medios para activar, tener y desactivar el enlace. El principal servicio proporcionado por la capa de enlace de datos a las superiores es el de detección de errores y control. Así con un protocolo de la capa de enlace de datos completamente operacional, la capa adyacente superior puede suponer transmisión libre de errores en el enlace. Sin embargo, si la comunicación es entre dos sistemas que no están directamente conectados, la conexión constará de varios enlaces de datos unidos, cada uno operando independientemente. De este modo no se libera a la capa superior de la responsabilidad del control de errores.

1.8.1.3 CAPA DE RED

La capa de red proporciona los medios para la transferencia de información entre los sistemas finales a través de algún tipo de red de comunicación. Libera a las capas superiores de la necesidad de tener conocimiento sobre la transmisión de datos subyacente y las tecnologías de conmutación utilizadas para conectar los sistemas. En esta capa, el sistema computador está envuelto en un diálogo con la red para especificar la dirección de destino y solicitar ciertas facilidades de la red, como prioridad.

Existe un espectro de posibilidades para que las facilidades de comunicación intermedias sean gestionadas por la capa de red. En un extremo, existe en enlace punto a punto (from point to point) directo entre las estaciones. En este

caso, no existe la necesidad de una capa de red ya que la capa de enlace de datos puede proporcionar las funciones necesarias de gestión del enlace. Lo siguiente puede ser un sistema conectado a través de una única red, coma una red de conmutación de circuitos a de conmutación de paquetes.

En el otro extremo, dos sistemas finales podrían desear comunicarse, pero sin estar conectados ni siquiera a la misma red. Pero están conectados a redes que, que directa o indirectamente, están conectadas unas a otras. Este caso requiere el uso de alguna técnica de interconexión entre redes.

1.8.1.4 CAPA DE TRANSPORTE

La capa de transporte proporciona un mecanismo para intercambiar datos entre sistemas finales. El servicio de transporte orientado a conexión asegura que los datos se entregan libres de errores, en secuencia y sin pérdidas o duplicados. La capa de transporte puede estar relacionada con la optimización del uso de los servicios de red y proporcionar una calidad del servido solicitada. Por ejemplo, la entidad de sesión puede especificar tasas de error aceptables, retardo máximo, prioridad y seguridad.

El tamaño y la complejidad del protocolo de transporte dependen de cómo seguras o inseguras sean las redes y sus servicios. De acuerdo a esto, ISO ha creado una familia de 5 estándares de protocolos de transporte, cada uno orientado a los diferentes servicios subyacentes. En la arquitectura de protocolos TCP/IP, existen dos protocolos comunes de la capa de transporte: el orientado a conexión TCP y el no orientado a conexión UDP (User Datagram Protocol).

1.8.1.5 CAPA DE SESIÓN

Las cuatro capas más bajas del modelo OSI proporcionan un medio para el intercambio rápido y seguro de datos. Aunque para muchas aplicaciones este servicio básico es insuficiente. Por lo tanto, se tuvo que mejorar algunos aspectos proporcionando unos mecanismos para controlar el diálogo entre aplicaciones en sistemas finales. En muchos casos, habrá poca o ninguna necesidad de la capa de sesión, pero para algunas aplicaciones, estos servicios si se utilizan. Los servicios clave proporcionados por la capa de sesión incluyen los siguientes puntos:

1.8.1.5.1 DISCIPLINA DE DIÁLOGO

Esta puede ser simultánea en dos sentidos o (full dúplex) o alternada en los dos sentidos, (semi-duplex).

1.8.1.5.2 AGRUPAMIENTO

El flujo de datos se puede marcar para definir grupos de datos. Por ejemplo, una tienda de venta al por menor esta transmitiendo datos de ventas a una oficina regional, estos se pueden marcar para indicar el final de los datos de ventas de cada departamento. Esto indicaría al computador que finalice la cuenta de totales para ese departamento y comience una nueva cuenta para el departamento siguiente.

1.8.1.5.3 RECUPERACIÓN

La capa de sesión puede proporcionar un mecanismo de puntos de comprobación, de forma que si ocurre algún tipo de fallo entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación.

1.8.1.6 CAPA DE PRESENTACIÓN

La capa de presentación define el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transformación de datos. La capa de presentación define la sintaxis utilizada entre entidades de aplicación y proporciona los medios para la selección y las subsecuentes modificaciones de la representación utilizada. Algunos ejemplos de los servicios específicos que se podrían realizar en esa capa son los de compresión y encriptado de datos.

1.8.1.7 CAPA DE APLICACIÓN

La capa de aplicación proporciona un medio a los programas de aplicación para que accedan al entorno OSI. Esta capa contiene funciones de administración y generalmente mecanismos útiles para admitir aplicaciones distribuidas. Además, se considera que residen en esta capa las aplicaciones de uso general como transferencia de ficheros correo electrónico y acceso terminal a computadores remotos.

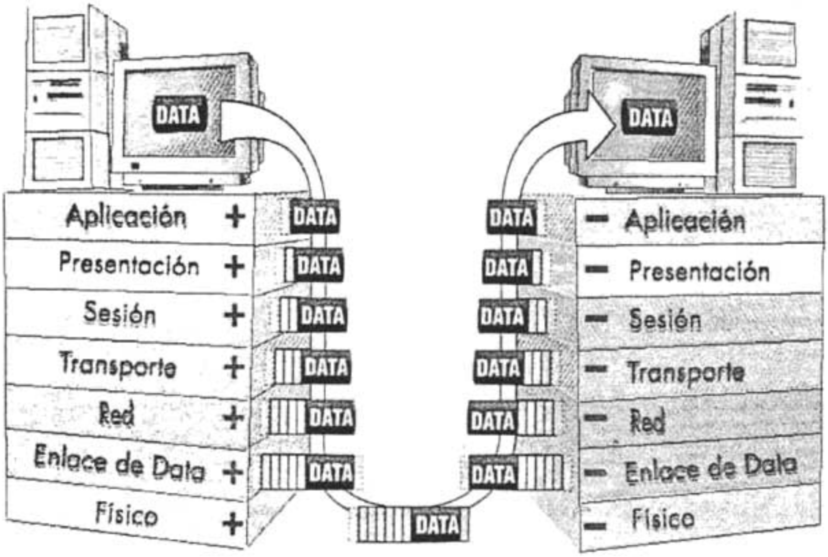


Fig. 1.10 las 7 Capas Conceptuales del Modelo OSI

1.9 REDES DE RADIO FRECUENCIA RF

El método de acceso, tal como la modulación de radio y el ancho de banda disponible, es importante para determinar la eficiencia y la capacidad de un sistema de radio. Los factores que permiten optimizar la capacidad de comunicación dentro de una área geográfica y del espectro de ancho de banda, son considerados más importantes que la forma de como son implementadas. Los diseñadores de sistemas únicamente pueden definir la utilización del espacio y del tiempo, y una aproximación de la eficiencia de la tecnología de transmisión por radio.

Los diseños de alta eficiencia han sido evitados en sistemas de radio y redes porque su utilización no es muy obvia en cuanto a rapidez y conveniencia. Uno de los aspectos más importantes de la eficiencia del tiempo es la asignación de frecuencia consolidada y el tráfico de cargas de usuarios no relacionados entre si. Por lo menos, el punto alto y el promedio de circulación de cada grupo deben de tener diferentes patrones; esto es muy difícil porque los canales incompartibles pueden ser vistos como viables, aunque su capacidad sea insuficiente para las necesidades máximas.

Independientemente del rango, un conjunto de enlaces puede únicamente dar servicio a una fracción del área total. Para una cobertura total del área, se debe de usar canales independientes, derivados por frecuencia, código o tiempo. No es fácil minimizar el número de canales independientes o conjunto de enlaces para una cobertura total. Mientras la distancia incrementa, se origina que la señal de radio disminuya, debido a la curvatura de la Tierra o a obstáculos físicos naturales existentes.

Este diseño es muy utilizado en interferencia limitada. Existe una trayectoria normal cuando en el nivel de transferencia, de estaciones simultáneamente activas, no prevén la transferencia actual de datos. Para este tipo de diseño, los siguientes factores son importantes:

1.- Es necesaria una relación (señal-ruido), para una comunicación correcta.

2.- Se requiere de un margen expresado en estadísticas para generar esta relación, aún en niveles de señal variables

3.- La posición de las antenas que realizan la transmisión. La cual puede ser limitada por las estaciones y perfectamente controlada por puntos de acceso fijos.

4.- La función de la distancia para el nivel de la señal. Esta dada por el valor promedio de la señal, considerando las diferencias en la altura de la antena de las terminales y los impedimentos naturales en la trayectoria.

1.9.1 EL FACTOR DE REUSO

El número del conjunto de canales requeridos es comúnmente llamado "Factor de Reuso" o "Valor N", para el sistema de planos celulares. El sistema de planos celulares original, contempla 7 grupos de canales de comunicación y 21 grupos de canales de configuración basados en una estructura celular hexagonal. (Un patrón de un hexágono con 6 hexágonos alrededor, da el valor de 7, y un segundo anillo de 14 da el valor de 21.)

Estos valores fueron calculados asumiendo la Modulación de Indexamiento 2 FM, previendo un valor de captura de cerca de 12 dB y un margen de cerca de 6 dB. En los sistemas digitales el Factor de Reuso es de 3 ó 4, ofreciendo menor captura y menor margen.

1.9.2 DISTANCIA DE AISLAMIENTO

El promedio de inclinación de curva es reconocido por tener un exponente correspondiente a 35-40 dB/Decena para una extensión lejana y de propagación no óptica. Para distancias cortas el exponente es más cerca al espacio libre o 20 dB/Decena. El aislamiento de estaciones simultáneamente activas con antenas omni-direccionales pueden requerir factores de Reuso de 49 o más en espacio libre. La distancia de aislamiento trabaja muy bien con altos porcentajes de atenuación media. Dependiendo de lo disperso del ambiente, la distancia de aislamiento en sistemas pequeños resulta ser en algunos casos la interferencia inesperada y por lo tanto una menor cobertura.

1.9.2.1 EL PUNTO DE ACCESO Y LA ANTENA

La infraestructura de un Punto de Acceso es simple: "Guardar y Repetir", son dispositivos que validan y retransmiten los mensajes recibidos. Estos dispositivos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones. Las características a considerar son:

1.- La antena del repetidor debe de estar a la altura del techo, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa.

2.- La antena receptora debe de ser más compleja que la repetidora, así aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.

Fig. 1. 11 Antena del Repetidor

Un punto de acceso compartido es un repetidor, al cual se le agrega la capacidad de seleccionar diferentes puntos de acceso para la retransmisión. (Esto no es posible en un sistema de estación-a-estación, en el cual no se aprovecharía el espectro y la eficiencia de poder, de un sistema basado en puntos de acceso)

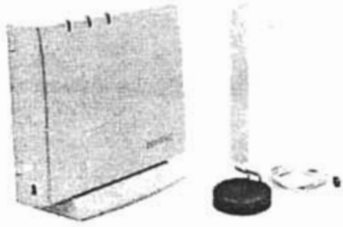


Fig. 1.12 Punto de Acceso y Receptor

La diferencia entre el techo y la mesa para algunas de las antenas puede ser considerable cuando existe en esta trayectoria un obstáculo o una obstrucción. En dos antenas iguales, el rango de una antena alta es 2x-4x, más que las antenas bajas, pero el nivel de interferencia es igual, por esto es posible proyectar un sistema basado en coberturas de punto de acceso, ignorando estaciones que no tengan rutas de propagación bien definidas entre si.

Los ángulos para que una antena de patrón vertical incremente su poder direccional de 1 a 6 están entre los 0° y los 30° bajo el nivel horizontal, y cuando el punto de acceso sea colocado en una esquina, su poder se podrá incrementar de 1 a 4 en su cobertura cuadral. El patrón horizontal se puede incrementar de 1 hasta 24 dependiendo del medio en que se propague la onda.

En una estación, con antena no dirigida, el poder total de dirección no puede ser mucho mayor de 2 a 1 que en la de patrón vertical. Aparte de la distancia y la altura, el punto de acceso tiene una ventaja de hasta 10 Db en la recepción de transmisión de una estación sobre otra estación.

Estos 10 Db son considerados como una reducción en la transmisión de una estación, al momento de proyectar un sistema de estación-a-estación.

1.9.2.2 AISLAMIENTO EN SISTEMAS CERCANOS

Con un proyecto basado en Puntos de Acceso, la cobertura de cada punto de acceso es definible y puede ser instalado para que las paredes sean una ayuda en lugar de un obstáculo. Las estaciones están recibiendo o transmitiendo activamente muy poco tiempo y una fracción de las estaciones asociadas, con un punto de acceso, están al final de una área de servicio; entonces el potencial de interferencia entre estaciones es mínimo comparado

con las fallas en otros mecanismos de transmisión de gran escala. De lo anterior podemos definir que tendremos dos beneficios del punto de acceso:

1.- El tamaño del Grupo de Reuso puede ser pequeño (4 es el valor usado, y 2 es el deseado).

2.- La operación asíncrona de Grupos de Reuso contiguos puede ser poca perdida, permitiendo así que el uso del tiempo de cada punto de acceso sea aprovechado totalmente.

Estos detalles incrementan materialmente el uso del tiempo.

1.9.2.3 MODULACION DE RADIO

El espectro disponible es de 40 MHz, según el resultado de 802.11 La frecuencia es "Desvanecida" cuando en una segunda o tercera trayectoria, es incrementada o decrementada la amplitud de la señal. La distribución de probabilidad de este tipo de "Desvanecimientos" se le denomina "Rayleigh". El desvanecimiento Rayleigh es el factor que reduce la eficiencia de uso del espectro con pocos canales de ancho de banda.

Si es usada la señal de espectro expandido, la cual es 1 bit/símbolo, la segunda o tercera trayectoria van a causar un "Desvanecimiento" si la diferencia de la trayectoria es más pequeña que la mitad del intervalo del símbolo. Por ejemplo, una señal a 10 Mbs, necesita de 0.1 μseg. de tiempo para propagar la señal a 30 mts. Diferencias en distancias mayores de 5 mts. causan mayor interferencia entre símbolos que el causado por el "Desvanecimiento". Si el símbolo es dividido en 7 bits, el mecanismo ahora se aplicara a una séptima parte de 30 mts. (o sea, 4 metros aproximadamente), una distancia en la trayectoria mayor de 4 metros no es causa de "Desvanecimiento" o de interferencia entre símbolos.

El promedio de bits debe de ser constante, en el espacio localizado en el espectro y el tipo de modulación seleccionado. El uso de ciertos símbolos codificados, proporcionaran una mejor resolución a la longitud de trayectoria.
Un espectro expandido de 1 símbolo y cada símbolo con una longitud de 7,11,13, ...31 bits, permitirá una velocidad de 10 a 2 Mbs promedio. El código ortogonal permite incrementar los bits por símbolo, si son 8 códigos ortogonales en 31 partes y si se incluye la polaridad, entonces es posible enviar 4 partes por símbolo para incrementar la utilización del espacio.

La canalización y señalización son métodos que compiten entre sí por el uso de códigos en el espacio del espectro expandido. Algunos de los códigos de espacio pueden ser usados por la canalización para eliminar problemas de superposición.

El espectro expandido puede proporcionar una reducción del "Desvanecimiento" Rayleigh, y una disminución en la interferencia a la señal para que el mensaje sea transmitido satisfactoriamente, lo cual significa que se reduce el Factor de Reuso.
Para una comunicación directa entre estaciones de un grupo, cuando no existe la infraestructura, una frecuencia común debe ser alternada para transmisión y recepción. La activación, en la transmisión no controlada, por grupos independientes dentro de una área con infraestructura definida, puede reducir substancialmente la capacidad de organización del sistema.

1.9.2.4 EL USO DEL TIEMPO

El tiempo es importante para poder maximizar el servicio, al momento de diseñar la frecuencia en el espacio. El uso del tiempo está determinado por los protocolos y por los métodos de acceso que regularmente usen los canales de transmisión de la estación.
Las características del método de acceso para que se considere que tiene un tiempo eficiente, pueden estar limitado por los métodos que sean utilizados. Algunas de estas características son:

1.- Después de completar una transmisión-recepción, la comunicación debe de estar disponible para su siguiente uso.

a.- No debe de haber tiempos fijos entre la transmisión-recepción.

b.- Rellenar la longitud de un mensaje para complementar el espacio, es desperdiciarlo.

2.- La densidad de distribución geográfica y tiempo irregular de la demanda del tráfico deben ser conocidas.

a.- Un factor de Reuso, es más eficiente por un uso secuencial del tiempo que por una división geográfica del área.

b.- Para la comunicación en una área, se debe de considerar la posibilidad de que en áreas cercanas existan otras comunicaciones.

c.- La dirección del tráfico desde y hacia la estación no es igual, el uso de un canal simple de transmisión y recepción da una ventaja en el uso del tiempo.

3.- Para tráfico abundante, se debe de tener una "lista de espera" en la que se manejen por prioridades: "El primero en llegar, es el primero en salir", además de poder modificar las prioridades.

4.- Establecer funciones para usar todo el ancho de banda del canal de comunicación, para que el tiempo que exista entre el comienzo de la transmisión y la disponibilidad de la comunicación, sea lo más corto posible.

5.- El uso de un "saludo inicial" minimiza tiempos perdidos, en el caso de que los paquetes transferidos no lleguen correctamente; cuando los paquetes traen consigo una descripción del servicio que requieren, hacen posible que se mejore su organización.

6.- La conexión para mensajes debe ser más eficiente que la selección, particularmente al primer intento, sin embargo la selección puede ser eficiente en un segundo intento cuando la lista de las estaciones a seleccionar sea corta.

Para transacciones de tipo asíncrona, es deseable completar la transacción inicial antes de comenzar la siguiente. Deben completarse en el menor tiempo posible.

El tiempo requerido para una transacción de gran tamaño es un parámetro importante para el sistema, que afecta la capacidad del administrador de control para encontrar tiempos reservados con retardos, como hay un tiempo fijo permitido para la propagación, el siguiente paso debe comenzar cuando termina el actual. El control del tráfico de datos en ambas direcciones, se realiza en el administrador de control.

1.9.3 LA LONGITUD DEL PAQUETE Y SU TIEMPO

Cuando el paquete es más pequeño, la proporción del tiempo usado al accesar el canal, es mayor, aunque la carga pueda ser pequeña para algunas funciones, la transferencia y descarga de archivos son mejor administrados cuando la longitud del paquete es de buen tamaño, para minimizar el tiempo de transferencia.

En paquetes grandes, se incrementa la posibilidad de que el paquete tenga errores en el envío, en sistemas de radio el tamaño aproximado ideal es de 512 octetos o menos, un paquete con una longitud de 100-600 octetos puede permitir la salida oportuna de respuestas y datagramas prioritarios junto con los datagramas normales.

Es necesario de proveer formas para dividir los paquetes en segmentos dentro de las redes inalámbricas. Para un protocolo propuesto, el promedio de

mensajes transferidos, es mayor para el tráfico originado por el "saludo inicial", que el originado por el punto de acceso. En este promedio se incluyen campos de dirección de red y otras funciones que son agregadas por el protocolo usado y no por el sistema de radio.

El mensaje más largo permitido para superar un retardo de acceso es de 1.8. μseg. Y un factor de Reuso de 4, utiliza menos de 600 μseg. Un mensaje de 600 octetos utiliza 400 μseg. A una velocidad de transmisión de 12 Mbs, los 200 μseg. Que sobran pueden ser usados para solicitar requerimiento pendientes.

El tiempo marcado para un grupo de Reuso de 4 puede ser de 2,400 μseg. Este tiempo total puede ser uniforme, entre grupos comunes y juntos, con 4 puntos de acceso. Sin embargo la repartición del tiempo entre ellos será según la demanda.

Las computadoras necesitan varios anchos de banda dependiendo del servicio a utilizar, transmisiones de datos, de vídeo y de voz etc. La opción es, si:

1.- El medio físico puede multiplexar de tal manera que un paquete sea un conjunto de servicios.

2.- El tiempo y prioridad es reservado para el paquete y los paquetes relacionados con el, la parte alta de la capa MAC es multiplexada.

La capacidad de compartir el tiempo de estos dos tipos de servicios ha incrementado la ventaja de optimizar la frecuencia en el espacio y los requerimientos para armar un sistema.

CAPITULO 2

ASPECTOS BASICOS DEL IEEE 802.11b

CAPITULO 2

2. INTRODUCCIÓN AL IEEE 802.11

Dado el aumento en productividad y la creciente popularidad de las comunicaciones inalámbricas en general, y particularmente las de transmisión de datos de forma inalámbrica, y las ventajas que esta tecnología presenta, en este capitulo se trataran los aspectos básicos de esta tecnología, su conformación y arquitectura del estándar, así como también de seguridad relacionados con esta.

En junio del año 1997 el IEEE (Institute of Engineering Electric and Electronics) ratificó el estándar para las WLAN, el IEEE 802.11, que alcanzaba una velocidad de 2 Mbit/s, con una modulación de señal de Espectro Expandido por Secuencia Directa (DSSS), aunque también contemplaba la opción de Espectro Expandido por Salto de Frecuencia, (FHSS) en la banda de 2,4 GHz, y se definió el funcionamiento y la interoperabilidad entre redes inalámbricas.

El estándar 802.11 se centra en los dos niveles inferiores del modelo OSI, el nivel Físico y el de enlace de datos Cualquier aplicación LAN, en red o protocolo, incluyendo TCP/IP y Novell Netware corren sobre 802.11 tan fácilmente como corren sobre Ethernet.

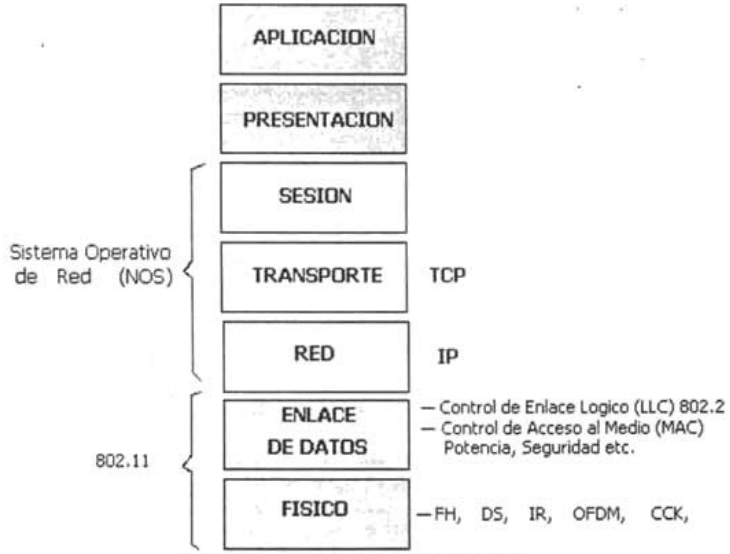


Fig. 2.1 802.11 y el modelo OSI

El Instituto de Ingenieros Eléctricos y Electrónicos IEEE, es el encargado de desarrollar y definir este estándar, actualmente, existen tres versiones disponibles de Wi-Fi®: 802.11a, 802.11b y 802.11g.

Por lo que se refiere a la distribución de las aplicaciones Wi-Fi®, se estima que los ordenadores personales (portátiles y de sobremesa) serán el principal destino de las mismas, pero no desestima el impacto que tendrán en teléfonos móviles y PDA´s, a continuación se muestra una grafica que representa el crecimiento de las aplicaciones Wi-Fi® en el mercado mundial.

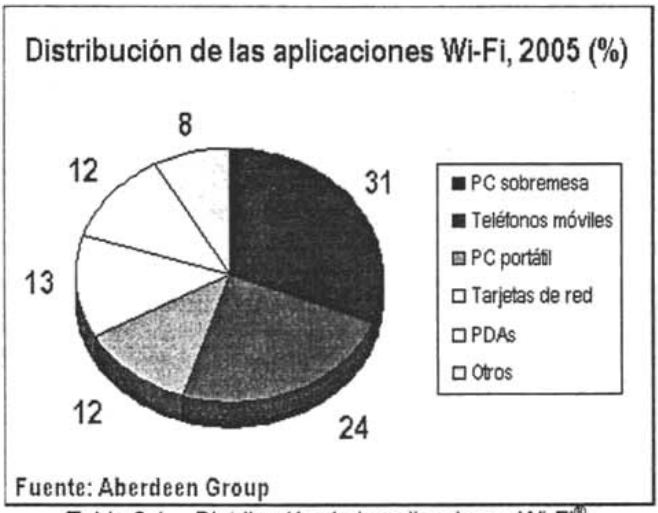


Tabla 2.1.- Distribución de la aplicaciones Wi-Fi®

Como muestra de las grandes expectativas que se están generando en torno al estándar Wi-Fi®, pueden citarse iniciativas como el proyecto Cometa Networks en los Estados Unidos, una alianza constituida por IBM, Intel y AT&T que pretende extender una red de acceso inalámbrico, con 20.000 puntos de acceso en los principales 50 núcleos metropolitanos del país, y que esta operando desde 2004, el objetivo de Cometa Networks es posibilitar que empresas de telecomunicaciones, ISP´s (Proveedores de Internet), operadoras inalámbricas y de cable puedan ofrecer a sus clientes acceso inalámbrico y de banda ancha a Internet desde su red de puntos de acceso.

Basándose en la tecnología Wi-Fi®, México a través de la empresa Telmex®, con el servicio de Prodigy Móvil®, se ofrece en mas de 350 Puntos de Acceso en todo el país, logrando así una gran cobertura en Aeropuertos, Restaurantes, Hoteles etc. sin dejar de mencionar el servicio de Internet de Alta velocidad para el Hogar y la Empresa, Prodigy Infinitum® que ha incluido recientemente en su servicio ADSL, un Modem Router ADSL, en particular, el

modelo 2Wire®, que tiene la opción de funcionar en modo Alambrico e Inalámbrico, es decir, que también es un Punto de Acceso (AP) para compartir el servicio de Internet de Alta velocidad, en una red inalámbrica, entre varias computadoras.

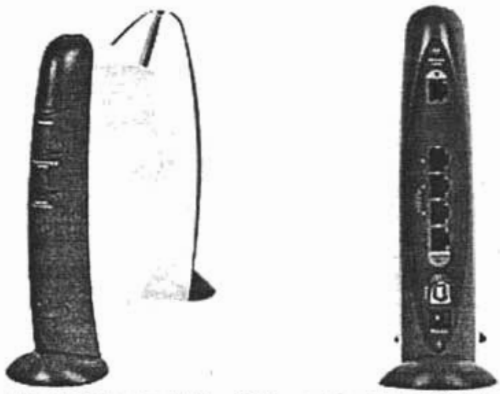


Fig. 2.2 Router 2Wire® Home Portal 1800HW

Sin embargo, al día de hoy, Wi-Fi® es todavía una tecnología novedosa y que ha empezado a utilizarse, en hogares o empresas. Antes de consolidarse definitivamente, deberá resolver una serie de incógnitas que penden en la actualidad sobre su viabilidad:

Seguridad: una de las mayores tareas pendientes, a la espera de 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 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 medio 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 valedor 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.

Como se ha comentado, el 802.11b fue el primero en aprobarse. Con unas velocidades de transferencia de 11Mbps y funcionando en el rango de frecuencias de 2,4Ghz.

El 802.11a, es un estándar que funciona en los 5GHz y ofrece una velocidad de transmisión de 54 Mbps. El problema en este caso fue su despliegue en Europa, pues la banda de los 5GHz está destinada a usos militares. De esta forma, mientras en países como Estados Unidos o Japón el 802.11a despegaba con fuerza, Europa se quedaba rezagada, pues hasta hace apenas unos meses no se había liberado ese rango de frecuencia y además, limitándose a una potencia determinada.

Sin embargo, los fabricantes no se dieron por vencidos ante los problemas europeos respondieron con la 802.11g, que funcionando en los 2,4Ghz y siendo completamente compatible con la 802.11b, ofrece la misma velocidad de transmisión que la 802.11a, aunque ésta última era una mejor tecnología.

Respecto a los otros estándares, como el IEEE 802.11i, IEEE 802.11h o el IEEE 802.11e, representan mejoras respecto a los a, b o g. La seguridad es la clave principal del 802.11i, que incluye mejoras respecto a los sistemas de encriptación de datos que se envían a través de la red inalámbrica.

La norma 802.11f habla de una especie de roaming. Los estándares mencionados hasta ahora permiten la conexión de los terminales dentro de una misma subred IP. Esta norma supone un nuevo estándar que define la intercomunicación entre puntos de acceso de distintos fabricantes (facilitando el roaming).

Finalmente, 802.11f es un estándar en el que se sigue trabajando para proveer un protocolo para compartir información entre puntos de acceso, que necesiten intercambiar datos.

El estándar IEEE 802.11b contiene varias características de seguridad, tales como los modos de autentificación del sistema abierto y de llave compartida, el Identificador del Juego de Servicios (Service Set Identifier-SSID), y el Equivalente a Privacidad Cableada (Wired Equivalent Privacy-WEP). Cada una de estas características provee diferentes grados de seguridad.

En este documento también se revisa información de cómo las antenas RF pueden ser usadas para limitar, y en algunas instancias darle forma a la propagación Wireless Médium (Medio Inalámbrico).

El 802.11 representa el primer estándar para los productos WLAN de una internacionalmente conocida organización independiente. El método de acceso al medio es mediante escucha pero sin detección de colisión, que se conoce como; DFWMAC (Distributed Foundation Wireless MAC).

La dificultad en detectar la portadora en el acceso WLAN consiste básicamente en que la tecnología utilizada es Spread-Spectrum y con Acceso por División de Código (CDMA), lo que conlleva que el medio radioeléctrico sea compartido, ya sea por Secuencia Directa DSSS o por Saltos de Frecuencia en FHSS.

El acceso por código CDMA implica que pueden coexistir dos señales en el mismo espectro utilizando códigos diferentes, y eso para un receptor de radio implica que detectaría la portadora inclusive con señales distintas de las de la propia red WLAN. Hay que mencionar que la banda de 2,4 GHz está reglamentada como banda de acceso pública y en ella funcionan gran cantidad de sistemas, entre los que se incluyen los teléfonos inalámbricos Bluetooth ®.

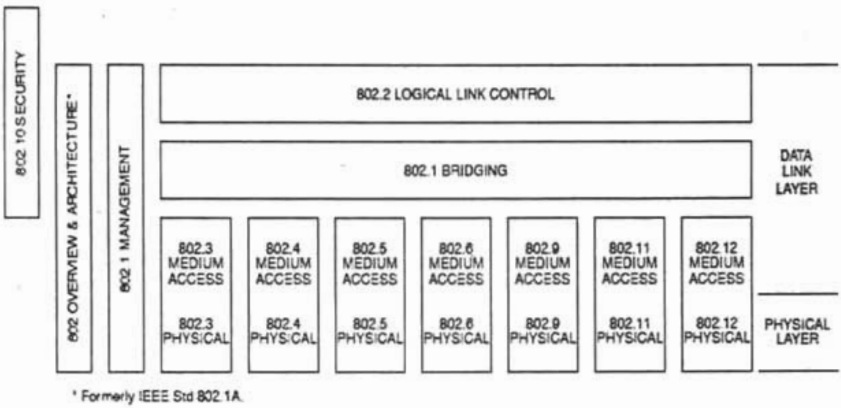


Fig. 2.3 Los Estandartes 802 de IEEE

2.1 ESPECIFICACIONES DEL IEEE 802.11b

Un poco más tarde, en el año 1999, se aprobó el estándar 802.11b, una extensión del 802.11 para WLAN empresariales, (Wireless Local Area Network) con una velocidad de 11 Mbit/s (otras velocidades normalizadas a nivel físico son: 5.5 - 2 y 1 Mbit/s) y un alcance de 100 metros, que al igual que Bluetooth y Home RF, también emplea la banda de ISM* (*(Industrial, Scientific and Medical).* de 2,4 GHz, pero en lugar de una simple modulación de radio digital y salto de frecuencia (FH/Frequency Hopping), utiliza una modulación lineal compleja (DSSS).

* ISM es una banda para uso comercial sin licencia

Este estándar define a la Capa Física (PHY - Physical) y la capa de Control de Acceso al Medio (MAC – Medium Access Control) para las WLAN's. Define capas físicas PHY para tasas de transmisión de 1 y 2 Mbps en la banda de radiofrecuencia (RF) sin licencia de 2.4 GHz y en la infrarroja (IR)

2.2 LA CAPA FÍSICA (PHY)

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos. En la capa física, se definen dos métodos de transmisión RF y un infrarrojo. El funcionamiento de la WLAN en bandas RF no licenciadas, requiere la modulación en banda ancha para reunir los requisitos del funcionamiento en la mayoría de los países.

Los estándares de transmisión RF, son de Espectro Expandido por Secuencia Directa (Direct-Sequence Spread Spectrum): DSSS, o El Espectro Expandido por Salto de Frecuencia (Frecuency-Hopping Spread Spectrum): FHSS. Ambas arquitecturas se definen para operar en la banda de frecuencia de 2.4 GHz, ocupando típicamente los 83 MHz de banda desde los 2.400 GHz hasta 2.483 GHz. (DBPSK: Differential BPSK) y DQPSK es la modulación para la Secuencia Directa.

La Frecuencia de Saltos utiliza los niveles 2-4 Gaussian FSK como el método de señalización de modulación. La Trama Física se describe como el diagrama;

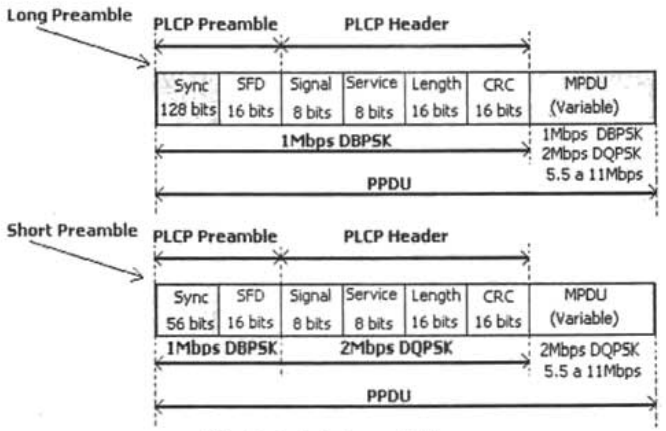


Fig. 2.4 La Trama Física

Preámbulo Largo: implementación obligatoria, trama normal
Preámbulo Corto: implementación optativa, para transmisión de vídeo y voz sobre IP

La especificación del FHSS de 2.4 GHz, y la especificación IR original del 802.11 normalmente no se usan. El rango limitado (aproximadamente 15 metros) del OFDM 5GHz para PHY lo hacen menos atractivo para la mayoría de los usuarios. Actualmente la mayoría de los productos implementan la tecnología DSSS del 802.11b para una velocidad de transmisión de datos de 11 Mbps por su ventaja de precio/desempeño. Debido a que las otras PHY son raramente usadas, el resto de este documento asume que se está usando 2.4 GHz DSSS PHY.

Especificado en el Estándar	Frecuencia de Radio (RF)	Infrarrojo (IR)	Mecanismo	Máxima Tasa de Transferencia (Mbps)
802.11	2.4 GHz ISM	850-950 nm	DSSS	2
802.11b	2.4 GHz ISM		DSSS	11
802.11g	2.4Ghz ISM		OFDM	54
802.11a	5 GHz ISM		DSSS	54

Tabla 2.2 Comparación entre las capas PHY del IEEE 802.11.

2.2.1 LA CAPA FÍSICA DSSS

En esta técnica se genera un patrón de bits redundante (señal de chip) para cada uno de los bits que componen la señal. Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11b recomienda un tamaño de 11 bits, pero el optimo es de 100. En recepción es necesario realizar el proceso inverso para obtener la información original.

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker (también llamado código de dispersión o PseudoNoise). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. Un ejemplo de esta secuencia es el siguiente:

+1 −1 +1 +1 −1 +1 +1 +1 −1 −1 −1 −1

Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

Esta secuencia proporciona 10.4dB de aumento del proceso, el cual reúne los requisitos mínimos para las reglas fijadas por la FCC*. La arquitectura de propagación usada en la capa física Secuencia Directa no debe confundirse

* Agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones

con CDMA. Todos los productos 802.11 adaptables utilizan la misma codificación PN y por consiguiente no tienen un juego de códigos disponible como se requiere para el funcionamiento de CDMA.

A continuación se puede observar como se utiliza la secuencia de Barker para codificar la señal original a transmitir:

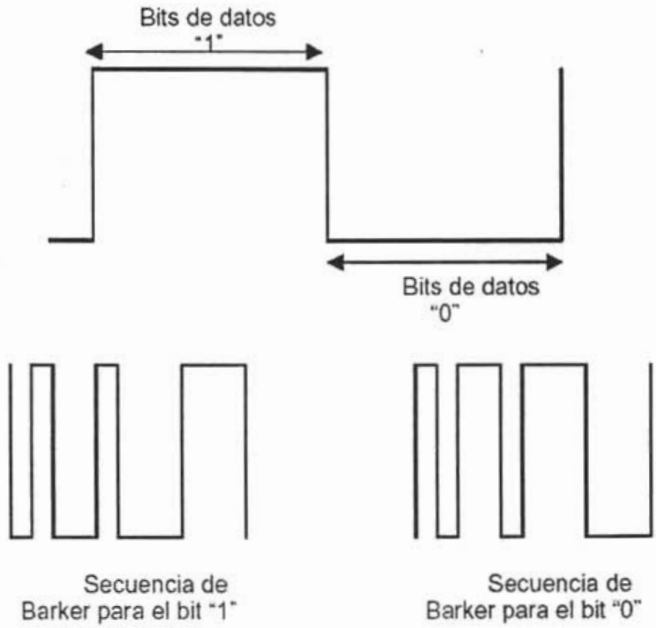


Figura 2.5 Codificación de Barker

Una vez aplicada la señal de chip, el estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de Espectro Expandido por Secuencia Directa (DSSS), la modulación DBPSK (Differential Binary Phase Shift Keying) y la modulación DQPSK (Differential Quadrature Phase Shift Keying), que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente.

Recientemente el IEEE ha revisado este estándar, y en esta revisión, conocida como 802.11b, además de otras mejoras en seguridad, aumenta esta velocidad hasta los 11Mbps, lo que incrementa notablemente el rendimiento de este tipo de redes.

En el caso de Estados Unidos y Europa la tecnología DSSS utiliza un rango de frecuencias que va desde los 2,4 GHz hasta los 2,4835 GHz, lo que permite tener un ancho de banda total de 83,5 MHz. Este ancho de banda se subdivide en canales de 5 MHz, lo que hace un total de 14 canales independientes. Cada país esta autorizado a utilizar un subconjunto de estos canales. En el caso de España se utilizan los canales 10 y 11, que corresponden a una frecuencia central de 2,457 GHz y 2,462 GHz.

En configuraciones donde existan mas de una celda, estas pueden operar simultáneamente y sin interferencias siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz. Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma

A continuación se muestra una tabla con las distintas frecuencias que tiene asignadas DSSS en diferentes regiones;

N: Canal	Frecuencias Norteamericanas	Frecuencias Europeas	Frecuencias Japonesas
1	2412 MHz	N/A	N/A
2	2417 MHz	N/A	N/A
3	2422 MHz	2422 MHz	N/A
4	2427 MHz	2427 MHz	N/A
5	2432 MHz	2432 MHz	N/A
6	2437 MHz	2437 MHz	N/A
7	2442 MHz	2442 MHz	N/A
8	2447 MHz	2447 MHz	N/A
9	2452 MHz	2452 MHz	N/A
10	2457 MHz	2457 MHz	N/A
11	2462 MHz	2462 MHz	N/A
12	N/A	N/A	2484 MHz

Tabla 2.3 Tabla de Frecuencias DSSS para operar en diferentes regiones

2.2.2 LA CAPA FÍSICA FHSS

La capa física FHSS tiene 22 modelos de espera para escoger. La capa Física de Frecuencia de Saltos se exige para saltar por la banda ISM 2.4GHz cubriendo 79 canales. Cada canal ocupa un ancho de banda de 1Mhz y debe brincar a la tasa mínima especificada por los cuerpos reguladores del país pretendido. Para los Estados Unidos se define una tasa de salto mínima de 2.5 saltos por segundo.

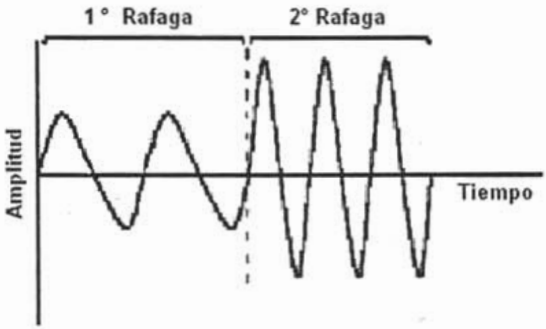


Fig. 2.6a. Grafica de Codificación con Salto de Frecuencia

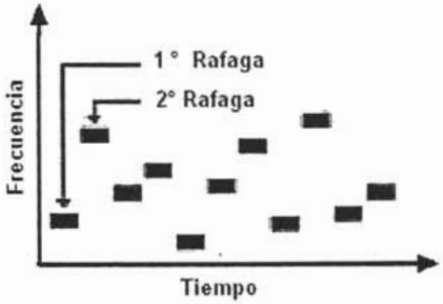


Fig. 2.6b. Grafica de Codificación con Salto de Frecuencia

Cada una de las capas físicas utiliza su propio encabezado único para sincronizar al receptor y determinar el formato de la señal de modulación y la longitud del paquete de datos. Los encabezamientos de las capas físicas siempre se transmiten a 1Mbps. Los campos predefinidos en los títulos proporcionan la opción para aumentar la tasa de datos a 2 Mbps para el paquete de los datos existente.

2.3 LA CAPA MAC

La especificación de la capa MAC (Control de Acceso al Medio) para la 802.11 tiene similitudes a la de Ethernet cableada de línea normal 802.3

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas. Ya que deben de tenerse en cuenta las dos topologías de una red inalámbrica:

- Ad-Hoc: redes peer-to-peer. Varios equipos forman una red de intercambio de información sin necesidad de elementos auxiliares. Este tipo de redes se utilizan en grupos de trabajo, reuniones, conferencias, etc.

- Basadas en Infraestructura: La red inalámbrica se crea como una extensión a la red existente basada en cable. Los elementos inalámbricos se conectan a la red cableada por medio de un punto de acceso o un PC Bridge, siendo estos los que controlan el tráfico entre las estaciones inalámbricas y las transmisiones entre la red inalámbrica y la red cableada.

Además de los dos tipos de topología diferentes se tiene que tener en cuenta:

- Perturbaciones ambientales (interferencias)
- Variaciones en la potencia de la señal
- Conexiones y desconexiones repentinas en la red
- Roaming. Nodos móviles que van pasando de celda en celda.

A pesar de todo ello la norma IEEE 802.11 define una única capa MAC (divida en dos subcapas) para todas las redes físicas. Ayudando a la fabricación en serie de chips.

2.3.1 MECANISMOS DE ACCESO

Existen de dos tipos de Mecanismos de Acceso al Medio:

1. Protocolos con arbitraje (**FDMA** - Frequency Division Multiple Access), Acceso Múltiple por División de Frecuencia, (**TDMA** - Time Division Multiple Access), Acceso Múltiple por División de Tiempo.

2. Protocolos de contienda (**CSMA** Carrier-Sense, Multiple Access), Acceso Múltiple con Deteccion de portadora, (**CSMA/CA** - Carrier-Sense, Multiple Access, Collision Avoidance), Acceso Múltiple con Detección de Portadora y Prevención de Colisiones, y el **CSMA/CD** (con Detección de Colisión).

Aunque también se han diseñado protocolos que son una mezcla de ambos.

2.3.1.1 PROTOCOLOS DE ACCESO CON ARBITRAJE

a) La multiplexación en frecuencia (FDM) divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

b) Una alternativa a este sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, se llama multiplexación en el tiempo (TDM) y requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

2.3.1.2 PROTOCOLOS DE ACCESO POR CONTIENDA

Tienen similitudes al de Ethernet cableada de línea normal 802.3.

a) CSMA (Acceso Múltiple con Detección de Portadora).

Se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia PN. En este esquema se asigna una secuencia PN distinta a cada nodo, y todos los nodos pueden conocer el conjunto completo de secuencias PN pertenecientes a los demás nodos. Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia PN del destinatario. De esta forma se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

b) CSMA/CD (Acceso Múltiple con Detección de Portadora / Detección de Colisión)

Como en estos medios de difusión (radio, infrarrojos), no es posible transmitir y recibir al mismo tiempo, la detección de errores no funciona en la forma básica que fue expuesta para las LAN alambradas. Se diseño una variación denominada detección de colisiones para redes inalámbricas.

En este esquema, cuando un nodo tiene una trama que transmitir, lo primero que hace es generar una secuencia binaria seudo aleatoria corta, llamada peine la cual se añade al preámbulo de la trama. A continuación, el

nodo realiza la detección de la portadora si el canal está libre transmite la secuencia del peine. Por cada 1 del peine el nodo transmite una señal durante un intervalo de tiempo corto. Para cada 0 del peine, el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y espera hasta que los otros nodos hayan transmitido su trama.

La eficiencia del esquema depende del número de bits de la secuencia del peine ya que si dos nodos generan la misma secuencia, se producirá una colisión.

c) CSMA/CA (Acceso Múltiple con Detección de Portadora / Prevención de Colisiones)

Este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3.

En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones.

La capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía RF de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI. Si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares.

El Estándar proporciona otra opción CCA que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible. Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11b.

2.3.2 FORMATO DE TRAMA MAC

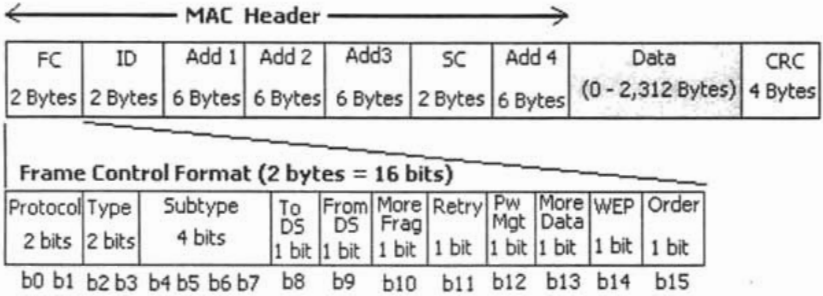


Fig. 2.7 Formato de Trama MAC

Formato de la Trama MAC donde:

- Frame Control (FC): versión de protocolo y tipo de trama (gestión, datos, control).
- Duration/ID (ID)
- Station ID se usa para el tipo de trama "Power -Save poll message"
- El valor de duración se usa para el cálculo del vector de reserva de red (Network Allocation Vector)
- Address fields (1-4) contienen hasta cuatro direcciones (origen, destino, transmisión, recepción), dependiendo del campo de control de trama (bits ToDS y FromDS)
- La secuencia de control consiste en un número de fragmento y un número de trama. Se usa para representar el orden de diferentes fragmentos pertenecientes a la misma trama, y para distinguir una posible duplicación de paquetes.
- Data: la información transmitida o recibida
- CRC: campo de Control de Redundancia cíclica de 32 bits.

2.3.3 FORMATO DE CONTROL DE TRAMA (FCF)

Formato de Control de Trama (Frame Control Format) donde;

- Versión del Protocolo (Protocol Version) indica la versión del estándar IEEE 802.11.
- Tipo (Type) : Gestión, Control, Datos
- Subtipo (Subtype): RTS, CTS, ACK etc

- To DS se pone a 1 cuando la trama se manda a un sistema de distribución (DS)
- From DS se pone a 1 cuando la trama se recibe de un sistema de distribución (DS)
- More Fragment se pone a 1 cuando hay más fragmentos después de éste perteneciente a la misma trama.
- Retry indica que este fragmento es una retransmisión de un fragmento previamente enviado. (Para que el receptor reconozca la transmisión duplicada de tramas)
- Power Management indica el modo de gestión de energía en el que la estación estará después de la transmisión de la trama.
- More Data indica que hay más tramas en cola hacia esta estación.
- WEP indica que el cuerpo de la trama está encriptado de acuerdo con el algoritmo WEP (wired equivalent privacy).
- Order indica que la trama se está enviando usando la clase de servicio "Estrictamente ordenado".

El mejor método a utilizar depende de los niveles de interferencia en el entorno operativo. El protocolo CSMA/CA permite opciones que pueden minimizar colisiones utilizando "peticiones de envío" (RTS), "listo para enviar" (CTS), datos y tramas de transmisión de reconocimientos (ACK), de una forma secuencial.

Las comunicaciones se establecen cuando uno de los nodos inalámbricos envía una trama RTS. La trama RTS incluye el destino y la longitud del mensaje. La duración del mensaje es conocida como el Vector de Asignación de Red (NAV).

El NAV alerta a todos los otros en el medio, para retirarse durante la duración de la transmisión. Las estaciones receptoras emiten una trama CTS, que hace eco a los remitentes y al vector NAV. Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS empiezan de nuevo. Después de que se recibe la trama de los datos, se devuelve una trama ACK, que verifica una transmisión de datos exitosa.

Una limitación común de los sistemas LAN inalámbricos es el problema del "nodo oculto". Esto puede romper un 40% o más de las comunicaciones en un ambiente WLAN muy cargado. Ocurre cuando hay una estación en un grupo de servicio que no puede detectar la transmisión de otra estación, y así descubrir que el medio está ocupado.

En la figura 8, las estaciones A y B pueden comunicar. Sin embargo, una obstrucción impide a la estación C recibir de la estación receptora A y no puede determinar cuándo está ocupado el canal. Por lo tanto, ambas estaciones A y C podrían intentar transmitir a la vez a la estación B. El uso de las secuencias RTS, CTS.

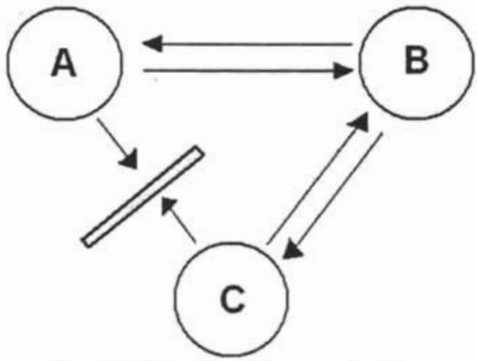


Fig. 2.8 Estaciones incomunicadas

En el estándar se dirigen suministros de seguridad como una característica optativa para aquellos afectados por la escucha secreta, es decir, por el "fisgoneo".

La seguridad de los datos se realiza por una compleja técnica de codificación, conocida como WEP (Wired Equivalent Privacy Algorithm), el Algoritmo de Privacia Equivalente del Cableado WEP se basa en proteger los datos transmitidos en el medio RF, cuando se habilita, sólo protege la información del paquete de datos y no protege el encabezamiento de la capa física para que otras estaciones en la red puedan escuchar el control de datos necesario para manejar la red. Sin embargo, las otras estaciones no pueden distinguir las partes de datos del paquete.

La gestión de la potencia se apoya en el nivel MAC para esas aplicaciones que requieren movilidad bajo el funcionamiento de la pila. Se hacen provisiones en el protocolo para que las estaciones portátiles pasen a "modo dormido" durante un intervalo de tiempo definido por la estación base.

Existen dos modos diferentes de operación para los dispositivos 802.11;

2.4 MODOS DE OPERACIÓN

2.4.1 REDES AD-HOC

Una red Ad-Hoc es una red simple donde se establecen comunicaciones entre las múltiples estaciones en una área de cobertura dada sin el uso de un punto de acceso o servidor. La norma especifica la etiqueta que cada estación debe observar para que todas ellas tengan un acceso justo a los medios de comunicación inalámbricos. Proporciona métodos de petición de arbitraje para utilizar el medio para asegurarse de que el rendimiento se maximiza para todos los usuarios del conjunto de servicios base.

Una red Ad-Hoc es usualmente aquella que existe por un tiempo limitado entre dos o más dispositivos inalámbricos que no están conectados a través de un punto de acceso (Access Point - AP) a una red cableada.

Por ejemplo, tres usuarios de una computadora Movil (LapTop) que deseen compartir archivos podrían poner una red Ad-Hoc usando tarjetas de red (NIC) compatibles con 802.11b y compartir archivos a través del medio inalámbrico sin la necesidad de usar medio externa.

Fig. 2.9 - Independent Basic Service Set (IBSS)

2.4.2 REDES INFRAESTRUCTURA (BSS)

Las redes Cliente/Servidor en una infraestructura (BSS - Basic Service Set) utilizan un punto de acceso que controla la asignación del tiempo de transmisión para todas las estaciones y permite que estaciones móviles deambulen por la columna vertebral de la red cliente / servidor. El (AP) Punto de Acceso se usa para manejar el tráfico desde la radio móvil hasta las redes Cliente/Servidor cableadas o inalámbricas. Esta configuración permite coordinación puntual de todas las estaciones en el área de servicios base y asegura un manejo apropiado del tráfico de datos. El punto de acceso dirige datos entre las estaciones y otras estaciones inalámbricas y/o el servidor de la red.

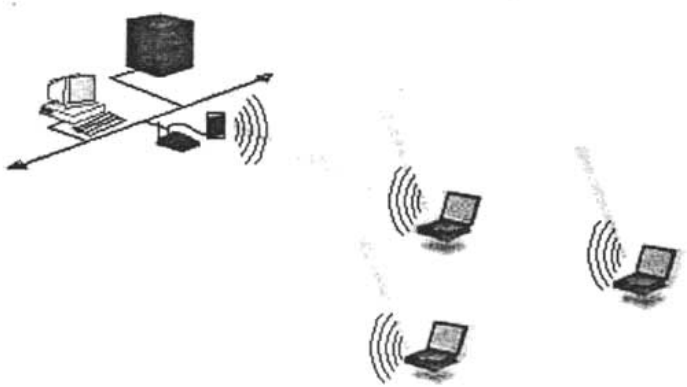


Fig. 2.10 Modo Infraestructura (BSS)

Típicamente las WLAN controladas por un punto de acceso central proporcionará un rendimiento mucho mayor

El modo de infraestructura asume la presidencia de uno o más APs puenteando el medio inalámbrico al medio cableado. El AP maneja la autentificación de la estación y la asociación con la red inalámbrica. Múltiples APs conectados por un Sistema de Distribución (DS) puede extender el alcance de la red inalámbrica a un área mucho mayor de la que puede ser cubierta por un solo AP.

En instalaciones típicas, el DS es simplemente la infraestructura de la red IP existente. Para propósitos de seguridad, LANs virtuales (VLANs) son usadas con frecuencia para segregar el tráfico inalámbrico de otro tráfico en el DS. Aunque 802.11b permite que las estaciones inalámbricas conmuten de forma dinámica la asociación de un punto de acceso a otro tal sería el caso de un usuario de un PDA caminando a través de un campus.

Fig. 2.11 Extended Service Set (ESS)

La infraestructura (Juego de Servicios Extendidos, ESS). Es una red Ad-hoc Híbrida, es decir auxiliada de una red cableada Ethernet. Como resultado de esto, las implementaciones de los diferentes vendedores son incompatibles en este sentido.

2.5 ASOCIACIÓN Y AUTENTIFICACIÓN

Este Estándar define una estación terminal para el mapeo de AP de tal forma que otras estaciones en la red cableada o inalámbrica tengan medios para contactar la estación terminal. A este mapeo se le llama "asociación." Mientras que a las estaciones terminales se les permite asociarse de forma dinámica con otros APs, en cualquier momento una estación terminal solamente puede estar asociada con un AP. El que una estación terminal esté "asociada" con un AP es muy parecido a que una estación terminal Ethernet esté colocada en una tabla de puenteo (bridge table) de un switch. Sin este mecanismo, el AP no tendría forma de determinar si debería o no avanzar frames recibidos en su puerto Ethernet hacia su puerto inalámbrico.

La asociación es un proceso de tres pasos: (1) desautentificado y desasociado; (2) autentificado y desasociado; (3) autentificado y asociado.
A los mensajes pasados durante estos pasos se les llama frames de administración (management frames). La parte importante en la que se debe hacer énfasis en este proceso es que la asociación no ocurrirá hasta que la autentificación se lleve a cabo.

2.6 MODOS DE AUTENTIFICACIÓN

Como se menciona unos párrafos atrás, antes de que una estación terminal pueda asociarse con un AP y conseguir acceso a la WLAN, debe llevar a cabo la autentificación. Dos tipos de autentificación de clientes están definidos:

2.6.1 AUTENTIFICACIÓN DE SISTEMA ABIERTO

Autentificación de sistema abierto es una forma muy básica de autentificación que consiste de una simple solicitud de autentificación que contiene la ID de la estación y una respuesta de autentificación que contiene el éxito o fracaso. En caso de éxito, se considera que ambas estaciones están mutuamente autentificadas.

Fig. 2.12 Sistema de Autentificación Abierto

2.6.2 AUTENTIFICACIÓN DE LLAVE COMPARTIDA.

Autentificación de llave compartida está basada en el hecho de que ambas estaciones tomando parte en el proceso de autentificación tiene la misma llave "compartida".

Se asume que esta llave ha sido trasmitida a ambas estaciones a través de un canal seguro que no es medio inalámbrico. En implementaciones típicas, esto podría ser configurado manualmente en la estación cliente y en el AP. El primero y el cuarto frame de autentificación de llave compartida son similares a aquellos encontrados en sistemas de autentificación abierta. La diferencia es que en el segundo y el tercer frame, la estación de autentificación recibe un paquete de texto que es un reto (creado usando el Generador de Números Pseudo Aleatorios de WEP- Pseudo Random Number Generador PRNG) desde el AP, lo encripta usando la llave compartida, y luego lo manda de regreso al AP.

Si después de la desencripción, el texto de reto es igual, entonces la autentificación de – un - sentido es exitosa. Para obtener la autentificación mutua, el proceso se repite en la dirección opuesta. El hecho de que la mayor parte de los ataques hechos contra WLAN's 802.11b están basados en capturar la forma encriptada de una respuesta conocida hace de esta forma de autentificación una elección pobre. Les da a los atacantes exactamente la información necesaria para derrotar la encripción WEP y es por lo que la llave de autentificación compartida nunca es recomendada.

Es mejor utilizar la autentificación abierta, la cual permitirá la autentificación sin la llave WEP correcta. Se mantendrá seguridad limitada porque la estación no estará preparada para enviar o recibir información de forma correcta con una llave WEP no válida.

Fig. 2.13 Sistema de Autentificación de Llave Compartida

2.7 LIMITACIÓN DEL ACCESO AL MEDIO

2.7.1 LIMITANDO LA PROPAGACIÓN DE RF

Antes de que se implemente cualquier otra medida de seguridad, es importante considerar las implicaciones de la propagación de RF por los APs en una red inalámbrica. Escogidas de una forma inteligente, la combinación adecuada de transmisor/antena puede ser una herramienta efectiva que ayudará a limitar el acceso a la red inalámbrica al área única pretendida de cobertura. Escogidas de forma poco inteligente, pueden extender la red más allá del área pretendida hacia un estacionamiento o más lejos.

Principalmente, las antenas se pueden caracterizar de dos formas-de direccionalidad y de ganancia. Las antenas omni-direccionales tienen un área de cobertura de 360 grados, mientras que las antenas direccionales limitan la cobertura a áreas mejor definidas (Vea la Figura 14). La ganancia de la antena típicamente es medida en dBi[1] y está definida como el incremento de la potencia que la antena agrega a la señal RF.

Debido a que los productos actuales 802.11b hacen uso de la banda sin licencia ISM (Industrial, Scientific, and Medical) de 2.4 GHz, están sujetas a las reglas promulgadas por la FCC en 1994 para uso de espectro distribuido. Estas reglas especifican que cualquier antena vendida con un producto debe ser probada y aprobada por un laboratorio de la FCC. Para evitar que los usuarios utilicen de forma incorrecta o ilegal antenas con productos 802.11, la FCC también requiere que cualquier AP capaz de utilizar antenas removibles deberá utilizar conectores no estándar.

[1] dBi está definida en referencia a una antena teóricamente isotrópica (propagación perfectamente esférica).

En los Estados Unidos, la FCC define el máximo de Potencia Efectiva Isotrópica Radiada (Effective Isotropic Radiated Power - EIRP) de una combinación transmisor/antena como 36 dBm, donde EIRP=potencia del transmisor+ganancia de la antena-perdida del cable.

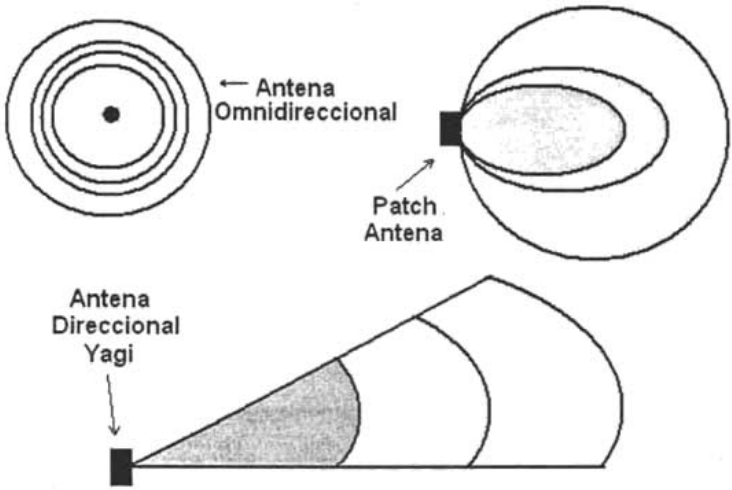


Fig. 2.14 Patrones de propagación de antenas comunes.

Esencialmente, esto significa que mientras la potencia del transmisor aumenta, la ganancia de la antena debe disminuir para permanecer abajo del máximo legal de 36 dBm. Por ejemplo un transmisor del 100-mW equivale a 20 dBm. Éste transmisor combinado con una antena de 16 dBi produce un total de 36 dBm, que es el límite legal. Para incrementar la ganancia de la antena, estaríamos legalmente obligados a reducir la potencia del transmisor. En la práctica, la mayor parte de las combinaciones transmisor/antena vendidas juntas están por debajo del máximo permitido por la FCC de 36 dBm.

Las implicaciones de todo esto son que las combinaciones del poder del transmisor/ganancia de la antena están estrictamente reguladas y limitan el área que legalmente puede ser cubierta por un solo AP. Cuando esté diseñando una WLAN, es importante llevar a cabo un reconocimiento a fondo del lugar y considerar los patrones de propagación RF de las antenas que se vayan a usar y la potencia efectiva de la combinación transmisor/antena.

También como la banda ISM está esencialmente abierta para ser usada por cualquier persona sin licencia, es importante considerar la posibilidad de la negación de servicio (Denial Of Service - DOS) de otras fuentes benignas tales como teléfonos inalámbricos de 2.4 GHz.

Finalmente, considerar que un atacante potencial podría no estar jugando dentro de las reglas de la FCC. Un atacante con recursos podría estar

usando transmisores de alta potencia, antenas de alta ganancia, y/o receptores más sensitivos. Cada uno de estos puede afectar el rango efectivo de una red inalámbrica.

2.7.2 IDENTIFICADOR DEL CONJUNTO DE SERVICIOS (SSID)

El estándar IEEE 802.11b define otro mecanismo por el cual se puede limitar el acceso: el SSID. el Identificador del Conjunto de Servicios (Service Set Identifier) El SSID es un nombre de red que identifica el área cubierta por uno o más APs. En un modo comúnmente usado, el AP periódicamente transmite su SSID. Una estación inalámbrica que desee asociarse con un AP puede escuchar estas transmisiones y puede escoger un AP al que desee asociarse basándose en su SSID.

En otro modo de operación, el SSID puede ser usado como una medida de seguridad configurando el AP para que no transmita su SSID. En este modo, la estación inalámbrica que desee asociarse con un AP debe tener ya configurado el SSID para ser el mismo que el del AP. Si los SSIDs son diferentes, los frames administrativos (management frames) enviados al AP desde el estación inalámbrica serán rechazados porque ellos contienen un SSID incorrecto y la asociación no se llevará a cabo.

Desgraciadamente, debido a que los frames de administración en las WLAN's 802.11 son siempre enviados de forma abierta, este modo de operación no provee seguridad adecuada. Un atacante fácilmente puede escuchar en el WM buscando frames de administración y descubrir la SSID del AP. Muchas organizaciones confían en el SSID para obtener seguridad sin considerar sus limitaciones. Esto es por lo menos parcialmente responsable de la facilidad con la que las WLAN's son comprometidas.

2.8 CAPA FÍSICA INFRARROJA

Se soporta un estándar infrarroja, que opera en la banda 850nM a 950nM, con un poder máximo de 2 W. La modulación para el infrarrojo se logra usando o 4 o 16 niveles de modulación "posicionamiento por pulsos". La capa física soporta dos tasas de datos:1 y 2Mbps.

2.9 DIRECCIONES MAC MOSTRADAS EN MODO AH-HOC

En primera instancia, la dirección MAC en el campo Punto de Acceso parece estar equivocado en modo Ah-Hoc porque cambia los dos primeros bytes de la dirección MAC a 02. Pero actualmente, esta es una funcionalidad metida en el código de las tarjetas inalámbricas WLAN.

Habitualmente una tarjeta inalámbrica está conectada a un punto de acceso "real". Entonces se muestra la dirección MAC correcta. Si cambia a modo Ad-Hoc (o "punto-a-punto"), uno de los ordenadores debe actuar como servidor para las otros ordenadores. El primero que entra en una red, se establecerá como servidor. Así, todas los demás ordenadores conectándose a la misma red Ad-Hoc verán ese primer ordenador como un servidor de red. Pero puesto que ese ordenador no es un servidor "real" (es decir, no es un punto de acceso permanentemente disponible), los clientes deberán notar que la red a la que se están conectando no es permanente.

Fig. 2.15 Tarjeta Inalámbrica Vigor® WLAN PCMCIA 520

Los estándares IEEE para direcciones MAC tiene un lugar reservado para estas ocasiones: las direcciones MAC que no sean globalmente válidas tienen "02" como primeros dos bytes (estas direcciones se llaman direcciones "localmente administradas").
Se puede comparar esto a las direcciones IP no homologados como: "192.168.x.x"

Así, los implementadores de Redes Wireless acordaron dar a estos servidores de red "virtuales" una dirección MAC que esté dentro del rango "localmente administrado". Para mantener únicas estas direcciones MAC virtuales, usaron un pequeño truco: sólo cambiaron los dos primeros bytes de la dirección MAC de la tarjeta wireless LAN, y puesto que los 10 restantes bytes son aún únicos en el mundo, tienen una dirección única para usar como servidor de red.

CAPITULO 3

PROTOCOLOS DE SEGURIDAD EN LAS REDES WLAN

CAPITULO 3

3. INTRODUCCIÓN A LOS PROTOCOLOS DE SEGURIDAD

En los años recientes, la proliferación de ordenadores portátiles y PDA's ha provocado la expansión de los entornos en los que las personas utilizan los ordenadores. Simultáneamente, la conectividad se está convirtiendo en una parte integral de los entornos de trabajo. 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 por el que existe la necesidad de emplear técnicas adicionales para proteger las comunicaciones.

Aunque las ventas de dispositivos WLAN están siendo elevadas, no se está produciendo la explosión que se vaticinaba. Las causas a las que se atribuyen este hecho son fundamentalmente dos: los problemas de seguridad y al desconocimiento de cómo emplear estas tecnologías para aumentar la productividad u otros beneficios inmediatos.

Las redes inalámbricas son inseguras aunque sólo sea porque el medio de transporte que emplean es el aire; por tanto, un elemento esencial a tener en cuenta en este tipo de redes al utilizarse la radio, es la encriptación.

El estándar 802.11b provee de un sistema de cifrado (WEP) "Wired Equivalent Privacy", es el algoritmo de Privacidad Equivalente del Cableado, que es un protocolo para redes Wireless que permite encriptar la información que se transmite. Proporciona encriptación a nivel 2.

Otro mecanismo de seguridad definido en el estándar IEEE 802.11b es el conocido como SSID (Service Set Identifiers) o Identificadores del Conjunto de Servicios, que es como un gestor de asignación de nombres, que proporciona un control de acceso muy rudimentario, razón por la que apenas se utiliza en las implementaciones comerciales.

3.1 PROTOCOLO DE SEGURIDAD: WEP

WEP, el Algoritmo de Privacidad Equivalente del Cableado, es el mecanismo de seguridad utilizado en las redes inalámbricas que emplean el estándar 802.11b o Wi-Fi ® Está diseñado para evitar el acceso a una red por parte de intrusos que cuenten con computadoras dotadas de dispositivos inalámbricos compatibles capaces de examinar el tráfico que fluye a través de la red.

Fig. 3.1 Logo de Certificación Wi-Fi

Existen dos métodos de cifrado WEP:

a. 64 (40) Bits.
b. 128 Bits.

Una clave de 64 (40) bits consiste en 10 números hexadecimales distribuidos en dos grupos de cinco dígitos: *Ejemplo;*

a. Clave No. 1**: 10111 21314**
b. Clave No. 2**: 20212 22324**
c. Clave No. 3**: 30313 23334**
d. Clave No. 4**: 40414 24344**

Y de 128 Bits basada en 26 números hexadecimales distribuidos en dos grupos de cinco dígitos y cuatro grupos de cuatro dígitos: Ejemplo*;*

a. Clave No. 1**: 10111 21314 1516 1718 191ª 1B1C**
b. Clave No. 2**: 20212 22324 2526 2728 292ª 2B2C**
c. Clave No. 3**: 30313 23334 3536 3738 393ª 3B3C**
d. Clave No. 4**: 40414 24344 4546 4748 494ª 4B4C**

El algoritmo de codificación WEP se deriva de la tecnología RC4, un producto desarrollado por la firma RSA Associates,® es considerado un algoritmo simétrico por qué utiliza la misma llave para cifrar y para descifrar la Unidad de Información de Protocolo (PDU) de texto plano. Para cada transmisión el texto plano es XOR con una llave seudo aleatoria para producir texto cifrado.

El proceso es invertido para la desencripción. Se convirtió en un estándar de seguridad. Originalmente estuvo basado en una codificación de 40-bit que con las impresionantes capacidades computacionales de los equipos actuales, mostró rápidamente su fragilidad en vista de que podía ser violado con relativa facilidad.

Hoy en día los equipos son despachados con tecnología de 128-bit lo cual dificulta el ingreso no autorizado a las redes.

El algoritmo WEP produce un número de gran longitud que no muestra un patrón predecible. El equipo origen indica al receptor en que dígito debe dar inicio y qué cantidad deberá restar a cada número en el mensaje. Un intruso que detecte el punto de inicio no podrá leer el mensaje porque desconoce el número secreto.

Como lo define el IEEE, WEP está diseñado para proteger a usuarios de una WLAN de espías casuales y su intención es tener las siguientes propiedades:

- *Encriptación razonablemente fuerte.* Depende de la dificultad de recuperar la llave secreta a través de un ataque de fuerza bruta. La dificultad crece con el tamaño de la llave.
- *Auto-sincronización.* No hay necesidad de lidiar con los paquetes perdidos. Cada paquete contiene la información requerida para desencriptarlo.
- *Eficiente.* Puede ser implementado en software de forma razonable.
- *Exportable.* Limitar el largo de la llave conlleva a una mayor posibilidad de exportar más allá de las fronteras de los Estados Unidos.

3.1.1 ENCRIPTACIÓN

El administrador de la red está en capacidad de definir un conjunto de claves a cada uno de los "usuarios" inalámbricos basándose en un número secreto que se someterá al algoritmo de encriptado. Cualquier usuario que no disponga de una clave estará incapacitado para acceder a la red.

WEP confía en una clave secreta k compartida entre los partícipes del grupo de comunicaciones para proteger el cuerpo del mensaje de una trama de datos.

La encriptación de una trama se efectúa según sigue:

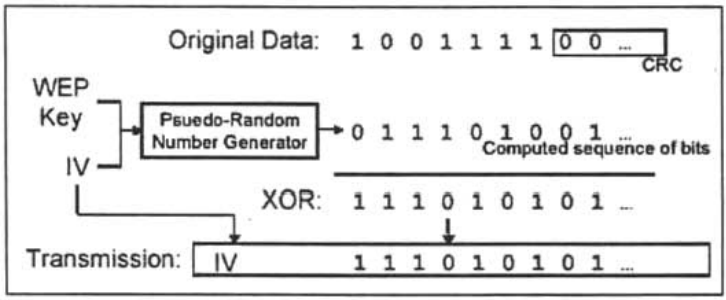


Fig. 3.2a Proceso de Encriptación

y el proceso inverso para la desencripción.

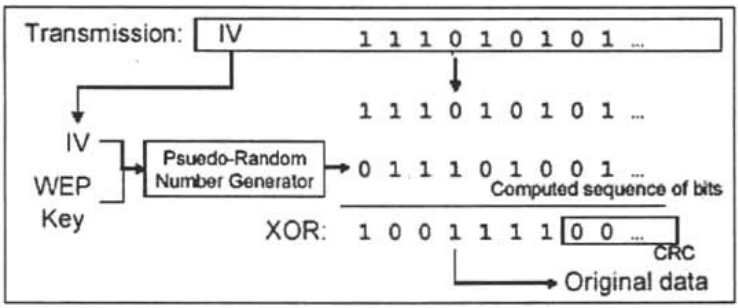


Fig. 3.2b Proceso de Desencripcion

1ª ETAPA: SUMA DE COMPROBACIÓN (*CHECKSUM*)

Primero, se calcula una suma de integridad *c(M)* sobre el mensaje *M*. Concatenamos ambos para obtener un texto sin cifrar *P = (M, c(M))*, el cual será empleado como entrada para la segunda etapa. Nótese que *c(M)*, y por ende *P*, no depende de la clave *k*.

2ª ETAPA: ENCRIPTACIÓN CON EL ALGORITMO RC4

En la segunda etapa encriptamos el texto plano *P* con el algoritmo RC4. elegimos un Vector de Inicialización, (simbólicamente, IV). El algoritmo RC4 genera un *keystream* –una secuencia larga de bytes seudo aleatorios- como una función de (IV) *v* y la clave *k*. Este *keystream* viene referido como RC4(v, k). Una vez obtenido realizamos un or-exclusivo (XOR, denotado por (+)) sobre el texto plano con el *keystream* obtenido para conseguir el texto cifrado:

$$\mathbf{C = P (+) RC\,4 (v, k)}$$

3ª ETAPA: TRANSMISIÓN

Finalmente, transmitimos el Vector de Inicialización (IV) y el texto cifrado a través del enlace de radio.

Simbólicamente, este proceso puede ser representado como:

A -> B: v,(P (+) RC4(v, k)); donde **P = (M, c(M))**

A partir de ahora usaremos el término *mensaje* (simbólicamente, *M*) para referirnos a la trama inicial de datos que deseamos procesar, el término *texto plano* (*P*) para hacer referencia a la concatenación de mensaje y *checksum* como es enviado al algoritmo de encriptación RC4, y el término *texto cifrado* (*C*) para referirnos al texto encriptado tal cual es transmitido por el enlace de radio.

Para desencriptar una trama protegida por WEP, el receptor sencillamente invierte el proceso de encriptado. Primero, genera el *keystream* RC4(v, k) y efectúa un or-exclusivo contra el texto cifrado para recuperar el texto plano original:

$$P' = C \,(+)\, RC4(v, k)$$

$$P' = (P \,(+)\, RC4(v, k)) \,(+)\, RC4(v, k)$$

$$P' = P$$

Después, el receptor verifica el *checksum* del texto desencriptado *P'* separándolo en la forma (M', c'), recalculando el *checksum* c(M'), y comprobando que coincide con el *checksum* recibido *c'*. Esto asegura que sólo las tramas con un *checksum* válido son aceptadas por el receptor.

3.1.2 OBJETIVOS DE SEGURIDAD

El protocolo WEP fue diseñado para imponer tres metas de seguridad principales:

3.1.2.1 CONFIDENCIALIDAD

El objetivo fundamental de WEP es evitar escuchas fortuitas.

3.1.2.2 CONTROL DE ACCESO

Un segundo objetivo del protocolo es proteger el acceso a la infraestructura de red inalámbrica. El estándar 802.11b incluye una característica opcional para desechar aquellos paquetes que no estén

apropiadamente encriptados usando WEP, a la vez que los fabricantes proporcionan la habilidad de WEP para proveer control de acceso.

3.1.2.3 INTEGRIDAD DE DATOS

Un objetivo relacionado es prevenir la manipulación de los mensajes transmitidos; el campo checksum se incluye con este propósito.

En los tres casos, la afirmación de la seguridad del protocolo reside en la dificultad de obtener la clave pública por medio de ataques por fuerza bruta.

Hoy día hay dos clases de implementación WEP: la clásica, tal cual viene estipulada en el estándar, y una versión extendida desarrollada por algunos fabricantes para proveer claves más largas. El estándar WEP especifica el uso de claves de 40 bits, así elegidas por las restricciones aplicadas por el gobierno norteamericano para la exportación de tecnología criptográfica vigentes cuando el protocolo fue definido.

Esta longitud de clave es lo suficientemente corta como para realizar ataques prácticos de fuerza bruta a individuos y organizaciones, con recursos de cálculo bastante modestos. No obstante, es trivial extender el protocolo para usar claves más largas, y de hecho algunos fabricantes ofrecen en sus productos, versiones de 128 bits (que realmente emplean 104 bits, a pesar de su engañoso nombre). Esta extensión convierte en imposibles los ataques por fuerza bruta incluso para el adversario con los mayores recursos, dada la tecnología actual.

A pesar de ello, se demostrara que hay atajos que permiten evitar el uso de ataques por fuerza bruta a la clave para descubrir la misma, lo que convierte en inseguras incluso a las implementaciones WEP de 128.

A continuación se expondrá que WEP no cumple ninguno de sus tres objetivos primordiales de seguridad. Primero mostraremos, de modo práctico, ataques que permiten escuchas no deseadas. Más adelante se mostrara que es posible alterar el campo checksum y modificar los contenidos de un mensaje transmitido, violando la integridad de los datos.

En último lugar se demostrara que los ataques pueden ser extendidos para inyectar tráfico completamente nuevo en la red.

3.1.3 ATAQUES A LA CAPA FISICA

En adición a las consideraciones criptográficas comentadas antes, una barrera común a los ataques en subsistemas de comunicación es el acceso a los datos transmitidos.

A pesar de ser transmitido a través de ondas de radio abiertas, el tráfico 802.11b requiere una infraestructura significante para ser interceptado. Un agresor necesita equipo capaz de monitorizar frecuencias de 2.4GHz y entender la capa física del protocolo 802.11b; para ataques activos, además es necesario estar en disposición de transmitir en las mismas frecuencias. Una inversión considerable que realizan los fabricantes en investigación y desarrollo va a parar en esta clase de dispositivos y herramientas.

Por este motivo podría existir la tentación de desestimar los ataques que requieran acceso a la capa física como impracticables; por ejemplo, esta actitud se estableció en las comunicaciones celulares hace tiempo. Sin embargo, tal posición es peligrosa.

En primera instancia no protege contra agresores con alto nivel de recursos tecnológicos que tengan la capacidad de invertir tiempo y dinero en conseguir acceso a los datos. Esto resulta especialmente peligroso cuando aseguramos una red inalámbrica interna de una compañía, ya que el espionaje industrial es un negocio muy rentable (lo que permitiría amortizar los costosos equipos necesarios para abrir una brecha en la seguridad).

Segundo, el equipo necesario para monitorizar e inyectar tráfico 802.11b está disponible para los consumidores en forma de interfases inalámbricos Ethernet. Lo único necesario es alterarlos para monitorear y transmitir tráfico encriptado. Es posible realizar ataques pasivos usando equipos de serie modificando la configuración de los controladores. Los ataques activos son más complejos, pero no por ello quedan fuera de nuestro alcance. Las tarjetas PCMCIA Orinoco® fabricadas por Lucent Technologies® permiten actualizar su Firmware (programa fijo); un concentrado esfuerzo de ingeniería inversa podría permitir una versión modificada que permitiera la inserción de tráfico arbitrario. La inversión de tiempo requerida es importante; pero hay que tener en cuenta que es un esfuerzo de una única vez, ya concluido, el Firmware alterado puede ser distribuido a través de un servidor Web o por medio de círculos clandestinos.

Por este motivo consideramos que es prudente asumir que agresores motivados podrían disponer de acceso total a la capa física para ataques tanto pasivos como activos. Otros argumentos que justifican esta postura son los propios documentos WEP. En ellos se dice que "la escucha furtiva es un problema familiar para los usuarios de otros tipos de tecnología inalámbrica". No se profundizará más en las dificultades asociadas a los ataques dirigidos a

la capa física del acceso. A partir de ahora se centrara la atención en los ataques con propiedades criptográficas.

3.1.4 ATAQUES CON PROPIEDADES CRIPTOGRÁFICAS.

WEP proporciona confidencialidad de datos por medio de un algoritmo de cifrado de flujo llamado RC4. Los cifrados de flujo funcionan expandiendo una clave secreta (o, como en el caso de WEP, una pública "IV" y una secreta) en una clave arbitrariamente larga de bits seudo aleatorios (el *keystream*). La encriptación se lleva a efecto aplicando or-exclusivos al *texto plano*. La desencriptación consiste en generar un *keystream* idéntico basado en (IV) y la clave secreta, para después aplicar de nuevo la función XOR sobre el texto cifrado.

Una debilidad bien conocida de los algoritmos de cifrado de flujo es que encriptando dos mensajes con la misma clave y vector (IV) se puede revelar información sobre ambos mensajes:

Si **C1 = P1 (+) RC4(v, k)**

y **C2 = P2 (+) RC4(v, k)**

entonces

C1 (+) C2 = (P1 (+) RC4(v, k)) (+) (P2 (+) RC4(v, k))

C1 (+) C2 = P1 (+) P2

En otras palabras, aplicando XOR a los dos textos cifrados (*C1* y *C2*) provocamos la cancelación del *keystream*, y el resultado que obtenemos es el or-exclusivo de ambos textos planos (P1 (+) P2).

Por lo tanto, la reutilización del *keystream* puede llevar a un número de ataques: como caso especial, si el texto plano de uno de los mensajes es conocido, el texto plano del otro está disponible inmediatamente. Más generalmente, los textos planos habituales que se manejan a menudo tienen una redundancia suficiente como para permitir recuperar *P1* y *P2* dado sólo P1 (+) P2; existen técnicas conocidas como, por ejemplo, resolver este problema buscando dos textos en inglés sobre los que, aplicados a un XOR, resulten en el valor dado P1 (+) P2. Es más, si tenemos *n* textos cifrados en los que se reutilice un mismo *keystream* tendremos lo que comúnmente se denomina un problema de profundidad *n*. Descifrar el tráfico en profundidad se facilita en tanto en cuando *n* aumente, ya que el resultado del XOR de cada par de textos planos puede ser calculado, y se conocen varias técnicas clásicas para resolver esta clase de problemas (por ejemplo el análisis de frecuencias, y demás).

Hágase notar que se requieren dos condiciones para que esta clase de ataque tenga éxito:

- La disponibilidad de textos cifrados en lo que alguna porción del *keystream* sea utilizado más de una vez.
- Un conocimiento parcial de parte del texto plano.

Para prevenir estos ataques, WEP utiliza un (IV) diferente por cada paquete para variar el proceso de generación del *keystream* para cada trama de datos transmitida. WEP genera el *keystream* RC4(v, k) como una función de la clave secreta *k* (que es la misma para todos los paquetes) y un vector de inicialización público *v* (que cambia para cada paquete); de este modo, cada paquete recibe un *keystream* diferente. El vector (IV) se incluye en la parte no encriptada de la transmisión, de modo que el receptor pueda saber qué debe utilizar el (IV)para obtener el *keystream* necesario para la decodificación. (IV) está por tanto disponible también para los agresores, pero la clave secreta sigue siendo desconocida y mantiene la seguridad del *keystream*.

El uso de un (IV) diferente por cada paquete tiene la intención de prevenir ataques derivados de la reutilización reiterada de un mismo *keystream*. A pesar de todo, WEP no consigue alcanzar esta meta. Se describira a continuación varios casos prácticos de ataques al WEP basados en la reutilización del *keystream*. Antes de nada, se comentara cómo localizar casos de reutilización de *keystream*; entonces se mostrara cómo aprovechar estos casos sacando ventaja de información parcial que se espera contengan los textos planos más comunes.

Una debilidad potencial de la reiteración del *keystream* puede producirse por una gestión inadecuada de (IV). Nótese que, puesto que por lo general la clave compartida *k* no cambia, la reutilización de IV's casi siempre provoca la reutilización de claves *keystream*. Ya que los IV's son públicos, el duplicado de IV's puede ser fácilmente detectado por los posible agresores. Por lo tanto, cualquier reciclado de valores de (IV) expone el sistema a ataques por reutilización de un mismo *keystream*. Nos referiremos a tales reiteraciones de valores de IV como *colisión*.

El estándar WEP recomienda (pero no requiere) que (IV) cambie en cada paquete. Sin embargo, no dice nada acerca de los mecanismos aconsejables para seleccionar IV's y, por esta razón, algunas implementaciones del sistema lo hacen precariamente. En concreto, las tarjetas PCMCIA reestablecen IV a 0 cada vez que eran reiniciadas, e incrementaron IV en uno en cada paquete posterior. Estas tarjetas se reinician automáticamente cada vez que se introducen en un portátil, algo que se espera pase a menudo. En consecuencia, los *keystream* correspondientes a IV's de valor bajo son susceptibles de ser reutilizados muchas veces durante el tiempo de vida de la clave privada.

Este estándar WEP tiene defectos de arquitectura que exponen a todas las implementaciones WEP sin importar lo cuidadoso de su implementación a riesgos serios de reutilización del *keystream*. El campo IV utilizado en WEP tiene una longitud de tan sólo 24 bits, prácticamente garantizando que se usará un mismo IV en múltiples mensajes. Un cálculo rápido muestra que un Punto de Acceso ocupado que transmita paquetes de 1500 bytes a una media de 5Mbps de ancho de banda (la velocidad máxima correspondería a 11Mbs) agotará todos los valores posibles de IV en menos de doce horas. Incluso en instalaciones con menor ocupación de canal, un agresor paciente puede encontrar duplicados fácilmente. Dado que la longitud de IV está predefinida en 24 bits, sin dependencia de otros parámetros, esta vulnerabilidad es inevitable.

Detalles de implementación pueden provocar reusos del *keystream* más frecuentemente. Una implementación que utilize un (IV) aleatorio para cada paquete produciría una *colisión* cada 5000 paquetes aproximadamente, que se resumen en tan sólo varios minutos de transmisión. El estándar 802.11 no exige que (IV) cambie en cada paquete, lo que podría permitir el uso de un (IV) idéntico en todos los paquetes sin que ello suponga una disconformidad con la norma estándar.

3.1.5 LA REUTILIZACIÓN DEL KEYSTREAM

Una vez localizados dos paquetes con el mismo (IV) se pueden aplicar varios métodos para recuperar el texto plano. Si el texto plano de uno de los mensajes es conocido resulta sencillo derivar directamente los contenidos del otro.

Muchos campos del tráfico IP son predecibles, ya que los protocolos utilizados usan estructuras de mensaje perfectamente conocidas con contenidos predecibles. Por ejemplo, las secuencias de entrada a sistemas son bastante uniformes para la mayor parte de los usuarios, y también lo son los contenidos por ejemplo, la palabra *Password:* como mensaje de bienvenida, que pueden ser utilizados para ataques a la clave. Otro ejemplo podría consistir en la posibilidad de reconocer por análisis de tramas de tráfico y longitud una librería compartida que estuviese siendo transferida en un sistema de red. Esto suministraría una gran cantidad de texto plano conocido que permitiría su utilización para realizar una ataque al *keystream* por reutilización.

Hay métodos más arteros para obtener el texto plano. Por ejemplo, es posible provocar la transmisión de textos planos conocidos enviando tráfico directamente al terminal móvil desde un ordenador conectado a internet en manos del agresor. El agresor también puede enviar correo electrónico a usuarios y esperar que lo descarguen por medio del enlace inalámbrico. Enviar correo no solicitado (*Spam*) puede ser un buen método para hacer esto sin levantar sospechas.

A veces obtener texto plano conocido puede ser incluso más sencillo. Un Punto de Acceso emite paquetes broadcast de modo encriptado y no encriptado cuando la opción de controlar el acceso a la red estaba desactivada. En este caso, un agresor con una tarjeta 802.11b puede transmitir broadcasts al punto de acceso (que serán aceptados, porque el control de acceso está desactivado) y observar su forma encriptada durante la retransmisión. Es inevitable que esto suceda en una subred que contiene una mezcla de clientes WEP con otros sin soporte para encriptación, ya que los paquetes broadcast deben llegar a todos y cada uno de los clientes; no hay forma de evitar esta técnica para recoger texto plano conocido.

Como conclusión a este apartado se recuerda que, como se indicó con anterioridad, incluso sin conocer ningún texto plano todavía es posible analizar, por medio de suposiciones, posibles textos planos susceptibles de ser transmitidos que puedan desembocar en la obtención del la clave privada.

3.1.6 DICCIONARIOS DE DESENCRIPTACIÓN

Una vez que se obtiene el texto plano de un mensaje interceptado el agresor puede aislar el valor del *keystream* utilizado para encriptar el mensaje, ya sea por análisis de IV's o por otros métodos. Es posible usar este *keystream* para desencriptar cualquier otra trama que utilice un mismo IV. Según transcurre el tiempo, el agresor puede construir una tabla de *keystreams* que correspondan a distintos (IV). La tabla completa requerirá poco espacio –unos 1500 bytes por cada una de las 2^{24} (IV) posibles, así que es concebible que un agresor dedicado pueda, después de un poco de esfuerzo, acumular datos suficientes como para construir todo un diccionario de decodificación, especialmente cuando consideramos que las claves sólo son cambiadas de forma ocasional.

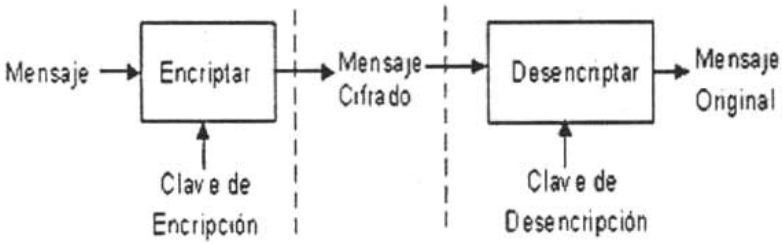


Fig.3.3 Diagrama a Bloques del Proceso de Encriptación y Desencriptacion

La ventaja para el agresor radica en que una vez que tiene la tabla disponible es posible desencriptar inmediatamente cada texto cifrado con muy poco esfuerzo.

Desde luego, la cantidad de trabajo necesario para construir semejante diccionario restringe este ataque sólo a lo individuos más persistentes, que deseen emplear tiempo y dinero en vencer la seguridad WEP. Podría decirse que WEP no está diseñado para defenderse de tales ataques, ya que las claves de 40 bits se pueden descubrir fácilmente por medio de la fuerza bruta en una cantidad de tiempo relativamente corta con recursos moderados. A pesar de todo, los fabricantes ya han comenzado a extender WEP con soporte para claves más largas, aunque esto no implique cambio alguno en el tamaño efectivo del diccionario del agresor (el tamaño del diccionario no depende de la longitud de la clave, sino del tamaño de (IV), que está prefijado en 24 bits).

Es más, el diccionario del agresor puede hacerse más práctico aprovechando el comportamiento de las tarjetas PCMCIA que reinician el vector (IV) a 0 cada vez que son reiniciadas. Puesto que en los casos más comunes las tarjetas son iniciadas al menos una vez al día, el agresor puede limitarse a construir un diccionario centrado sólo en los primeros miles de IV's, lo que le permitirá desencriptar la mayoría de los paquetes que circulen a través del punto de acceso. En una red con numerosos clientes 802.11b, las colisiones en los primeros miles de IV's serán abundantes.

3.1.7 GESTIÓN DE CLAVES

El estándar 802.11b no especifica cómo llevar a cabo la distribución de claves. Depende de un mecanismo externo para poblar la matriz de cuatro claves compartida globalmente. Cada mensaje contiene un campo identificador de clave especificando el índice de la matriz que se utiliza para la encriptación. El estándar también permite asociar una clave específica de la matriz para cada estación móvil; sin embargo, está práctica no es habitual. La mayoría de las instalaciones usan una única clave para la toda red.

Esto perjudica severamente la seguridad del sistema, puesto que un secreto compartido por muchos no es fácil de ocultar. Algunos administradores de red intentan aliviar este problema no revelando la clave secreta a los usuarios, configurando ellos mismos cada terminal. Sin embargo esta forma de actuar sólo conduce a una mejora mínima, ya que las contraseñas siguen permaneciendo almacenadas en los terminales clientes. Como ejemplo, basta mencionar que se conoce a un grupo de estudiantes universitarios que obtuvieron la clave privada de la red simplemente para poder usar sistemas operativos no soportados por los administradores de red.

La reutilización de una clave única por muchos usuarios ayuda también a convertir los ataques en algo más práctico, porque aumenta la posibilidad de

colisión de IV's. La posibilidad de una colisión casual aumenta proporcionalmente con número de usuarios, y si además tenemos en cuenta que las tarjetas PCMCIA establecen a 0 el vector (IV) cada vez que son reiniciadas todos los usuarios reutilizarán *keystreams* correspondientes a un pequeño rango de IV's. El hecho de que muchos usuarios compartan las mismas claves también significa que es difícil sustituir esta información, porque resulta comprometido ponerla en boca de todos.

Además esto no será habitual puesto que cambiar una clave requiere que todos y cada uno de los usuarios reconfiguren su adaptador inalámbrico. En la práctica se estia que puedan pasar meses, o incluso más tiempo, antes de que se cambien las claves privadas, lo que permite al agresor disponer de una generosa cantidad de tiempo para buscar instancias de reutilización de *keystreams*.

Los ataques descritos demuestran que el uso de cifrados de flujo es peligroso porque la reutilización de *keystreams* puede tener consecuencias devastadoras. Cualquier protocolo que utilice un cifrado de flujo debe prestar especial cuidado en asegurar que el *keystream* nunca sea reutilizado.

Esta propiedad es difícil de imponer. El protocolo WEP contiene vulnerabilidades a pesar del aparente conocimiento por parte de sus autores de los ataques por reutilización. No se trata del primer protocolo en sucumbir ante esta clase de ataques; Bajo estas premisas, un diseñador de protocolos debe prestar especial atención a las complicaciones que supone añadir cifrado de flujo en cualquier algoritmo de encriptación.

3.1.8 CODIGO DE AUTENTICACION

3.1.8.1 AUTENTICACIÓN DE MENSAJES

El protocolo WEP utiliza el campo de *checksum* para verificar la integridad de los paquetes y que estos no sean modificados durante su tránsito. El *checksum* viene implementado como un CRC-32, el cual es parte de la carga encriptada del paquete.

A continuación se expondrá que una suma CRC es insuficiente como para asegurar que un agresor no puede manipular un mensaje: No es un código de autenticación criptográficamente seguro. Los códigos CRC fueron diseñados para detectar errores aleatorios en mensajes; no son resistentes contra ataques maliciosos. Como se demostrará, esta vulnerabilidad del CRC esta exagerada todavía más por el hecho de que los datos del mensaje están encriptados usando un cifrado de flujo.

3.1.8.2 MODIFICACIÓN DEL MENSAJE.

En primera instancia, se mostrará que los mensajes pueden ser modificados en tránsito sin que el cambio sea detectado, violando las metas de seguridad.

Usaremos la siguiente propiedad del los *checksum* WEP:

1ª PROPIEDAD: WEP FUNCION LINEAL

El checksum WEP es una función lineal del mensaje.

Esto quiere decir que la suma de comprobación se distribuye sobre la operación XOR, por ejemplo, c(x (+) y) = c(x) (+) c(y) para todas las elecciones posibles de *x* e *y*. Esta propiedad es genérica para todas las sumas CRC.

Una consecuencia de la propiedad superior es que es posible hacer modificaciones controladas en un texto cifrado sin corromper el CRC. A continuación; un hipotético texto cifrado *C* que se ha interceptado antes de que pudiera llegar a su destino:

$$\mathbf{A \rightarrow (B) : (v, C)}$$

Se Asume que *C* corresponde a un mensaje desconocido *M*, así que:

$$\mathbf{C = RC4(v, k) (+) (M, c(M))}$$

Se mantiene que es posible encontrar un nuevo texto cifrado *C'* que desencripta a *M'*, donde;

$$\mathbf{M' = M (+) d}$$

Y *d* puede ser elegida arbitrariamente por el agresor. Entonces, se estara en disposición de sustituir la transmisión original con el nuevo texto cifrado engañando al origen,

$$\mathbf{(A) \rightarrow B : (v, C')}$$

y en la desencriptación, el receptor *B* obtendrá el mensaje *M'* con CRC correcto.

Lo que resta es describir cómo obtener *C'* desde *C* de forma que *C'* desencripte a *M'* en lugar de *M*. La observación clave es darse cuenta de que los cifrados de flujo, como el RC4, también son lineales, por lo que se puede reordenar los términos. Por ejemplo hagcer un XOR de (d, c(d)) en ambos lados de la primera ecuación que le mostramos arriba para obtener un nuevo texto cifrado *C'*:

$$C' = C (+) (d, c(d))$$

$$C' = RC4(v, k) (+) (M, c(M)) (+) (d, c(d))$$

$$C' = RC4(v, k) (+) (M (+) d, c(M) (+) c(d))$$

$$C' = RC4(v, k) (+) (M', c(M (+) d))$$

$$C' = RC4(v, k) (+) (M', c(M'))$$

En esta derivación, se usa el hecho de que el *checksum* WEP es lineal, o sea, que $c(M) (+) c(d) = c(M (+) d)$. Como resultado, se ha mostrado como modificar *C* para obtener un nuevo texto cifrado *C'* que desencriptará a $P (+) d$. Esto implica que se pueden realizar cambios arbitrarios a un mensaje encriptado sin temor a ser detectado. Por este motivo el *checksum* WEP no cumple proveyendo integridad en los datos, una de sus tres metas principales.

Hágase notar que este ataque puede aplicarse sin un conocimiento total de *M*: el agresor sólo necesita conocer el texto cifrado original *C* y la diferencia en texto plano deseada *d* para poder calcular $C' = C (+) (d, c(d))$. Por ejemplo, para invertir el primer bit de un mensaje, el agresor establecerá $d=1000...0$. Esto permitirá al agresor modificar un paquete solamente con un conocimiento parcial de su contenido.

Ahora se demostrará que WEP no proporciona un control de acceso seguro. Se utilizará la siguiente propiedad del *checksum* WEP:

2ª PROPIEDAD: WEP FUNCION SIN CIFRAR

El checksum WEP es una función sin cifrar del mensaje.

Como consecuencia, el campo *checksum* también puede ser calculado por el adversario que conoce el mensaje.

Esta propiedad de la suma de integridad de WEP permite la evasión de las medidas de control de acceso. Si un atacante puede conseguir un texto plano correspondiente a alguna trama transmitida, estará en disposición de inyectar tráfico arbitrario en la red. Como ya se analizó, el conocimiento del texto plano y el texto cifrado de una misma trama revela el *keystream*. Este *keystream* puede ser reutilizado para crear nuevos paquetes, usando un mismo (IV).

Esto significa que si el agresor alguna vez consigue obtener el texto plano íntegro *P* de cualquier paquete cifrado *C*, puede resolver el *keystream* empleado para encriptar el paquete:

$$\mathbf{P (+) C = P (+) (P (+) RC4(v, k)) = RC4(v, k)}$$

Podría ahora construir la forma encriptada para un mensaje *M'*:

$$\mathbf{(A) -> B : (v, C')}$$

Donde:

$$\mathbf{C' = (M', c(M')) (+) RC4(v, k)}$$

Se hace notar que el mensaje generado utiliza el mismo valor de (IV) que el mensaje original. Por ende, el ataque funciona sólo porque:

3ª PROPIEDAD: REUTILIZACIÓN DE VALORES IV

Es posible reutilizar viejos valores de (IV) sin disparar ninguna alarma en el receptor.

Cuando conocemos un (IV) junto con su correspondiente secuencia *keystream* RC4(v, k), esta propiedad permite reutilizar el *keystream* conocido y burlar el mecanismo de control de acceso WEP.

Una defensa natural contra este ataque podría ser no permitir la reutilización de IV's en múltiples paquetes, requiriendo que todos los receptores se atengan a esta prohibición. Sin embargo, aunque el estándar 802.11b recomiende encarecidamente no utilizar un mismo (IV), no obliga a ello.

Por este motivo cada receptor debe aceptar IV's repetidos o arriesgarse a no ser compatible con dispositivos semejantes. Consideramos esto como una falta del estándar 802.11b.

En redes, uno escucha a menudo la máxima "sea prudente con lo que envía y liberal con lo que acepte". Sin embargo, cuando la seguridad es la meta, esta guía puede ser muy peligrosa: ser liberal con el material que aceptamos significa que cada opción de baja seguridad ofrecida por el estándar ha de ser soportada por todos, y por extensión también disponible para el atacante. Esta situación es análoga a los ataques descubiertos para el cifrado SSL, los cuales también emplean uso de las debilidades de un sistema con un sistema que incluía opciones de alta y baja seguridad. En consecuencia, el estándar 802.11b debería ser más específico respecto a la prohibición del reempleo de IV's y otros comportamientos potencialmente dañinos.

Este ataque no depende de la *Propiedad 1* del *checksum* WEP (linealidad). De hecho, sustituir cualquier función sin cifrar en lugar del CRC no tendrá efectos sobre la viabilidad del ataque. Sólo un mensaje con código cifrado de autenticación (MAC) tal como SHA1-HMAC proveerá suficiente fuerza como para prevenir este ataque.

3.1.9 MANIPULACIÓN DEL PUNTO DE ACCESO

3.1.9.1 DESENCRIPCIÓN DE LOS MENSAJES

Lo que puede resultar sorprendente es que la habilidad para modificar paquetes en el aire sin posibilidad de ser detectados nos lleva a desencriptar paquetes en tránsito. Considerando WEP desde el punto de vista del adversario. Ya que WEP utiliza un cifrado de flujo supuestamente seguro (RC4) atacar a la criptografía directamente carece de sentido. Pero aunque no podamos desencriptar el tráfico por nosotros mismos, todavía hay alguien que puede: el punto de acceso.

En cualquier protocolo criptográfico el desencriptador legítimo debe en todos los casos disponer la clave secreta para desencriptar por definición. La idea es engañar al punto de acceso para que desencripte algún texto cifrado por nosotros. Como se desprende de lo dicho anteriormente, la posibilidad de modificar paquetes transmitidos pone a nuestra disposición dos formas sencillas que explotar al punto de acceso en este sentido.

3.1.10 ATAQUES EN LA DESENCRIPCION DEL MENSAJE

1° ATAQUE: REDIRECCIÓN IP

El primero recibe el nombre de Ataque de "redirección IP", y puede ser empleado cuando el punto de acceso WEP opera como un enrutador IP con conexión a Internet; algo habitual, porque WEP se emplea normalmente para suministrar acceso a usuarios móviles y otros.

En este caso, la idea es capturar un paquete encriptado del aire, y emplear la técnica de Modificación del Mensaje para modificarlo de modo que tenga una nueva dirección de destino: una que controle el agresor. El punto de acceso decodificará el mensaje y lo reenviará a su nuevo destino, donde el agresor podrá leer el paquete, ahora sin encriptar. Hágase notar que nuestro paquete modificado viajará desde la red inalámbrica hacia Internet, y por ese motivo la mayoría de los firewalls permitirán su tránsito sin ninguna traba.

2° ATAQUE: MODIFICANDO LA IP DE DESTINO

El método más sencillo para modificar la IP de destino consiste en imaginar la dirección de destino original y entonces aplicar la técnica descrita en la Modificación del Mensaje para cambiarla por otra cualquiera. Hacerse una idea de la dirección de destino original suele ser sencillo; por ejemplo, todo el tráfico entrante tendrá como destino una IP correspondiente a la subred inalámbrica, la cual debería ser sencilla de determinar. Una vez que el tráfico entrante es desencriptado, la dirección IP de los otros extremos se revela, y el tráfico saliente puede ser desencriptado del mismo modo.

Para que este ataque funcione no sólo se ha de modificar la dirección de destino, sino que además hay que asegurarse de que el *checksum* IP del paquete modificado es correcto –de otra forma, el paquete sería rechazado por el punto de acceso.- Puesto que el paquete alterado difiere del original sólo en la dirección IP de destino, y ya que ambos valores de IP –original y modificado- se conocen, podemos calcular el *checksum* para después aplicarlo al paquete.

Supongamos que las palabras de 16 bits más y menos significantes de la dirección IP de destino fueran *DH* y *DL*, y que quisieramos cambiarlas a *D'H* y *D'L*. Si el antiguo *checksum* fuera *X* (que no tiene por qué ser necesariamente conocido, ya que está encriptado), el nuevo sería;

$$X' = X + D'H + D'L - DH - DL$$

Donde las sumas y restas corresponden a operaciones de complemento a uno. El reto reside en que sólo sabemos cómo modificar un paquete aplicando un XOR, y que no estamos obligados a saber qué valor necesitamos aplicar a *X* para obtener *X'*, incluso a pesar de que sabemos lo que necesitamos sumar (o sea, D'H + H'L – DH – DL).

3.1.11 INTENTAR CORREGIR EL CHEKSUM DEL IP

Ahora se discutirá tres mecanismos para intentar corregir el *checksum* IP del paquete modificado:

3.1.11.1 CONOCIENDO EL CHECKSUM DEL IP ORIGINAL

Si esto sucediera, entonces se calcularia *X'* según la fórmula anterior, y modificaremos el paquete aplicando un XOR en X (+) X', lo que ajustaría el *checksum* IP al valor correcto para *X'*.

3.1.11.2 DESCONOCIENDO EL CHECKSUM DEL IP ORIGINAL

Si desconocemos *X* la labor se complica. Dado E = X' – X, necesitamos calcular d = X' (+) X.

De hecho, no hay información suficiente para calcular *d* dado sólo *E*. Por

Ejemplo, si **E = 0xCAFE,** podría ser que:

X' = 0xCAFE, X = 0x0000, así que D = 0xCAFE

X' = 0xD00D, X = 0x050F, así que D = 0xD502

X' = 0x1EE7, X = 0x53E8, así que D = 0x4D0F

Sin embargo, no todos los 2^{16} valores posibles son válidos para *d*, y algunos son mucho más probables que otros. En el ejemplo superior se tienen cuatro valores para *d* (0x3501, 0x4B01, 0x4D01, 0x5501) que se dan menos del 3% de las veces. cualquier asunción incorrecta será silenciosamente ignorada por el Punto de Acceso.

Dependiendo del valor de *E*, se pueden intentar un pequeño número de intentos con alto porcentaje de éxito. Finalmente, la desencriptación exitosa de un paquete puede ser empleada para fomentar la desencriptación de otros; por ejemplo, el único campo que varía en la cabecera IP entre dos máquinas que mantenga un flujo de comunicación es el identificador de cabecera. Por esto, el conocimiento de la cabecera IP completa de un paquete puede ser utilizado para predecir la cabecera de paquetes circundantes, o para estrechar la búsqueda a un pequeño abanico de posibilidades.

3.1.11.3 CONSEGUIR QUE X = X'

Otra posibilidad es compensar el cambio aplicado en el campo de destino por un cambio en otro campo, tal que el *checksum* para el paquete permanezca intacto. Cualquier campo de cabecera conocido que no afecte al envío del paquete es susceptible de ser útil, como por ejemplo el campo de IP de origen. Asumiendo que la dirección IP de origen de un paquete que se quiera desencriptar sea conocida (se puede obtener, por ejemplo, efectuando alguno de los ataques descritos anteriormente), basta conque sustraigamos *E* de los 16 bits menos significativos de la IP de origen, y tendremos un paquete con el mismo *checksum* que el original.

Sin embargo, es posible que al modificar la dirección de origen de esta forma el paquete sea rechazado, basándose en reglas de filtrado; pueden emplearse otros campos del encabezado para ajustar el *checksum*.

Agresores con recursos avanzados monitoreando una red de clase B completa podrían incluso realizar los ajustes necesarios sólo en el campo de destino, eligiendo D'L = DH + DL – D'H. Si el destino original para un paquete es 10.20.30.40 y el agresor controla la subred 192.168.0.0/16 seleccionando la dirección 192.168.103.147 obtenemos un *checksum* idéntico para ambos paquetes, pero el paquete será enviado a una dirección de su control.

3.1.12 MONITOREANDO EL PAQUETE TCP

Hay otro método para manipular un punto de acceso y romper la seguridad WEP que es aplicable siempre y cuando WEP sea empleado para proteger tráfico TCP/IP. Este ataque no requiere conectividad a Internet, así que podría aplicarse incluso cuando los ataques de redirección son imposibles. A pesar de todo, sólo es efectivo contra tráfico TCP; otros protocolos IP no pueden ser desencriptados utilizando esta técnica.

Se puede monitorear, la reacción de un receptor de un paquete TCP, para deducir información sobre el texto plano desconocido. Un paquete TCP es aceptado sólo si el *checksum* TCP es correcto, y cuando es aceptado, se envía un paquete de confirmación como respuesta. Hágase notar que los paquetes de confirmación son fácilmente identificables por su tamaño, sin que requieran ser desencriptados. Por este motivo, la reacción del receptor revelará cuándo el *checksum* es válido cada vez que un paquete es desencriptado.

El ataque se efectúa según lo siguiente. Se Intercepta un texto cifrado (v, C) con un texto plano desconocido *P*.

A -> (B) : (v, C)

Se invierte unos cuantos bits en *C* y se ajusta el CRC encriptado, obteniendo un nuevo texto cifrado *C'* con un *checksum* WEP válido. Transmitimos *C'* al punto de acceso:

(A) -> B : (v, C')

Por último, se observa si el eventual receptor devuelve un paquete TCP ACK; esto nos descubrirá si el texto modificado pasó las comprobaciones *checksum* TCP y si fue aceptado por el receptor.

Téngase en cuenta que se puede elegir los bits de *C* e invertirlos de la forma que quiera, usando técnicas antes descritas.

El truco es el siguiente: Con una elección inteligente de los bits que se inviertan, se puede asegurar que el *checksum* TCP permanece inalterado exactamente cuando la condición Pi (+) Pi+16 = 1 se mantiene en el texto plano -condición de un sólo bit-. Por ende, la presencia o ausencia de un paquete ACK

revelará un bit de información del texto plano *P*. Repitiendo el ataque para muchos valores de *i*, podemos obtener prácticamente todo el texto plano *P*, deduciendo las pocas variables que resten con técnicas clásicas.

Más adelante se explicará cómo elegir qué bits alterar. Por ahora, los detalles no son demasiado importantes. Lo principal es que hemos explotado la buena voluntad del receptor para desencriptar textos cifrados arbitrarios. La respuesta del receptor a nuestro paquete –ya sea aceptar o ignorar- puede ser vista como un canal secundario, semejante a aquellos explotados en ataques de consumo de potencia y capacidad de respuesta, que permite aprender sobre el texto plano, utilizando al receptor como oráculo que desencripte el texto crifrado por nosotros. Esto se conoce como ataque de reacción, *ya que* funciona analizando las reacciones del receptor ante nuestras falsificaciones.

Inicialmente los ataques de reacción fueron descubiertos por Bellovin y Wagner, en el contexto del protocolo IPSec, lo que provocó la inclusión de MAC para la autenticación de los mensajes. Como resultado, Bellovin propuso un principio de diseño para IPSec: todos los modos de operación encriptados deberían emplear MAC. Lo mismo debería aplicar a los protocolos WEP, lo que prevendría estos ataques.

3.1.13 DETALLES TÉCNICOS

Hasta ahora se he aplazado la explicación de los detalles técnicos sobre cómo elegir nuevos paquetes *C'* que engañen al receptor para ir resolviendo el texto plano *P*.

Se recuerda que el *checksum* TCP es la suma en complemento a uno de las palabras de 16 bits del mensaje *M*. Es más, la suma en complemento a uno es equivalente más o menos a la suma módulo $2^{16} - 1$. De aquí se desprende que, hablando aproximadamente, el *checksum* TCP de un texto plano *P* es válido sólo cuando *P* equivale a 0 mod $2^{16} - 1$.

Se define $C' = C (+) d$, de modo que *d* especifique qué posición de bit invertir, eligiendo *d* como sigue: se escoge un *i* arbitrariamente, se ponen los bits *i* e *i + 16* en *D* a uno, y cero en las demás posiciones. La propiedad clave de la suma módulo de $2^{16} - 1$ es que $P (+) D$ es equivalente a P mod $2^{16} - 1$ mientras $Pi (+) Pi+16 = 1$.

Puesto que se asume que el *checksum* TCP es válido para el paquete original (*P* equivale a 0 mod $2^{16} - 1$), esto significa que el *checksum* TCP será válido para el nuevo paquete ($P (+) D = 0$ mod $2^{16} - 1$) justamente cuando $Pi (+) Pi+16 = 1$. Este mecanismo ofrece un bit de información del texto plano, como se ha comentado.

En esta sección, se ha mostrado la importancia de utilizar códigos de autenticación de mensajes seguros, como SHA1-HMAC*, para proteger la integridad de las transmisiones. El uso de CRC es inapropiado para este propósito, y de hecho cualquier función sin codificar falla a la hora de defenderse contra los ataques descritos en esta sección.

Un MAC seguro es particularmente importante a la hora de diseñar protocolos, ya que la pérdida de integridad en los mensajes en una capa del sistema puede llevar a romper el secreto en el sistema global.

3.1.14 MEDIDAS DE SEGURIDAD DE WEP

Un administrador de red dispone de opciones de configuración que puede reducir la viabilidad de los ataques descritos. La mejor alternativa es disponer la red inalámbrica fuera del Firewall de la organización. Es más sencillo considerar que está expuesta a los mismos riesgos que una conexión a Internet que intentar asegurar la infraestructura inalámbrica.

El cliente típico de una red inalámbrico es un ordenador portátil, móvil por naturaleza, y empleará con frecuencia soluciones VPN para acceder a los ordenadores que se encuentren dentro del Firewall cuando lo haga a través de conexiones telefónicas. Exigir que la misma VPN sea también utilizada para las conexiones sobre 802.11b elimina la necesidad de procurar seguridad al nivel de enlace.

* Algoritmos de integridad "HMAC: Keyed-hashing for message authentication"

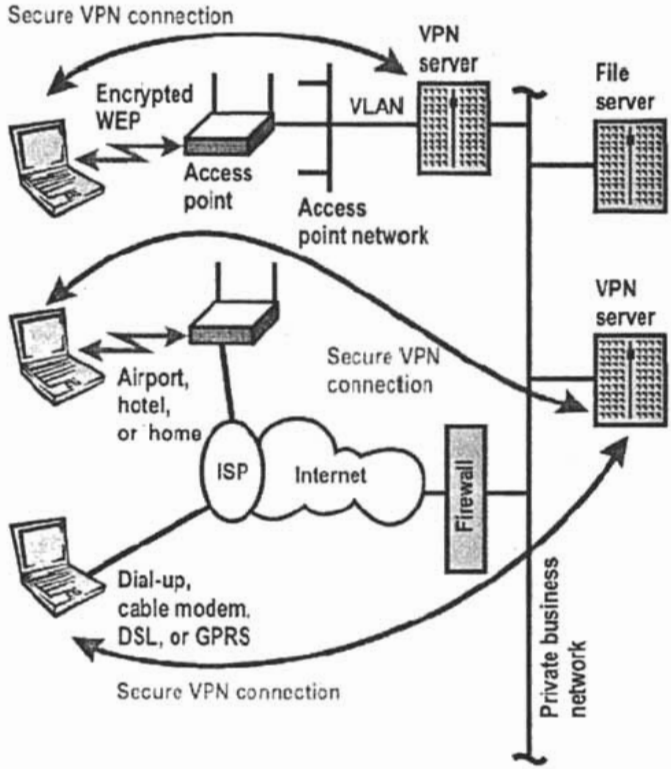


Fig. 3.4 Seguridad Inalámbrica VPN

Para ofrecer control de acceso, la red puede ser configurada de forma tal que no existan rutas hacia Internet desde el interior de la red inalámbrica. Así prevenimos que personas ajenas que se encuentren dentro del área de cobertura de radio usurpen el ancho de banda de Internet (a pesar de esto, sería deseable permitir a los visitantes acceder a Internet de modo inalámbrico sin la necesidad de configuraciones administrativas adicionales).

Una medida adicional muy útil es mejorar la gestión de la clave de cualquier instalación inalámbrica. Siempre que sea posible, cada ordenador debería tener su propia clave de encriptación, y las claves deberían ser cambiadas con frecuencia. El diseño de un mecanismo para la distribución automática de claves para todos los usuarios seguro y fácil de utilizar es un buen tema de estudio. Sin embargo, una buena gestión de claves no soluciona todos los problemas descritos en este documento; en particular, los ataques ya descritos seguirían siendo aplicables.

3.1.15 CONSIDERACIONES ACERCA DE WEP

Los ataques descritos en este documento sirven para demostrar un hecho bien conocido en la comunidad criptográfica: el diseño de protocolos es difícil, y está plagado de complicaciones. Requiere habilidades especiales que van más allá de las adquiridas en la ingeniería de protocolos de red. Un buen entendimiento de las primitivas criptográficas y sus propiedades es crítico. Desde un punto de vista de ingeniería, el uso de CRC-32 y RC4 se justifica por su velocidad y facilidad de implementación. Sin embargo, muchos de los ataques descritos dependen de las propiedades de los cifrados en flujo y CRC's, que podrían haberse vuelto inocuos con el empleo de otros algoritmos. Existen otras interacciones más sutiles con las decisiones de ingeniería que no dependen directamente del uso de la criptografía.

Por ejemplo, los protocolos aceptados es un principio reconocido en la ingeniería de redes. Pero desde la perspectiva de la seguridad estos principios son peligrosos, dado que ofrecen al agresor mayor libertad de acción y, por extensión, los ataques por inyección de tráfico se magnifican con esta libertad. La seguridad es una propiedad que afecta al sistema completo, y cada decisión debe ser estudiada con la seguridad en mente.

Los diseños anteriores deberían ser utilizados siempre que fuera posible. WEP podría haberse beneficiado de la experiencia ganada en el diseño del protocolo IPSec. A pesar de que los objetivos de IPSec son de alguna manera diferentes, también apunta a proveer seguridad a nivel de enlace, y como tal necesita enfrentarse con muchas cuestiones semejantes a las de WEP.

Incluso si el protocolo no pudiera utilizarse tal cual, un vistazo a su diseño y análisis hubiesen sido instructivos. Algunos de los problemas sobre IPSec comparten similitud con los ataques presentados en este documento.

3.1.16 ALTERNATIVAS AL CIFRADO WEP

En este documento se ha dejado constancia de las mayores vulnerabilidades de seguridad en el protocolo WEP, a la par que descrito varios ataques prácticos que resultan de ellas. Consecuentemente, recomendamos que WEP no sea considerado como un protector total de la seguridad a nivel de enlace, y que se tomen medidas adicionales para asegurar el tráfico de red. Esperamos que nuestros descubrimientos motiven un rediseño del protocolo WEP que solvente los defectos encontrados. El objetivo de este capitulo es que exponga principios importantes de seguridad y prácticas de diseño para la gran audiencia, y que las lecciones que se identifican beneficien a futuros diseñadores de WEP y otros protocolos de seguridad para comunicaciones móviles.

El cifrado WEP no es muy seguro en realidad. es un algoritmo de cifrado deficiente. Actualmente, existe software que explota un enorme agujero de seguridad en el estándar de cifrado. Este software escucha el tráfico de red cifrado, lo analiza, y después sólo de unas horas revela la contraseña para entrar en la red en texto en claro. Cuanto más tráfico en la red, más fácil es encontrar el password.

Este sistema es reemplazado por el sistema Wi-Fi Protected Access o WPA que ofrece métodos más robustos para el cifrado y la autenticación.

3.2 SSID (SERVICE SET IDENTIFIER)

Definido también en el 802.11b, el procedimiento SSID (Service Set Identifier) el Identificador de Conjunto de Servicios incluye un identificador único en la cabecera de los mensajes que actúa como contraseña cuando un dispositivo quiere conectarse al sistema. Dado que un "jacker" puede capturarlo del texto del mensaje incorpora poca seguridad.

Desde sus comienzos, 802.11b ha proporcionado algunos mecanismos de seguridad básicos para impedir que esta libertad mejorada sea una posible amenaza. Por ejemplo, los puntos de acceso (o conjuntos de puntos de acceso) 802.11b se pueden configurar con el Identificador del Conjunto de Servicios.

La tarjeta NIC también debe conocer este SSID para asociarlo al AP y así proceder a la transmisión y recepción de datos en la red. Esta seguridad, si se llegase a considerar como tal, es muy débil debido a estas razones:

- Todas las tarjetas NIC y todos los AP conocen perfectamente el SSID
- El SSID se envía por ondas de manera transparente (incluso es señalizado por el AP)
- La tarjeta NIC o el controlador pueden controlar localmente si se permite la asociación en caso de que el SSID no se conozca
- No se proporciona ningún tipo de cifrado a través de este esquema

Aunque este esquema puede plantear otros problemas, esto es suficiente para detener al intruso más despreocupado.

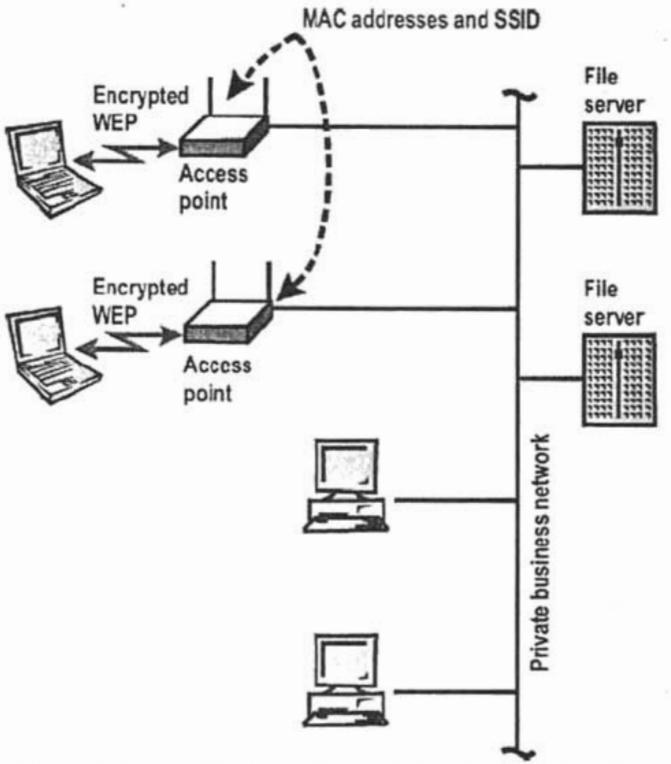


Fig. 3.5 Seguridad 802.11b usando SSID, filtro en la dirección MAC y WEP

3.3 FILTRADO EN LA DIRECCIÓN MAC

Otro procedimiento de seguridad es el filtrado. Las WLAN garantizan el acceso a la red a cualquier PC que lo solicite y para evitar accesos no autorizados se utiliza el filtrado. En toda red de área local, ya sea inalámbrica o no, todo elemento hardware tiene una dirección MAC (Control de Acceso al Medio) única y permanente que no se puede cambiar. Esta dirección MAC es un atributo de la tarjeta NIC y no del dispositivo donde esté alojada.

Está formada por 48 bits que se suelen representar mediante dígitos hexadecimales que se agrupan en seis pares (cada par se separa de otro mediante dos puntos ":" o mediante guiones "-"). Por ejemplo, una dirección MAC podría ser **E1:B1:CF:3D:4A:AA** .

Normalmente viene impresa en la tarjeta de red, aunque también se puede consultar mediante el comando *ipconfig /all* en MS-DOS.

En Windows 2000 o XP pulsamos en *Inicio -> Ejecutar -> cmd.*
Se abrirá la ventana del intérprete MS-DOS, en la que introducimos el comando *ipconfig /all.*

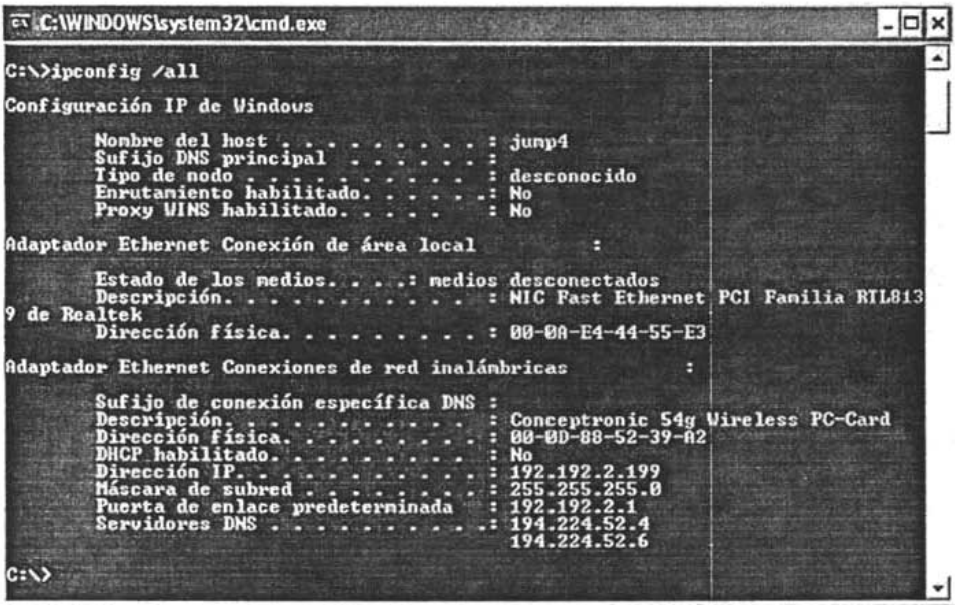


Fig. 3.6 Editor de comandos que revela la MAC

Al activar el filtrado de direcciones MAC del router estamos autorizando el acceso al mismo únicamente a las tarjetas de red que introduzcamos en la lista.

Dentro de la seguridad de las redes, la máxima preocupación es limitar, evidentemente, quien conecta y quien no. A parte, también cabe destacar la privacidad de los datos. En una red Ethernet clásica generalmente se limitaba a establecer una barrera en la conexión a Internet, puesto que se partía de que desde dentro de la red (los propios usuarios) no fuesen a atacar su propio sistema.

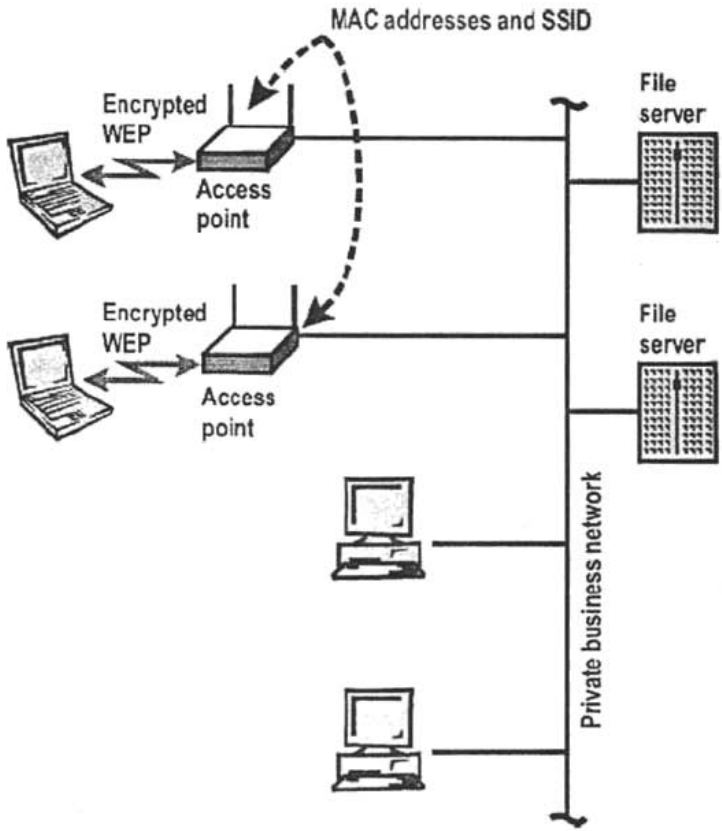


Fig. 3.7 802.11 usando SSID, Filtrado en la MAC Address y WEP

En la implementación de las redes wireless se crea una facilidad física para conectar pero un inconveniente a su vez: eliminar las barreras físicas de la privacidad de la información. Así al radiar en todas direcciones y no poder "frenar" el flujo de paquetes (que salgan del edificio, etc...) se crea una necesidad de encriptarlos para ocultar ante miradas indiscretas su contenido.

Los Routers Ethernet y los puntos de acceso de la red de área local deben tener la capacidad de filtrado de todas las transmisiones que se realicen de acuerdo con una lista de direcciones MAC que todos ellos tienen para autorizar el acceso a la red, pero esta característica no la tienen todos los equipos, por lo que es conveniente asegurarse de su implantación, ya que el filtrado es una herramienta de seguridad cómoda y eficiente.

3.4 PROTOCOLO DE SEGURIDAD: 802.1X

Para ofrecer una mayor seguridad de la que proporciona WEP, el equipo de conexiones de red de Windows XP ® trabajó con IEEE, distribuidores de red y otros colaboradores para definir IEEE 802.1X. que es un borrador de estándar para el control de acceso a redes basado en el puerto que se utiliza para proporcionar acceso a red autenticado para las redes Ethernet.

Fig. 3.8 Logo Microsoft® Windows®XP, IEEE®

Este control de acceso a red basado en puerto utiliza las características físicas de la infraestructura LAN conmutada para autenticar los dispositivos conectados a un puerto LAN. Si el proceso de autenticación no se realiza correctamente, se puede impedir el acceso al puerto. Aunque este estándar se ha diseñado para redes Ethernet con cable, se puede aplicar a las redes LAN inalámbricas 802.11.

Concretamente, en el caso de las conexiones inalámbricas, el punto de acceso actúa como autenticador para el acceso a la red y utiliza un servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) para autenticar las credenciales del cliente. La comunicación es posible a través de un "puerto no controlado" lógico o canal en el punto de acceso con el fin de validar las credenciales y obtener claves para obtener acceso a la red a través de un "puerto controlado" lógico. Las claves de que dispone el punto de acceso y el cliente como resultado de este intercambio permiten cifrar los datos del cliente y que el punto de acceso lo identifique. De este modo, se ha agregado un protocolo de administración de claves a la seguridad de 802.11b.

Los pasos siguientes describen el planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red.

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando una estación inalámbrica entra en el alcance del punto de acceso, éste envía un desafío a la estación.

- Cuando la estación recibe el desafío, responde con su identidad. El punto de acceso reenvía la identidad de la estación a un servidor RADIUS que realiza los servicios de autenticación.

- Posteriormente, el servidor RADIUS solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad. La estación envía sus credenciales al servidor RADIUS (a través del "puerto no controlado" del punto de acceso).

- El servidor RADIUS valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.

- El punto de acceso utiliza la clave de autenticación para transmitir de manera segura las claves correctas a la estación, incluida una clave de sesión de unidifusión para esa sesión y una clave de sesión global para las multidifusiones.

Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.

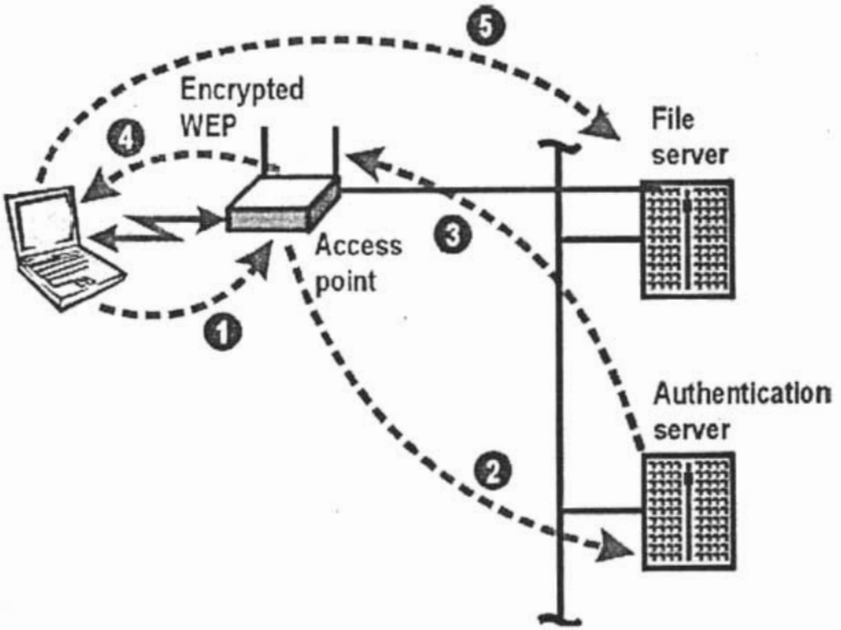


Fig. 3.9 802.1x /Autenticación RADIUS

1. El Usuario requiere Autenticación del AP para acceder a la Red.
2. Se Encriptan las credenciales para enviar la autenticación al Servidor Radius.
3. La Autenticación del Servidor valida al Usuario y garantiza el acceso.
4. El Puerto del AP es habilitado y las llaves WEP son asignadas al cliente
5. El Usuario Inalámbrico accesa a la Red General de Servicios.

3.4.1 SERVIDOR RADIUS

Este planteamiento de 802.1x saca partido del uso extendido y creciente de RADIUS para la autenticación. Un servidor RADIUS puede realizar consultas en una base de datos de autenticación local si ello es adecuado para el escenario. O bien, la solicitud puede transmitirse a otro servidor para su validación.

Cuando RADIUS decide que se puede autorizar el equipo en esta red, vuelve a enviar el mensaje al punto de acceso y éste permite que el tráfico de datos fluya hacia la misma. Para ofrecer este nivel de seguridad, Microsoft incluye una implementación del cliente 802.1X en Windows XP y mejora el servidor RADIUS de Windows, el servidor de autenticación de Internet (IAS), para admitir la autenticación de dispositivos inalámbricos.

Microsoft también ha trabajado con muchos distribuidores de dispositivos 802.11 para que admitan estos mecanismos en sus controladores NIC y en el software de punto de acceso. Actualmente, muchos de los principales distribuidores incluyen o pronto incluirán la compatibilidad con 802.1x en sus dispositivos.

3.5 PROTOCOLO DE SEGURIDAD: WPA

Los consorcios reguladores, conscientes de la gravedad de la debilidad de el Algoritmo WEP y su fuerte impacto en el crecimiento de las WLAN, han propuesto una recomendación denominada WPA (Wi-Fi Protected Access) que conjuga todas las nuevas técnicas anteriormente expuestas.

Fig. 3.10 Interoperabilidad WPA

El procedimiento WAP se ha sido anunciado por Wi-Fi Alliance con el fin de sustituir a WEP. WAP necesita una clave maestra por cada usuario.

Esta clave maestra es una contraseña que WAP utiliza para generar una clave para cifrar el tráfico de la red y esta clave de cifrado es generada automáticamente usando la clave maestra cada vez que se produce una transmisión, lo que aumenta sensiblemente la seguridad. WAP ha sido diseñada como una mejora de WEP por lo que la mayoría de los dispositivos inalámbricos podrán ser actualizados a esta nueva tecnología.

La autenticación de WPA se basa en las especificaciones de 802.1x, la cual utiliza el RFC 2284 Protocolo de Autenticación Extendida (EAP), que es una extensión del Protocolo Punto a Punto (PPP) para proveer autenticación centralizada de usuario y/o red inalámbrica, así como el manejo de claves de encripción y de su distribución.

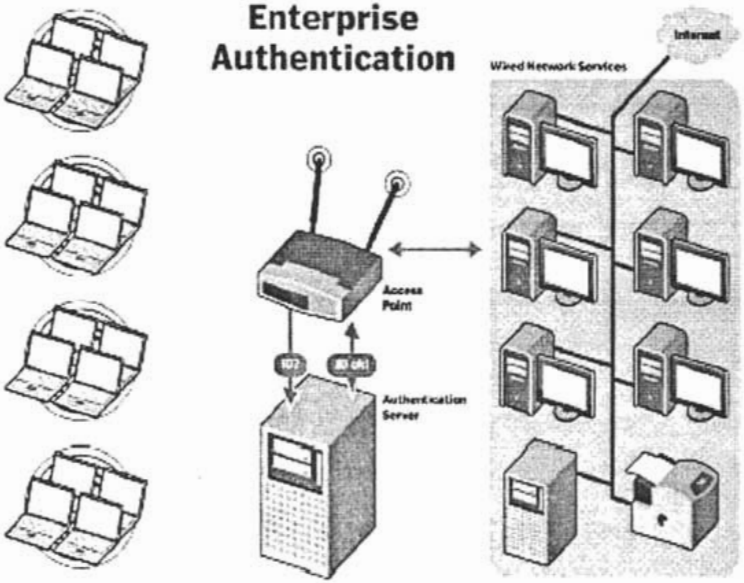


Fig. 3.11 Autenticación WPA

3.5.1 CONTROL DE ACCESO Y AUTENTICACIÓN DE USUARIOS

Como ya se ha estudiado, los protocolos 802.1X y EAP establecen las bases de un control de acceso seguro. Sin embargo en el caso de Wi-Fi son un añadido externo que, por suerte, se puede usar con el protocolo para fortalecerlo. En el caso de WPA ambos forman parte intrínseca de la especificación.

Como ya se comprobó el uso de 802.1X implica normalmente la puesta en marcha de un servidor de autenticación RADIUS, lo cual no está al alcance de todos los usuarios.

En entornos empresariales en los que exista (o sea fácil poner en marcha) un servidor RADIUS actuará de forma similar a las soluciones que hemos visto en los artículos precedentes, por lo que no entraremos de nuevo en su funcionamiento.

Sin embargo en entornos domésticos o de pequeñas oficinas en los que no esté disponible tal servidor existe un modo excepcional de trabajo que no necesita nada especial para funcionar pero ofrece una cierta seguridad en el acceso de todas formas. Esta es otra de las grandes diferencias de WPA respecto a lo existente.

3.5.2 MODO DE CLAVE COMPARTIDA (PSK)

Este modo específico de trabajo se llama Modo de Clave Compartida con Antelación o *Pre-Shared Key* (PSK) para abreviar. Como su propia denominación nos indica, su único requerimiento es compartir una clave entre los diferentes clientes que se van a autenticar contra un determinado punto de acceso que también la conoce. Si la clave de un cliente inalámbrico coincide con la del correspondiente AP se le otorga acceso, denegándolo en caso contrario. Como es obvio esta clave no se envía al AP al intentar la autenticación sino que es el origen de un trabajo criptográfico que finalmente conduce a la autenticación, por lo que no es posible averiguarla rastreando las emisiones.

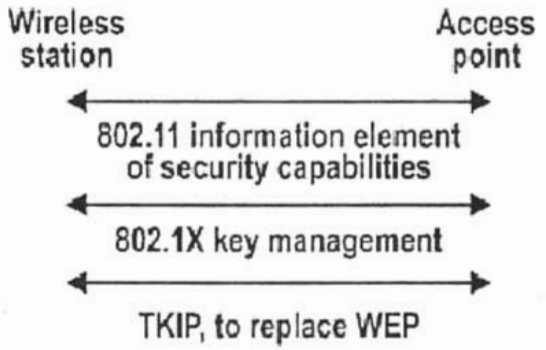


Fig. 3.12 WPA PSK (Pre-Shared Key)

Está claro que no es tan seguro como el uso de un servidor RADIUS pero será más que suficiente en entornos que necesitan conectar de forma segura a pocos equipos.

3.5.3 PROTOCOLO DE CLAVE TEMPORAL DE INTEGRIDAD (TKIP)

Este sistema de encriptación genera una llave nueva para cada paquete radiado (10.000 bytes), mediante la tecnología de encriptación TKIP (Temporal Key Integrity Protocol) o Protocolo de Clave Temporal de Integridad. Haciendo lo siguiente:

- Incrementa el tamaño de las claves pares y claves en grupo para la encripción de datos, de 40 a 128bits
- Un mecanismo de refrescamiento de la clave, requiere una nueva clave entre el cliente móvil y el punto de acceso cada 10 mil paquetes.

- Un Vector de Inicialización (IV) y un contador de secuencia IV vence a los ataques XOR repetidos. Una mezcla de IV por paquete derrota la correlación utilizada por el ataque de clave débil en WEP.

3.5.4 INTEGRIDAD DEL MENSAJE WPA: MIC

Chequeo de Integridad del Mensaje (Message Integrity Check), es un codigo de 8 bytes con las utilidades de cálculo disponibles en los dispositivos inalámbricos. El código MIC se coloca entre la parte de datos del marco IEEE 802.11 y el valor ICV de 4 bytes. El campo MIC se cifra junto con los datos del marco y los de ICV.

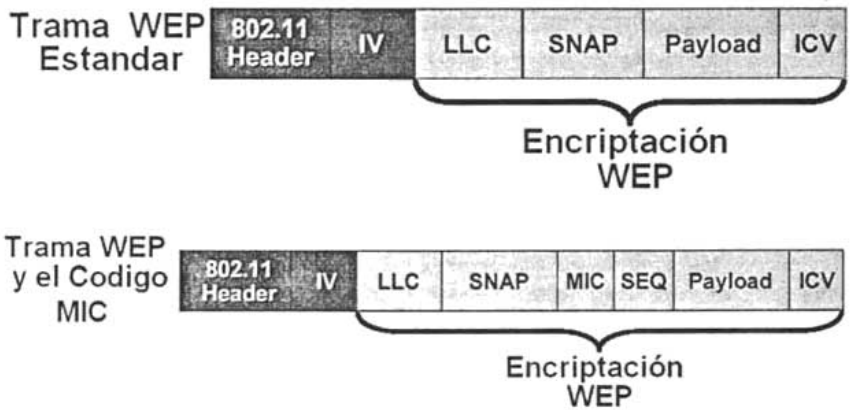


Fig. 3.13 Trama del campo MIC junto con Encriptación WEP

Ha sido diseñado para prevenir que intrusos capturen paquetes, los alteren y los re-envien. La función MIC, la cual se le conoce como "Michael", es un hash criptográfico de un solo sentido, el cual re-emplaza el Checksum CRC-32 utilizado en WEP. Michael provee una función matemática de alta fortaleza en la cual el receptor y transmisor deben computar, y luego comparar, si no coinciden la data se asume como corrupta y se desecha el paquete.

3.5.5 INTEROPERABILIDAD DE WPA Y WEP

Para admitir la transición gradual de las redes inalámbricas basadas en WEP a WPA, un punto de acceso inalámbrico puede admitir ambos clientes WEP y WPA al mismo tiempo. Durante la asociación, el punto de acceso inalámbrico determina qué clientes utilizan WEP y cuáles utilizan WPA. El inconveniente de admitir una mezcla de clientes WEP y WPA es que la clave de cifrado global no es dinámica. Esto se debe a que los clientes basados en WEP no lo admiten. Se mantienen todas las demás ventajas de los clientes WPA, como la integridad.

	WEP	WPA
Cifrado	Dañado por científicos y hackers	Corrige todos los defectos de WEP
	Llave de 40-bits	Llave de 128-bits
	Estático - misma llave usada por cada uno sobre la red	Llaves dinámicas de sesión. Por usuario, por sesión, y llaves por paquete
	Distribución manual de llaves en cada dispositivo	Llaves de distribución automáticas
Autenticación	Dañado, autenticación usado para sí mismo	Autenticación de usuario fuerte que utiliza 802.1x y EAP

Tabla 4.1 Grafica WEP vs. WPA

Esta interoperabilidad entre dispositivos antiguos y nuevos no forma parte de la especificación WPA aunque sí es posible que aparezca reflejada en 802.11i (WPA2). La Alianza Wi-Fi recomienda que no se utilice este modo de trabajo mixto debido a que casi invalida las ventajas de WPA. De hecho el proceso de certificación Wi-Fi para WPA incluye una prueba para asegurar que el dispositivo que se está evaluando no soporta el modo mixto en su configuración.

3.5.6 CAMBIOS EN LOS PUNTOS DE ACCESO INALÁMBRICOS

Los puntos de acceso inalámbrico deben tener su Firmware actualizado para admitir lo siguiente:

- El nuevo elemento de información de WPA

Para anunciar su compatibilidad con WPA, los puntos de acceso inalámbrico envían el marco de señal con un nuevo elemento de información 802.11 WPA que contiene la configuración de seguridad del punto de acceso inalámbrico (algoritmos de cifrado e información de configuración de seguridad inalámbrica).

- La autenticación en dos fases de WPA

Sistema abierto, a continuación, 802.1x (EAP con RADIUS o clave compartida previamente).

- TKIP
- Michael (MIC)
- AES (opcional)

Para actualizar sus puntos de acceso inalámbrico de modo que admitan WPA, obtenga una actualización de Firmware de WPA de su proveedor y cárguela en su punto de acceso inalámbrico.

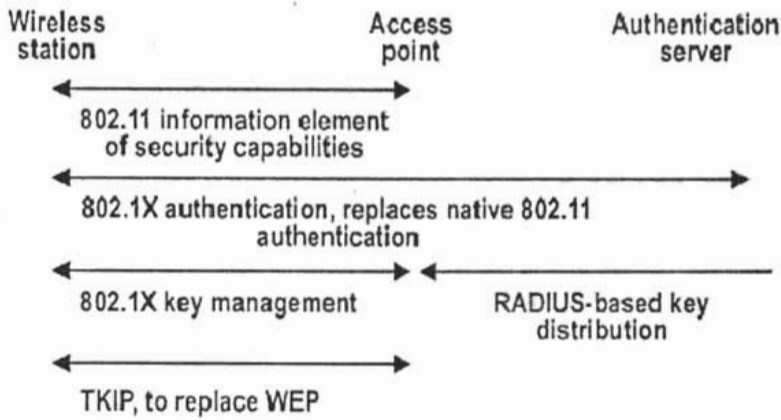


Fig. 3.14 WPA 802.1x/Solución RADIUS

Para los clientes inalámbricos de Windows, debe obtener un controlador del adaptador de red actualizado que admita WPA. Para los controladores de adaptadores de red inalámbricos que sean compatibles con Windows XP (Service Pack 1) y Windows Server 2003, el controlador actualizado de red debe poder pasar las características WPA del adaptador y la configuración de seguridad al servicio de configuración inalámbrica rápida.

3.5.7 CONFIGURACION MANUAL DE LA WLAN CON WPA

Microsoft® recomienda seguir estos sencillos pasos para configurar el protocolo WPA en plataforma Windows® XP®, para lograr así un nivel de seguridad alto.

Hasta que no disponga de compatibilidad con el objeto de directiva de grupo en Windows Server® 2003 Service Pack 1, deberá configurar WPA en el equipo cliente de forma manual. WPA es compatible con Windows XP® Service

Pack 1 con la descarga del cliente WPA instalada (o en Windows XP Service Pack 2).

Cuando disponga de compatibilidad con el objeto de directiva de grupo, se podrá utilizar el siguiente procedimiento para crear una directiva de red inalámbrica con la misma configuración.

Para configurar manualmente la WLAN con WPA:

1. Abrir las propiedades de la interfaz **Red inalámbrica**. Si en la lista **Redes disponibles** aparece WLAN, seleccionarla y hacer clic en **Configurar** o en **Agregar** (en la sección **Redes preferidas**).

2. Escribir el nombre de la WLAN en el campo **Nombre de red (SSID)** (si no aparece ya) y, en el campo **Descripción**, escribir una descripción para la red. **Nota:** si ya se posee una WLAN configurada y se desea ejecutarla en paralelo con la WLAN basada en 802.1X de esta solución, se debe utilizar un Identificador del conjunto de servicios (SSID) para la nueva WLAN. Este nuevo SSID deberá utilizarse aquí.

3. En la sección **Clave de red inalámbrica**, seleccionar **WPA** (no seleccionar **WPA PSK**) como el tipo de **Autenticación de red** y **TKIP** como el tipo de **Cifrado de datos**. Si el hardware es compatible, seleccionar el estándar de cifrado avanzado más seguro (**AES** en lugar de **TKIP**).

4. Hacer clic en la ficha **IEEE 802.1x** y seleccionar **EAP protegido (PEAP)** de la lista desplegable **Tipo de EAP.**

5. Hacer clic en el botón **Configuración** para modificar la configuración PEAP. En la lista **Entidad emisora raíz de confianza**, seleccionar el certificado de entidad emisora raíz para la entidad emisora, que es la que se instala para emitir certificados del servidor IAS **Importante:** si se necesita instalar de nuevo la entidad emisora desde cero (no sólo restaurarla desde la copia de seguridad), se deberá modificar la configuración del cliente y seleccionar el certificado de entidad emisora para la nueva entidad emisora.

6. Asegúrarse de que se selecciona **Contraseña protegida (EAP-MS-CHAP v2)** en **Seleccione el método de autenticación** y comprobar la opción **Habilitar reconexión rápida.**

7. Cerrar cada una de las ventanas de propiedades haciendo clic en **Aceptar.**

Microsoft® ha trabajado con muchos proveedores inalámbricos para incorporar la actualización de Firmware de WPA en el controlador del adaptador inalámbrico. Por tanto, para actualizar el cliente inalámbrico de Windows, lo único que tiene que hacer es obtener el nuevo controlador compatible con WPA e instalarlo. El Firmware se actualiza automáticamente cuando el controlador del adaptador de red inalámbrica se carga en Windows.

3.6 PROTOCOLO DE SEGURIDAD: 802.11i (WPA2)

La seguridad ha sido uno de los grandes obstáculos para el crecimiento de las redes inalámbricas. WPA reemplazó al defectuoso protocolo WEP, para reforzar la seguridad inalámbrica antes de que el estándar completo 802.11i fuera ratificado. WPA utiliza una clave de encriptación dinámica, a diferencia de la clave fija utilizada por WEP, además de mejorar el proceso de autenticación de usuario.

El estándar 802.11i es la versión completa del estándar de seguridad preliminar WPA (Wi-Fi Protected Access) lanzado en el 2004, mientras que el 802.11e es un nuevo estándar que mejorará la calidad de las redes inalámbricas que transmiten voz y vídeo.

3.6.1 TECNOLOGÍA AES

El estándar 802.11i añade la tecnología AES (Advanced Encryption Standard), un mayor nivel de seguridad que el utilizado en WAP. Con los nuevos estándares, corporaciones y gobiernos, que necesiten un mayor nivel de seguridad, podrían tener que reemplazar algunos de sus equipamientos de redes con el objetivo de soportar el estándar AES.

Los nuevos equipamientos de conexión de redes probablemente tengan suficiente potencia como para gestionar el aumento de rendimiento que requiere la seguridad AES.

Las compañías con equipamiento antiguo deberán decidir primero si los datos que viajan por sus redes inalámbricas son lo suficientemente críticos como para justificar un cambio.

3.7 PROTOCOLO DE SEGURIDAD: 802.11e

La actualización hacia 802.11e hará que las redes inalámbricas VoIP (Voz sobre IP) sean una elección real para los directores de redes. Próximamente los fabricantes de teléfonos móviles empezarán a lanzar al mercado terminales

duales que soportarán tecnología inalámbrica WLAN como 802.11 además de GSM (Global System for Mobile Communications).

3.7.1 TECNOLOGÍA WME

Próximamente la Wi-Fi Alliance empezará a certificar los productos que utilicen un subconjunto de 802.11e denominado WME (Wireless Media Extensions) para mejorar la calidad del servicio. WME identifica paquetes de voz, vídeo, audio u otros tipos de datos y prioriza su reparto dependiendo de las condiciones del tráfico. Por ejemplo, los vídeos transmitidos a través de redes inalámbricas se resienten si los paquetes se retrasan o se pierden, por lo que a este tipo de datos se les dará prioridad sobre otros que viajen por la misma red.

3.7.2 TECNOLOGIA WSM

Por otra parte, el estándar 802.11e íntegro incluirá una tecnología adicional denominada WSM (Wi-Fi Scheduled Media), pero la organización quiere asegurarse de que los productos tienen alguna clase de certificación para poder utilizarse en redes para el hogar. WSM asigna parte del ancho de banda para diferentes tipos de datos inalámbricos, e incrementa el ancho de banda necesario para las aplicaciones de vídeo y voz.

3.8 PROBLEMÁTICA EN LOS DESPLIEGUES DE WLAN

Una vez conocidas las inseguridades de las Redes Wireless, no tardaron en aparecer los ataques. Y una de las más sofisticadas formas se ha denominado "wardriving".

Consiste en que expertos en Redes Wireless Ethernet se desplazan en un coche con un portátil con tarjeta de red inalámbrica y una antena pequeña, realizando una exploración de las frecuencias empleadas por estas redes en zonas empresariales y centros de negocios de grandes ciudades.

Los resultados de estas búsquedas revelan que con mínimo esfuerzo se puede penetrar en una gran mayoría de las redes. Las razones de ello son: elevados porcentajes de redes con los parámetros por defecto de los equipos, no activadas las reglas de seguridad básicas o sólo parcialmente, exceso de potencia de señal que permite su fácil recepción desde el exterior, empleados que implantan su propio punto de acceso inalámbrico sin conocimiento de la empresa, seguridad sólo basada en WEP, etc.

3.9 SOLUCIONES SEGURAS CON REDES WIRELESS ETHERNET

Definitivamente las redes inalámbricas pueden alcanzar niveles de seguridad análogos a los de sus equivalentes cableadas. Para ello es necesario seguir una serie de recomendaciones básicas:

1. Considerar a estas Redes como una alternativa seria. Es inexplicable la dejadez con que algunos responsables implantan estas redes, sobre todo considerando los esfuerzos y presupuesto que dedican a la securización de sus redes fijas. Y a tenor de los resultados, el porcentaje es elevado. También puede atribuirse en otros caso a un cierto desconocimiento de la tecnología, pero que en muchos casos no les ha retraído de realizar una experiencia por sí mismos.

2. Implantar soluciones de seguridad avanzadas y la solución WPA.

3. Replantear la política de seguridad de las redes locales. Una buena de gestión de seguridad ha sido el aislar la red empresarial del exterior (seguridad "fronteriza"), considerando que toda posible amenaza provenía siempre de más allá del Firewall (cortafuegos) corporativo, mientras que la red interna permanecía como un espacio de máxima confianza. Sin embargo es conocido el hecho de que multitud de fugas de información provienen desde el interior de las propias redes (sniffers internos, usurpación de direcciones MAC, acceso a terminales sin autentificación activada, usuarios y claves triviales,).

   Las soluciones para las WLAN establecen un mecanismo de elevada seguridad extremo a extremo, entre el terminal de usuario y el servidor de la aplicación considerando que el medio que los comunica no es confiable (susceptible de escucha) e incluso la posible intrusión o usurpación de personalidad. Esto normalmente cubre tanto el tramo inalámbrico como parte de la red cableada que es necesario atravesar, creando una comunicación difícilmente violable. Los equipos y aplicaciones necesarios para esta tarea no son sólo adecuados para entornos wireless, sino que se pueden extender a cualquier medio existente. La solución ideal radicaría en una combinación de ambas filosofías de seguridad.

4. Contactar con una empresa de ingeniería con experiencia en esta materia. Posiblemente en algunos casos las deficiencias puedan ser debidas a que el responsable encargó el despliegue a personal sin la adecuada formación.

CAPITULO 4

WI-FI TECNOLOGIA, APLICACIONES Y SERVICIOS

CAPITULO 4

4. TECNOLOGIA WI-FI

Wi-fi es ya una tecnología madura y consolidada y es que ha tenido una aceptación social muy rápida y beneficiosa, Esta tecnología es cada vez mas objeto de estudios para muchos, ya que cada día se reconocen más este tipo de redes en un amplio número de negocios y Campus Universitarios

Debido al éxito en el mercado se desarrollan gran número de nuevas aplicaciones y servicios. Y los estándares para redes inalámbricas incorporan mecanismos de seguridad suficientes en cantidad y calidad para hacer que las redes sean tan seguras como las cableadas.

Se encuentran aplicaciones en todos los sectores de la sociedad, tanto el sector privado como publico. Más allá del campo empresarial, el acceso a Internet e incluso a sitios corporativos, es disponible a través de zonas activas de redes inalámbricas públicas. Y es que Mucha gente está interesada en las Redes Wireless como medio barato de acceder a Internet usando la conexión de otro.

El uso más frecuente de las WLAN es como extensión de las redes cableadas de modo que se da una conexión a un usuario final móvil, con las ventajas que esto significa;

- En entornos dinámicos: se minimiza la sobrecarga causada por extensiones de redes cableadas, movimientos de éstas u otros cambios instalando red sin cable.

- En centros de formación, universidades, corporaciones, etc., donde se usa red sin cable para tener fácil acceso a la información, intercambiar ésta y aprender.

- En viejos edificios es también más adecuada.

- Los trabajadores de almacenes intercambian información con una base de datos central mediante red sin cable de modo que aumenta la productividad. También para funciones críticas que requieren rapidez.

- Para la improvisación de una red temporal, un WLAN es ideal.

4.1 COMPONENTES DE UNA WLAN

Cuando se han tomado en cuenta las múltiples ventajes que tiene la Tecnología Wi-Fi, y se quiere instalar una red es importante definir las características que va a tener la red, como el estándar y la topología a utilizar y para esto se debe saber cuales son las necesidades; se debe también conocer que tipo de datos se desean transmitir, cuantos host tendrá nuestra red, y saber si será implementada como anexo a una red cableada existente, o una nueva inalámbrica.

Normalmente el fabricante del Hardware de dispositivos inalámbricos incluye dentro de sus productos un manual de instalación, o fichas técnicas del mismo donde indica la compatibilidad de este con los sistemas operativos.

Cabe mencionar que en el mercado existen productos compatibles con las principales plataformas existentes como son: Windows®, Linux® y Unix®, aunque los productos inalámbricos corren casi en cualquier protocolo de comunicaciones, pero de cualquier manera hay que verificar la compatibilidad antes de adquirir cualquier producto.

Se debe de considerar que las ondas de radiofrecuencia pueden atravesar obstáculos como son: Paredes, madera, plástico, vidrio, muebles etc. Pero entre mas obstáculos se tengan que atravesar para llegar al receptor significara una perdida de señal ya que dichos obstáculos van absorbiendo las ondas, esto es importante considerar al momento de ubicar el, o los Access Point.

Las ondas de radiofrecuencia no pueden atravesar cosas hechas de materiales metálicos ya que estos reflejan las señales.
Y elementos como agua y humedad causan una gran interferencia y pérdida de calidad en la señal.

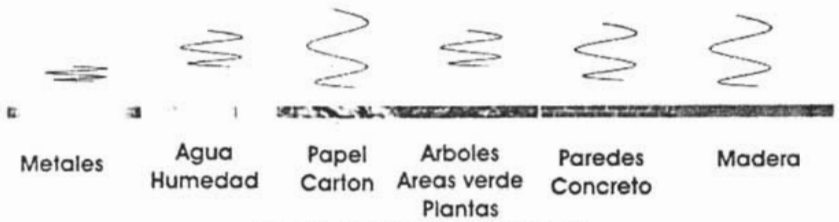


Fig. 4.1 Ondas Radiofrecuencia

Otro importante factor de considerar es que la señal de alcance que tienen los dispositivos inalámbricos se mide en distancia radial a partir de donde es colocado el dispositivo, siempre y cuando estos cuenten con antenas omnidireccionales.

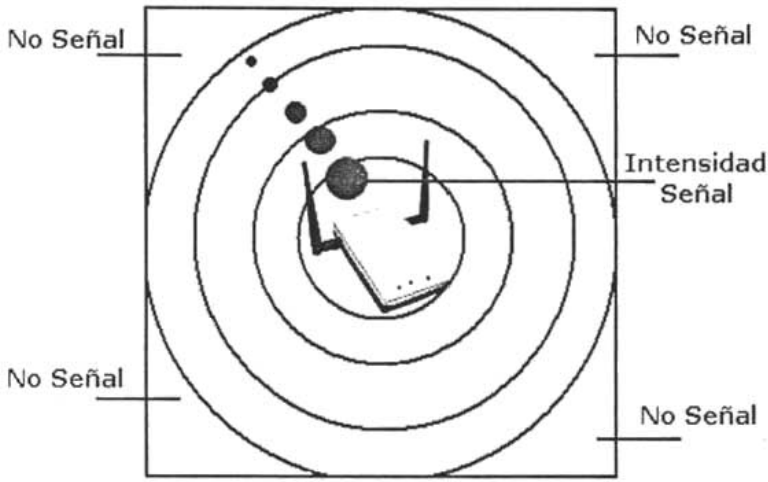


Fig. 4.2 Radiación de un AP con antena Omnidireccional

Es decir que mientras más despejado sea el camino entre los dispositivos wireless y menor sea el nivel de cosas que puedan causar interferencias, mejor será la señal, más estable y se lograra mayores alcances.

Para tener un mejor conocimiento y saber los elementos que conforman una red WLAN, se describe a continuación los detalles del Hardware que conforma una red.

4.1.1 LAS ANTENAS

Las antenas son un elemento fundamental para la comunicación entre los dispositivos, estas captan las señales enviadas por los dispositivos inalámbricos. En este caso nos vamos a centrar en las antenas para 2.4Ghz que son las usadas para 802.11b y para la próxima 802.11g de pronta expansión en el mercado de las Comunicaciones.

Existen dos tipos de antenas las Direccionales y las Omnidireccionales.

Las antenas Direccionales: envían la información a una cierta zona de cobertura o mejor dicho hacia un punto en concreto, a un ángulo determinado.

Las antenas Omnidireccionales: envían toda la información en un rango de 360 grados por lo que es posible establecer comunicación independiente del punto en que se este.

4.1.1.1 ANTENAS DIRECCIONALES

Estas antenas son capaces de enfocar toda la señal que le aplica la tarjeta o punto de acceso, a una dirección concreta, a un ángulo determinado, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores. Normalmente estas antenas se usan para establecer enlaces punto a punto (direccional contra direccional) o para enlazar con un nodo que tenga una antena Omnidireccional.

Dentro de la gama de Antenas Direccionales, existen también varios modelos y formas, cada una con un uso concreto:

a) Antena Direccional de rejilla, o parabólica:

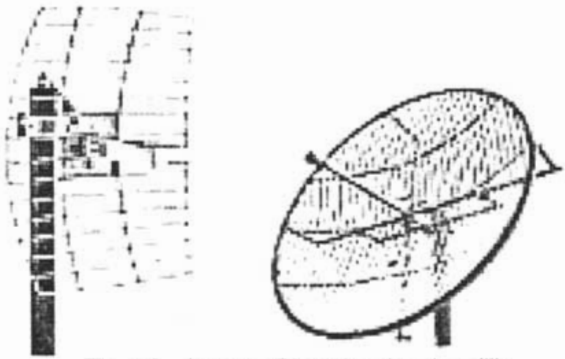


Fig. 4.3 Antenas Direccionales de rejilla

Es la típica antena para establecer enlaces punto a punto o para conectar a un nodo. Se caracterizan por su alta ganancia, que va desde unos discretos 15dBi, llegando en los modelos superiores hasta los 24dBi. Cuanta más alta es la ganancia de este tipo de antenas, más alta es su direccionalidad, ya que se reduce muchísimo el ángulo en el que irradian la señal, llegando a ser tan estrechos como 8º de apertura.

La siguiente imagen representa a la radiación de una antena direccional de poca ganancia. Nótese que la elipse en negrita es ancha, y que su extremo superior también lo es, eso quiere decir que no es tan directiva como pudiera parecer, admitiendo un margen de error considerable a la hora de apuntar con ella.

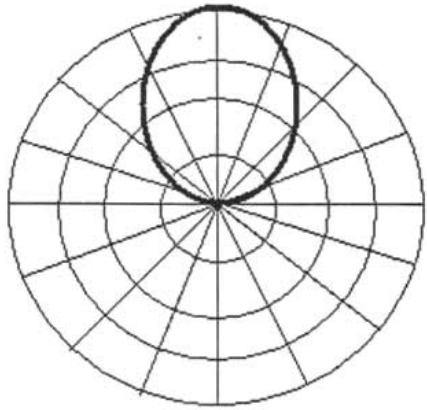


Fig. 4.4 Antena Direccional de poca Ganancia

En ésta otra imagen se nota claramente un haz mucho más estrecho, lo que la hace bastante más directiva y más crítica de apuntar. Esta gráfica podría ser perfectamente la de una antena de 24dBi, ya que por sus características se corresponde plenamente.

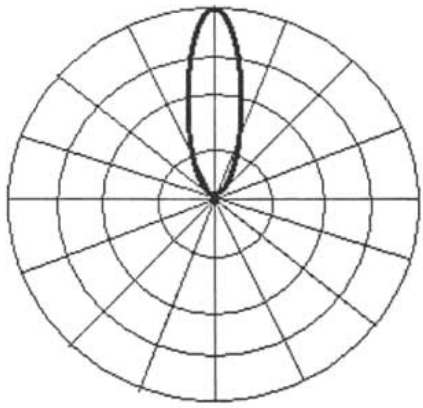


Fig. 4.5 Antena Direccional de Mayor Ganancia

Un detalle de estas antenas es que, la rejilla lo único que hace es concentrar la señal que llega hasta ella, y enviarla al 'dipolo' que está cubierto por un plástico protector.

b) Antena Direccional tipo Patch Panel:

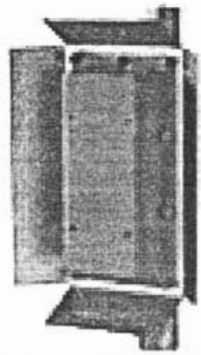


Fig. 4.6 Antena tipo Patch Panel

Con estas antenas se consigue crear pequeñas zonas de cobertura, tanto como recintos, estaciones de metro y similares, consiguiendo con varias de ellas establecer 'células' (como en telefonía móvil). Otra utilidad puede darse para sustituir una antena omnidireccional, tras la cual pudiera encontrarse un edificio u otra estructura que impidiera que la señal se propagase, poniendo varias de ellas para cubrir la zona deseada y no desperdiciar señal. A esta unión de antenas se les llama 'Array'.

Normalmente la anchura del haz que irradian estas antenas es de 25º tanto en vertical como en horizontal
Hay que decir que cuanta más alta sea la ganancia de la antena, mayores distancias se pueden cubrir con una antena, y con mejor calidad se podran captar señales que pudieran llegar muy débilitadas.

4.1.1.2 ANTENAS OMNIDIRECCIONALES

Como su nombre indica, estas antenas son capaces de emitir señal en todas las direcciones, pero esto tiene un pequeño matiz; las figuras de abajo son el ejemplo de una antena omnidireccional y el espectro de radiación, vista desde arriba.

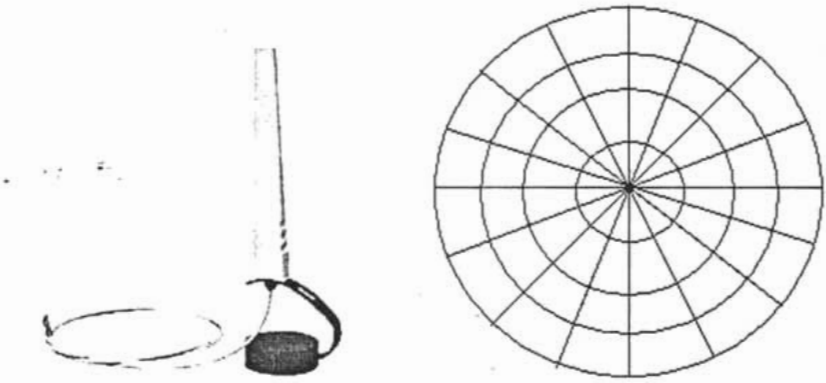


Fig. 4.7 Antena Omnidireccional y su espectro de radiación

En la figura de abajo; las líneas representan hasta dónde la señal es emitida. Esto quiere decir que realmente estas antenas no emiten señal en todas las direcciones, sino más bien sobre su propio plano es donde se conseguirá la máxima potencia.

Una situación que pasa de forma bastante habitual, es que se pone la antena en un lugar muy alto, y luego a la altura de la calle no llega la señal, queda claro con este dibujo que es lo que está pasando: la señal no llega porque la antena es omnidireccional sólo sobre su mismo plano.

Con la ganancia de las antenas omnidireccionales pasa algo muy similar a lo que ocurría con las direccionales: cuanta más alta es su ganancia, más estrecha es la radiación horizontal que estas emiten.

Fig. 4.8 Antena Omnidireccional radiando sobre su mismo plano

Las antenas son elementos fundamentales para el buen funcionamiento de este tipo de redes así que es mejor asegurarse que sean de calidad, y tener en cuenta la que seria la más indicada para nuestra aplicación.

4.1.2 LOS CABLES

Las Redes WLAN también utilizan en ocasiones algún tipo de cables sobre todo para colocar las antenas y se debe poner atención en la elección de ellos ya que son fundamentales para el rendimiento de la red.

Los conectores que se utilizan principalmente son el llamado Pig Tail (cola de cerdo) y los cables extensión, que son para agregar extensiones a las antenas. El Pig Tail es un cable que sirve de adaptación entre la tarjeta de red y la antena o el cable que va hacia la antena.

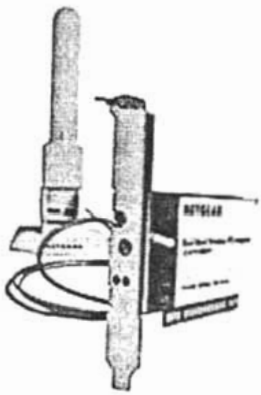


Fig. 4.9 Cable Pig Tail como extensión de la Tarjeta de Red

Este elemento es indispensable para la conexión entre dichos dispositivos, aunque en algunos casos este componente ya viene integrado.

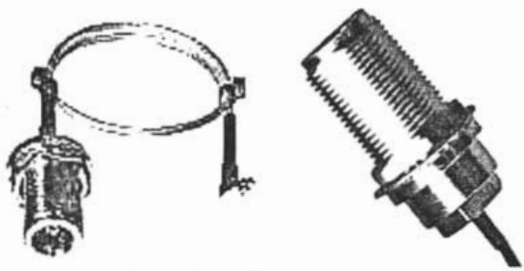


Fig. 4.10 El Cable Pig Tail

El Pig Tail tiene dos conectores; uno llamado Propietario, que es definido por cada empresa y del otro extremo un conector en N, que por lo regular es estándar. Aunque no todos los Pig Tail son estándar ya que cada fabricante puede tener su propio diseño.

4.1.3 PUNTO DE ACCESO (ACCES POINT)

Como se ha venido utilizando dentro de este documento, este dispositivo es abreviado por sus siglas en ingles AP (Acces Point). Estos son los encargados de recibir la información de los diferentes dispositivos cliente para su centralización o bien para su encaminamiento. Y reenviarla a los otros dispositivos que la soliciten.

Tal es el ejemplo que describo a continuación el Access Point 1100 de Cisco ®

Los Access Point Cisco Serie 1200 imponen el estándar para las redes inalámbricas de área local de la próxima generación, con alto desempeño, seguras, fáciles de administrar y confiables, mientras que protege su inversión gracias a su capacidad de actualización y compatibilidad con los estándares actuales.

El diseño modular del Cisco Aironet 1100 soporta las tecnologías IEEE 802.11b y 802.11g en modos de operación sencillo y dual. Es posible configurar el Cisco Aironet 1100 de acuerdo a los requerimientos específicos del cliente al tiempo de la compra y luego reconfigurar el producto y actualizarlo en el lugar de uso al evolucionar sus requerimientos.

Además, la Serie 1100 de Cisco Aironet crea una infraestructura inalámbrica que proporciona a los clientes máxima movilidad y flexibilidad, permitiéndoles una conexión constante a todos los recursos de la red desde virtualmente cualquier lugar en el que exista acceso inalámbrico.

Fig. 4.11 Access Point 1100* Cisco ®

* Punto de Acceso (AP) 802.11b y g, 2.4 GHz, 11/54 Mbps Power-over-Ethernet, Power inyector WPA, VoIP, VLan's, QoS, Roaming, 100 mW 45 a 122 m interiores y 244 a 610 m exteriores Wireless Router 802.11a/b/g 2.4/5.8 GHz, 11/54/108 Mbps Power-over-Ethernet y Antena Omnidireccional de 8 dBi.

Puertos del AP 1100

1	Puerto de Energía 48VCD	4	Boton de Modo
2	Puerto Ethernet	5	Status de LED´s
3	Cable de slot	6	Antena

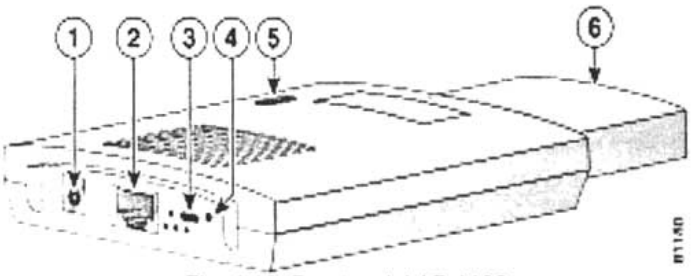


Fig. 4.12 Puertos del AP 1100

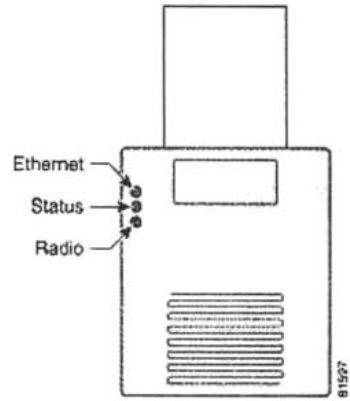


Fig. 4.13 Led de Estado

Detalles de los Led de Estado:

- El indicador de Ethernet señala el tráfico en la LAN inalámbrica o la infraestructura de Ethernet. Este indicador esta normalmente en verde cuando un cable Ethernet es conectado y parpadea en verde es que un paquete es recibido o transmitido sobre la infraestructura de Ethernet. El indicador esta apagado cuando el cable no esta conectado.

- El indicador de Status señala el status operacional, si esta en verde indica que el Access Point esta asociado con al menos un cliente inalámbrico. Si parpadea en verde indica que el Access Point esta operando normalmente, pero que no esta asociado con ningún dispositivo inalámbrico.

- El indicador de Radio parpadea en verde para indicar la actividad de tráfico. La luz esta normalmente apagada pero parpadea en verde cuando un paquete es recibido o transmitido sobre el radio del Access Point.

Un Punto de Acceso puede complementar a un Hub o Switch de redes inalámbricas, o bien sustituirlo. La velocidad de transmisión / recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante.

Al configurarlos permiten enlazar varios Puntos de Acceso para ampliar la cobertura, la distancia o alcance de estos Puntos de Acceso es proporcionada en las características del fabricante y en promedio es de 100m en interiores, y de 200m en exteriores.

4.1.4 DISPOSITIVOS CLIENTE

Los dispositivos Cliente son componentes principales de estas redes, estos dispositivos son los que serán colocados en los equipos que se quieren incluir en la red.

Se catalogan como dispositivos cliente, por que aquí no solo se clasifican tarjetas de red sino también tarjetas para Lap Tops, o dispositivos USB que se pueden incorporar a la PC para tener compatibilidad o para equipos PDA, etc.

A continuación la figura muestra un ejemplo de Tarjetas de Red para PC de escritorio, estas son de fácil instalación y configuración, ya que son tecnología Plug & Play, lo que significa que cuando son insertadas en la ranura PCI de la computadora, son reconocidas automáticamente por el Sistema Operativo utilizado.

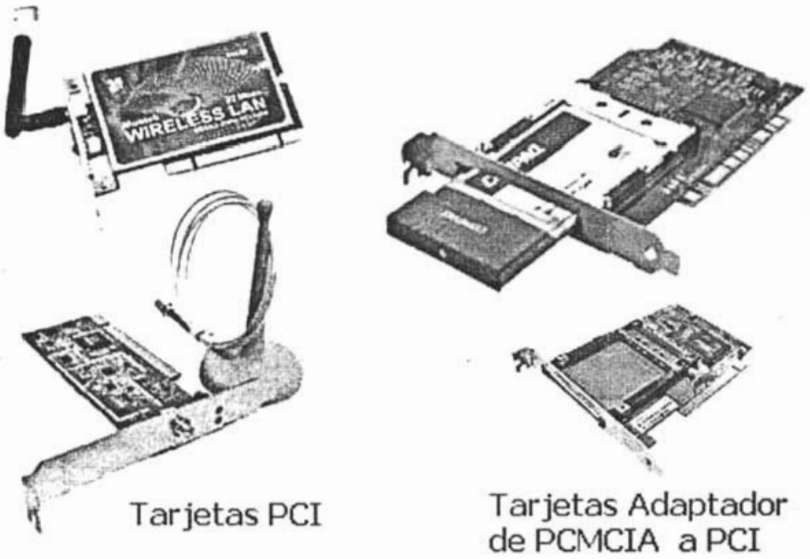
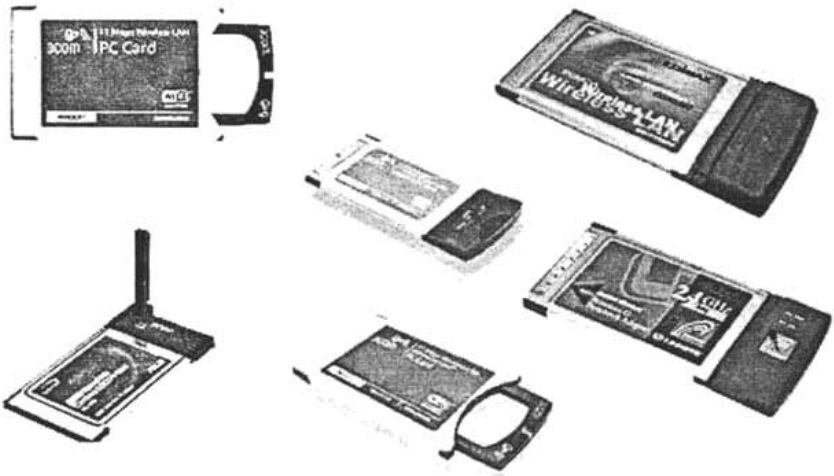


Fig. 4.14 Tarjetas de Red tipo PCI y adaptadores para PC

De la misma manera que las tarjetas PCI, las PCMCIA que son las tarjetas compatibles con el Hardware de las Computadoras Móviles, (Lap Top), también son reconocidas por el Sistema Operativo para su configuración, en caso contrario, el fabricante de estos productos, incluye un CD-ROM con los controladores necesarios, para sincronizar el puerto de red de la computadora con el Punto de Acceso.



Dispositivos PC-CARD / PCMCIA

Fig. 4.15 Tarjetas de Red tipo PCMCIA para Lap Top

Estos dispositivos recibirán y enviaran la información hacia su destino desde el equipo que estemos trabajando.

Existen varios formatos para los distintos tipos de equipos ya sean computadoras de escritorio, Portátiles o PDA.

4.1.5 PUENTES (BRIDGES)

Los equipos Bridges permiten crear puentes entre redes de tipo alámbricas e inalámbricas y aunque algunos Access Point permiten realizar esta función, estos son especialmente diseñados para conectar lugares remotos y así poder crear el enlace, esto es usado normalmente para conectar redes LAN entre dos edificios como mostraría la figura siguiente.

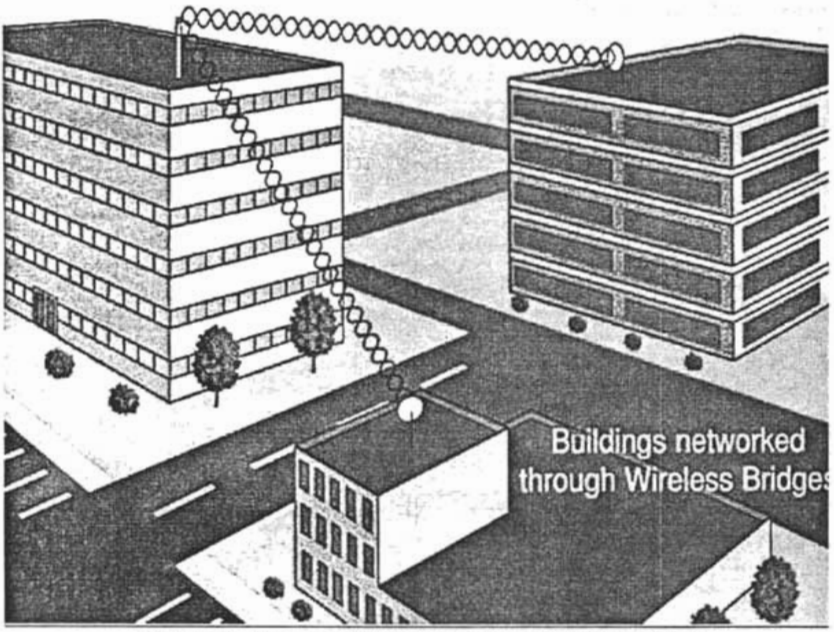


Fig. 4.16 Funcionalidad típica de un Puente (Bridge)

Como ejemplo se muestra a continuación el Bridge que interconecta LAN Inalámbricas el 3Com® 11g 54Mbps Wireless LAN Outdoor Building-to-Building Bridge.

Fig. 4.17 Bridge 3Com® 11g 54Mbps Wireless LAN

Que tiene un alcance extendido y evita gastos y problemas de instalación de cables de fibra o cuotas mensuales de líneas T1/E1 al conectar LANs mediante enlaces inalámbricos seguros y de alta velocidad. El bridge de exteriores entre edificios con antena de panel integrada de alta ganancia de 18dBi está diseñado para comunicaciones de corta o larga distancia (hasta 17

Km. ó 10 millas), conectándolo a otro bridge. El bridge de exteriores ofrece una solución inteligente y económica para conectar LANs en contextos de tipo campus, cuando se despliega con bridges Wíreless LAN.

El bridge 11g de exteriores a 54 Mbps ofrece de diez a veinte veces el ancho de banda de enlaces T1/E1 y soporta hasta 1.000 clientes. Funciona en configuración punto a punto o punto a multipunto (dentro del ángulo de haz de 19°) para responder a las demandas de crecimiento y de aplicaciones.

La encriptación y autenticación WPA-PSK y AES ofrecen altos niveles de seguridad usando los últimos estándares de la industria. El soporte de VPN y VLAN mantiene la privacidad de los datos de red y protege las transmisiones de posibles rupturas en la seguridad. El software de asistente de configuración facilita la instalación y configuración. Una vez completado el ajuste, el bridge entre edificios puede administrarse de forma remota usando un navegador Web estándar o herramientas de administración SNMP.

4.1.6 ENRUTADORES (ROUTERS)

Estos dispositivos ofrecen acceso compartido a Internet de una manera más rápida y sencilla que la de estar configurando programas o software, además en ocasiones incluyen Firewalls dependiendo del modelo y características.

Cuando el router no tiene integrado un modem ADSL, entonces se requerirá interconectar con este la línea del Proveedor del Servicio con un modem, mismo que normalmente se incluye con la contratación del servicio, y el router que funcione como Acces Point. Cabe mencionar que la mayoría de los productos inalámbricos existentes en el mercado, tiene interoperabilidad entre los diferentes protocolos, de funcionamiento, es decir en la actualidad existentes Routers /Acces Point que combinan el protocolo 802.11b y el 802.11g.

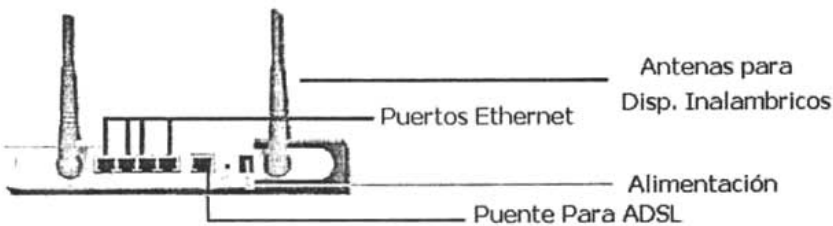


Fig. 4.18 Router sin Modem ADSL incluido

El diagrama de conexión representa la conexión vía cable de conector RJ-11 hacia el modem ADSL mismo que proporciona el servicio de Internet.

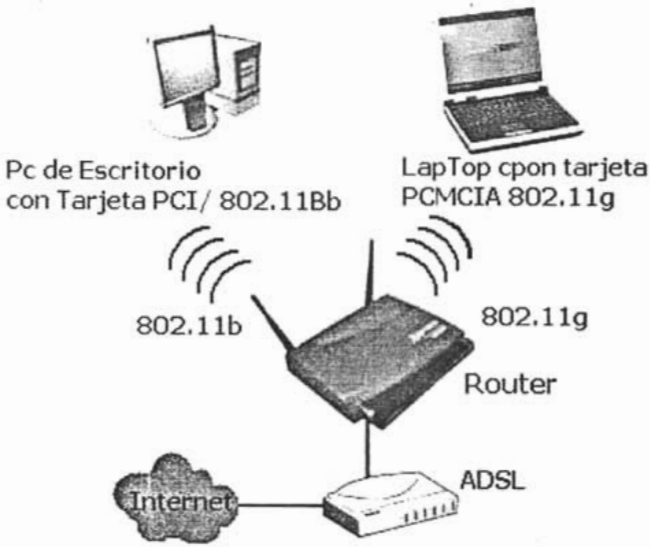


Fig. 4.19 Router interconectado con un Modem ADSL

Sin embargo, hay productos, que integran en hardware, la conexión de ADSL. Lo que nos brinda el acceso y la conexión al Internet. Así que facilitaría la conexión al poderse conectar directamente la línea del servicio al Router.

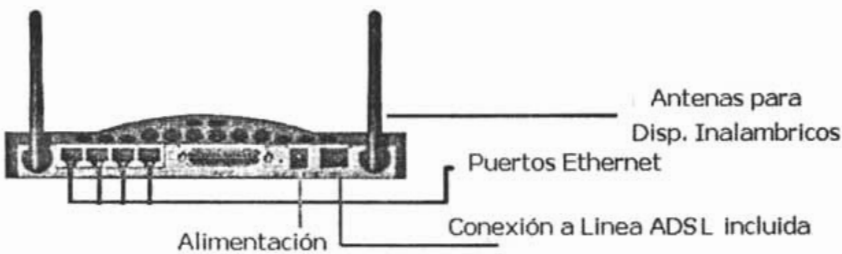


Fig. 4.20 Router con sin Modem ADSL

El diagrama de conexión quedaría así:

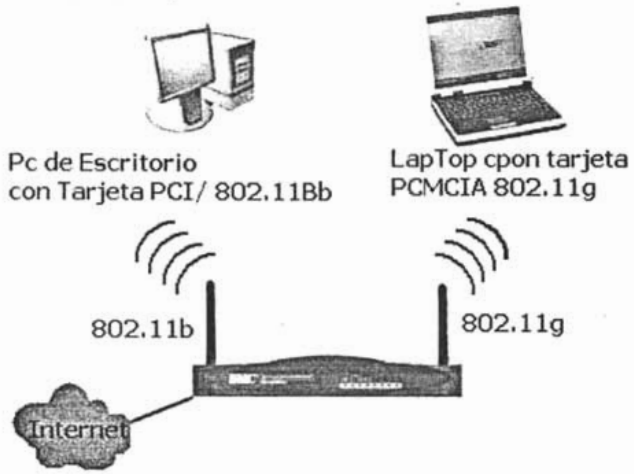


Fig. 4.21 Router con Modem ADSL

Existen modelos que incluyen funciones como:

Combinación de un Firewall de Inspección de estado de paquetes; un Switch Fast Ethernet de 4 puertos, con un modem ADSL y un Punto de Acceso Inalámbrico 802.11g para proporcionar una comparticion segura y de Alta Velocidad.

Tal es el caso del modem anteriormente mencionado en el Capitulo 2 de este documento, el Modem "Router 2Wire® Home Portal 1800HW" que es utilizado por la empresa mexicana Telmex®, con su servicio Prodigy Infinitum, que tiene la opción de funcionar en modo Alambrito e Inalámbrico, es decir, que también es un Punto de Acceso (AP) para compartir el servicio de Internet de Alta velocidad, en una red inalámbrica, entre varias computadoras.

Fig. 4.22 Router 2 Wire ® Home Portal 1800 HW

El Router 2Wire® tiene un Modem Integrado ADSL que mejora el funcionamiento DSL sobre todo para casas más lejanas del la red local. Reduce al mínimo la interferencia común DSL con otros dispositivos. Provee de velocidades de transferencia de datos rápidas entre la casa y la Internet, el Firewall de Grado Profesional Activamente descubre y defiende contra amenazas comunes de Internet. Se puede conectar de la línea telefónica de una casa ya que tiene un spot para phoneline (HomePNA), y otro para conectarse mediante USB e HiperG™ inalámbrico.

Es de fácil instalación, tiene un gateway preconfigurado para trabajar con cada proveedor principal DSL así no hay ninguna necesidad de conocer detalles técnicos.

El Acceso Remoto vía Web proporciona el acceso fácil al Home Portal que es el sistema que le permite monitorear desde una PC tanto la Administración como la Gestión de la Red.

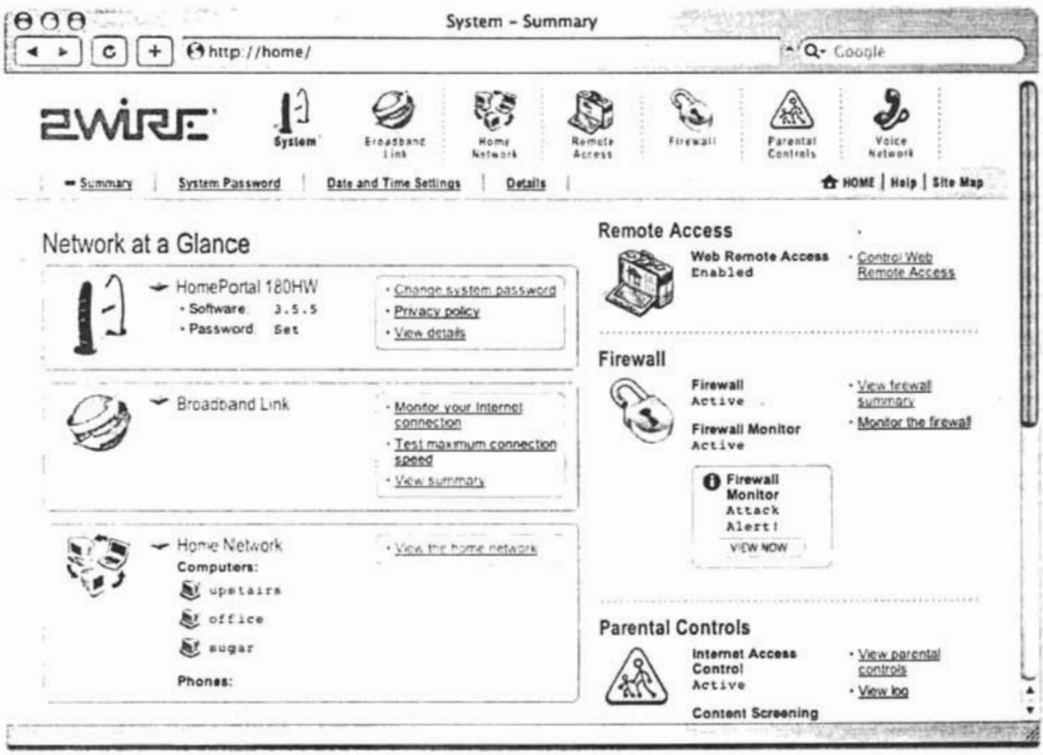


Fig. 4.23 Home Portal Sistema de Monitoreo del 2 Wire®

La figura anterior es el Home de la página Web del 2 Wire, misma que viene incluida en el CD-ROM de configuración del modem.

Físicamente el 2 Wire tiene los siguientes detalles técnicos:

a)Interfaces de Red Local

- Puerto de Red Ethernet: Auto-crossover (RJ-45)
- 1 puerto OR Built-in de alto rendimiento o 4 puertos 10/100 de Switch Ethernet
- Puertos USB 1 USB 1.1 series-B
- HomePNA: 1 HomePNA 2.0 en Line1 y en el Line 2 (RJ-11)
- Certificado Wireless: Wi-Fi 802.11g o 802.11b Punto de Acceso Inalámbrico

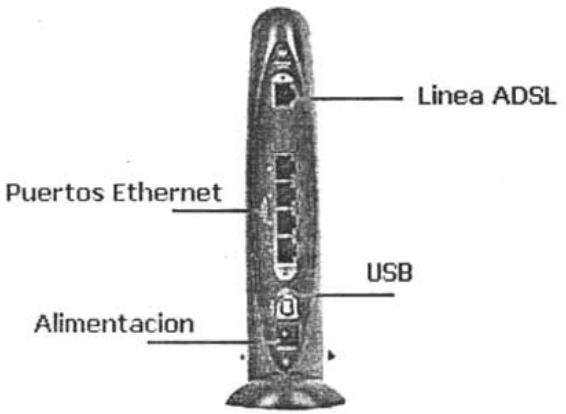


Fig. 4.24 Modem 2 Wire Vista Trasera

b) Interfaces de Red de Banda Ancha

- Modem integrado ADSL que soporta G.dmt (ITU-G.992.1), y ANSI T1.413
- Detector automático de señal ADSL en el Line1 y Line2 (RJ-11)
- Software de Herramientas para la PC
- Instalación Rápida basada en Sistema Operativo Windows y MacOS
- Uso de monitor de red de fondo suministro de supervisión continua y auto configuración de ambiente de red

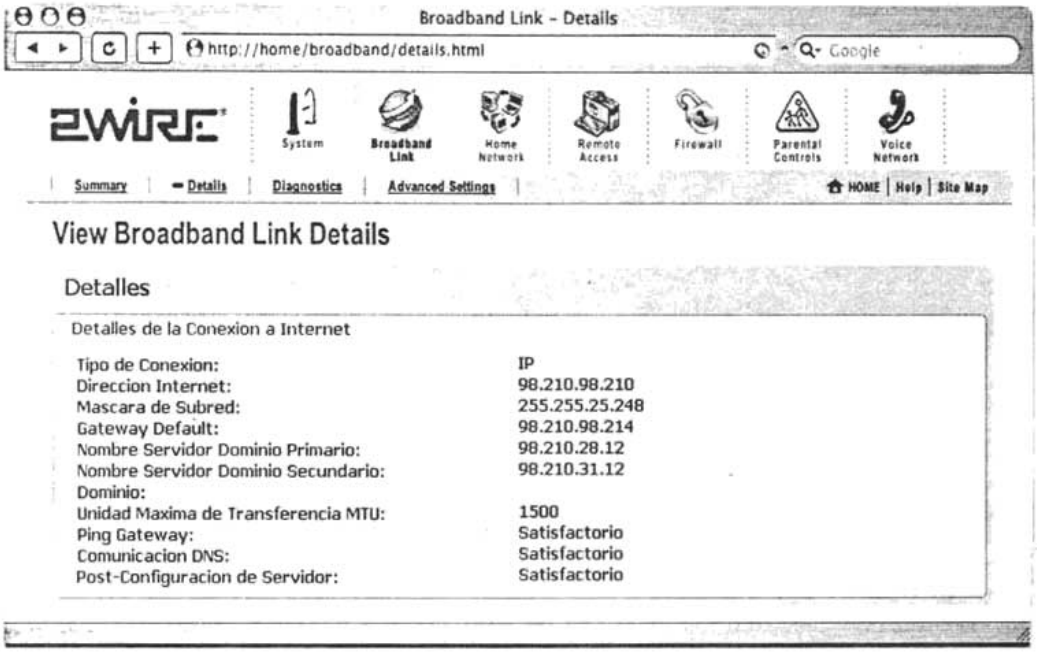


Fig. 4.25 Detalles de la Conexión a Internet

El Home Portal también nos proporciona detalles de la conexión de Banda Ancha y de la Red LAN; en al figura de arriba se muestra la dirección IP que adquiere de la Internet a si mismo la Mascara de Subred, la dirección IP del Gateway que cuando no hay físicamente uno configurado, este valor es el mismo que el de Internet.

Si se tiene configurada una LAN en administración de tipo servidor. Es decir en un Dominio, el Home Portal también nos mostrara los detalles del DNS Primario y el Secundario.

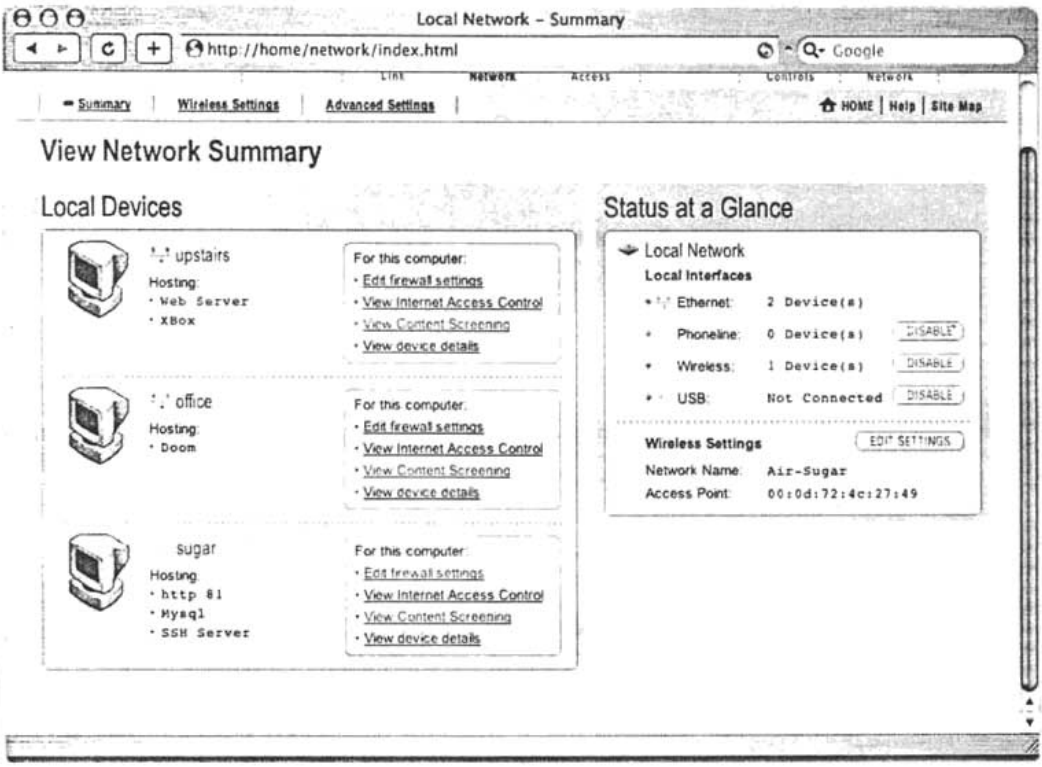


Fig. 4.26 Detalles de Red LAN

Respecto a la configuración de la Red; tiene una interfaz de usuario simple a base de Web para configuración fácil y diagnóstico, la ya mencionada página rápida de sumario con accesos rápidos a características más comúnmente usadas, y la ayuda dinámica en línea presenta la última información a usuarios y al administrador.

Y hablando de interoperabilidad soporta los siguientes protocolos.

Protocolos Soportados

- ATM UNI
- IPv4, TCP, UDP, ARP, ICMP
- DHCP cliente y servidor, DNS cliente y servidor
- HTTP cliente y servidor
- SNMP agente de soporte (deshabilitado por default)
- PPPoE, PPPoA, PAP, CHAP, RFC 2684/1483 encapsulacion Ethernet
- Soporta PPPoE 8-byte MSS ajustado para prevenir fragmentación de IP en Internet, proviniendo máxima interoperabilidad con Servidores de Internet

- Detección Automática del circuito AAL5 y encapsulacion.
- Servicios LAN
- Conmuta entre todas las interfaces LAN disponibles (HomePNA, Ethernet, USB, y Wireless)
- DHCP integrado y servidores DNS para conectividad de plug and play
- Descubre automáticamente direcciones IP estáticas en la subred local para prevenir duplicar direcciones de IP

Lo que se refiere al diagnóstico y detección de fallas, se cuenta con Leds Indicadores que supervisan la conexión y ayudan con la solución de problemas.

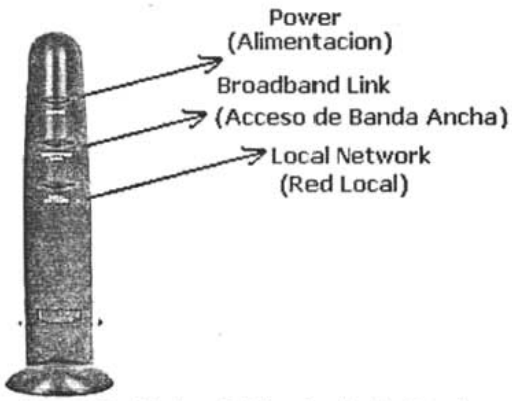


Fig. 4.27 Modem 2 Wire Led's de Estado

Una característica que es muy importante es la seguridad, y en este modelo de router, tiene un Firewall integrado que incluye la inspección de paquetes IP, tienen llave de seguridad única fabricada en cada Home Portal para autenticar conexión de dirección remota de CMS, como cifrado Inalámbrico habilitado por defecto con llave de cifrado única impresa sobre cada unidad y soporta (WPA) Wi-Fi Acceso Protegido y la seguridad WEP.

Resumiendo; esta diseñado para brindar alto nivel de seguridad a nuestra red, como se muestra en la siguiente figura;

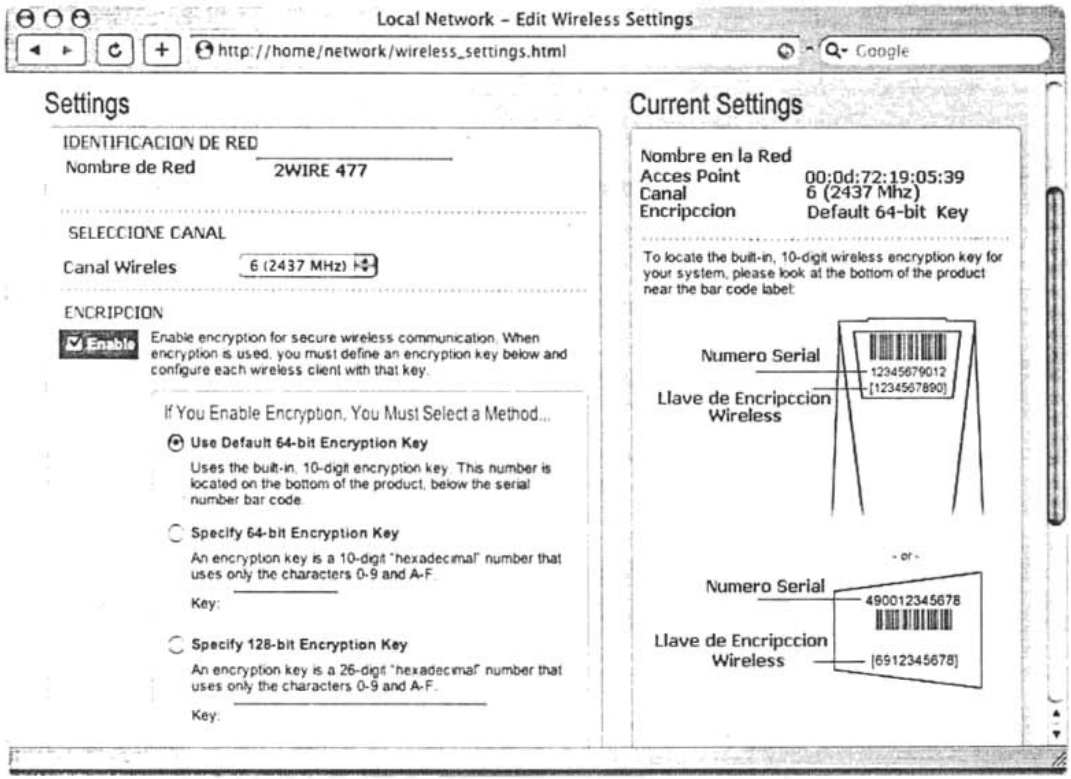


Fig. 4.28 Detalles de la configuración de Seguridad.

El protocolo HyperG aumenta la amplitud de banda inalámbrica por usar un alto poder de 400mW en el transmisor. El Gateway HyperG tiene protocolos de seguridad para la red como el cifrado WEP y WPA. Usando un diseño a base de normas de interoperabilidad, El HyperG mejora el funcionamiento de la red inalámbrica 802.11b y 802.11g; añadiendo adaptadores de HyperG a todos los componentes de la red para experimentar el aún mejor funcionamiento.

4.2 APLICACIONES DE LA TECNOLOGIAS Wi-Fi

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

Las aplicaciones más típicas de las redes de área local que podemos encontrar actualmente son las siguientes:

- Implementación de redes de área local en edificios históricos, de difícil acceso y en general en entornos donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Estas redes permiten el acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes...

En la actualidad, las redes WLAN han encontrado una gran variedad de nuevos escenarios de aplicación, tanto en el ámbito residencial como en entornos públicos.

4.2.1 ESCENARIOS POSIBLES

- **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 varios ordenadores en el hogar. Una variable de este escenario seria el de comunidades de propietarios de viviendas que acuerdan compartir un acceso común.
- **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.
- **Escenario Comercial:** Este quizás es uno de los escenarios en donde las redes WLAN han encontrado expansión pues al pensar que se puede tener acceso publico a Internet Desde cafeterías, tiendas, etc. en base de los llamados Hot Spot, hacen de esta opción una herramienta con muchas ventajas.

También se puede tener acceso publico de Banda Ancha en Pequeños Pueblos, donde es difícil propagar el Internet debido, a lo difícil que a veces resulta extender el cableado, en lugares, de difícil acceso, evidentemente se necesitan múltiples puntos de acceso para garantizar la cobertura del área considerada. En esto se podría incluir zonas geográficas mayores hasta llegar a lo que algunos han denominado Hot City's.

Es necesario distinguir entre: dos tipos de redes: Redes sin animo de lucro (redes libres): que ofrecen un servicio gratuito a una comunidad. Y las Redes con servicios de pago: mismas que ofrecen servicios a los clientes que residen o transitan por la zona de cobertura o las también WLAN para cobertura de "Hot Spot" (escenario publico):

Cuando las Redes Publicas son de pago por servicios, suele haber un operador de telecomunicaciones detrás de su gestión. Un operador establecido, especialmente si es móvil, dispone de gran parte de la infraestructura necesaria para ofrecer un servicio de amplia cobertura.

4.2.2 SERVICIOS PÚBLICOS (HOT SPOTS)

Los Hot Spot, surgieron como un beneficio adicional de la tecnología de Wi-Fi, que se desarrolló para evitar el complejo y costoso proceso de cableado en las casas y edificios de los usuarios.

Se denomina Hot Spot o Zona de Cobertura Inalámbrica, a un lugar donde una Red de área local está disponible para dar acceso público inalámbrico. Esta LAN a su vez puede estar conectada a una Intranet o a la Internet.

En realidad, la instalación de un Hot Spot no es muy complicada, no requiere gran infraestructura. Basta con una línea telefónica para el acceso a Internet, un módem inalámbrico y un Access Point o antena que propague el servicio. Sin embargo los Hot Spots ha encontrado su gran desarrollo en el ámbito comercial, es decir, la facilidad de tener acceso a Internet en lugares públicos y no solamente en casa o en la oficina.

Los Hot Spot suelen ubicarse principalmente en zonas de alto tráfico humano como Aeropuertos, Estaciones de Transporte Terrestre, Hoteles, Centros Comerciales, Centros de Convenciones, Restaurantes, Campus Universitarios, Cafés, Librerías, e incluso ya se están experimentando en algunos aviones comerciales, donde esta tecnología permite al usuario cumplir con su trabajo o hacer uso recreacional de la Internet.

Fig. 4.29 Hot Spot en una Universidad

4.2.3 OPERADORES WIRELESS ISP

En algunos casos el acceso inalámbrico es gratuito (patrocinado por los dueños del lugar), en otros, el Wiireless ISP (Proveedor del Servicio de Internet inalámbrico) establece un cobro por el uso del servicio.

Obviamente, estar suscrito a un ISP inalámbrico con gran cobertura multiplica las posibilidades para poder usar el servicio, pero imaginemos que toda la ciudad fuera un Hot Spot; es decir múltiples Puntos de Acceso cubriendo al Valle de México, proporcionando así múltiples ventajas, tanto en el ámbito de los negocios, con la ventaja de seguir trabajando, o en constante comunicación con la oficina o fuera de ella, para el personal de ventas de cualquier empresa, teniendo acceso a recursos que proporciona la red de la empresa o la misma Internet, en las Universidades, colaborando el aprendizaje del estudiante, y el intercambio de recursos que podría proporcionar la misma escuela. Son inmensas las aplicaciones que se podrían encontrar teniendo a nuestra ciudad como un Hot Spot.

En el caso de los Hot Spot de Prodigy Móvil® de Telmex®, si eres cliente de su servicio de Prodigy Infinitum®, ya tienes el servicio de acceso gratuito a sus Hot Spot que se encuentran ubicados en distintos lugares en la Republica Mexicana.

Wi Fi™
ZONE

Fig. 4.30 Logo que indica un Hot Spot

A continuación se en lista una tabla con los registros de disponibilidad de Hot Spots en México.

Localidad	Hot Spots
Aguascalientes	2
Baja California	5
Baja California Sur	4
Campeche	2
Chiapas	4
Chihuahua	5
Ciudad de México	224
Coahuila	8
Colima	4
Durango	3
Edo de Méx.	34
Guanajuato	6
Guerrero	13
Hidalgo	2
Jalisco	41
Michoacán	2
Morelos	3
Nayarit	1
Nuevo León	34
Oaxaca	2
Puebla	13
Querétaro	12
Quintana Roo	24
Sn Luís Potosí	3
Sinaloa	6
Sonora	5
Tabasco	3
Veracruz	9
Tamaulipas	4
Tlaxcala	N.D.
Yucatán	4
Zacatecas	1
Total	483

Tabla 4.1 Localidades WI-Fi en México

Fuente según Movilspot.com® que es un portal en Internet que ofrece de forma gratuita una base de datos actualizada de puntos de acceso al Internet inalámbricos en el país.

Existen otros proveedores de acceso como Cablevisión®, MVS ®, Megacable® y Boingo ®, con sus propios esquemas tarifarios, y también sitios donde el dueño del lugar cobra el consumo del servicio directamente como lo hacen los Cafés Internet. Actualmente, las velocidades de acceso varían de 11Mbps hasta 54 Mbps, dependiendo del tipo de tecnología instalada en el Hot Spot (802.11b o 802.11g), y del acceso de banda ancha contratado (ej. Infinitum de 256 kbps o 2 Mbps) y del número de usuarios que se conecten.

Fig. 4.31 Los Hot Spot proporcionan múltiples ventajas

Parte de los Hot Spot en el Distrito Federal funcionan en los restaurantes de las cadenas Sanborn´s, Vips, La Estrella de Galicia; cafeterías como Café Caffe, la Librería Porrúa, Parque Duraznos, el Aeropuerto, e instituciones educativas, como las universidades del Valle de México, la Universidad Panamericana y recientemente la Universidad Autónoma de México.

Con esta nueva alternativa tecnológica, los comercios serán más atractivos para los clientes debido a que, además de comer o beber una taza de café, podrán estar conectados permanentemente a Internet, con lo cual podrán continuar con su trabajo o recreamiento.

El correo electrónico es la aplicación más utilizada vía Hot Spot. Otras aplicaciones que son posibles, son la recepción de los archivos adjuntos ("attachment") de correos electrónicos, video en "vivo" (Webcast), audio directo ("streamming audio") y conexión a la Red de la empresa de trabajo (Intranet).

Las LapTops son los dispositivos primarios utilizados para accesar a los Hot spot. Sin embargo, hay interés por utilizar teléfonos inteligentes y PDAs en el futuro gran porcentaje de los usuarios actuales de LAN inalámbrico (WLAN)

han aumentado el uso que le dan a su Wi-Fi, esto como resultado de la disponibilidad de los Hot spot.

Debido a que este sistema está diseñado básicamente para computadoras portátiles, se requiere una tarjeta de Red Inalámbrica de tipo Wi-Fi, sin embargo las nuevas computadoras portátiles que traen el procesador Centrino de Intel® ya tienen dicha tecnología integrada, por lo que están técnicamente listas para acceder a cualquier Hot spot.

4.2.4 CONFIGURACIÓN TÍPICA DE UN HOT SPOT

La forma de ingresar a un Hot Spot y empezar a utilizar sus ventajas, es muy sencillo, dependiendo de la administración del proveedor, en el Capitulo 2 de este documento, se describen las técnicas de acceso y asociación a un Punto de Acceso, para formar parte de la red.

Sin embargo se resumirá explicando la siguiente figura.

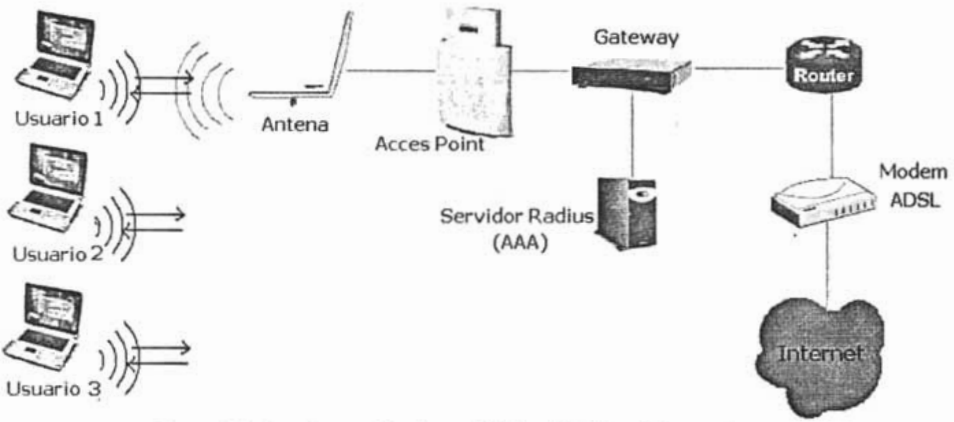


Fig. 4.32 Configuración de un Típica, Hot Spot Pequeño

El ejemplo anterior nos describe un pequeño Hot Spot, en el que forman parte tres usuarios seguros. Suponiendo que se conoce el MAC Address, de la tarjeta de red, y previamente ya se tienen un Username asignado así como una IP, de esta manera se tiene tenemos la siguiente información.

Usuarios	IP Address	MAC Address
1	192.168.1.2	00:04:23:53:B4:4C
2	192.168.1.3	00:0F:1F:CE:8E:DF
3	192.168.1.4	00:04:23:86:B4:32

De tal manera que cuando el Usuario 1 solicita acceso, el Acces Point lee la dirección del MAC del equipo, y el Servidor Radius, busca si ese usuario forma parte de la lista de clientes permitidos, así que el Radius busca el tipo de servicio del usuario, y como la encuentra con permiso, le indica al Gateway que autorice la IP del equipo para que el Router le de salida a Internet, entonces, el Acces Point le regresa su petición como afirmativa.

Lo mismo sucedería con los otros dos usuarios, en la tabla de abajo se encuentra la información que almacena el Servidor Radius, y también puede ver que hay otros dos usuarios, uno; el Usuario 4 el que ya no cuenta con permiso para asociarse a la red, y otro; el Usuario 5 el que tiene configurado un permiso temporal, es decir, que esta restringida su permanencia en la red.

Username	MAC	IP	Expiracion
Usuario 1	00:04:23:53:B4:4C	192.168.1.2	Unlimited
Usuario 2	00:0F:1F:CE:8E:DF	192.168.1.3	Unlimited
Usuario 3	00:04:23:86:B4:32	192.168.1.4	Unlimited
Usuario 4	00:02:2D:6D:5B:53	192.168.1.5	Expired
Usuario 5	00:02:2D:7E:56:6E	192.168.1.6	3884 hr 23 m

Existen Software que permite administrar la red de esta manera, mismo que casi siempre viene incluido con el Gateway, o en el Router, con lo que se puede tener mejor control de nuestro Hot Spot.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso 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.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

Para indicar la compatibilidad entre dispositivos inalámbricos, tarjetas de red o puntos de acceso de cualquier fabricante, se les incorpora el logo "Wi-Fi" (estándar de Fidelidad Inalámbrica), y así los equipos con esta marca se pueden incorporar en las redes sin ningún problema, siendo incluso posible la incorporación de terminales telefónicos Wi-Fi a estas redes para establecer llamadas de voz.

CONCLUSIONES

CONCLUSIONES

Este estándar permite mayor velocidad pero presenta un menor de seguridad, en su implementación normal, y el alcance puede llegar a los 100 metros, suficientes para un entorno de oficina u hogar.

La especificación 802.11b fue ratificada por el IEEE en julio de 1999 y opera en un ancho de banda que abarca las frecuencias dentro del rango de 2.4 a 2.497 GHz del espectro de radio. El método de modulación seleccionado fue DSSS (Modulación de Secuencia Directa de Espectro Extendido) usando CCK (Modulación por Cambios de Código Complementarios), que permite una velocidad máxima de 11 Mbps.

La especificación 802.11a también fue ratificada en esa fecha, pero los productos se hicieron disponibles en el mercado en el año 2001, de tal forma, que su despliegue no fue tan amplio como sucedió con 802.11b. El 802.11a opera en frecuencias entre 5.15 y 5.875 GHz y utiliza el método de modulación OFDM (Multiplexación por División de Frecuencias Ortogonales), el cual hace posible velocidades de hasta 54 Mbps.

El IEEE también está trabajando en el estándar 802.11g, compatible con el 802.11b, capaz de alcanzar una velocidad de hasta 54 Mbit/s, para competir con los otros estándares, que prometen velocidades mucho más elevadas pero son incompatibles con los equipos 802.1b ya instalados, aunque pueden coexistir en el mismo entorno debido a que las bandas de frecuencias que emplean son distintas.

Y referente a la interoperabilidad; en 1999, los líderes de la industria inalámbrica (3Com®, Airones®, Lucent®, Nokia®, etc.) crearon la WECA (Wireless Ethernet Compatibility Alliance), una alianza para la Compatibilidad Ethernet Inalámbrica, cuya misión es la de certificar la ínter-funcionalidad y compatibilidad de los productos de redes inalámbricas 802.11 y promover este estándar para la empresa y el hogar.

Estos son los Estándares para Redes Inalámbricas que ha desarrollado el IEEE.

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
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 Integras –Seguras–Temporales), y AES (Estándar de Encriptación Avanzado).

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 de compañías desde la calle.

La seguridad WLAN abarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica generalmente vienen de los puntos de acceso no autorizados, aquéllos 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).

Un protocolo al nivel de enlace debe tener en cuenta interacciones con diferentes entidades simultáneamente. Los ataques por redirección de IP se basan en la colaboración entre un agente inyector de mensajes al nivel de enlace y un ordenador en algún lugar de Internet. La compleja funcionalidad de un punto de acceso 802.11b lo hace susceptible de tales ataques por todos los flancos. Encarando tales dificultades incluso el profesional de seguridad más experimentado puede cometer serios errores.

Dos formas interesantes de conseguirlo es reutilizar diseños anteriores u ofrecer nuevos diseños para su revisión pública.

Por todo esto se sugieren alternativas para mejorar los mecanismos de seguridad de nuestra red.

Mecanismo de seguridad	Descripción
Especificación original 802.11	Utiliza tres mecanismos para proteger las redes WLAN: - SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para accesar a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía (beacon). - Filtrado con dirección MAC (Control de Acceso al Medio): Restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico. - WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.
802.1X	Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autenticación remota de usuarios entrantes (RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes).

	Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de Llaves Integras –Seguras– Temporales). TKIP fue construido tomando como base el estándar WEP, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación.
WPA (Wi-Fi Protected Access)	Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi. Esta especificación proporciona una mayor encriptación de datos para corregir las vulnerabilidades de seguridad WEP, además de añadir autenticación de usuarios que no se habían contemplado.

Y es que las características del protocolo WEP hacen difícil configurar un sistema seguro. Si se está realmente preocupado por la seguridad no se recomienda utilizar este protocolo. Si sólo se está estableciendo una red casera de dos ordenadores entonces creo que el protocolo WEP será suficiente.

Originalmente las redes WLAN fueron diseñadas para su empleo en redes empresariales. En este tipo de aplicaciones una red WLAN, compuesta por varios Puntos de Acceso, se conecta a una red cableada que permite acceder a todos los servicios disponibles en la empresa, lo que es muy parecido a los Hot Spot.

Los Hot Spot, surgieron como un beneficio adicional de la tecnología de Wi-Fi, que se desarrolló para evitar el complejo y costoso proceso de cableado en las casas y edificios de los usuarios.

Para indicar la compatibilidad entre dispositivos inalámbricos, tarjetas de red o puntos de acceso de cualquier fabricante, se les incorpora el logo "Wi-Fi" (estándar de Fidelidad Inalámbrica), y así los equipos con esta marca se pueden incorporar en las redes sin ningún problema, siendo incluso posible la incorporación de terminales telefónicos Wi-Fi a estas redes para establecer llamadas de voz.

REFERENCIAS Y BIBLIOGRAFIAS

Nota: Para la realización de este documento se consultaron diferentes medios, tanto electrónicos como impresos. Este material esta basado principalmente de paginas Web, se revisaron documentos de fabricantes, proveedores de equipo informático y paginas de consulta. La mayoría de las referencias bibliográficas que se presentan están en idioma ingles, por lo que la traducción de los documentos es personal.

REFERENCIAS Y BILIOGRAFIAS

- **"Wireless LAN; Redes de Área Local Inalámbricas"**
  Fuente: TutoMedia (Tutoriales Multimedia de informática) CD-ROM
  Autor: Alejandro Hernández email: soporte@tutomedia.com

- **"Wi-Fi: Como construir una red inalámbrica"**
  Fuente: 2ª edición Feb 2005
  Autor: Jose Carballar Edit. Alfaomega

- **"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 1999 Edition.**
  Fuente: Web Oficial del Estándar 802.11 URL: http://www.ieee802.org/11

- **"IEEE LAN /MAN STANDARS"**
  En línea URL: http://standards.ieee.org/getieee802/portafolio.html
  Autor: IEEE 802® Dec 27, 2004

- **"IEEE Wireless Standards Zone; Publishes Second Edition to "IEEE 802.11 Handbook: A Designer's Companion"**
  En línea URL: http://standards.ieee.org/wireless/
  Autor: Stuart J. Kerry. (Miembro del Comité IEEE)

- **"IEEE Wireless Standards Zone; IEEE Begins Work to Improve Security of IEEE 802.11"**
  En línea URL: http://standards.ieee.org/wireless/
  Autor: Bob O'Hara (Miembro del Comite IEEE)

- **"IEEE Wireless Standards Zone; IEEE Wireless Communication Standards: A Study of 802.11™, 802.15™, and 802.16™"**
  En línea URL: http://standards.ieee.org/wireless/
  Autor: Todor Cooklev (Miembro del Comite IEEE)

- **"What is Wi-Fi ?"**
  En línea URL: http://www.wi-fi.org
  Autor: Wi-Fi Alliance®. Members

- **"Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks"**
  En línea URL: http://www.wi-fi.com
  Autor: Wi-Fi Alliance April 29, 2003

- **"Wireless Application Protocol Architecture Specification"**
  En línea URL: http://www.wapforum.org
  Autor: Open Mobile Alliance Copyright 2003 ©

- **"WAP Public Key Infrastructure Specification "**
  En línea URL: http://www.wapforum.org
  Autor: Open Mobile Alliance Copyright 2003 ©

- **"Wireless LAN Security"**
  En línea URL: http://www.wlana.org/
  Autor: Wireless LAN Asociation©

- **"Wireless LAN Applications"**
  En línea URL: http://www.wlana.org/
  Autor: Wireless LAN Association©

- **"General Information"**
  En línea URL: http://www.wlana.org/
  Autor: Wireless LAN Association© Cisco Systems, Inc.

- **"Wi-Fi Protected Access"**
  En línea URL: http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf
  Autor: Lisa Grantham (WECA) 03/23/2005

- **"Seguridad en LAN inalámbricas con PEAP y contraseñas"**
  En línea URL:
  http://www.microsoft.com/latam/technet/seguridad/guidance/lan/peap_b.mspx
  Autor: Microsoft ® 4/2/2004

- **"Wi-Fi Protected Access™ (WPA) Overview"**
  En línea URL:
  http://www.microsoft.com/technet/columns/cableguy/cg0303.mspx
  Autor: Microsoft ® 4/2/2004

- **"Tecnologías para redes LAN inalámbricas y Windows XP"**
  En línea URL: http://www.microsoft.com/windowsxp
  Autor: Tom Fout Microsoft Corporación © Julio de 2001

- **"Estándar WLAN"**
  En línea URL:
  www.intel.com/ebusiness/strategies/wireless/wlan/standards.htm
  Agosto 25, 2004

- **"Estándares y mecanismos de seguridad"**
  En línea URL:
  http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm
  Autor: Jaime **Cuéllar Ruiz**

- **"Hot Spot (Acceso Público a Internet)"**
  En línea URL: http://www.srm.com.mx/hotspot.htm
  Autor: Nomadix Service Engine©

- **"Puntos de Acceso Inalambricos"**
  En línea URL: http://www.movilspot.com/
  Autor: Techila Networks, S.A. de C.V. © Copyright 2004,

- **"Manual para verificación de usuarios conectados"**
  Fuente: Red Uno Profigy Movil
  Autor: Diego Carrillo 2005

- **"Detalles Tecnicos 2Wire, Inc. "**
  En línea URL: www.2Wire.com
  Autor: 2Wire, Inc. 2004

- **"Security 802.11 Wireless Networks"**
  En línea URL: www.cisco.com
  Autor: Cisco System´s 2002

- **"Productos Wireless"**
  En línea URL: www.3com.com/wireless
  14 de agosto de 2001

- **"Wireless Security in 802.11 (Wi-Fi) Networks"**
  En línea URL: www.dell.com
  Enero 2003

- **"Wi-Fi, el estándar inalámbrico "**
  En línea URL: http://www.baquia.com/com/20030117/bre00004.html
  Autor: Baquia Inteligencia©

- **"Estandares para el entorno de las Redes Inalámbricas bajo la denominación 802.11b"**
  En línea URL: http://www.e-advento.com/tecnologia/estandares.php#arriba
  Autor: Advento Networks ©

- **"Seguridad en Redes Wireless"**
  En línea URL:
  http://www.e-advento.com/tecnologia/tecnologia_seguridad.php
  Autor: Advento Networks ©

- **"Redes Inalámbricas: Comunicación sin cables"**
  En línea URL: http://www.viedma-web.com.ar/
  Autor: Gpo Financiero Vital 2005

- **"Listado de Hot Spots disponibles en Mexico"**
  En línea URL http://www.vnetmexico.com/entre.html
  Autor: Gpo Financiero Vital 2005

- **"Introduction to IEEE 802.11"**
  En línea URL: http://www.intelligraphics.com/articles/80211_article.html
  Autor: Intelligraphics inc. ©