UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DIVISIÓN DE INGENIERÍA ELÉCTRICA

ESTUDIO Y ANÁLISIS DEL DESEMPEÑO DE REDES WLAN IEEE 802.11

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N:

LUIS DANIEL CERVANTES GONZALEZ
SIGRID YAHAIRA MENESES NIELSEN

DIRECTOR DE TESIS:
DR. JAVIER GÓMEZ CASTELLANOS

CIUDAD UNIVERSITARIA. MARZO, 2005.

m342185

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

DEDICATORIAS

Dedico esta tesis principalmente a mis padres que han sido durante todos los años de mi vida mis principales pilares en todos los aspectos. A ellos que han trabajado tan duro y me han dado todo cuánto cualquiera pudiera desear sin importar lo cansados o enfermos que estuvieran, siempre han estado ahí para ayudarme. En verdad todo lo que soy es gracias a ellos y esta tesis no es sólo un triunfo mío sino de los tres, ya que cada esfuerzo hecho por mi, cada trabajo entregado, cada proyecto realizado, cada examen aprobado estuvo siempre respaldado por palabras de aliento, por un desayuno, comida y cena preparados con cariño, por cuidados y atenciones... por amor paternal.

También dedico esta tesis a mis tías en Tamaulipas, a mi tía Lupi, tía Carmen y tía Margarita que sin que yo se los pidieran siempre estuvieron al pendiente de lo que necesitara, siempre preocupadas por mi salud y desempeño, y siempre dándome ánimos para seguir adelante.

La dedico así mismo a mis hermanos Alexandra y René por ayudarme en esos momentos de urgencia y por haberme ayudado a despejar la mente pasando ratos agradables con ellos.

Y finalmente, a una persona muy especial que ha traído a mi vida lo más grande y maravilloso que jamás soñé... el amor. A ti Nath-Yeli, también te dedico esta tesis por todos los momentos tan hermosos que hemos compartido, por todos los bellos recuerdos que hemos formado juntos, y sobre todo por haberme enseñado que de nada sirve tener el mejor promedio o el mejor empleo si no se tiene con quien compartir la dicha y el júbilo de los triunfos logrados.

-Luis Daniel

DEDICATORIAS

A mis padres Guillermo y Siegrit,
Por el cariño y dedicación
que han puesto en mi
y mi hermano Alistair
por su apoyo incondicional
Con todo mi amor
¡Gracias ¡

Sigrid

AGRADECIMIENTOS

Agradezco a Dios el haber guiado mis pasos hasta este momento.

Doy gracias a mis padres y es a ellos a quien principalmente dedico esta tesis como un triunfo por haberme infundado todos mis principios morales, todo su amor y cariño y su incomparable apoyo y cuidados durante toda mi vida, dejando que me preocupara por cumplir con mis deberes mientras ellos se ocupaban del resto.

Agradezco a los profesores que tuve durante toda mi vida, a los buenos por que supieron transmitir sus conocimientos y enriquecer los míos propios, y a los malos por que me enseñaron a no conformarme con lo poco sino a buscar por mi propia cuenta formando en mi una conciencia autodidacta.

Agradezco a mis familiares y a los amigos que siempre me ayudaron y apoyaron y sin cuya ayuda no habría llegado hasta aquí.

Agradezco a la DGAPA/PAPIIT por el material brindado para las pruebas y por las becas otorgadas.

Finalmente, agradezco a mi novia Nath-Yeli todo su amor, cariño y apoyo ya que ha llenado mi vida de gran dicha y felicidad. ¡Te amo!.

Luis Daniel Cervantes González.

AGRADECIMIENTOS

Doy infinitas ¡Gracias! a mis padres, que me dieron la vida y me han dado todo aquello necesario para hacer de mí una persona de bien y de valores íntegros; por sus consejos, y su paciencia. Además, les agradezco que me hayan infundado el amor por el conocimiento y darme la ocasión e instrumentos para perseguirlo. Gracias infinitas, por apoyarme en cada etapa y momento de mi vida, y brindarme la oportunidad única de tener mi carrera universitaria.

Agradezco a mi hermano Alis, por ser mi mejor amigo y confidente, me has enseñado muchas cosas, todavía tenemos mucho que aprender y espero que lo hagamos juntos.

Agradezco a mis profesores, por guiarme y acercarme al conocimiento, creando en mi, tener una firme conciencia de lo que me rodea, así como de crearme un juicio y criterio amplio, que me permite día a día afrontarme a la vida.

A Elizabeth, por tu gran amistad, apoyo y ayuda incondicional.

A Trini, Ariadna, Lorena y Vanesa por ser mis mejores amigas, por brindarme su confianza, amistad y su apoyo en estos años, por sus consejos en tiempos buenos y malos. Y recuerden que tienen una amiga para siempre.

A todos mis amigos y compañeros de carrera, que no me atrevo a enumerar por no querer excluir a nadie, les agradezco de igual manera su apoyo y por todos aquellos momentos divertidos que hemos pasado.

Al Dr. Javier Gómez, por ser nuestra guía en la realización de esta tesis y darnos sugerencias para hacer un mejor trabajo.

A la DGAPPA PAPIIT, por permitirnos participar en este proyecto, y apoyarnos con material para desarrollar nuestras ideas y plasmarlas en esta tesis.

A la Facultad de Ingeniería, por brindarme la oportunidad de tener una educación de primer nivel y darme todas las herramientas para hacer de mi una excelente profesionista conciente de las necesidades de mi país.

Y a mi alma mater, la UNAM, por estos años en que ha compartido su fuente de conocimientos e inculcarme un espíritu de universitario. ¡Gracias por todo lo que me has brindado!

Y por ultimo ¡Gracias! A todas aquellas personas que me han ayudado a llegar a este punto del camino, sin su ayuda y apoyo no lo hubiera logrado, nuevamente Gracias y espero que nos volvamos a encontrar en esta senda que es la vida.

¡Gracias!

Sigrid Yahaira Meneses Nielsen

TABLA DE CONTENIDO.

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

OBJETIVOS

Con el paso de los años, el ritmo de vida se ha vuelto mas dinámica, por lo tanto se requiere de nuevas herramientas y tecnología que resuelvan estas necesidades: mayor movilidad, mayor capacidad de transmisión de datos y costo económico. A partir de ese momento, se han ido desarrollado nuevas soluciones en TI que resuelvan esta necesidad. Con el nacimiento y auge de la telefonía celular, se pensó que se tenia el camino ganado, pero en muy poco tiempo esta se volvió insuficiente y plana, las necesidades crecieron, era necesario una tecnología mas eficiente que permitiera la transmisión de elementos multimedia :imágenes y video en tiempo real. De ahí el nacimiento de la redes inalámbricas, estas a pesar de que no han cubierto las características de una red alámbrica, son una solución viable y económica. A partir de ese momento, este tipo de redes han tenido una rápida proliferación y expansión, esto debido a que las empresas han visto en esta solución de TI, una respuesta a las necesidades del usuario. Por lo tanto cada vez los costos son menores y sus beneficios mayores. Sin embargo, para poder administrar y monitorear estas redes existen pocas herramientas que brinden la información necesaria para su análisis. Las herramientas o software propietario en ocasiones resulta insuficiente y no es posible su modificación, para lograr los objetivos deseados; es por eso que este trabajo tiene como objetivo:

- Realizar un estudio y análisis de las redes inalámbricas bajo el estándar IEEE 802.11b, entender su funcionamiento en cada una de las capas que le conforman : PHY y MAC , así como identificar ventajas y desventajas de esta tecnología, así como sus debilidades y poder enfrentar sus problemas y proponer soluciones.

- Analizar las diversas herramientas de monitoreo y administración, bajo la plataforma Linux; para definir las características de estas herramientas y con estas crear un punto de partida para la creación de una herramienta propia dinámica y sencilla que englobe los beneficios de las herramientas anteriores y que proporcione los datos más representativos y útiles en el diseño, control e implementación de estas redes. Dicha herramienta estará enfocada a los estudiantes e investigadores del habla hispana. Es importante hacer notar que la herramienta será diseñada para el sistema Linux debido a sus políticas de software libre

- Caracterizar una red inalámbrica, con el uso de la herramienta creada y definir las características reales de transmisión de este tipo de redes de datos.

CAPÍTULO 1
INTRODUCCIÓN.

1.1 Técnicas de acceso al medio (MAC).

En los protocolos IEEE 802 para redes LAN compartidas de acceso múltiple, la capa de enlace (data link) está dividida en dos sub-capas: la capa superior LLC (Logical Link Control), que provee una forma de direccionar una estación en una LAN e intercambiar información con ella y la capa inferior MAC provee la interfaz entre el LLC y el medio en particular de la red que esté siendo utilizada (Ethernet, Token ring, etc.).

La capa MAC reparte datos agrupados en un frame para que se transmitan por la red, y luego pasa este frame a la interfaz de capa física donde son transmitidos en forma de bits. La información se envía en distintos frames que se transmiten uno a la vez por la red. Si un frame se corrompe (tiene errores) durante la transmisión, sólo es necesario reenviar dicho frame y no la información completa.

El otro trabajo de la capa MAC es la de controlar el acceso al medio que es compartido por todos los dispositivos conectados a la red. Si dos estaciones fueran a transmitir al mismo tiempo, los datos se mezclarían y se dañarían por lo que no sería posible la comunicación. Los métodos de acceso primario son *de contención* y *de detección de portadora.*

1.1.1 Protocolos de contención.

1.1.1.1 ALOHA.

Este método de acceso al medio es el precursor de varias estrategias de acceso aleatorio actuales. En este esquema un usuario que desee transmitir lo hace en cualquier momento. A causa de esto es probable que dos o más mensajes se traslapen en tiempo, causando una colisión. Dicha colisión es detectada por cada estación y cada una de estas intenta retransmitir después de transcurrido un tiempo aleatorio, siguiendo un algoritmo de resolución de colisiones, para evitar una nueva colisión.

Figura 1-1. Ejemplo de estaciones transmitiendo en cualquier momento.

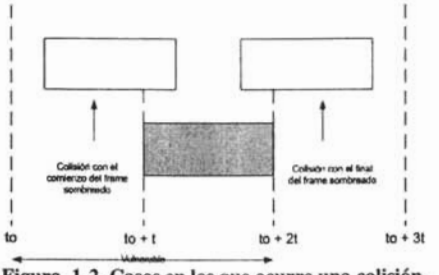


Figura 1-2. Casos en los que ocurre una colisión.

Sin embargo esta estrategia de ALOHA, aunque muy simple, representa un gran desperdicio de ancho de banda, consumiendo solo un 18% de la capacidad del canal como máximo.

1.1.1.2 ALOHA Ranurado.

La limitante y los problemas del protocolo ALOHA son tratados en este método donde se tiene la variante de dividir el tiempo en intervalos o "ranuras". Las estaciones que deseen transmitir sólo podrán hacerlo al inicio de cada intervalo de tiempo. Este esquema requiere que todas las estaciones estén en un sistema sincronizado de tiempo.
Puesto que los paquetes de datos sólo pueden ser transmitidos en los intervalos de tiempo mencionados, pueden ocurrir colisiones cuando dos o más estaciones intenten transmitir al mismo tiempo. Si ocurre una colisión cada estación espera un tiempo aleatorio dado por una distribución exponencial. En la figura 1-3 se muestra una comparación de paquetes transmitidos efectivamente según el número de intentos de retransmisión.

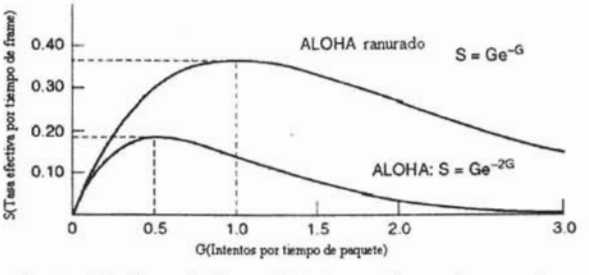


Figura 1-3 . Tasa efectiva vs. Intentos por tiempo de paquete.

1.1.2 Protocolos de detección de portadora.

1.1.2.1 CSMA no persistente (Carrier Sense Multiple Access).

En este tipo de protocolos la estación que desea transmitir "escucha" primero el canal de transmisión para ver si está libre. Si es así, la estación transmite sus datos. En caso contrario la estación no transmite y espera un tiempo aleatorio antes de volver a escuchar el canal.
Aún así, se puede dar el caso de que dos estaciones que quieren transmitir escuchen el canal al mismo tiempo, y al ver que el canal se encuentra libre transmiten sus datos respectivos ocasionando una colisión. También se puede dar el caso que por retardos de propagación una estación detecte erróneamente un canal libre.
Este tipo de esquema reduce en gran manera el número de colisiones sin embargo es algo ineficiente ya que desperdicia el uso de canal, ya que existen tiempos muertos en los que no se realiza ninguna transmisión.

1.1.2.2 CSMA 1-persistente.

El CSMA 1 persistente es una variación del no persistente, aquí la estación que desea transmitir escucha el canal. Si está libre transmite, en caso contrario continua escuchando el canal (sin esperar un tiempo aleatorio) hasta que detecte que se encuentra disponible para transmitir. Las colisiones se generan de la misma manera que en el CSMA no persistente.
Después de detectarse una colisión, cada estación espera un tiempo aleatorio antes de intentar transmitir de nuevo.

1.1.2.3 CSMA p-persistente.

Similar al protocolo anterior, sin embargo cuando encuentra el canal libre **transmite dada una probabilidad *p*.** El tiempo de espera antes de volver a escuchar es de ***q=1-p***. Este esquema se utiliza en canales con tiempo ranurado por lo que la espera probabilística es hasta la siguiente ranura. En la siguiente figura mostramos una comparación del desempeño de los protocolos hasta ahora vistos.

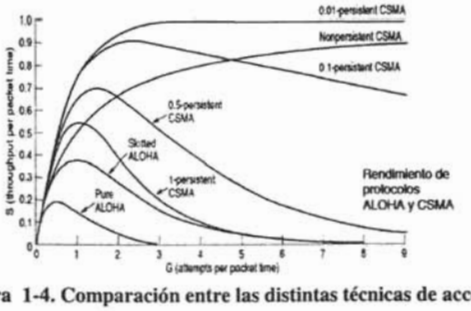


Figura 1-4. Comparación entre las distintas técnicas de acceso.

1.1.2.4 CSMA C/D (CSMA con detección de colisiones).

El concepto básico de este protocolo es muy simple. El funcionamiento en general es similar a los CSMA vistos anteriormente. Cuando ocurre una colisión es detectada por las estaciones y transmiten una señal a las demás estaciones para que aborten sus transmisiones. Entonces cada estación espera un tiempo aleatorio (de contención) antes de intentar retransmitir. Si el canal sigue ocupado (o se detecta otra colisión), el tiempo de espera aleatorio aumenta al doble. Este esquema se repite hasta que el tiempo de espera aleatorio llega a un valor máximo y es en este punto donde la estación se rinde y notifica a los niveles de capas superiores que la transmisión fue fallida.

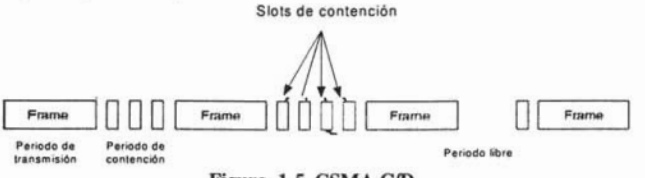


Figura 1-5. CSMA C/D

El aumentar al doble el intervalo de espera es referido a un procedimiento de *backoff* binario y es realizado para mejorar el desempeño del sistema. La figura 1-5 ilustra un esquema del protocolo CSMA C/D.

1.1.3 Protocolos de tecnologías inalámbricas.

Hasta ahora se han descrito de forma breve algunos protocolos de acceso al medio para redes que utilizan un canal alámbrico. Hemos visto que el más utilizado es el de CSMA por su desempeño y capacidad de detectar colisiones.
Sin embargo este tipo de esquemas no funcionan en el medio inalámbrico debido a ciertas complicaciones:

- La fuerza de la señal disminuye proporcionalmente a $2<n<4$ de la distancia entre base y estación.
- El transmisor podría aplicar CS y CD pero las colisiones ocurren en el receptor.
- Se puede dar el caso que el transmisor no "escuche" la colisión. (CD no funciona).
- CS podría no funcionar (caso de terminal oculta).

Es por eso que se desarrollaron diferentes métodos de acceso para las tecnologías inalámbricas (telefonía móvil, WLAN). A continuación veremos una breve descripción de métodos de acceso al medio para este tipo de tecnologías.

1.1.3.1 FDMA (Acceso Múltiple por División de Frecuencia).

En el esquema de telefonía móvil, consiste en dividir un canal con un ancho de banda específico en varios canales virtuales con un ancho de banda menor, esto es, se segmenta el espectro disponible en canales independientes y se asigna a los distintos abonados. Se asigna a cada uno de éstos una frecuencia específica, la cual debe estar dentro del rango de

frecuencias que constituyen el canal total. Llevando al límite el esquema FDMA, puede dividirse el ancho de banda disponible en miles de sub-canales que se asignan a los abonados aisladamente o en grupos, de acuerdo con las necesidades de capacidad de transmisión de cada uno. Cada frecuencia sólo puede ser usada por un usuario durante una llamada. Debido a la limitación en ancho de banda, esta técnica de acceso es muy ineficiente ya que se saturan los canales al aumentar el número de usuarios alrededor de una celda.

Como ya se mencionó anteriormente, en este esquema a cada comunicación se le asigna un canal virtual particular. El móvil y la base deben filtrar la información recibida de tal manera que sólo escuchen la conversación que están llevando a cabo. Este esquema de acceso es muy común. De hecho se utiliza en todos los sistemas para dividir el espectro de frecuencias en dos canales: Un canal que lleva información de la base al móvil y que se llama *forward-link*, y un canal que lleva información del móvil a la base y que es el *reverse-link*. El esquema de acceso múltiple FDMA es el único que puede ser utilizado en telefonía celular analógica, aunque también puede ser utilizado para telefonía celular digital. FDMA no necesita sincronía pero sí un control de potencia para evitar interferencia entre celdas adyacentes.

1.1.3.2 TDMA (Acceso Múltiple por División de Tiempo).

Consiste en dividir un canal con ancho de banda determinado en ranuras de tiempo, de manera que los canales virtuales se crean asignando a cada comunicación una ranura de tiempo. Si se tiene, por ejemplo, un canal de 30 Khz. y lo dividimos en tres ranuras de tiempo, podemos enviar información de tres comunicaciones que utilicen cada una 10 Khz. La primera comunicación utilizaría siempre la primera ranura, la segunda comunicación la segunda y así sucesivamente. Por el canal de comunicaciones se transmiten en secuencia la primera ranura, la segunda, la tercera, de nuevo la primera, la segunda, etc.
De esta manera, todos los abonados comparten la totalidad del ancho de banda disponible pero sólo lo utilizan durante los períodos de tiempo en los que les es permitido. Estos períodos se llaman slots o ranuras temporales. Un sistema más eficiente asignaría dinámicamente los slots a los usuarios que los requirieran para optimizar el uso del espectro.

El esquema de acceso múltiple TDMA normalmente se aplica en conjunto con el FDMA. Se utiliza FDMA para dividir el canal físico en varios canales lógicos, y cada canal lógico se multiplexa utilizando TDMA. Un sistema puro TDMA tendría sólo una frecuencia de operación, y no sería un sistema útil.

TDMA implica el uso de técnicas de compresión de voz digitales, que permite a múltiples usuarios compartir un canal común utilizando un orden temporal. La codificación de voz moderna reduce mucho el tiempo que se lleva en transmitir mensajes de voz, eliminando la mayoría de la redundancia y periodos de silencio en las comunicaciones de voz.

1.1.3.3 CDMA (Acceso Múltiple por División de Códigos).

CDMA es un término genérico que define una interfase inalámbrica basada en la tecnología de espectro disperso (spread spectrum). En los sistemas CDMA todos los usuarios transmiten en el mismo ancho de banda simultáneamente.

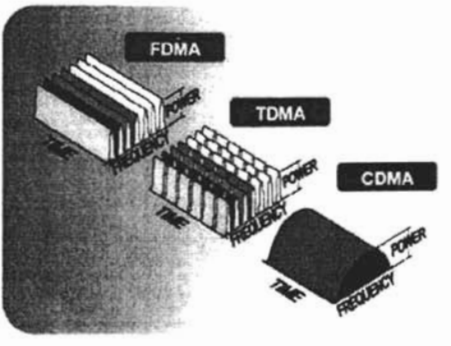


Figura 1-6. FDMA, TDMA y CDMA.

En esta técnica de transmisión, el espectro de frecuencias de una señal de datos es esparcido usando un código no relacionado con dicha señal. Como resultado el ancho de banda es mucho mayor. En vez de utilizar las ranuras de tiempo o frecuencias, como lo hacen las tecnologías tradicionales, usa códigos matemáticos para transmitir y distinguir entre conversaciones inalámbricas múltiples. Los códigos usados para el esparcimiento tienen valores pequeños de correlación y son únicos para cada usuario. Esta es la razón por la que el receptor de un determinado transmisor, es capaz de seleccionar la señal deseada.

Una señal de espectro disperso CDMA es creada para modular la señal de radiofrecuencia con una sucesión esparcida (un código que consiste de una serie de impulsos binarios) conocido como un pseudo-ruido (PN), esta es una secuencia de números con un periodo determinado. El PN de código se ejecuta a una tasa más alta que la señal binaria y determina el ancho de banda real de transmisión.

1.1.3.4 CSMA C/A (Supresión de Colisiones).

Uno de los principales problemas con los métodos de acceso en capa MAC (datos) convencionales eran las terminales ocultas. Supongamos que una estación A desea transmitir a una estación B al mismo tiempo que una estación C desea transmitir información a B. Debido a la separación geográfica A y C no se pueden escuchar, por lo que ambas estaciones detectarían el canal libre, transmitirían y obviamente ocurriría una colisión.
Se dice en este caso que A es terminal oculta de C y viceversa.

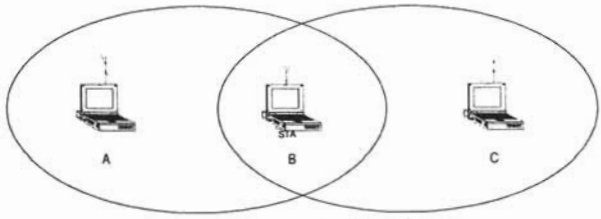


Figura 1-7. Terminales ocultas.

El protocolo CSMA C/A resuelve este conflicto.
Si la estación A desea transmitir a B primero pide permiso a dicha estación mediante un paquete RTS (*Request To Send*). Si está libre, B manda como respuesta un CTS (*Clear To Send)* y A puede mandar los datos hacia B. Si la información llegó por completo, B manda un ACK (ACKnowlegment) hacia todas las estaciones indicando la transmisión exitosa y que el canal virtual está libre. Aquellas estaciones cercanas al rango de A que hayan escuchado el RTS y aquellas cercanas a B que hayan escuchado el CTS calculan un periodo durante el cual detendrán todo intento de transmisión. Dicho periodo es conocido como NAV (*Network Allocation Vector*).

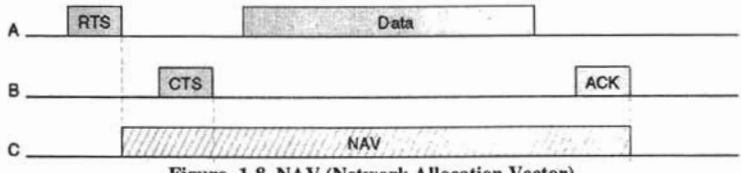


Figura 1-8. NAV (Network Allocation Vector)

En el caso de que ambas estaciones A y C envíen un RTS al mismo tiempo se produce una colisión por lo que ambas estaciones esperan un tiempo aleatorio corto antes de volver a retransmitir. Si llegara a ocurrir un segunda colisión (este caso tiene una probabilidad muy baja) se incrementa el tiempo de espera por medio de un algoritmo llamado *exponential backup* que alarga el tiempo de espera en forma exponencial. En el caso extraño que ocurra una tercera colisión, se aplica nuevamente el algoritmo.

1.2 Redes Inalámbricas de Área Local (WLAN).

El objetivo de una red inalámbrica es el permitir a dispositivos fijos y portátiles comunicarse entre si de manera inalámbrica, eliminando o minimizando la infraestructura cableada, además permite a los usuarios tener movilidad y no permanecer en un punto fijo, permitiendo que exista comunicación en zonas geográficamente limitadas. Estas ventajas permiten que las redes inalámbricas sean utilizadas en cualquier campo.
A lo largo de esta sección, daremos un panorama un poco más detallado de lo que son las WLAN, sus formas de trabajo, su arquitectura, etc.

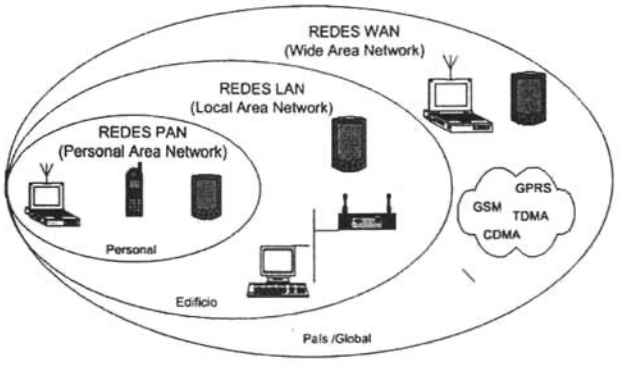


Figura 1-9. Ubicación de las Redes WLAN.

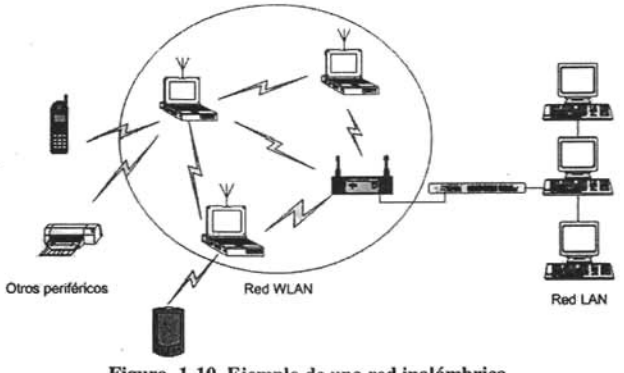


Figura 1-10. Ejemplo de una red inalámbrica.

1.2.1 Antecedentes históricos.

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

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread-spectrum"(frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en "spread-spectrum". ISM es una banda para uso comercial

sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda.
La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

1.2.2 Componentes de una red inalámbrica.

Veremos lo principales tipos de equipo utilizados para la construcción de una red inalámbrica, y que serán utilizados por las estaciones para una apropiada interconexión y comunicación entre los equipos.

1.2.2.1. Terminales-cliente.

Las terminales cliente necesitan adaptadores específicos, como PC-Cards, USB, etc. En algunos casos el adaptador y el equipo forman un conjunto indisoluble orientado a cumplir una función muy específica (adaptadores multimedia, servidores de impresión, etc.).

- *PC-CARDS.* De uso muy difundido entre las computadoras portátiles, y otros dispositivos móviles. Son de tamaño pequeño, y su mayor desventaja son sus pequeñas antenas (en algunos casos pueden ser sustituidas por unas más grandes).
- *PCI.* Utilizado en equipos de sobremesa, cuando estas deben cambiarse de ubicación con frecuencia. Su inconveniente es la necesidad de abrir el equipo para insertar la tarjeta. Su antena puede ser sustituida por una de mayores prestaciones.
- *USB.* Su mayor ventaja es no necesitar alimentación externa, son de tamaño pequeño y se pueden orientar fácilmente y tener una mejor recepción. Muy recientemente han aparecido adaptadores con la especificación USB 2.0. La razón de ello es que el potencialmente elevado bit rate que se puede obtener mediante los estándares 802.11g y 11a (54 Mbps teóricos, por debajo de 25 Mbps en la práctica), superaba con creces las capacidades de la antigua especificación del bus USB 1.1 (7 Mbps útiles) lo que representaba un cuello de botella ya solucionado en la nueva versión.

1.2.2.2 Equipos dedicados.

Nuevos equipos en el sector hogar han ido apareciendo como: adaptadores para consolas de juegos, equipos de sonido, televisiones y pantallas, cámaras fotográficas, cámaras de vigilancia, adaptadores para la interconexión a cualquier elemento multimedia, etc. con interfaces Wi-Fi. Para la oficina ya se disponen, además de los anteriores, de adaptadores para impresoras remotas, sistemas de proyección de PC, PDA y terminales para usos de logística, etc. Pero quizás la clave esté destinada a otro uso: la telefonía y transmisión de voz por IP sobre redes inalámbricas.

1.2.2.3 Puntos de Acceso (Access Point ó AP).

Es un nodo especial que actúa como punto centralizador y gestor del tráfico del resto de equipos (terminales de cliente) subscritos a él y dentro de la celda de cobertura. Dispone comúnmente de una interfaz Ethernet que le permite estar interconectado a una red cableada (LAN), además de la interfaz inalámbrica por la cual se conectan los equipos de dicha naturaleza. Permite la comunicación entre ambas interfaces y entre los propios equipos inalámbricos a nivel 2 (modelo OSI). En general en un mismo lugar pueden coexistir más de un punto de acceso siempre que no interfieran fuertemente sus frecuencias de funcionamiento. Los equipos presentes estarán subscritos sólo a uno.
Los puentes de acceso tienen a parte de su función fundamental, otras funciones como son:

- *Puentes (Bridges).* Son elementos que interconectan dos o más redes locales (a nivel 2 OSI). Poseen dos interfaces, uno Ethernet y otro inalámbrico.
- *Repetidores* .Extienden la cobertura de los Puntos de Acceso mediante la regeneración y re-envío de información a zonas anteriormente sin suficiente señal. Su desventaja: dado que toda la información que un equipo le transmite la tiene que remitir al Punto de Acceso, la eficiencia de la solución es inferior al 50%. También es factible encadenar numerosos repetidores para ampliar todavía más el alcance, pero numerosos problemas que aparecen por colisiones, retardos de señal y penalización en el uso del espectro, no aconsejan emplear más de uno.
- *Enrutadores y Puertas de Enlace (Routers y Gateways).* Poseen capacidad de enrutamiento (niveles 3 y 4 OSI) de los paquetes de información que los atraviesan. Una de sus interfaces es inalámbrica, existiendo al menos otra fija Ethernet a la cual se suele denominar puerto WAN. La mayoría de modelos existentes en el mercado no posee funcionalidades puras de enrutador, sino que están especialmente diseñados para actuar como pasarela entre la red inalámbrica directamente gestionada por el equipo (genéricamente llamada LAN) y las redes externas (red local de empresa, red de acceso a Internet u otras). Por ello con frecuencia se les denomina puertas de enlace (gateway).

1.2.2.4 Antenas.

Los equipos anteriores poseen habitualmente uno o dos conectores mediante los cuales se pueden acoplar antenas externas para la emisión de la señal inalámbrica. También se encuentran otros modelos con antenas internas o no reemplazables, lo que limita su uso en muchas instalaciones. Atendiendo a la ubicación, las antenas pueden ser de interiores o de exteriores. En las primeras prima el volumen pequeño, la estética y no suelen ser de gran potencia. En las segundas es su robustez frente al medio. Por la forma de su patrón de emisión, hay omnidireccionales (cobertura circular), direccionales o sectoriales (cubren un determinado ángulo) y muy directivas (ángulos por debajo de los 12 grados). Además de todo lo anterior, hay que tener en cuenta la ganancia que presenta cada modelo de antena para realizar correctamente un diseño, encontrando modelos comerciales desde 2 a 24 decibelios (dB). Otras clasificaciones atienden a la tecnología de diseño (parabólicas, Yagi, helicoidales, de panel, etc.) y a la polarización de la señal (lineal -horizontal o vertical- y circular -izquierda o derecha-).

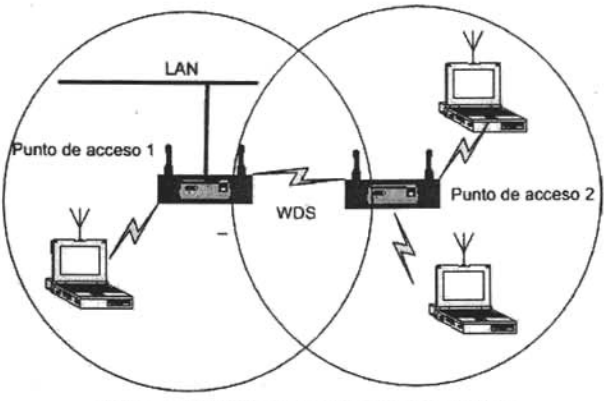


Figura 1-11. Punto de acceso en modo repetidor

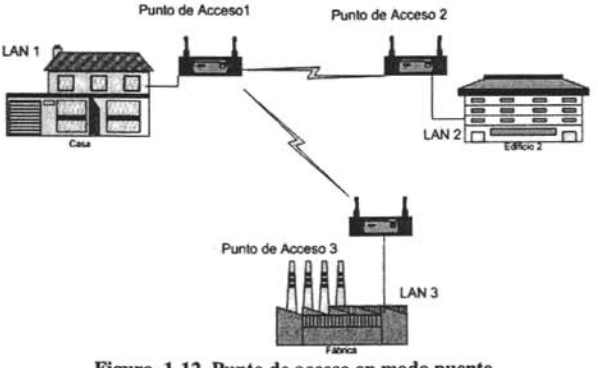


Figura 1-12. Punto de acceso en modo puente.

1.2.3 Arquitectura de una red WLAN.

El BSS (Basic Service Set- Conjunto de Servicio Básico) es el elemento fundamental en la arquitectura de este tipo de redes. Un BSS se define como un grupo de estaciones que se encuentran bajo el control directo de una función de coordinación sencilla (DFC o PFC). El área de cobertura cubierta por la BSS es conocida como BSA (Basic Service Area), la cual es análoga a una célula en una red celular. Por concepto, todas las estaciones en una BSS pueden comunicarse directamente con todas las estaciones dentro de la BSS. Como sea, todas las degradaciones del medio de transmisión provocadas por multi-trayectorias o la interferencia provocada por BSS cercanas que utilizan las mismas características de la capa física (frecuencia, patrón de saltos), pueden causar que algunas estaciones sean ocultas a otras estaciones. Por lo tanto una BSS es una entidad independiente que puede tener su vinculación con otros BSS a través del punto de acceso mediante un sistema de distribución (Distribution System-DS). El DS puede ser: integrado (comunica al BSS con una red externa), cableado (con otros BSS a través de un tendido de cable por ejemplo una

red Ethernet) o también inalámbrico en cuyo caso se denomina WDS (Wireless Distribution System).

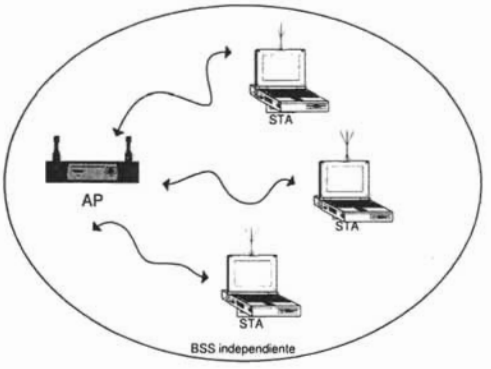


Figura 1-13. BSS Independiente.

Bajo estos conceptos se desprenden otro concepto: el ESS (Extended Service Set- Conjunto de servicios extendidos), el cual es representado por un conjunto de BSS asociados mediante un sistema de distribución. Esto permite una serie de prestaciones avanzadas opcionales como el roaming entre celdas.

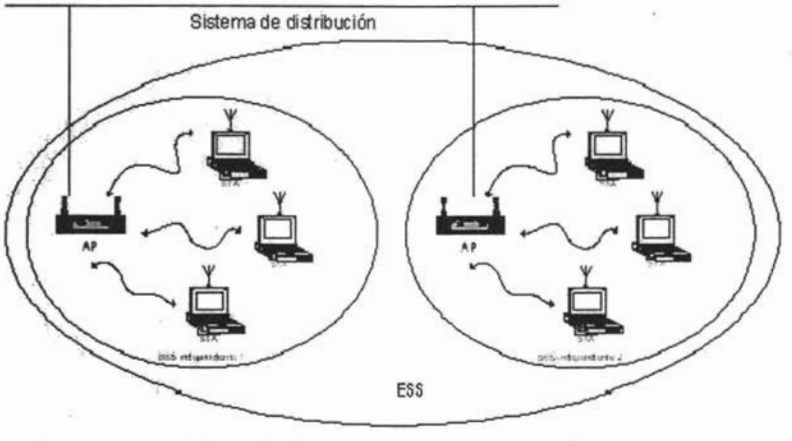


Figura 1-14. Conjunto de servicios extendidos.

1.2.4 Topologías de red.

1.2.4.1 Red Tipo AD-HOC.

Este tipo de red, consiste en un grupo de estaciones dentro de una sola BSS con el propósito de interconectarse y comunicarse entre ellas de manera económica y flexible. Su nombre formal es Conjunto de Servicios Básicos Independiente (IBSS- Independent Basic Service Set). Cualquier estación puede establecer una sesión de comunicación directa con cualquier otra estación con un alcance de transmisión limitado (solo dentro de la BSS) sin el uso de ningún servidor u otro medio como puntos de acceso; es decir que no necesita de ningún sistema de control ni de transmisión central. Uno de los métodos básicos para encaminar los paquetes en este modo, sería tratar a cada uno de los nodos que forman la red como un enrutador y utilizando entre ellos un protocolo convencional (basados en vector de distancia) para encaminarlos hacia su destino. Por ejemplo, si dos nodos no se encuentran dentro del rango de cobertura de cada una; estas se podrán comunicar con la ayuda de nodos intermedios. Estos nodos mandan los paquetes de uno a otro, de tal manera que se transfieren completamente los paquetes del nodo fuente al nodo destino. Un nodo procesa paquetes que le son dirigidos y por otro lado, éste manda el paquete a uno de sus vecinos, bajo la ruta más eficiente para así llegar a su destino.

Una red de este tipo se puede instalar, por ejemplo, en una sala de conferencias para conectar sistemas portátiles que se usarán en una reunión. Además este tipo de redes son una alternativa muy viable en zonas rurales, al no necesitar un troncal (backbone), es decir que confía plenamente en nodos fijos inalámbricos, en vez de en estaciones base, y siendo así no estrictamente una red móvil.

Ventajas:

- Comunicación punto a punto sin punto de acceso.
- Instalación rápida y costo mínimo.
- Configuración simple.

Inconvenientes:

- Alcance limitado.
- Número de usuarios limitado.
- No integración en estructuras LAN existentes.

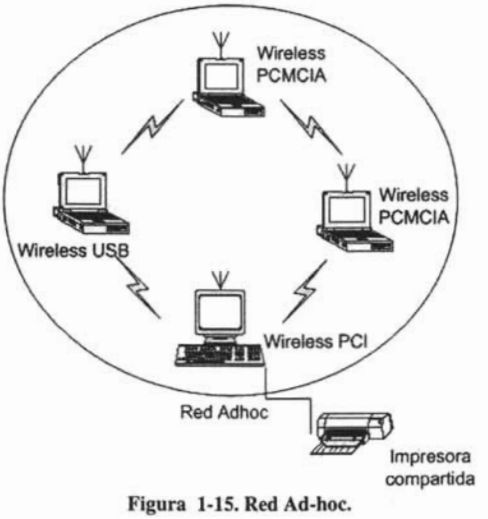


Figura 1-15. Red Ad-hoc.

1.2.4.2 Red tipo INFRAESTRUCTURA.

Las estaciones (dispositivos inalámbricos y computadoras fijas), se comunican a través de un Punto de Acceso (AP), que además de gestionar y coordinar el tráfico entre las estaciones, provee la conexión del mundo de radio frecuencia con el de la LAN alámbrica. Por lo tanto, aquí las tareas del punto de acceso son realizar funciones de coordinación. Todo el trafico tiene que pasar por el AP, por lo que hay una clara perdida de eficiencia cuando dos estaciones dentro de un mismo BSS desean comunicarse entre sí. Es una arquitectura apropiada cuando la mayor parte del tráfico se origina o finaliza en las redes exteriores a las cuales esta conectado el Punto de Acceso. La cobertura alcanza una distancia cercana al doble de la distancia entre un punto de acceso y la estación.

Estos puntos de acceso tienen en promedio un limite de 64 a 120 usuarios (cada uno con su tarjeta de conexión) dentro de su área de cobertura. Para enfrentar este problema se opta por poner en funcionamiento varios Puntos de acceso al mismo tiempo, ampliando así las posibilidades de *roaming* de un equipo móvil sin perder la conexión.

Ventajas:

- Incluso las estaciones que no están en línea de vista o no se ven físicamente entre sí se pueden comunicar.
- Simple integración en estructuras de cable ya existentes.

Inconvenientes:

- Costos más elevados del equipo.
- Instalación y configuración más complejas.

Para poder identificar de manera inequívoca a las celdas inalámbricas se les asigna un nombre de red consistente en una cadena con longitud máxima de 32 caracteres llamada SSID (Service Set Identifier- Identificador del conjunto de servicios).

Por lo tanto hay que seguir estas normas de configuración:

Puntos de acceso:

- SSID idéntico. Canales distintos, por ejemplo 1, 6 y 13.
- Si se utiliza el filtrado de direcciones MAC, debe configurarse la dirección MAC de los sistemas móviles en todos los puntos de acceso.

Sistemas móviles:

- SSID idéntico al punto de acceso para integrarse a una determinad celda, pero si se desea que la estación se conecte a cualquier celda inalámbrica presente, se deberá establecer el parámetro ANY. Inmediatamente el equipo analizará todas las celdas que estén presentes y se conectará a una de ellas adoptando su SSID.
- Si se ha configurado la encriptación WEP, el sistema móvil debe utilizar la misma clave que los puntos de acceso.

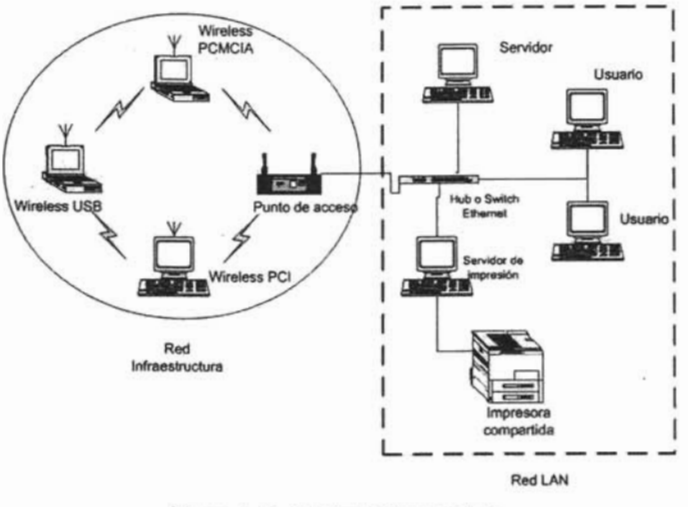


Figura 1-16. Red tipo Infraestructura.

1.2.5 Roaming.

Se denomina *roaming* a la posibilidad por parte de una estación inalámbrica de desplazarse fuera de la cobertura de su celda y conectarse a otra manteniendo la continuidad de las aplicaciones que anteriormente ejecutaba.
El punto de partida lo tenemos en una estación autentificada en varios BSS y asociada a uno de ellos. A medida que se desplaza comenzará a perder nivel de señal por lo que a partir del momento que su valor decaiga por debajo de un cierto umbral, la estación procederá automáticamente a una búsqueda de alternativas. El primer proceso que se establece es el análisis de los diversos canales de emisión posibles en busca de alternativas, proceso denominado *Sweep*. Dentro de un canal determinado procede a la evaluación de las estaciones presente como alternativa de conexión, denominado *scanning*. Se evaluará el nivel de señal y se obtendrá el SSID de la nueva celda. Obviamente, la primera condición para que se pueda producir el roaming es que nos encontremos en un sistema ESS (ambas celdas estén comunicadas entre sí por un sistema de distribución) y que las identificaciones SSID sean idénticas. El scanning puede ser de dos formas:

- Pasivo. Los AP emiten periódicamente unos paquetes especiales de información denominados *beacons* cuya misión es la de sincronizar temporalmente a los equipos conectados e informar sobre el SSID de la celda. Las estaciones utilizan además estos mensajes para evaluar el nivel de señal. Con esta información una nueva estación puede adoptar la decisión de conectarse.
- Activo. La estación es la que emite un mensaje especial (probe) forzando a los AP dentro de su radio de cobertura y canal de emisión a que respondan con un beacon.

Una vez realizado el sweep entre canales y el scanning en cada uno, la estación ya puede tomar la decisión de a qué AP se conecta. En primer lugar, recupera los paquetes de información que pudiesen haber llegado a la antigua celda e inmediatamente solicita la re-asociación a la nueva. En múltiples casos, y debido a la inmadurez del protocolo IAPP, es necesario realizar de nuevo la autentificación. Finalmente, el nuevo AP comunica al antiguo la suscripción de la estación para que elimine los datos sobre la misma. Todo este proceso puede llevarse a cabo cuando ambas celdas poseen un rango de direccionamiento IP en la misma subred, de tal forma que el equipo mantiene la dirección IP y no se produce la interrupción de las sesiones en curso, lo cual implica que están interconectados a través de bridges (nivel 2). Si los rangos son diferentes y se atraviesan enrutadores (conectividad a nivel 3), este mecanismo no es válido y se requieren otras opciones como el establecimiento de redes privadas virtuales (VPN) o nuevos mecanismos todavía en desarrollo como MobileIP.

1.2.6 Tipos de enlaces.

Una red de grandes extensiones puede utilizar dos tipos de enlaces entre nodos:
Punto a multipunto: que utiliza antenas omnidireccionales.
Punto a punto: utiliza antenas unidireccionales.

1.2.6.1 Punto a multipunto.

Una antena omnidireccional emite señales RF de manera uniforme en un patrón circular alrededor del nodo transmisor. Esto hace más fácil el incrementar el número de nodos sin necesidad de alguna re-configuración. Como sea, para la misma distancia del enlace, este tipo de antenas son más caras para operar que las unidireccionales, la cual requiere amplificadores de señal. Para incrementar el rango de kilómetros, las antenas omnidireccionales deben ser más grandes de un metro de altura, la cual requiere su instalación en torres robustas. Sabemos que las antenas pueden enviar señales más lejos si estas las concentramos en una sola dirección. Ya que una antena omnidirecional emite señales en una dirección horizontal, todas las antenas en la red deben estar a la misma altura lo cual es casi imposible de lograr, Finalmente, estas señales esparcen la señal en toda una área, exponiendo la red a los hackers.

1.2.6.2 Punto a punto.

Las antenas unidireccionales están disponibles de muchas maneras. Las más utilizadas son la tipo Match, ya que tiene un bajo perfil, son ligeras y no muy caras, pero tiene una cobertura corta y un ancho de banda muy estrecho. Las antenas Yagi son las más efectivas, ya que combinan una cobertura larga con un buen haz ancho. Las antenas parabólicas dan una cobertura muy amplia por el mismo precio, pero su haz es muy estrecho, lo que hace que el alineamiento de línea de vista sea muy difícil. Una red que utiliza múltiples antenas unidireccionales requiere diferentes alimentadores de señal para cada antena. Una alternativa es utilizar NIC y una antena por cada link. Las dos tarjetas en cada punta utilizaran un canal diferente, así se evitan la interferencia y así formar una gran red ad-hoc.

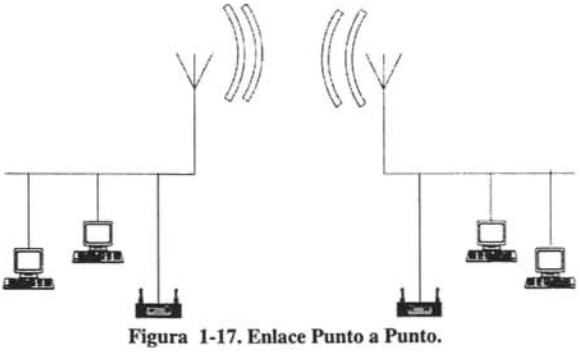


Figura 1-17. Enlace Punto a Punto.

1.2.7 Bandas de frecuencias utilizadas.

Dependiendo del país en el que un usuario viva y donde se instale una WLAN, existen distintas restricciones gubernamentales para las compañías que ofrecen estos productos, así como para consumidores que los utilicen.
La banda de frecuencia de 2.4 GHz es compartida por WLAN y por otras tecnologías (Bluetooth, HOME RF, hornos de microondas) lo que incrementa la posibilidad de congestionar dicha banda. Para solventar esta problemática se decidió utilizar también la banda de 5 GHz para aplicaciones WLAN aumentando el ancho de banda disponible y la capacidad de tráfico de forma considerable.

Tabla 1-1. Bandas de frecuencia.

No. de Canal	*Frecuencia (Mhz)*	*REGIÓN*				
		América	*ETSI*	*Israel*	*China*	*Japón*
1	2412	X	X	-	X	X
2	2417	X	X	-	X	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	-	X	X
11	2462	X	X	-	X	X
12	2467	-	X	-	-	X
13	2472	-	X	-	-	X
14	2484	-	-	-	-	X

1.2.8 Aspectos a considerar.

Cuando deseamos implementar o diseñar un sistema WLAN, hay que considerar diversos aspectos técnicos, entre los principales se encuentran: tamaño, consumo de energía, bit rate, throughput, rango de cobertura, interferencia. , seguridad, etc.

1.2.8.1 Asignación de Canales.

A pesar de que hay 14 canales de frecuencia disponibles para su uso, hay que hacer notar que la frecuencia que se menciona, se refiere a la frecuencia central utilizada por el transmisor y receptor para entablar la comunicación entre ellos. Una señal de radio tipo 801.11b consume aproximadamente 30 Mhz del espectro, dejando solo 5 Mhz de separación entre frecuencias centrales. Esto significa que la señal se extiende mas de 15 Mhz a los lados a partir de la frecuencia central.

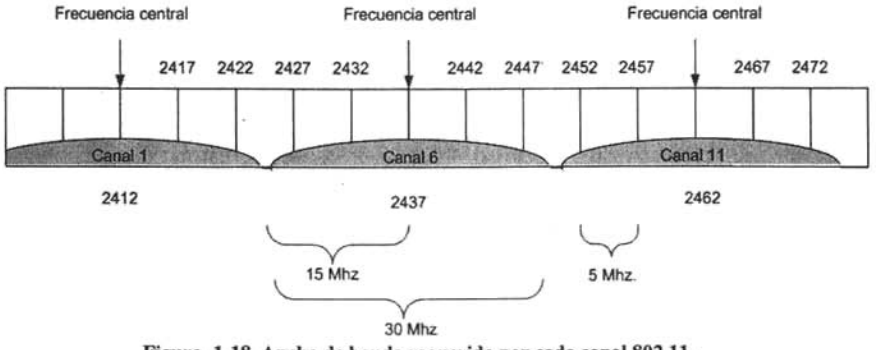


Figura 1-18. Ancho de banda requerido por cada canal 802.11.

Como resultado, el ancho de banda requerido por cada señal, se sobre encima a varias frecuencias adyacentes. Para evitar solapamiento entre canales, la norma del IEEE 802.11 indica que se debe dejar una separación entre las frecuencias centrales mayor de 22 MHz Esta condición significa que en la banda de 2.4 Ghz hasta 3 Puntos de acceso pueden coexistir en una misma celda (ver figura 1-18). La banda de 5 Ghz permite la utilización de hasta 8 puntos de acceso coexistiendo en la misma celda.

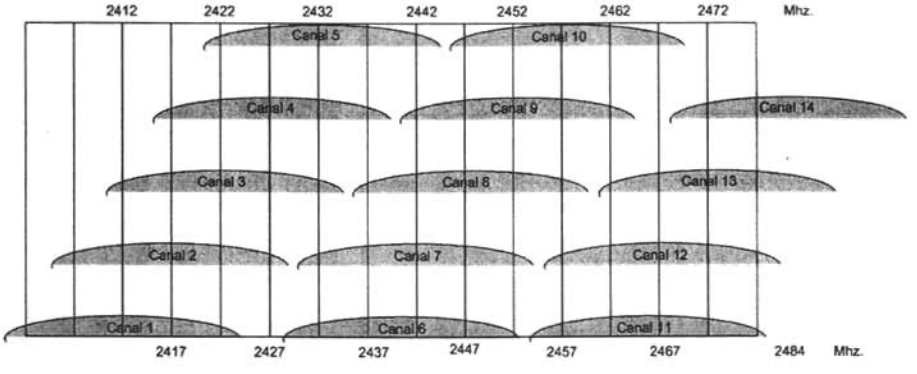


Figura 1-19. Traslape de canales de frecuencias.

1.2.8.2 Throughtput.

La capacidad de las redes inalámbricas de área local idealmente debería aproximarse a sus contrapartes alámbricas. Como sea, debido a las limitaciones físicas y al ancho de banda disponible, las WLAN tienen como objetivo operar a velocidades entre los 1-54 Mbps Para soportar varias transmisiones simultáneas utiliza técnicas de espectro disperso.

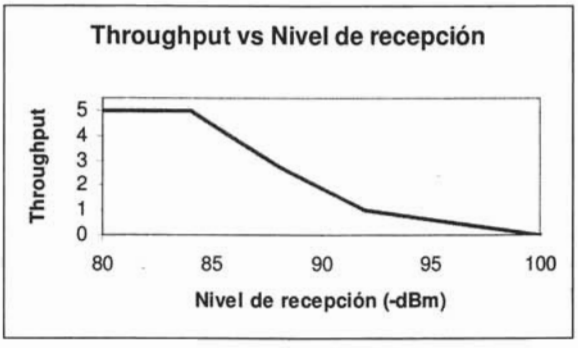


Figura 1-20. Throughtput vs. Nivel de recepción.

1.2.8.3 Cobertura.

Para tener una cobertura confiable, se consideran un modelo de perdidas dependiendo el ambiente: En espacios abiertos, semiabiertos y cerrados.

Tabla 1-2. Cobertura.

Velocidad de transmisión (MBPS)	1	2	5.5	11
Sensibilidad del receptor para un BER de 10-5 (dBm)	-93	-90	-87	-84
Potencia del TX para tener un rango de cobertura del 99%	15 dbm			
Espacios Abiertos	485 m	354 m	259 m	189 m
Espacios Semiabiertos	105 m	85 m	69 m	56 m
Espacios Cerrados	46 m	40 m	34 m	29 m

El rango de cobertura confiable puede ser afectada por las multi-trayectorias cuando se opera a 11 Mbps y 5.5 Mbps (en espacios abiertos) y por la presencia de paredes de concreto en todas las velocidades de transmisión.

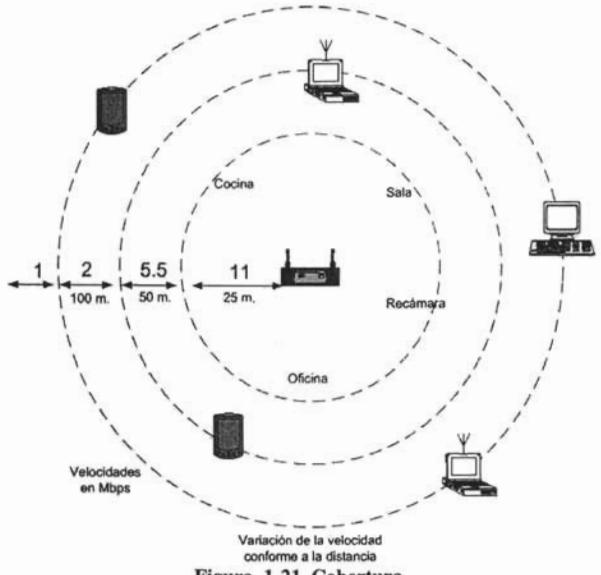


Figura 1-21. Cobertura.

1.2.8.4 Diseño de la célula.

Existen dos aspectos importantes cuando se requiere diseñar una red WLAN: el throughput y la cobertura. Por una parte una red puede ser diseñada e instalada tomando en cuenta solo la cobertura, dicha red tendrá un bajo throughput y células grandes, su instalación requerirá menos AP y por lo tanto será más barata. Por otra parte, podemos tener como punto de partida el throughput, esto implica una célula más pequeña (dando una cobertura total), que requiere más APs y por lo tanto será más cara.

En el caso de células adyacentes éstas pueden funcionar independientemente si sus frecuencias centrales están espaciadas 15 MHz Teniendo en cuenta este factor se puede hacer un plan de frecuencias para cada uno de las diferentes regiones mundiales teniendo sus propias restricciones en la banda ISM (2.4 – 2.5 GHz). La distancia para la reutilización de frecuencias puede ser encontrada utilizando un modelo de perdidas en conjunto con la sensibilidad del receptor. Si existe un traslape total de células, se deberá utilizar un espaciamiento de 25 MHz

1.2.8.5 Interferencia.

La interferencia es uno de los temas más importantes que hay que considerar en el diseño, operación y mantenimiento de un sistema de comunicaciones inalámbricas. Ésta puede ser causada por transmisiones simultáneas (por ejemplo colisiones) de una o más fuentes que comparten la misma banda de frecuencia y por la ineficacia de los filtros en los receptores. Las colisiones son típicamente el resultado de múltiples estaciones que esperando que el canal este despejado, comienzan a transmitir todas al mismo tiempo. Las colisiones,

también son provocadas por el problema de "terminal oculta", donde una terminal, creyendo que el canal esta despejado, comienza a transmitir sin que sea detectada con éxito la presencia de su transmisión en progreso. Otra fuente de interferencia es provocada por las multi-trayectorias, las cuales se caracterizan por tener en el receptor fluctuaciones aleatorias en la amplitud y fase de la señal. Otros tipos de interferencias presentes son de Intermodulación e Intersímbolo que constituyen problemas a tomar en cuenta para la planeación del sistema. Los principales problemas a tomar en cuenta en el diseño de este tipo de sistemas son la proximidad de células adyacentes y la interferencia co-canal.

La confiabilidad de un canal de comunicaciones es medida por el Average Bit Error Rate (BER). Para voz codificada, las perdidas de paquetes están en el orden de 10^{-2} dB el cual es un valor aceptable. Para datos no codificados un BER en el orden de 10^{-5} dB es aceptable. También se utilizan algunas técnicas de corrección de errores como el ARQ (Automatic Repeat Request) y el FEC (Forward Error Correction), para así aumentar la confiabilidad en las transmisiones.

1.2.8.6 Control de potencia.

Típicamente, los dispositivos conectados a una red alámbrica, obtienen su energía por el sistema local de energía de 110V. Los dispositivos inalámbricos, están diseñados para ser portátiles y/o móviles, y obtienen su energía a través de una batería. Por lo tanto es necesario que sean diseñados para que sean muy eficientes, haciendo que los costos contra desempeño y de costos contra capacidad sean óptimos.

Por lo tanto, lo que se espera de un óptimo control de potencia, es el poder reducir el promedio de potencia consumida por las NIC (Network Interface Cards). El estándar 802.11 define protocolos de control de potencia que pueden ser utilizados por las terminales móviles. Los esquemas de control de potencia propuestos, tienen como resultado un menor consumo de potencia (batería) comparada con la operación tradicional donde la terminal esta siempre monitoreando el medio mientras se encuentra en espera de la llegada de un paquete. Para obtener un ahorro en el consumo de potencia de una NIC en una terminal, debe tener un valor especial de potencia bajo de operación llamado estado DOZE. En este estado la NIC no monitoreará el medio y no estará disponible para recibir algún frame. Este estado difiere del estado OFF en el sentido de que la tarjeta podrá hacer la transición del estado DOZE al estado completamente operacional de recepción (AWAKE) en un tiempo muy corto (250micros segundos). La transición del estado OFF al AWAKE toma mucho más tiempo. La administración de la potencia permite a la terminal el gastar más de su tiempo en espera en el estado DOZE mientras todavía mantiene conexión con el resto de la red para recibir mensajes no solicitados.
Para un último requerimiento, las otras terminales dentro del rango del mismo AP deben temporalmente guardar los mensajes que son destinados a la terminal que opera bajo el esquema de administración de potencia y dicha terminal deberá "despertar" en tiempos regulares de tiempo para verificar si hay mensajes guardados para sí.

Por cada frame transmitido por la terminal, existe un bit llamado PM, el cual indica el modo de operación de la estación. Cuando PM = PS, la terminal está operando en el modo

de ahorro de energía, y el PM = A indica que la terminal esta en modo activo (continuamente activo). En una red basada en puntos de acceso, todos los puntos de acceso verán vía el bit PM si una estación esta en modo activo o en de ahorro de energía. Y así saber cuando guardar los mensajes para la terminal que así lo requiera. Los puntos de acceso también guardaran los mensajes tipo multicast y además mandaran frames tipo beacon en un tiempo regular (100 ms), en cada frame beacon el punto de acceso anunciará para que estaciones hay mensajes guardados. Las estaciones que utilicen un esquema de administración de energía despertarán justo a tiempo para una transmisión de beacons de alta prioridad. (Véase Apéndice 5, para ver los niveles de potencia permitidos).

1.2.8.7 Seguridad de uso.

Varias investigaciones están determinando si las transmisiones de radio frecuencia (RF) de los radios y teléfonos celulares están relacionadas con enfermedades humanas. Las redes deben ser diseñadas para minimizar al máximo la potencia utilizada por todos los dispositivos de red. Para sistemas infrarrojos, los transmisores ópticos deben ser diseñados de tal manera que se evite el deterioro de la visión.

1.2.8.8 Movilidad.

A diferencia de las terminales alámbricas, las cuales permanecen estáticas mientras trabajan en la red, una de las ventajas primordiales de las terminales inalámbricas es la libertad de movimiento. Por lo tanto, cuando se diseña un sistema se debe adaptar la existencia de "Handoffs" entre los límites de transmisión y enrutar el tráfico de los usuarios en movimiento.

1.2.8.9 Seguridad.

En las redes alámbricas, la transmisión puede ser físicamente segura, y el acceso a la red puede ser fácilmente controlado. En una red inalámbrica es mas difícil asegurar una buena seguridad, ya que el medio de transmisión es abierto a cualquiera que este dentro del limite geográfico de transmisión. Las redes inalámbricas que se rigen bajo la norma del IEEE 802.11 enfrentan el problema de la seguridad utilizando 3 tipos de sistemas: abiertos, por autentificación por clave compartida y encriptación tipo RC4. En los sistemas abiertos, cualquier estación será autentificada por el punto de acceso. En la autentificación por llave compartida, implica que solo serán autentificadas aquellas estaciones que conocen la clave, y no reconocerá aquellas que no lo son. La autentificación por clave compartida, realiza esto de manera perfecta sin la necesidad de transmitir la clave secreta en el espacio; y por lo tanto requiere el uso de un mecanismo alámbrico equivalente como el WEP. Los sistemas de autentificación cerrados, son un esquema propietario (por ejemplo ORINOCO), los cuales proveen mayor seguridad. Las redes WLAN están previstas para ser utilizadas en ambientes empresariales y corporativos, por lo tanto los esquemas de seguridad de la actualidad no son suficientes para este tipo de ambientes. En general un corporativo, tiene una red LAN basada en tecnología Ethernet con un procedimiento de autentificación basado en algún tipo de sistema operativo (Unix, Microsoft, etc.) , entonces si quieren implementar una red LAN inalámbrica completamente cerrada con un nivel de seguridad

razonable, se puede lograr nombrando a la red y utilizando autentificación por clave compartida. Se dice razonable, por que estos procesos mencionados no son muy seguros. Otras preocupaciones de las empresas es la periodicidad en la que se cambiará el personal a corto y largo plazo. Otro sistema de seguridad utilizado es Kerberos. Kerberos se basa en Unix, y éste incluye autentificación, control de acceso, y encriptado. En ambientes públicos, los usuarios hacen uso de utilidades de comunicación no muy confiables para acceder a sistemas de su trabajo o de su proveedor de servicio de Internet, entonces es necesario un proceso de autentificación y de seguridad en la sesión. Este tipo de necesidades son dominadas por la plataforma de Microsoft. Los operadores y proveedores de servicio utilizan RADIUS (Remote Authentification Dial In User Service). Los servicios de RADIUS son utilizados principalmente cuando la gente se mueve y requiere un acceso a su red corporativa o cuando la gente quiera a acceder a un ISP a través de su hogar.

1.3 Ventajas y desventajas de las WLAN.

Hasta ahora hemos descrito las características del estándar IEEE 802.11, sin embargo es necesario discutir la viabilidad de implementar dicha tecnología como un medio más de transmisión de datos. Algunos aspectos a considerar incluyen la **seguridad, costos, interferencia con otras señales, velocidad de transmisión, etc.**

La seguridad en la WLAN ha sido la causa principal de preocupación y el punto más débil desde sus inicios. Los primeros mecanismos de seguridad resultaron insuficientes ante usuarios que lograban entrar a las redes y utilizar parte del ancho de banda e incluso obtener archivos y datos privados. Dado que el medio es inalámbrico, es relativamente fácil que una persona con conocimientos y equipo básico pueda infiltrarse a una red y sustraer información confidencial, o bien modificarla. Para evitar dichos accesos ilegales es posible encriptar la información que se transmite y recibe, entre más bits se usen para encriptar más segura será la red inalámbrica. Sin embargo, todo tiene un costo ya que el utilizar bits para encriptar la información disminuye el desempeño y la velocidad de transmisión de los datos.

Una ventaja a luces de la tecnología inalámbrica es la movilidad. Los usuarios conectados desde sus terminales son capaces de transportarse a cualquier parte que se encuentre dentro del radio de transmisión del punto de acceso, y en un esquema distribuido es posible que se realice un *handoff* cuando la terminal se encuentre muy lejana del punto de acceso original para así cambiar a otro con mejor nivel de señal. Sin embargo, este esquema tiene hasta ahora sus limitantes puesto que la movilidad del usuario se refleja en el decremento de la velocidad de transmisión para evitar la ocurrencia de errores y la pérdida de la señal. También, si la geografía del lugar presenta obstáculos como lugares cerrados, materiales conductores, o columnas demasiado gruesas es probable que la señal se atenúe casi de forma inmediata.

La velocidad de transmisión es otro factor determinante, ya que si el medio inalámbrico resultase demasiado lento, no tendría un atractivo comercial con respecto al medio alámbrico. El estándar IEEE 802.11b funciona a velocidades de 1, 2, 5.5 y hasta 11 Mbps

en la banda de los 2.4 GHz, el IEEE 802.11a funciona a 54 Mbps en la banda de los 5GHz y el estándar IEEE 802.11g funciona a 54 Mbps en la banda de los 2.4 GHz Todas estas velocidades se escuchan muy prometedoras, sin embargo sólo son válidas para distancias cercanas al punto de acceso y considerando que la terminal se mueve a una velocidad lenta (o bien que está estática). Al variar estas condiciones disminuye la tasa de transferencia y por lo tanto, la velocidad de transmisión de datos.

Otro factor importante es la frecuencia en la que se trabaja. En los estándares IEEE 802.11b/a/g, se usan las frecuencias denominadas *ISM (*Industrial, científica y médica por sus siglas en inglés), cuyo uso es libre, lo cual abarata los costos de comercialización, además de permitir un desarrollo más rápido de la tecnología, ya que se evitan los procesos de regulación y normatividad de canales de radiofrecuencia. Sin embargo, al tratarse de canales de frecuencia libres se tiene el problema de que el canal se comparte con otras tecnologías de diversas áreas (incluso de otras tecnologías de redes inalámbricas) lo cual conlleva a interferencias y ruido constante.

El hecho antes mencionado nos lleva a otro punto de interés: interferencia y confiabilidad. La interferencia en las comunicaciones inalámbricas puede ser causada por transmisiones simultáneas (colisiones) de dos o más fuentes que comparten la misma banda de frecuencia. Las colisiones se deben en general a que varias estaciones están a la espera de transmitir, y cuando detectan que el canal está libre todas transmiten al mismo tiempo. También pueden ser causadas por un problema llamado "terminal oculta", donde una estación que detecta que el canal está libre comienza a transmitir sin darse cuenta de una transmisión que estaba en progreso.
La interferencia puede ser causada también por el desvanecimiento de multitrayectoria, el cual se caracteriza por fluctuaciones aleatorias de la amplitud y fase de la señal en el receptor.

Otro factor importante en el desarrollo de sistemas inalámbricos es la potencia de transmisión necesaria para obtener un buen BER, ahorrando la mayor energía posible para otras funciones, y evitar que la potencia sea tan grande que cause interferencia a otros dispositivos o incluso que pueda dañar al ser humano.

1.4 Viabilidad económica de las redes inalámbricas.

Es importante destacar que la tecnología WLAN, tiene un gran panorama de éxito, ya que complementa y extiende aplicaciones móviles y fijas. Lo más probable es que la mayor parte de los dispositivos móviles vayan equipados con esta tecnología en el futuro. Por otra parte, como complemento al negocio de la telefonía fija se usará como extensión de los accesos de banda ancha.
Es por eso importante destacar varios puntos clave para hacer un análisis de la viabilidad económica de esta tecnología:

- La tecnología WLAN, puede servir como una puerta a la industria informática, para capturar el valor y el negocio asociado a las comunicaciones móviles, el cual ha sido casi monopolizado por la industria europea en el ámbito de la telefonía móvil.
- Además, también hay que considerar la próxima coexistencia a corto y mediano plazo con la tecnología móvil de 3G, las cuales hasta el día de hoy solo se han mantenido complementarias.
- En la estandarización debe considerarse la importancia de converger hacia un estándar único que de ser posible cubriera el ámbito de las WLAN y WMAN. Cada país debe de tener una mayor participación en los distintos organismos de normalización competentes, favoreciendo una postura de apoyo a la convergencia de los estándares.
- Es necesario fomentar la creación de foros de carácter nacional donde todos los involucrados en el negocio de WLAN, compartan información para la identificación y consolidación de las posiciones más convenientes para el desarrollo global y del lugar en particular, de la Sociedad de la Información.
- En el tema de la regulación, se debe tener un panorama flexible, libre, complementario que permita la convergencia con otras tecnologías, así como la inversión y la innovación y generar nuevos ámbitos de actividad.
- Este tipo de tecnología se convertirá en un complemento o alternativa de las LAN cableadas en todos los sectores: empresarial y domestico. Lo cual ofrece nuevas posibilidades de negocio como los Hotspots o la implantación de redes privadas, entre otros.
- Vemos que cada día mas, el sector productivo en esta área se esta incrementando: fabricantes de equipos y componentes, operadores de telefonía fija y móvil, etc. Más sin embargo la prestación de servicios no esta muy consolidada.
- Las administraciones públicas deben adoptar un papel mas activo en la financiación de infraestructuras de acceso de banda ancha en zonas geográficas desfavorecidas, que no presentan atractivo económico de inversión para los operadores, siempre desde el respecto de las reglas de competencia establecidas y con transparencia de actuación y cooperación con el sector privado.

Las WLAN pueden jugar un papel importante como tecnología de transición que permita llevar acceso de banda ancha a zonas geográficas rurales que quedan fuera de la cobertura de las tecnologías de acceso de banda ancha más extendidas. En estas zonas, los operadores no encuentran la viabilidad económica para realizar el despliegue de tecnologías de acceso de banda ancha (ADSL, cable, etc.). En estas condiciones, deben valorarse los programas

de subsidio para el despliegue de redes de acceso de banda ancha. Desde el punto de vista del subsidio, las administraciones públicas deben respetar la neutralidad tecnológica, considerando diferentes alternativas, y priorizando la eficacia, eficiencia y fiabilidad de las diferentes soluciones que presenten los agentes interesados. Entre estas soluciones alternativas Wi-Fi puede jugar un papel destacado, aunque sin duda no único.
En aquellas localidades donde existen ofertas al público de conectividad de banda ancha sobre otras redes, una oferta subsidiada a precios reducidos realizada por parte de una administración pública supondría una competencia desleal. Una opción más lógica de apoyo a los ciudadanos más necesitados debería basarse en ayudas directas, de modo que los usuarios pudieran de este modo escoger entre las tecnologías disponibles (principio de neutralidad tecnológica).

1.5 Otros tipos de redes inalámbricas de datos.

Hasta este momento solo hemos hablado de las redes de área local inalámbricas (WLAN). Sin embargo existen más tecnologías como Bluetooth, UMTS, etc. Para entender mas diferencias entre estas tecnologías, estas las podemos clasificar dependiendo del criterio del que se atienda. En este caso las vamos a clasificar de acuerdo a su alcance. Llamaremos alcance a la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica. En la figura siguiente se muestran algunas tecnologías de redes inalámbricas según su campo de acción.

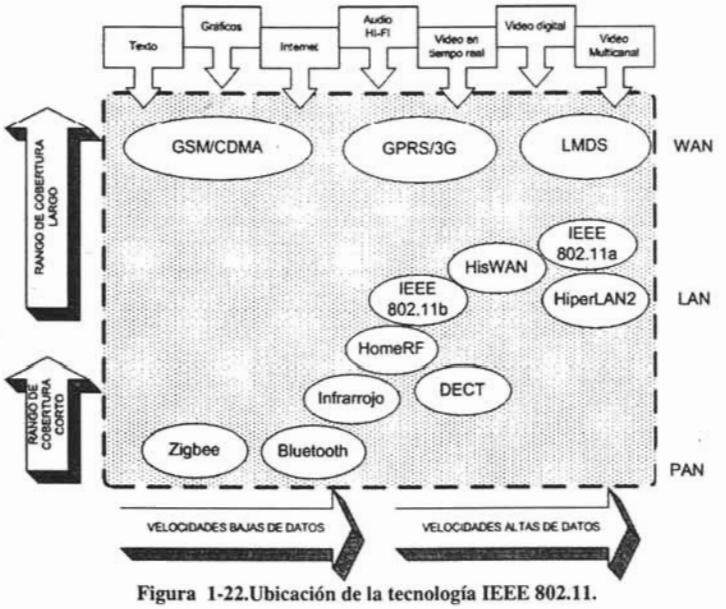


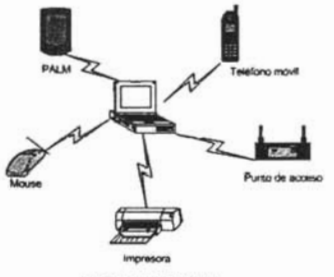
Figura 1-22.Ubicación de la tecnología IEEE 802.11.

1.5.1 Redes inalámbricas de área personal (WPAN).

Las WPAN (Wireless Personal Area Network) cubren distancias inferiores a los 10 m. Este tipo de redes solo están pensadas para interconectar distintos dispositivos en un área de cobertura muy pequeña. Podemos mencionar tecnologías como Bluetooth (IEEE 802.15), DECT e Infrarrojos por mencionar las más importantes.

1.5.1.1 Bluetooth.

Diseñado para formar redes personales tipo Ad-hoc, Bluetooth facilita la transmisión de voz y datos entre diferentes dispositivos por medio de un enlace de radiofrecuencia. Surge en 1994, bajo iniciativa del Ericsson Mobile Communications, formándose en 1998 el Bluetooth SIG (Special Interest Group). Bluetooth define un canal de comunicación de 721Kbps en *dowstream* y 56kbps en *upstream* con un radio de cobertura de 10 metros, el cual se puede ampliar hasta 100 m, con repetidores. La frecuencia de trabajo esta en el rango de 2.4 a 2.48 GHz Trabaja bajo jerarquías: maestro o esclavo. El maestro envía información del reloj así como la ID del dispositivo (patrón de saltos). La formación de redes con este tipo de dispositivos se denomina piconets. Estas redes tienen la posibilidad de crecer hasta poder conectar cada maestro a 7 dispositivos activos simultáneamente o 200 esclavos estacionados simultáneamente (park mode). Estas se pueden extender mediante la formación de scatternets. Una scatternet es la red producida al establecer comunicación dos dispositivos pertenecientes a dos piconets diferentes. Se permiten formas dos tipos de enlaces: El asíncrono (ACL – Asynchronous Connection-less Link) utilizado para datos y el síncrono (SCO- Synchronous Connection- Oriented Link) para voz. En la figura 1- 23 se muestra un esquema de una red Bluetooth.

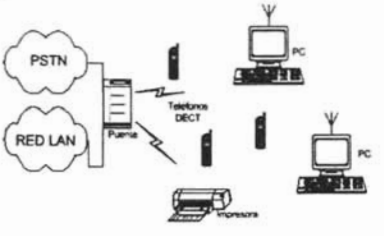


RED BLUETOOTH

Figura 1-23. Bluetooth.

1.5.1.2 DECT

La tecnología DECT (Digital Enhanced Cordless Telecommunications) es un estándar que provee acceso general por radio a comunicaciones inalámbricas, operando en los 1880 a 1900 Mhz utilizando modulación tipo GFSK. DECT ha sido diseñado para proveer acceso a cualquier red, soportando numerosas aplicaciones y servicios. Algunas de las aplicaciones del DECT son en el ámbito residencial, la red PSTN, acceso ISDN, PABX inalámbrico, acceso GSM, WLL, además redes de área local que soporten telefonía, fax, MODEM, Internet. X.25. Un sistema DECT consta de una parte fija tipo DECT (FP), utilizando una o más estaciones bases (RFP), y uno o más partes móviles tipo DECT (PP). No existe un límite de estaciones base y terminales inalámbricas que co-existan. Aquellas infraestructuras que utilizan la tecnología DECT pueden soportar densidades de trafico de 10000 Erlang/ Km2.
La velocidad máxima actual a la que trabaja DECT es de 1. Mbps, aunque existe una propuesta para aumentar esta velocidad hasta los 20 Mbps y conseguir alcances de hasta 17 Km. A pesar de que, técnicamente, DECT podría ser un competidor de Bluetooth o, incluso, de otros sistemas inalámbricos de mayor alcance, el hecho de que trabaje en la banda de 1,9 GHz (utilizada en Europa para esta tecnología pero con barreras regulatorias en Norteamérica y otras partes del mundo) y que esté muy orientada a voz le pone grandes limitaciones para competir con esas otras tecnologías. En la figura 1-24 se muestra un esquema de una red DECT.



RED DECT
Figura 1-24.DECT.

1.5.1.3 Infrarrojos.

IrDA (*Infrared Data Association*) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Actualmente tiene creados dos estándares: IrDA-Control e IrDA-Data. La tecnología de infrarrojos parece que ha encontrado su nicho en las comunicaciones a muy corto alcance. Esto convierte a IrDA en compatible con tecnologías como Bluetooth. Además, IrDA ofrece la ventaja adicional de la seguridad, ya que las emisiones de haces infrarrojos se quedan en un entorno mucho más privado que las propagaciones de ondas de radio. Los dispositivos IRDA utilizan LED infrarrojos. La Longitud de onda utilizada es 875nm. Los dispositivos IrDA conforme a los estándares 1.0 y 1.1 abarcan distancias por arriba de 1m con un BER (Bit Ratio Ratio-Relación de Bit por Error) de 10^{-9} . Estos valores son definidos a 15 grados de deflexión del receptor y el transmisor. Las velocidades van de los 2400 a los 115200kbps.

1.5.1.4 ZigBee.

Zigbee es un protocolo basado en el estándar IEEE 802.15.4. Zigbee trabaja en bandas sin licencia, incluyendo la 2.4GHz (Global), 915 MHz (América) y 868 MHz (Europa). El rango de throughput es de 250Kbps en la banda de 2.4Ghz (10 canales), 40Kbps a 915Mhz (6 canales) y 20Kbps a 868Mhz (1 canal). La distancia de transmisión abarca de 10 a 75 m dependiendo de la potencia de salida y las características del entorno.

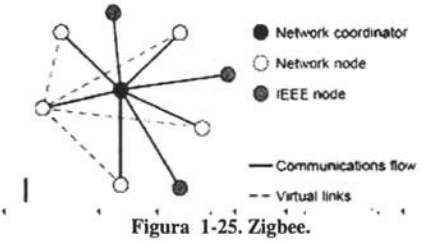


Figura 1-25. Zigbee.

Zigbee utiliza una topología tipo estrella, sin embargo también es posible la conexión peer to peer. Se permiten hasta 255 dispositivos por red.

El coordinador de la red, es aquel que levanta la red, transmite beacons a la red, administra los nodos, guarda información de los nodos y también manda mensajes entre los nodos. Por su parte los nodos de la red, están en modo activo (máximo gasto de potencia), en busca de redes disponibles, y si es necesario transferir información, solicita información al coordinador de la red. Las redes Zigbee tiene 3 tipos diferentes de tráfico: periódicos, intermitentes y repetitivos de baja latencia.

1.5.2 Redes inalámbricas de área local (WLAN).

Las redes inalámbricas de área local o **WLAN** (*Wireless Local Area Networks*) son las redes que tienen una cobertura de unos cientos de metros. Estas redes están pensadas para crear un entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios. 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 HomeRF y Wi-Fi (IEEE 802.11b). Otras tecnologías son HiperLAN, HiSWAN y OpenAir, las cuales no tienen un ámbito de aplicación extendido.

1.5.2.1 HomeRF.

La HomeRF (*Home Radio Frequency* - Radiofrecuencia del Hogar) surge ante la iniciativa de promover un sistema de red inalámbrica para el hogar, además de tener la habilidad de integrar teléfonos inalámbricos en los ordenadores, que funcionarían como contestadores automáticos y como el PBX doméstico. Los teléfonos podrían convertirse en periféricos de habla de E/S para manejar aplicaciones de Internet y del PC.

Trabaja bajo el esquema de SWAP (*Shared Wireless Access Protocol* - Protocolo de Acceso Compartido Inalámbrico). Se definió esta arquitectura que soporta comunicaciones de datos (CSMA/CA) y voz (TDMA) en tiempo real. SWAP trabaja en la banda de frecuencias de 2,4GHz y permite configuraciones de comunicaciones punto a punto y comunicaciones con punto de comunicación central.

La versión 1.0 permite transmitir datos a 1,6Mbps y mantener hasta cuatro comunicaciones dúplex de voz. Tiene un alcance de unos 50 metros y una potencia de transmisión de 100mW. Utiliza un protocolo similar a IEEE 802.11 para datos y otro similar a DECT para voz. La versión 2.0 alcanza los 10Mbps, fácil de configurar, posibilidad de encriptación, con un rango de cobertura de 50 m ofreciendo la compatibilidad con Home RF v1, sin tener interferencias con dispositivos que trabajan a 2.4Ghz, ni con dispositivos Bluetooth.

1.5.2.2 HIPERLAN/2

En 1992, la ETSI formo un comité para establecer el estándar HIPERLAN (High Performance Radio LAN)

Las características y capacidades de HIPERLAN son muy similares al estándar IEEE 802.11. En la ETSI, HIPERLAN se refiere como un sistema de equipo y de radio (RES). La CEPT (European Conference of Postal and Telecommunications Administration) identificó la banda de 5.15 a 5.25 GHz (esta asignación permite 3 canales), con una posible expansión a los 5.30Ghz (con 5 canales). Además, se le asigno una segunda banda de 17.1 a 17.3GHz, sin embargo todavía esta banda no es muy utilizada por los fabricantes.

El estándar HIPERLAN/1 provee de comunicaciones inalámbricas con una velocidad máxima de 23.5 Mbps en la banda de 5 GHz La capa de control de acceso al medio (MAC) define varios protocolos, lo que permite tener sistemas de ahorro de energía, seguridad, enrutamiento tipo multi-saltos. Como sea, debido a su propia complejidad e implementación, así como la alta utilización de potencia HIPERLAN /1 no es muy utilizado por la industria. La ETSI, la HIPERLAN/2 y el IEEE 802.11ª convergieron en muchos aspectos, como el utilizar OFDM, así como la operación en la banda de los 5 GHz, pero son muy diferentes en capas superiores. Tiene la misma velocidad de transferencia de datos de 54 Mbps En contraste con el CSMA/CA de 802.11ª, el HIPERLAN/2 adoptó el sistema de reservación de tiempo a través de TDMA con un mecanismo TDD. Además utiliza DFS (Dynamic Frequency Selection) para reducir el problema de la interferencia y utilizar más eficientemente el espectro. HIPERLAN ofrece una QoS superior. Además también tiene como proyecto el poder trabajar con distintos tipos de redes a diferentes niveles de QoS.

HIPERLAN/2 se basa en la topología de redes celulares combinadas con las características de redes ad-hoc. Soporta dos modos básicos de operación: el modo centralizado y el modo directo. El modo centralizado es utilizado en la topología de una red celular donde cada célula es controlada por un punto de acceso que cubre cierta área geográfica. En este modo una terminal móvil se comunica con otras terminales móviles o con la red principal por medio de un punto de acceso. Este modo de operación es utilizado principalmente en aplicaciones de negocios, ya sea en interiores o exteriores, donde el área a cubrir es mayor

al de una célula. El modo directo es utilizado en topologías del tipo ad-hoc, principalmente en ambientes de redes privadas y pequeñas (en el hogar, una oficina), donde una célula cubre el área de interés. En este modo, las terminales móviles pueden intercambiar datos directamente a través de una red conformada por una sola célula.

1.5.2.3 MMAC- HiSWAN.

El MMAC (Multimedia Mobile Access Comunications) comenzó en Japón en 1996. Este fue desarrollado para transmitir información con alta calidad a velocidades muy altas en cualquier lugar y en cualquier momento sin necesidad de conexiones a redes de fibra óptica. Existen dos frecuencias de trabajo para la MMAC-HiSWAN (High Speed Wireless Access Network), la de 5Ghz para HiSWANa y 25Ghz para HiSWANb. El HiSWANa es muy parecido al estándar HIPERLAN/2 de la ETSI. HiSWAN adoptó una capa física tipo OFDM, entregando velocidades cercanas a los 27Mbps Las diferencias entre HIPERLAN/2 e HiSWAN son la planeación de frecuencia regional. En lugar de utilizar DFS, utiliza funciones de Detección de portadora. Además la sincronización entre Puntos de acceso está especificada de tal manera que se suprima toda interferencia sumada por éstos. Las especificaciones de la versión 1.1 fueron publicadas el 12 de Abril de 1999.

1.5.3 Redes inalámbricas de área metropolitana (WMAN).

Se llama **redes inalámbricas de área metropolitana**, **WMAN** (*Wireless Metropolitan Area Networks*), a aquellas redes que tienen una cobertura desde unos cientos de metros hasta varios kilómetros. El objetivo es poder cubrir el área de una ciudad o entorno metropolitano.

1.5.4 Redes Inalámbricas Globales.

Por último, tenemos las **redes globales** con posibilidad de cubrir toda una región (país o grupo de países). Estas redes se basan en la tecnología celular y han aparecido como evolución de las redes de comunicaciones de voz. Éste es el caso de las redes de telefonía móvil conocidas como 2,5G o 3G. En comunicaciones móviles de voz se les llama **1G** (primera generación) a los sistemas analógicos (tipo NMT o AMPS), **2G** a los digitales (tipo GSM o CDMA), **2,5G** a los digitales con soporte para datos a alta velocidad (tipo GPRS, IS-95B o EDGE) y **3G** o tercera generación a los nuevos sistemas de telefonía celular con capacidad de gran ancho de banda (tipo UMTS o CDMA-2000).

Tabla 1-3.Tabla de tecnologías de redes inalámbricas.

Estándar	*Banda de Frecuencia*	*Máx. Velocidad*	*Técnica de acceso al medio*	*Modulación*	*Usuarios Por canal*	*Tamaño del canal*	*Rango de Cobertura*
Bluetooth	2.402-2.480Ghz (América-Europa) 2.447-2.473Ghz (España) 2.448-2.482Ghz (Francia) 2.473-2.495Ghz (Japón)	721Kbits US 56Kbits DS	Frequency Hopping	Shaped Binary FM	7 activos 200 inactivos	1Mhz	10m
DECT	1880-1900Mhz	1.152Mbps	TDMA/FDM	GFSK	12	1728Mhz	
ZigBee	2.402-2480Ghz (América) 2.412-2.472Ghz (Europa) 2.483Ghz (Japón)	250/ 28kbits	TDMA	GFSK	255	4Mhz	10-75m
HomeRF	2.402-2.480Ghz (América-Europa) 2.447-2.473Ghz (España) 2.448-2.482Ghz (Francia) 2.473-2.495Ghz (Japón)	10Mbps	Frequency Hopping	FHSS:GFSK	8	1Mhz-3.5Mhz	50mts
HIperLAN/1	5Ghz	23.5Mbps	TDMA	GMSK		OFDM 20Mhz	50mts
HIperLAN/2	5GHz	54 Mbps	TDMA	QAM		OFDM 20MHz	50mts indoor 300mts outdoor
MMAC HiSWAN	5Ghz	27Mbps					100-150 m

CAPÍTULO 2
EL ESTÁNDAR IEEE 802.11 a/b/g.

2.1 Modelo de referencia OSI.

Para poder comprender las características y el modo de operación de los estándares de redes, es necesario primero tener una referencia acerca del nivel o capa sobre la que trabaja dicho estándar. Para ello revisaremos de manera breve pero descriptiva todas las capas que establece el modelo de referencia OSI para protocolos de interconexión.
OSI es el modelo para comunicaciones de *Sistemas de Interconexión Abiertos – Open System Interconnection model*. Se trata de un conjunto de especificaciones para protocolos bien definidos que realizan tareas de interconexión entre aplicaciones o equipos dependiendo del nivel para el que hayan sido diseñados. Hoy en día son pocas las aplicaciones que toman en cuenta cada uno de los parámetros del modelo. Más bien es utilizado como un punto de referencia para discutir especificaciones de otros protocolos.

2.1.1 Capas del Modelo de Referencia OSI.

El modelo OSI consiste de 7 capas que definen diferentes características o niveles de comunicación. A continuación se presenta una breve descripción de cada una de ellas así como ejemplos de su aplicación:

Tabla 2-1. Modelo de referencia OSI.

Nombre de la Capa	*Descripción*	*Ejemplos*
Aplicación (Capa 7)	Se refiere a los servicios de comunicación para aplicaciones. Por ejemplo un procesador de textos que carece de capacidad de comunicación no implementaría códigos para comunicación por lo que no implementaría esta capa.	FTP, Navegadores del WWW, NFS, SMTP.
Presentación (Capa 6)	El propósito principal de esta capa es el de definir formatos de datos, como textos ASCII, texto EBCDIC, binario, BCD y JPEG. El encriptado también se define en esta capa como un servicio.	TIFF, GIF, JPEG, PICT, ASCII, EBCDIC, encriptado, MPEG, MIDI, HTML.
Sesión (Capa 5)	Define como comenzar, controlar y terminar conversaciones (llamadas *sesiones*). Esto incluye al control y manejo de múltiples mensajes bidireccionales de modo que la aplicación pueda ser notificada si sólo algunos mensajes de una serie son completados. La capa de sesión tiene formas para especificar que flujos de datos son parte de una misma sesión y donde flujos de datos deben completarse antes de que algún otro pueda considerarse completo.	RPC, SQL, NFS, NetBIOS, AppleTalk, ASP, SCP.
Transporte (Capa 4)	La capa 4 incluye la opción de protocolos que pueden o no proveer corrección de errores. Se incluye el reordenamiento de flujo de datos entrante cuando los paquetes llegan fuera de orden, así como también la reconstrucción de los datos si los paquetes fueron fragmentados durante la transmisión.	TCP, UDP, SPX
Red (Capa 3)	Define una entrega de paquetes de extremo a extremo. Para lograr esto se define un direccionamiento lógico de modo que el destino pueda ser identificado. También se define como fragmentar un paquete en paquetes más pequeños	IP, IPX, AppleTalk DDP

	para acomodarlos en el medio con tamaños de unidades de transmisión los más pequeñas posibles.	
Enlace de Datos (Capa 2)	Las especificaciones de la capa 2 se refieren a enviar y recibir datos a través de un enlace o medio en particular. Los protocolos de capa 2 definen entrega de datos a través de un enlace individual. Estos protocolos se desarrollan acorde al tipo de medio en cuestión.	Frame Relay, HDLC, PPP, IEEE 802.3/802.2, 802.11, FDDI, ATM
Física (Capa 1)	Las especificaciones en esta capa tratan con las características físicas del medio físico. Conectores, pines, corrientes eléctricas, codificaciones, modulaciones, todas son parte de diferentes especificaciones de la capa física.	EIA/TIA -232, EIA/TIA-449, V.35, V.24, RJ45, Ethernet, 802.3, 802.5, 802.11, FDDI, NRZI, NRZ.

En este capítulo discutiremos el estándar IEEE 802.11 el cual define técnicas y protocolos propios de las capas 1 y 2 para que pueda haber interconexión en redes de datos inalámbricas.

2.2 PHY (Capa Física).

La capa física (PHY) es la interfaz entre el MAC y el medio inalámbrico donde los frames se transmiten y reciben. La capa física realiza tres funciones:

- Provee de una interfaz para intercambiar frames con la capa MAC superior para la transmisión y recepción de datos.
- Utiliza una señal portadora y modulación de espectro disperso para transmitir frames de datos por el medio.
- Provee un indicador de detección de portadora de regreso al MAC para verificar la actividad en el medio.

El estándar 802.11 provee tres opciones diferentes de PHY. Tanto FHSS (*Salto en Frecuencia por Espectro Disperso- Frequency Hopping Spread Spectrum)* y DSSS (*Espectro Disperso por Secuencia Directa- Direct Sequence Spread Spectrum)* permiten tasas de transmisión de 1 y 2 Mbps OFDM permite tasas de hasta 54 Mbps
La primera extensión de 802.11, *802.11b* define tasas de transmisión de 11 Mbps y 5.5 Mbps (además de 1 y 2 Mbps) utilizando una extensión del DSSS llamado *DSSS de alta transmisión – High Rate DSSS (HR/DSSS).* El 802.11b también define una técnica de conmutación de tasas de transmisión donde las redes de 11 Mbps pueden caer a 5.5 Mbps, 2 Mbps o 1 Mbps cuando haya condiciones de alto ruido o bien, para ínter operar con modelos PHY 802.11 anteriores.
La segunda extensión es la *802.11a* define diferentes técnicas de multiplexaje que pueden alcanzar tasas de hasta 54 Mbps
Finalmente la extensión *802.11g* define tasas de transmisión parecidas a las de la 802.11a sin embargo para la banda de frecuencias del 802.11b. También tiene la particularidad de ser compatible con ambas extensiones.

2.2.1 Espectro Disperso.

La meta de la técnica del espectro disperso, es utilizar más ancho de banda de lo que el sistema realmente necesita para la transmisión de modo que se reduzca el efecto de interferencia en el medio. La técnica de espectro disperso dispersa el ancho de banda transmitido de la señal resultante, reduciendo la potencia máxima pero manteniendo la potencia total en un mismo nivel.

2.2.1.1 FHSS

FHSS (Frequency Hopped Spread Spectrum – Espectro disperso por salto en frecuencia). Las técnicas que utilizan salto en frecuencia dependen de la diversidad de frecuencias para combatir la interferencia. Básicamente la señal "salta" de frecuencia en frecuencia siguiendo un patrón dado por un código que dispersa la potencia de la señal sobre un ancho de banda dado (ver figura 2-1). En comparación con la modulación FSK binaria, que sólo tiene dos posibles frecuencias, FHSS puede tener hasta $2x10^{20}$ o más.

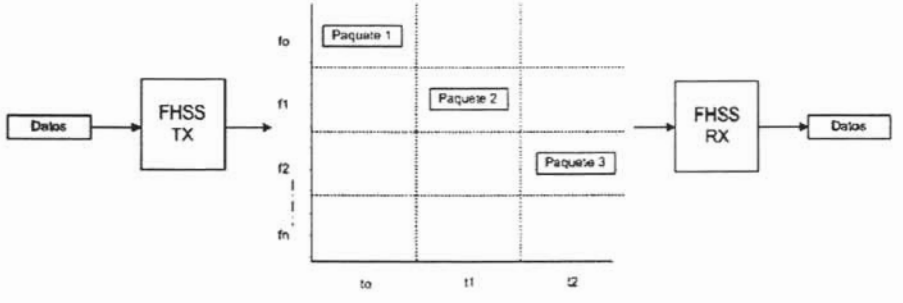


Figura 2-1. FHSS.

El transmisor FHSS es un sintetizador de frecuencia de pseudo-ruido controlado por código. La frecuencia de salida instantánea del transmisor salta de un valor a otro basado en una entrada pseudo-aleatoria del generador de códigos. Al variar la frecuencia instantánea se tiene un espectro de salida disperso sobre el rango de frecuencias generado.
El salto en frecuencia en el estándar 802.11 es realizado con modulación de frecuencia gaussiana (GFSK). Se utiliza 1 Mbps con GFSK de dos niveles y se utilizan 2 Mbps con una modulación de 4 niveles. Existen ciertas variaciones por supuesto: Norteamérica y Europa permiten saltos en el rango de los 2402-2480 MHz con un espaciamiento de canal de 1 MHz Japón permite saltos en el rango de los 2402-2478 MHz

2.2.1.2 DSSS

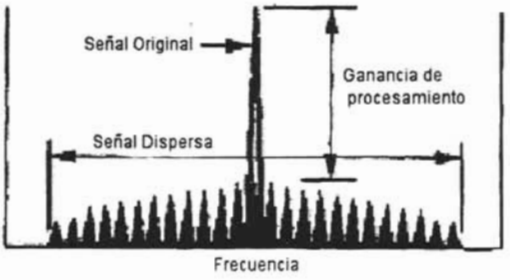


Figura 2-2. DHSS.

DSSS (Direct Sequency Spread Spectrum – Espectro Disperso por Secuencia Directa).El Espectro Disperso por secuencia directa utiliza una secuencia con un código de alta velocidad y modulación BPSK para modular a la portadora y realizar la dispersión. Se combinan estas características con tasas de transmisión de datos más pequeñas que también modulan a la portadora ya sea con BPSK o DQPSK (cuadratura diferencial). El código de alta velocidad es un *código Barker* de 11 bits que tiene buenas propiedades de auto correlación y le da a la forma de onda protección contra la interferencia y multitrayectoria.

Cabe mencionar que en el estándar IEEE 802.11, la técnica de Secuencia Directa a diferencia de los sistemas CDMA, sólo utiliza una señal de dispersión predefinida. El receptor común puede operar con una tasa de señal a ruido de 0 dB en el ancho de banda disperso y por lo tanto puede tolerar problemas de multitrayectoria mayores. Algunas de las características de Secuencia Directa en el estándar 802.11 son:

- Tasas de transmisión de 1 y 2 Mbps (Con modulación DBPSK y DQPSK respectivamente),
- Tasa de símbolos de 1 MHz,
- Tasa de *chipping* de 11 MHz con una secuencia Barker de 11 Chips,
- De 3 a 4 canales en la banda de 2.4 a 2.4835 GHZ,
- 10 dB en ganancia de procesamiento para una modulación eficiente en potencia y desempeño robusto contra interferencia y ruido (10 dB de supresión), y
- Protección contra dispersión por retardo en el tiempo.

Pueden operar hasta 3 canales de secuencia directa sin pérdidas del *troughput* espaciándolos en frecuencia en la banda ISM. El espaciamiento recomendado es de 30 MHz DSSS tiene más eficiencia de potencia que el GFSK utilizado en FHSS, de modo que una cantidad dada de la potencia de la portadora llevará a la señal más lejos. Puesto que la señal soporta mejor la interferencia, las redes en el mismo canal pueden ser colocadas más cercanas que con la técnica de FHSS. La mayoría de las implementaciones de DSSS utilizan las tasas 1 y 2 Mbps ya que el costo de hardware es el mismo. La versión del estándar 802.11 b incluye dos nuevas tasas de datos, 5.5 y 11 Mbps
Puesto que a secuencias mayores se generan tasas de transmisión más grandes sobre el aire, el estándar IEEE 802.11 define secuencias pequeñas. La forma de colocarlas se resuelve alojando en cada transmisor una banda propia. Debido a que la distancia entre las

frecuencias centrales de las bandas tiene que ser de 30 MHz (para 1 y 2 Mbps) o de 25 MHz (para 5.5 Mbps y 11 Mbps), sólo es posible colocar tres sistemas. El estándar define cuatro modos de operación, uno para cada tasa de transmisión disponible: 1 Mbps (IEEE 802.11), 2 Mbps (IEEE 802.11), 5.5 Mbps (IEEE 802.11b), y 11 Mbps (IEEE 802.11b).

Operación a 1 Mbps (LR/DSSS – Low Rate DSSS – DSSS de tasa baja).

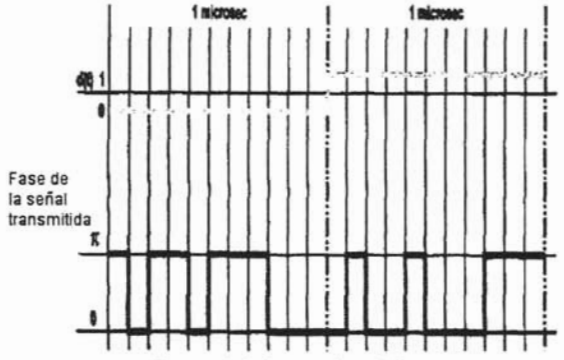


Figura 2-3. Operación a 1Mbps

Los datos se organizan en símbolos de un bit (los valores de los símbolos son 1 o 0). Cada símbolo es representado en el aire por la misma secuencia de 11 chips análogos (fases) +1; -1; +1; +1; -1; +1, +1; +1; -1; -1; -1. Para representar los dos valores posibles de símbolos (0,1) es necesario que la secuencia puede aparecer con corrimiento 0 o corrimiento π.

Cada chip análogo toma uno de dos posibles valores. 11 chips análogos con dos posibles valores cada uno dan un total de $2^{11} = 2048$ combinaciones. De estas 2048 combinaciones, sólo dos son seleccionadas para representar los dos posibles valores de los símbolos (se eligen las combinaciones con propiedades más acordes). La modulación actual es DBPSK.

Operación a 2 Mbps (LR/DSSS – Low Rate DSSS – DSSS de tasa baja).

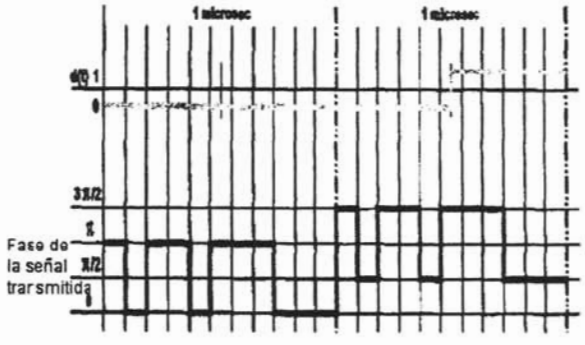


Figura 2-4. Operación a 2Mbps

Los datos se organizan en símbolos de dos bits (los valores de los símbolos son 00 01 11 10). Cada símbolo es representado en el aire por la misma secuencia de 11 chips análogos

(como en el caso de 1 Mb). Se definen cuatro fases sobre el aire, y la secuencia puede aparecer con corrimiento 0, corrimiento de $\pi/2$, corrimiento de π, y de $3\pi/2$. Cada chip análogo toma uno de cuatro posibles valores, $4^{11} = 4194304$ combinaciones. De todas estas combinaciones se seleccionan las cuatro más adecuadas para representar cuatro posibles valores. La modulación utilizada actualmente es la DQPSK.

Operación a 5.5 Mbps (HLR/DSSS –High Rate DSSS – DSSS de tasa alta) – Estándar IEEE 802.11 b.

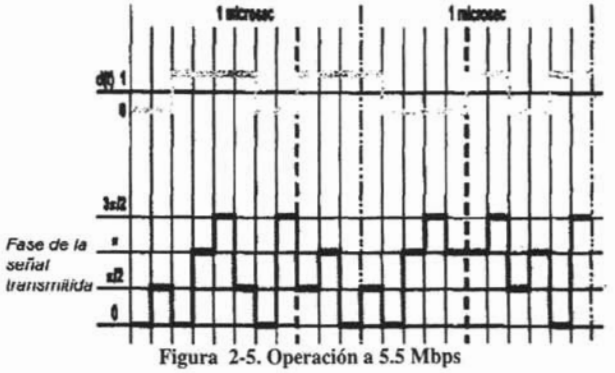


Figura 2-5. Operación a 5.5 Mbps

Los datos se organizan en símbolos de cuatro bits (16 posibles valores de símbolos). Cada símbolo es representado en el aire por una secuencia de 8 chips análogos. Para representar los 16 posibles valores de los símbolos, se definen cuatro fases sobre el aire. Cada chip análogo toma uno de cuatro posibles valores $4^8 = 65536$ combinaciones, de las cuales sólo se seleccionan 16. La modulación utilizada actualmente es CCK (*Complementary Code Keying),* la cual genera 8 chips análogos (comenzando de 8 bits de datos), y la DQPSK.

Operación a 11 Mbps (HLR/DSSS –High Rate DSSS – DSSS de tasa alta) – Estándar IEEE 802.11 b.

Los datos se organizan en símbolos de ocho bits (256 posibles valores de símbolos). Cada símbolo es representado en el aire por una secuencia de 8 chips análogos. Para representar los 256 posibles valores de los símbolos, se definen cuatro fases sobre el aire. Cada chip análogo toma uno de cuatro posibles valores $4^8 = 65536$ combinaciones, de las cuales sólo se seleccionan 256. La modulación utilizada actualmente es CCK, la cual genera 8 chips análogos (comenzando de 8 bits de datos), y la DQPSK. (Ver figura 2-6).

Además de las tasas de transmisión aquí comentadas utilizadas con la técnica de espectro disperso, existen otras variantes definidas en los estándares 802.11 a y 802.11 g que se comentarán más adelante ya que utilizan otras técnicas para su transmisión.

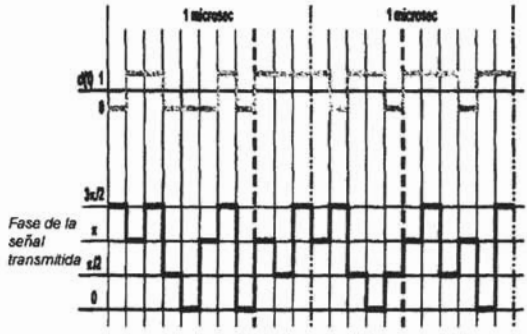


Figura 2-6. Operación a 11Mbps

2.2.2 OFDM (Orthogonal Frequency Division Multiplexing – Multiplexaje por división Ortogonal de Frecuencia)

El multiplexaje por división de frecuencia (FDM) transmite varias señales al mismo tiempo sobre un solo camino de transmisión. Cada señal viaja dentro de un rango de frecuencias único (portadora), que es modulada por los datos (transmisiones de voz y video). *La figura siguiente* muestra la relativa relación de las portadoras dentro de un ancho de bando dado.

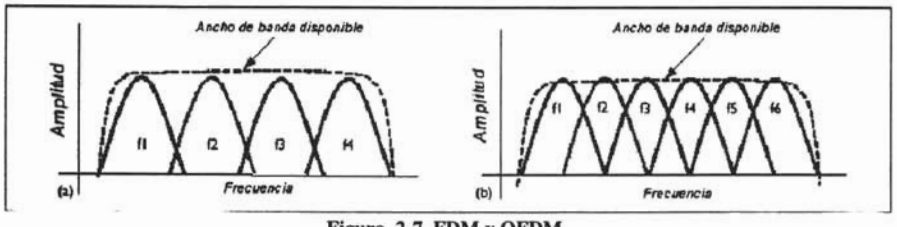


Figura 2-7. FDM y OFDM.

Aunque el beneficio principal de FDM es un mayor ancho de banda, también reduce la interferencia intersimbólica por multitrayectoria (ISI). El incremento del ancho de banda llega a un nivel de ineficiencia: hasta un 50 % del espectro disponible es desperdiciado en bandas de guarda lo cual asegura el aislamiento entre frecuencias.

La técnica de OFDM de espectro disperso utiliza además modulación QAM y procesamiento avanzado digital de señales, con lo cual se distribuyen los datos sobre varias portadoras espaciadas a frecuencias precisas.

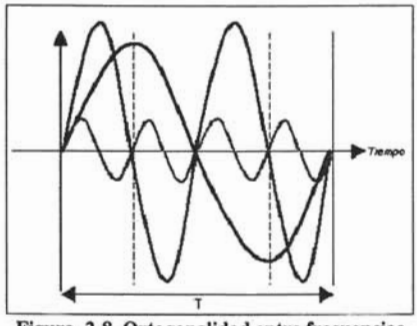


Figura 2-8. Ortogonalidad entre frecuencias.

El espaciamiento tan preciso permite la ortogonalidad que previene que los demoduladores capten frecuencias ajenas a la suya. Como cada portadora puede ser claramente identificada, las bandas de guarda se eliminan incrementando la eficiencia del uso del espectro de frecuencias. *La figura 2-8* muestra la ortogonalidad de las diversas portadoras.

Los beneficios de OFDM son su alta eficiencia espectral, protección contra interferencia de RF y baja distorsión por multi-trayectoria .

2.2.3 Infrarrojo (IR).

Los infrarrojos son ondas electromagnéticas que se propagan en línea recta, siendo susceptibles de ser interrumpidas por cuerpos opacos. Su uso no precisa licencias administrativas y no se ve afectado por interferencias radioeléctricas externas, pudiendo alcanzar distancias de hasta 200 metros entre cada emisor y receptor. Se encuentra de momento menos desarrollada, las distancias que se cubren son sensiblemente más cortas y existen aún una importante serie de problemas técnicos por resolver. Pese a ello, presenta la ventaja frente a las microondas de que no existe el problema de la saturación del espectro de frecuencias, lo que la hace tremendamente atractiva ya que se basa en un "espacio libre" de actuación. De acuerdo al ángulo de apertura con que se emite la información en el transmisor, los sistemas de infrarrojos pueden clasificarse en sistemas de corta apertura, también llamados de rayo dirigido o de línea de vista (line of sight, LOS) y en sistemas de gran apertura, reflejados o difusos:

- Sistemas de infrarrojos de corta apertura: funcionan de manera similar a los controles remotos de los televisores. Mediante este sistema, el emisor debe orientarse hacia el receptor antes de transferir información, lo que limita un tanto su funcionalidad. Por ejemplo, resulta muy complicado utilizar esta tecnología en dispositivos móviles, pues el emisor debe reorientarse constantemente. Por otra parte, este mecanismo permite enlaces punto a punto exclusivamente.
- Los sistemas de gran apertura permiten la transmisión de información en un ángulo mucho más amplio, por lo que el transmisor no tiene que estar alineado con el receptor. Una topología muy común para redes locales inalámbricas basadas en esta tecnología, consiste en colocar en el techo de la oficina un nodo central llamado punto de acceso, hacia el cual los dispositivos inalámbricos dirigen su información, y desde el cual ésta

es difundida hacia esos mismos dispositivos. Desgraciadamente, la dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor que limita notablemente la velocidad de transmisión.

La tecnología de infrarrojos cuenta con muchas características sumamente atractivas para utilizarse en WLAN, y otras que no lo son tanto. En principio, los infrarrojos tienen una longitud de onda cercana a la de la luz y, por lo tanto, con un comportamiento similar, es decir, no pueden atravesar objetos sólidos como paredes, por lo cual es un sistema seguro contra receptores no deseados, aunque esta característica también supone un serio inconveniente a su capacidad de difusión. Asimismo, y debido a su alta frecuencia, presenta una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por otros dispositivos. Además, se pueden alcanzar grandes velocidades de transmisión, de hecho, se han desarrollado sistemas que operan a 100 Mbps En cuanto a las restricciones de uso, la transmisión de infrarrojos con láser o con diodos no requiere autorización especial en ningún país, excepto por los organismos de salud que limitan la potencia de la señal transmitida. Y, por último, como atractivo, la mayoría de fabricantes, utilizan componentes sumamente económicos y de bajo consumo energético, importantes características muy a tener en cuenta en aquellos dispositivos que deban formar parte de equipos móviles portátiles.

Entre las limitaciones principales que se encuentran en esta tecnología se puede señalar que es sumamente sensible a objetos móviles que interfieren y perturban la comunicación entre emisor y receptor. Además, las restricciones en la potencia de transmisión limitan la cobertura de estas redes a unas cuantas decenas de metros, y lo que de aún más grave, la luz solar directa, las lámparas incandescentes y otras fuentes de luz brillante pueden interferir seriamente la señal.

En conclusión, a pesar de sus buenas cualidades y características, la gran influencia del entorno representa un enorme contratiempo para la fiabilidad de las comunicaciones y, por tanto, reduce sus posibilidades de implantación masiva. Se utilizan en los mandos a distancia del hogar (TV, video, DVD, etc.), y últimamente se han incorporado en los PDA y los teléfonos GSM, lo cual permite intercambiar ficheros a velocidades de hasta 4 Mbps El inconveniente es que deben apuntarse los respectivos sensores, lo cual obliga a hacer puntería con el mando a distancia desde el sillón del salón a la TV.

2.2.4 Formato del frame en la capa PHY.

La capa física se encuentra dividida en dos subcapas PDM (Physical Médium Dependent) y la PLCP (Physical Layer Convergent Protocol); la primera tiene la función de definir las características de transmisión y recepción en el medio inalámbrico; la capa PLCP es llamada así por utilizar dicho protocolo, el cual se encarga de establecer una comunicación con entre las capas PDM y MAC. Esta subcapa puede emplear dos formatos de trama una con preámbulo largo y otra con preámbulo corto, desarrollado posteriormente para mejorar el rendimiento de la red.

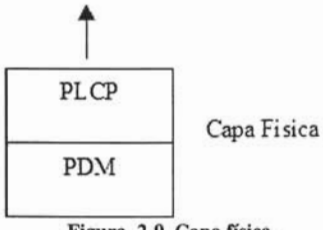


Figura 2-9. Capa física.

El preámbulo PLCP consiste en dos campos, uno de sincronización de la señal de 128 bits para preámbulo largo y 56 bits para preámbulo corto y el delimitador de inicio de trama, como su nombre lo indica, delimita el inicio de trama. Ambos son transmitidos a 1 Mbps con DBPSK.
El encabezado PLCP, contiene 48 bits de información y consta de 4 campos:

- Señal.- Indica que tan rápido serán transmitidos los datos contenidos en el PSDU (PLCP Service Data Unit).
- Servicio.- Indica la modulación empleada para el PSDU.
- Longitud .- Indica la longitud del campo PSDU.
- CRC (Cyclic Redundancy Check).- Valor calculado, de acuerdo con la información de los cuatro campos del encabezado para la detección de errores.

El contenido del encabezado es el mismo para preámbulo largo y corto, sin embargo para el primero la información es transmitida a 1Mbps con DBPSK y para el segundo a 2 Mbps con DQPSK. Los datos contenidos en el PSDU pueden ser transmitidos con velocidades de 2, 5.5 11 Mbps para preámbulo corto y 1,2 ,5.5 y 11 para Preámbulo largo.
La trama completa compuesta del preámbulo PLCP, encabezado y PSDU es denominada PPDU (PLCP Protocol Data Unit).

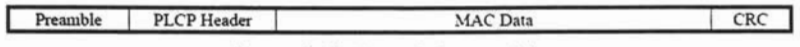


Figura 2-10. Frame de la capa física.

2.2.5 Comparación entre modalidades PHY.

A continuación presentamos una tabla comparativa que resume las diferentes características de cada una de las modalidades del IEEE 802.11

Tabla 2-2. Estándares a/b/g.

Estándar	802.11a	802.11b	802.11g
Frecuencia	5 GHz La banda poco utilizada de 5 GHz puede coexistir con las redes de 2.4 GHz sin interferencia	2.4 GHz Una banda muy utilizada por lo que hay interferencia de otros dispositivos que utilicen la misma banda.	2.4 GHz Una banda muy utilizada por lo que hay interferencia de otros dispositivos que utilicen la misma banda.
Velocidad	54 Mbps	11 Mbps	54 Mbps
Throughput promedio actual	27 Mbps	4-5 Mbps	20-25 Mbps
# Canales / utilizables	12 / 8	11 / 3	11 / 3
Rango*	Rango menor que en 802.11 b y g. Debido su frecuencia de operación tan alta, ofrece menor rango y capacidad de trabajar a través de pisos y paredes	Mejor rango que 802.11 a y puede trabajar entre pisos y paredes	Mejor rango que 802.11 a y puede trabajar entre pisos y paredes
Compatibilidad	Incompatible con 802.11b o 802.11g	Ampliamente adoptado. Tendrá compatibilidad con 802.11g	De antemano compatible con las redes 802.11 b (a 11 Mbps); Incompatible con 802.11a
Popularidad	Poco uso en la actualidad. Poco equipo 802.11 a	Actualmente es el de uso más extendido. 802.11b es utilizado en varios hotspots como aeropuertos, hoteles, escuelas y áreas públicas. Amplia selección de equipos.	Ultimo estándar creado. Con velocidades 5 veces mayores al 802.11b, se espera que pronto reemplace al 802.11b.
Costo	El más caro	El más barato	Desde el lanzamiento oficial, los precios han disminuido. Precios competitivos con 802.11b. Más barato que 802.11a

*** (El rango dependerá de la ganancia de la antena, potencia de transmisión, sensibilidad de recepción del radio y de los obstáculos entre origen y destino.)**

2.3 Capa MAC.

Las principales funciones de la capa MAC (Medium Access Control) dentro del DLC (Data Link Control) del IEEE 802.11 no es solo gestionar y coordinar el acceso al canal de transmisión, si no que es responsable de los procedimientos relacionados a la reservación del canal, direccionamiento de PDU (Unidad de Datos del Protocolo – Protocol Data Unit), formato del frame, control de errores, así como de la fragmentación y reensamble de los paquetes, y hasta cierto punto se encargan de la autentificación, así como de otras tareas de administración y de seguridad.

La capa MAC de manera virtual, es la que permite el monitoreo de la portadora en forma física a través de la interferencia aérea de las radio ondas. Es difícil descubrir colisiones en una red de transmisión RF y es por esta razón por la que se usa la supresión de colisiones. La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. 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 arriba 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 802.11. El mejor método a utilizar depende de los niveles de interferencia en el entorno operativo.

2.3.1 Formato del frame.

El IEEE 802.11, soporta tres tipos de frames: administración, control y datos. Los frames de administración son utilizados para la asociación y des-asociación de las estaciones con el Punto de Acceso, de la señal de reloj y la sincronización, así como de la autentificación y des-autentificación. Los frames de Control se usan para el handshaking durante el CP, para ACKs positivos durante este, y para la terminación del CFP. Los frames de Datos son usados para la transmisión de datos durante el CP y el CFP, y pueden ser combinados con peticiones y ACKS durante el CFP.
Cada frame se conforma de los siguientes componentes:

- Un encabezado MAC, que comprende los frames de control, duración, dirección, e información de secuencias de control.
- Un cuerpo del frame (Frame Body) de longitud variable, que contiene información específica de acuerdo al tipo de frame.
- Un FCS (Frame Check Sequence), que contiene un CRC (Cyclic Redundancy Code)de 32 bits.

Un MPDU (MAC Protocol Data Unit- Unidad de dato del protocolo MAC) es descrito como una secuencia de campos en un orden específico. Los campos son pasados al PLCP (Physical Layer Convergente Protocol), en el orden que se describen de izquierda a derecha.

El formato del frame de acuerdo al estándar se ilustra a continuación:

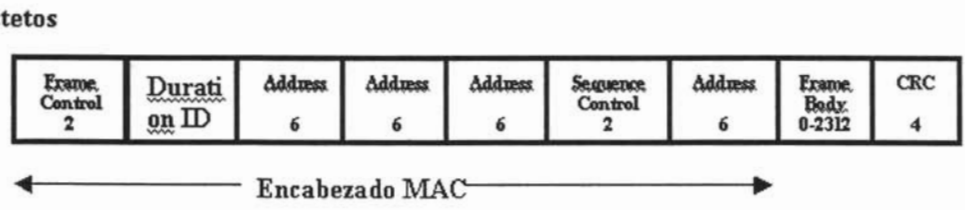


Figura 2-11. Formato del frame. Capa MAC.

- En el campo de duración se contiene el Duration value (Valor de duración) el cual es menor a 32768, y que sirve para actualizar el NAV (Network Allocation Vector)
- Los campos de Address (4 en total), indican el BSSID, la dirección destino (DA), la estación origen, la dirección de la estación que transmite (TA), la dirección de la estación que recibe (RA)
- El campo Sequence control, nos indica en caso de que un MPDU sea fragmentado, su secuencia, así como el número del fragmento.
- El campo Frame Body es un campo variable que contiene información específica de acuerdo al tipo y subtipo de frame.
- Campo FCS, contiene el CRC de 32 bits, y se calcula con el encabezado y el campo de cuerpo del frame, a través de un polinomio de grado 32.

2.3.1.1 Frame de Control.

El frame de control es de suma importancia para la transferencia de archivos, veamos en que consiste:

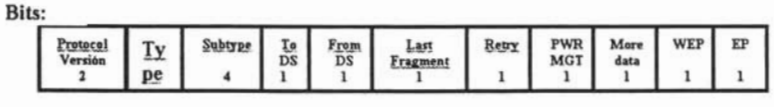


Figura 2-12. Frame de Control. Capa MAC.

- Campos Type y Subtype trabajan de manera conjunta para establecer la función del frame: Control, datos y administración.
- Campo DS, se establece en 1 cuando los frames de datos son destinados al DS.
- Campo From DS, se establece en 1 cuando un frame de datos viene del DS. Estos campos también trabajan de manera conjunta.
- Campo Retry, es 1 si un frame de datos o administración es una retransmisión de otro frame. Se evitan frames duplicados.
- Campo Power Management se indica el modo de administración de energía de la estación después de haber completado con éxito un intercambio de frames. Un valor 1 establece un modo de ahorro de energía y un 0 que la estación estará en modo activo.
- Campo More data. Si su valor es 1, le indica a la estación que está en modo de ahorro de energía, que un MSDU o un MPDU esta guardado para ella en el punto de acceso. Esta presente en frames de datos y de administración.
- Campo WEP, indica que la información contenida en el campo del cuerpo del frame ha sido procesada por un algoritmo WEP.

2.3.2 Descripción funcional de la capa MAC.

El medio de transmisión puede operar en dos modos distintos o alternar entre estos: el modo de contención, en la que todas las estaciones compiten por el canal para cada paquete por transmitir llamado CP (Contention Period– Periodo de Contenciones), y el CFP (Contetion Free Period-Periodo Libre de Contenciones), aquí el medio a utilizar es controlado por el Punto de acceso, eliminando así la necesidad de que las estaciones compitan por el canal de acceso.

El IEEE 802.11 MAC, también, especifica el soporte de transferencias asíncronas de datos, así como de DTBS (Distributed Time Bounded Services- Servicios sensibles al tiempo). Las transferencias asíncronas se refieren a un tráfico que es relativamente insensible a retardos de tiempo, como por ejemplo: transferencias de archivos, correo electrónico, etc. El tráfico DTBS o sensible al tiempo, por otro lado, es un trafico que esta limitado por retardos específicos de tiempo para así lograr una QoS (Quality of Service -Calidad de servicio) aceptable, como es el caso de video y voz.

Para esto, se definen dos tipos de esquemas MAC para el transporte de servicios: asíncronos y DTBS. El primer esquema, DCF (Distributed Coordination Function – Función de Coordinación distribuida), es similar a la tradicional repartición de paquetes en redes bajo el esquema del "mejor esfuerzo" (Best effort). EL DCF esta diseñado para el transporte de datos asíncronos, en donde todos los usuarios con datos a transmitir tienen la misma oportunidad de acceder a la red.

El segundo esquema es el PCF (Point Coordination Function- Función de coordinación por Punto). EL PCF esta basado en un sistema de peticiones que es controlado por un punto de acceso. EL PCF esta diseñado para la transmisión de tráfico sensible al tiempo o DTBS

2.3.2.1 Función de Coordinación Distribuida.

La DCF (Distribution Coordination Function – Función de Coordinación Distribuida) es un método de acceso fundamental para la transmisión asíncrona de datos bajo la base del "mejor esfuerzo". Como lo menciona el estándar, todas las estaciones tienen que soportar DCF. La arquitectura MAC es descrita a continuación:

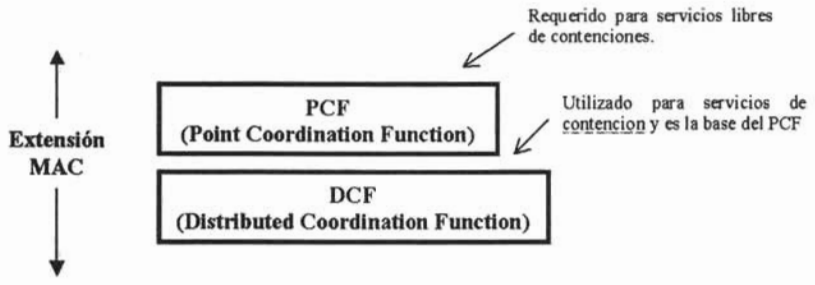


Figura 2-13. Funciones de distribución.

Observamos que el DFC se sitúa inmediatamente por arriba de la capa física y soporta servicios de contención. Estos servicios implican que cada estación con un MSDU en espera para ser transmitido debe competir por el canal, y una vez que el MSDU es transmitido, los frames subsecuentes deberán volver a competir por el canal.

EL DFC es basado en el protocolo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance- Acceso múltiple con detección de portadora con supresión de Colisiones). La razón es que, a pesar de que pensemos que las redes inalámbricas son un medio tipo Broadcast, el protocolo tradicional CSMA/CD (Collision Detection- Detección de Colisiones) no funcionaria correctamente, esto se debe a que la estación no esta habilitada para escuchar el canal y ver las colisiones mientras esta transmite.

2.3.2.2 CSMA/CA.

El grupo de estudio IEEE 802.11 estableció algunos requerimientos para un buen protocolo de control de acceso al medio MAC, los cuales se mencionan a continuación:

- *Eficiencia:* Se refiere al comportamiento del protocolo con relación al ancho de banda utilizado y su efectividad en la transmisión de los datos.
- *Retardo o demora*: Especialmente critico para servicios dependientes del tiempo como el vídeo y aplicaciones multimedia.
- *Transferencia para diferentes Capas Físicas*: Una manera de conseguir esto, es tener una capa física dependiente, una capa física de convergencia y una interfase MAC-PHY apropiada en cada estación. Basada en esa arquitectura, actualmente adoptada por el

comité IEEE 802.11 un simple MAC puede intercambiar información con diferentes capas físicas de forma transparente.

- *Capacidad para manejar datos, voz y vídeo*: Dirigido al auge en el desarrollo de aplicaciones multimedia.
- *Igualdad de acceso:* Referido a las características de desvanecimiento dentro de los canales, lo que puede causar una potencia recibida desigual en la estación base originándose falsos accesos a la red.
- *Máximo número de nodos.*
- *Handoff/Roaming entre áreas de servicio*: esta movilidad es una característica especial de las redes inalámbricas. Es importante tomar en cuenta el consumo de potencia en aquellas aplicaciones dependientes del tiempo.
- *Conexión punto a punto sin conocimiento a priori.*

El protocolo que representa esto es el CSMA/CA .Veamos como funciona este protocolo:

En el estándar IEEE 802.11, la detección de la portadora es llevado acabo por ambas capas, por la interfaz de aire (Capa Física) y por la capa MAC, a la cual a esta última se le llama un detección de portadora virtual.

Una estación fuente lleva a cabo una detección de portadora virtual mandando información de la duración del MPDU en los encabezados de los RTS (Request to Send) o del CTS (Clear to Send) y en los frames de datos. La detección de la portadora de manera virtual es utilizada por una estación fuente para informar a todas las estaciones en la BSS, por cuanto tiempo el canal va a ser utilizado para una transmisión exitosa de MPDU (MAC Protocol Data Unit- Unidad de datos del protocolo MAC). Como vimos en el formato del frame, las estaciones fuente establecen un campo de duración en el encabezado MAC de los frames de datos, o los frames de control RTS (Request to Send- Solicitud para mandar) y los CTS (Clear to Send- Libre para Mandar). El campo de duración indica cuanto tiempo (en microsegundos) después del final del presente frame, el canal será utilizado para completar una transmisión exitosa del este. Las estaciones dentro de la BSS utilizan la información del Campo "Duration" para ajustar su NAV (Network Allocation Vector), el cual indica la cantidad de tiempo que debe pasar entre la transmisión en curso sea completada y el canal puede ser puesto en estatus "libre" (Idle). El canal es marcado como ocupado si cualquiera de los dos ya sea la detección en la capa física o la detección virtual en la capa MAC indican que este esta ocupado.
El orden de acceso al medio inalámbrico es controlado a través del uso de intervalos de tiempo IFS (InterFrame Space – Espacio Entre Frames) entre la transmisión de los frames. Estos intervalos IFS son periodos ya establecidos de tiempo libre en el medio de transmisión.
Existen tres tipos de periodos IFS y se colocan en orden del más corto al más largo:

- SIFS (Short-IFS).
- PIFS (Point Coordination Function- PIFS).
- DIFS (distributed Coordination Function- DIFS).

Los diferentes IFS deben ser independientes de la velocidad de transmisión de la estación. Estos tiempos IFS son fijos para cada PHY.

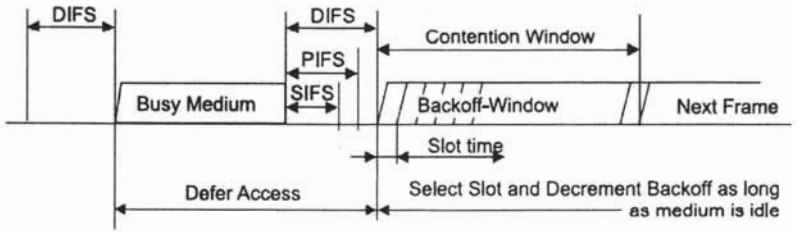


Figura 2-14. Relaciones entre tiempos IFS.

Short IFS (SIFS)

Es utilizado por un frame ACK, CTS, el Segundo o subsecuente MPDU, y por una estación que responda a una petición del PCF. También puede ser usado por el PC para cualquier tipo de frame durante el CFP. El SIFS es el tiempo del final del último símbolo del frame previo al principio del primer símbolo del preámbulo del frame subsecuente que es visto en la interfaz de aire. El SIFS es el IFS más corto. EL SIFS debe ser utilizado por la estación cuando se ha apoderado del medio y necesita mantenerlo por la el tiempo que dure el intercambio del frame que esta por llevarse a cabo. Este tiempo entre transferencias de frames previene a las otras estaciones, a que no utilicen el medio, así dándole prioridad a que a la transferencia en progreso.

PCF IFS (PIFS)

EL PIFS se usará cuando solo por una estación que opere bajo el PCF para tener un acceso prioritario al medio al comenzar el CFP.

DCF IFS (DIFS)

Es utilizado por una estación cuando opera bajo DCF para la transmisión de frames de datos y administración. Una estación utilizando DFC podrá transmitir solo si su mecanismo de detección de portadora determina que el medio esta libre después de haber pasado el tiempo DIFS después de una recepción exitosa del frame y que el tiempo de back-off haya expirado.

Para un método de acceso básico, cuando una estación detecta que el canal esta libre, la estación espera un tiempo DIFS y nuevamente verifica si el estatus del canal. Si este sigue libre, la estación transmite el MPDU. La estación destino calcula el checksum y determina si el paquete fue recibido correctamente. Una vez que se recibió el paquete correctamente, la estación destino espera un tiempo SIFS y transmite un ACK positivo a la estación fuente, indicando que la transmisión fue exitosa.
A continuación vemos una figura que ilustra una transmisión exitosa de un frame de datos.

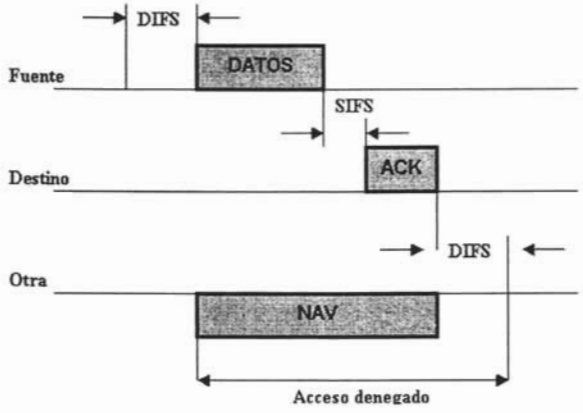


Figura 2-15. Transmisión de un MDPU sin RTS/CTS.

Cuando el frame de datos es transmitido, el campo de duración del frame es utilizado para permitir a las demás estaciones en la BSS saber por cuento tiempo el medio estará ocupado. Todas las estaciones que escuchan al frame de datos, ajustan su NAV basados en el valor del campo de duración, el cual incluye el intervalo SIFS y el frame ACK seguido del frame de datos.

Como una estación fuente en una BSS no puede escuchar sus propias transmisiones, cuando una colisión ocurre, la estación fuente continua transmitiendo el MPDU completo. Si el MPDU es largo, el ancho de banda se verá desperdiciado debido a un MPDU corrupto. Los frames de control RTS y CTS pueden ser usados por una estación para reservar el canal con anterioridad a la transmisión de un MPDU por lo tanto el ancho de banda desperdiciado debido a las colisiones puede ser minimizado. Los frames RTS y CTS son relativamente pequeños (RTS de 20 octetos y el CTS de 14 octetos) en comparación con el tamaño máximo de un frame datos (2346 octetos).

El frame de control RTS es primero transmitido por la estación fuente (después de haber contendido exitosamente por el canal) con un frame de datos o de administración a una especifica estación destino. Todas las estaciones en la BSS, escuchan el paquete RTS, leen el campo de duración y ajustan su NAV de acuerdo a este. La estación destino responde al paquete RTS con un paquete CTS después que ha pasado un periodo libre SIFS. Las estaciones que escucharon el paquete CTS ven el campo de duración y nuevamente actualizan su NAV. Hasta la recepción exitosa del CTS, la estación fuente esta virtualmente confiada que el medio esta estable y reservado para transmisiones exitosas de MPDU. Hay que notar que las estaciones son capaces de actualizar su NAV basados en un RTS de la estación fuente y del CTS de la estación destino, lo cual ayuda a combatir el problema de las "Terminales ocultas". En la figura vemos el mecanismo de transmisión de un MSDU utilizando RTS/CTS.

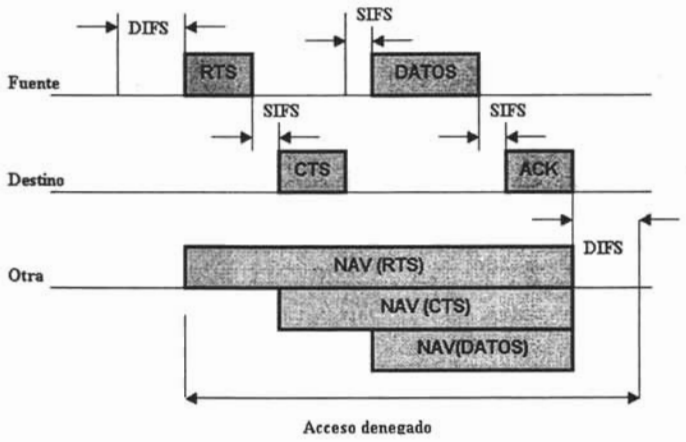


Figura 2-16. Transmisión de un MDPU con RTS/CTS.

Las estaciones pueden escoger si nunca van a utilizar RTS/CTS o utilizar RTS/CTS siempre que el MSDU exceda el valor de umbral RTS, o siempre usar RTS/CTS. Si una colisión ocurre con un MPDU RTS/CTS, menor ancho de banda es desperdiciado en comparación con la colisión de un MPDU largo. Sin embargo, para un tráfico medio, se puede presentar un retardo provocado por los encabezados de los frames RTS/CTS.

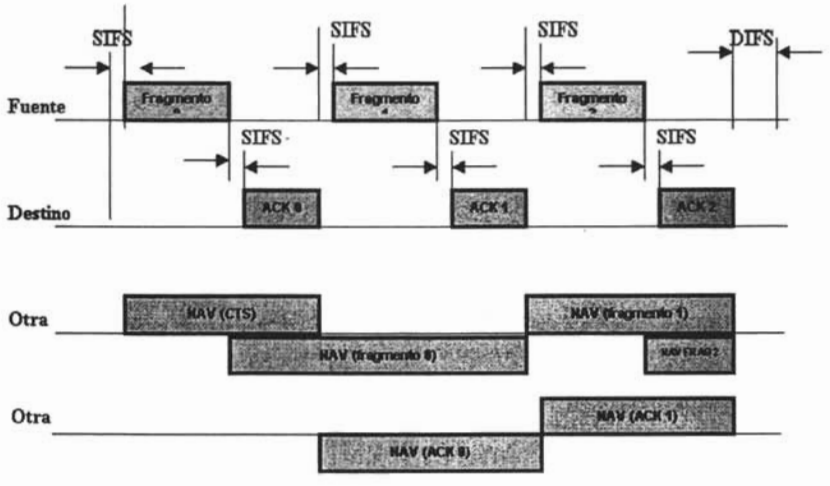


Figura 2-17. Transmisión de MPDU fragmentados.

Si los MSDU que vienen de la LLC a la capa MAC son muy largos, estos requieren ser fragmentados para incrementar la eficiencia de la transmisión. Para determinar como se llevara acabo dicha fragmentación, los MPDU son comparados con un parámetro llamado Umbral de fragmentación (Fragmentation_Threshold). Si el MPDU excede en tamaño el valor de este umbral, el MSDU es dividido en múltiples fragmentos. Los MPDU resultantes son del tamaño de este umbral de fragmentación, con excepción del último MPDU, el cual tiene un tamaño variable que no excede el del umbral de fragmentación. Cuando un MSDU es fragmentado, todos los fragmentos son transmitidos de manera secuencial.

El canal no es liberado hasta que el MSDU completo ha sido transmitido de manera exitosa, o que la estación fuente falle al recibir los ACK de un fragmento transmitido. La estación destino manda sus ACK por cada fragmento recibido mandando un DCF-ACK de regreso a la estación fuente. La estación fuente mantiene el control del throughtput en el canal en la transmisión del MSDU solo esperando un periodo SIFS después de recibir un ACK y transmitiendo el fragmento siguiente. Cuando un ACK no es recibido para un frame anteriormente transmitido, la estación fuente detiene la transmisión y nuevamente contiende por el canal. Una vez que gana el acceso, la fuente comienza a transmitir a partir del ultimo fragmento que si fue reconocido con un ACK.

Si es utilizado el esquema RTS/CTS, solo el primer fragmento es mandado utilizando un mecanismo de ACK. La duración del RTS y del CTS solo cuenta para la transmisión del primer fragmento a través de la recepción de su ACK. Las estaciones en la BSS después de eso mantienen su NAV, extrayendo la duración de la información de todos lo fragmentos subsecuentes.

La parte de supresión de colisiones del CSMA se lleva cabo por medio de un procedimiento aleatorio de BACKOFF. Si una estación con un frame a transmitir, ve que el canal esta ocupado, la estación espera hasta que el canal este desocupado por un periodo DIFS y después calcula un tiempo aleatorio de BACKOFF. Para el IEEE 802.11, el tiempo es repartido en ranuras de tiempo correspondientes a un Slot_Time. A diferencia del ALOHA Ranurado, donde la ranura de tiempo es igual a el tiempo de transmisión de un paquete, el Slot_Time utilizado en 802.11 es mucho mas pequeño que el MPDU y es utilizado para definir los intervalos IFS y determinar el tiempo de backoff para las estaciones en el CP. El Slot_Time es diferente para cada capa física. El tiempo de backoff aleatorio es un valor entero que corresponde a un número de ranuras de tiempo. Inicialmente, la estación calcula un tiempo de backoff uniforme en el rango de 0-7. Después que el medio esta libre al haber pasado el periodo DIFS, la estaciones decrementan su contador de backoff hasta que el medio este ocupado otra vez, o hasta que el contador se vuelva cero. Si el contador no ha llegado a cero, y el medio se ocupa, la estación detiene su contador. Cuando el contador finalmente llega a cero, la estación transmite su frame. Si dos o mas estaciones llegan a cero al mismo tiempo, ocurrirá una colisión y cada estación tiene que generar un nuevo tiempo de backoff en el rango de 0-15. Por cada intento de retransmisión, el tiempo de backoff se incremente a

$$[2^{2+i} . \text{ranf}( )]* \text{Slot\_Time}$$

donde I, es el numero de veces consecutivas que la estación ha intentado mandar un MPDU, ranf( ) es una variable aleatoria uniforme de (0 a 1). El periodo libre después de un intervalo de tiempo DIFS se refiere como una CW (Contention Window- Ventana de Contención).

La ventaja de este método de acceso al medio, es que promueve imparcialidad entre estaciones, pero su debilidad radica en que no permite DTBS. La imparcialidad se mantiene por que cada estación debe contender por el canal después de cada transmisión de un MSDU. Todas las estaciones tienen la misma probabilidad de ganar el acceso al canal después de un periodo de tiempo DIFS. Los servicios sensibles al tiempo típicamente soportan aplicaciones en la que los paquetes de voz o video deben ser mantenidos con un retardo específico. El DFC, no es un mecanismo que garantice el retardo y así soportar servicios sensibles al tiempo.

2.3.2.3 Función de Coordinación Puntual.

El PCF (Point Coordination Function) es una función opcional, orientada a conexión, y que soporta la transferencia de frames libre de contenciones (CF). El PCF radica en un PC (Point Coordinator - Coordinador puntual) que lleva a cabo las peticiones, habilitando a las estaciones a transmitir sin pelear por el medio. La función de PC es llevado a cabo por el PUNTO DE ACCESO dentro de la BSS. Las estaciones dentro de la BSS que son capaces de operar en el periodo CF son conocidas como estaciones CF-Aware.
EL PCF requiere coexistir con el DCF y lógicamente se sitúa por arriba del DCF. El intervalo de repetición CFP (CFP_ Rate) es utilizado para determinar la frecuencia a la cual el PCF ocurre. Dentro de un periodo de repetición, una porción del tiempo es reservado para tráfico libre de contenciones, y el resto para tráfico basado en contenciones. El intervalo de repetición CFP es iniciado por un frame BEACON, donde este es transmitido por el punto de acceso. Una de sus principales funciones es la sincronización. La duración de este intervalo es un parámetro que podemos establecer, y consiste en un número entero de frames tipo beacons. Una ves que el CFP_Rate es establecido, la duración del CFP es determinado. El tamaño máximo del CFP es determinado por el parámetro CFP_Max_Duration. El valor mínimo del CFP_Max_Duration es el tiempo requerido para transmitir 2 MPDU con tamaño máximo, incluyendo encabezados, el frame beacon inicial y el frame CF-End. El máximo valor del CFP_Max_Duration es el intervalo de repetición CFP menos el tiempo requerido para transmitir de manera exitosa un MPDU de tamaño máximo durante el CP. Después, el tiempo debe ser reservado por lo menos un MPDU para ser transmitido durante el CP. Es tarea del Punto de acceso determinar cuanto tiempo debe operar el CFP durante cualquier intervalo de repetición. Si el tráfico no es muy intenso, el punto de acceso podría cortar el CFP y dar el resto del intervalo de repetición al DCF. También, el CFP debe ser acortado si el tráfico tipo DCF de un intervalo de repetición previos se sobrepone al intervalo presente. La máxima cantidad de retardos que pueden incurrir, es el tiempo que toma para transmitir un RTS/CTS, un MPDU máximo, y ACK.

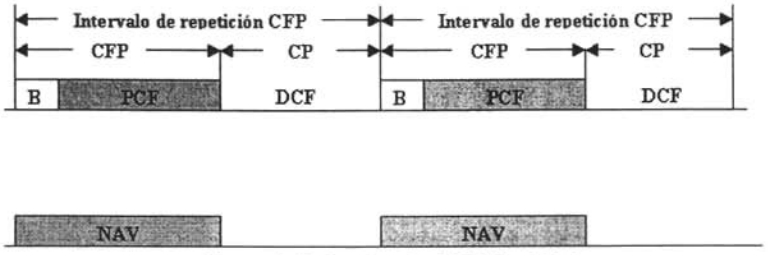


Figura 2-18. Coexistencia del PCF y DCF.

En el comienzo de cada intervalo de repetición CFP, todas las estaciones en la BSS actualizan su NAV a la máxima longitud del CFP (por ejemplo CFP_Max_Duration). Durante el CFP, el único momento en que las estaciones pueden transmitir esa petición del PC o para la transmisión de un ACK después de un intervalo SIFS después de la recepción de un MPDU. Cuando comienza el CFP, el PC sensa el medio. Si el medio sigue libre por un tiempo PIFS, el PC transmite un beacon para iniciar el CFP. El PC comienza la transmisión tipo CF a un intervalo SIFS después que el beacon es transmitido mandando un CF-Poll, Datos o Datos + CF- Poll. El PC puede inmediatamente terminar el CFP transmitiendo un frame CF-End, lo cual es común si la red no esta muy cargada y el PC no tiene tráfico guardado. Si una estación CF_Aware recibe un CF-Poll del PC, la estación puede responder al PC después de un SIFS, con un CF-ACK o un Datos + CF-ACK. Si el PC recibe un frame Datos + CF ACK de una estación, el PC puede enviar un frame Data + CF CK + CF POLL a una estación diferente, donde la porción del CF-ACK es utilizado para un ACK de que se recibió en el frame anterior.

La habilidad de combinar las peticiones y los ACK con frames de datos, transmitidos entre el PC y las estaciones, fue diseñada para mejorar la eficiencia. Si el PC transmite un CF-POLL y la estación destino no tiene un frame de datos por transmitir, la estación manda una función NULL de regreso al PC. Si el PC falla en la recepción de un ACK de un frame ya transmitido, el PC espera un tiempo PIFS y continúa transmitiendo a la estación siguiente en la lista de peticiones.

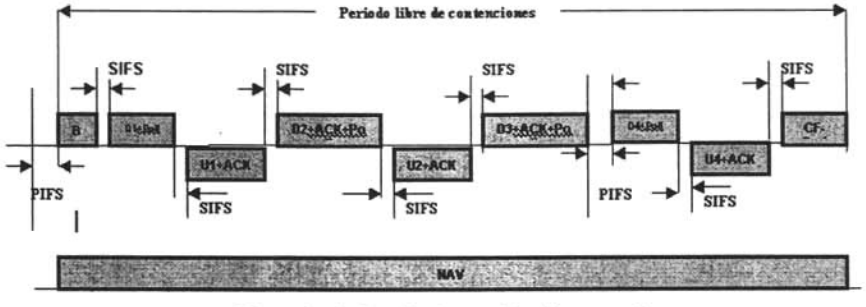


Figura 2-19. Función de coordinación puntual.

Después de recibir la petición del PC, la estación puede escoger si transmitir un frame a otra estación en la BSS. Cuando la estación destino recibe el frame, un DCF ACK es

regresada a la estación fuente, y el PC espera por un intervalo PIFS seguido de un frame ACK antes de transmitir frames adicionales.

El PC puede además escoger si transmitir a una estaciona NO aware. Desde una recepción exitosa de transmisión del frame, la estación deberá esperar un intervalo SIFS y contestar al PC con un frame ACK estándar. La fragmentación y el reensamblado son también administrados por el umbral de fragmentación. Es responsabilidad de la estación destino el reensamblar los fragmentos para forma el MSDU original.

2.3.3 Terminales ocultas.

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 LAN 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. El problema del nodo oculto ocurre en redes de punto a multipunto. Este problema puede surgir cuando hay tres (o más nodos) presentes.
Veamos un caso práctico, tenemos el caso de tres estaciones, y se da la siguiente situación:

- Estación A ve a la Estación B.
- La Estación B ve a la Estación A y a la Estación C.
- La Estación C ve a la Estación B.
- Estación A no ve a la Estación C.

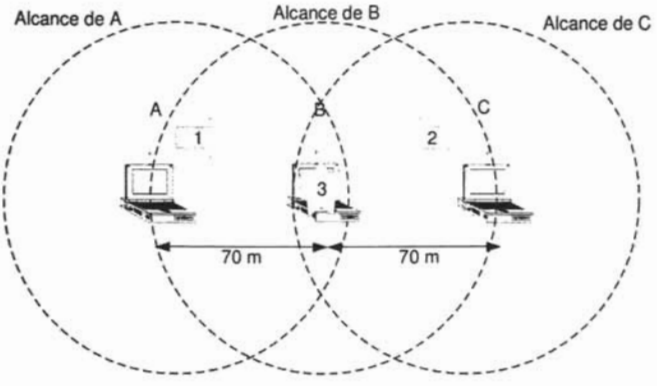


Figura 2-20. Problemas con las terminales ocultas.

1.A quiere transmitir un frame a B. Detecta que el medio esta libre y transmite.
2. Mientras A está transmitiendo C quiere enviar una trama B. Detecta el medio libre (pues no capta la emisión de A) y transmite.
3. Se produce una colisión en la intersección por lo que B no recibe ninguna de las dos tramas.

Solución:

Para resolver este problema, la MAC usa un esquema de reservación del canal, es decir que utiliza el esquema RTS/CTS, descrito anteriormente. Veamos nuevamente de manera general en que consiste:

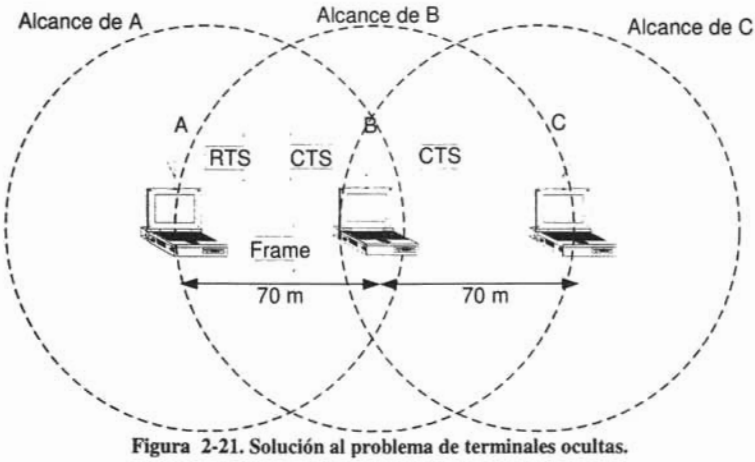


Figura 2-21. Solución al problema de terminales ocultas.

1. Antes de transmitir el frame, A envía un mensaje RTS.
2. B responde al RTS con un CTS.
3. C no capta el RTS, pero si el CTS. Sabe que no debe transmitir durante el tiempo equivalente a 500bytes.
4. A envía su frame de manera segura, evitando colisiones con otras estaciones.

A pesar de que el uso de RTS/CTS resuelve "el problema de la estación oculta" y evita las colisiones, también introduce una carga adicional en el protocolo y reduce el rendimiento. Por este motivo el protocolo RTS/CTS sólo se activa cuando los paquetes alcanzan un tamaño determinado.
En algunos sistemas WLAN este tamaño puede determinarlo el administrador (umbral de RTS/CTS).
Los porcentajes de errores de bits en las redes inalámbricas son bastante superiores a los de las redes cableadas tradicionales.
Puede que las tramas grandes se acerquen al número de bits en los casos en que la probabilidad de que se produzca un error sea del 100%. Esto implica que todos los bloques podrían fallar, incluida la retransmisión.
A fin de reducir esta posibilidad, el transmisor puede fragmentar las tramas grandes y, posteriormente, el nodo del receptor las puede volver a unir.
A pesar de que esto podría aumentar el tráfico, se reduce la probabilidad de error y, en caso de error, también se reduce la retransmisión.

En algunos sistemas WLAN, el tamaño del paquete más grande (umbral de fragmentación) puede ser ajustado por el administrador de red.
Para implantar redes o infraestructuras LAN inalámbricas es imprescindible realizar un trabajo de planificación y diseño previo. Hay que plantearse una serie de preguntas y tomar las decisiones en función de las respuestas dadas:

2.4 Seguridad.

En los últimos años, el uso de las redes inalámbricas se ha incrementado notablemente, dado su practicidad y flexibilidad que ofrecen; sin embargo se enfrenta con uno de sus mayores obstáculos: la seguridad. Este tipo de redes en el momento en que envían los datos hacia el aire, son susceptibles a ser interceptados, etc. por cualquier persona que sepa interceptar ondas de radiofrecuencia.

Existen varias formas de ataque como el llamado surveillance (espionaje), warchalking, y el wardriving. Las cuales en conjunto resultan una amenaza para la integridad de la red. De ahí las formas de intrusión son muy variadas que van desde el sniffing (escuchar) y eavesdropping (interceptar), donde un programa monitoriza los datos y determina hacia donde van, de donde vienen y qué son; hasta el Spoofing (burla) y hijacking (secuestro), que consiste en falsificar información, un identificador de usuario o contraseña permitidos por el sistema atacado, redefinir la dirección física o MAC de nuestra tarjeta inalámbrica por una válida y asociar una dirección IP válida del sistema atacado.

2.4.1 Mecanismos de seguridad.

El proceso de conexión del cliente a la red comienza cuando el cliente hace un barrido de todas las frecuencias usadas por 802.11b enviando su dirección MAC (Dirección física) y el ESSID (Extended Set Service ID), siendo este último el nombre de la red a la que deseamos acceder. Todos los APs en el rango responderán con su propio ESSID, canal y dirección MAC. Con esta información, el cliente puede limitar su señal y comenzar el proceso de autenticación.

2.4.1.1 Limitando la Propagación de RF.

Una combinación adecuada entre el transmisor/antena puede ser una herramienta efectiva que ayudará a limitar el acceso a la red inalámbrica al área pretendida de cobertura.
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 se diseña 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.

2.4.1.2 Autenticación abierta.

Es el protocolo por defecto para las redes 802.11. Todos los clientes que inician el proceso de autenticación ante un AP son registrados en la red. Ambos, envían en texto plano todos los *management frames,* incluso cuando el WEP (Wireless Encription Protocol) está activado.

Su vulnerabilidad: El propio sistema es una vulnerabilidad en sí mismo, absolutamente todos los clientes que piden ser autenticados en la red lo son.

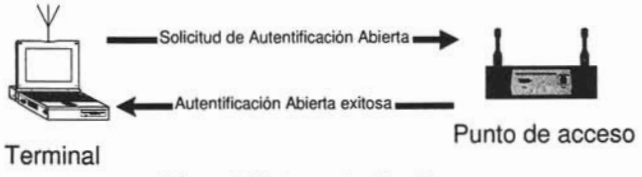


Figura 2-22. Autenticación abierta.

2.4.1.3 Autenticación por llave compartida.

Se basa en un desafío cliente – Punto de Acceso, en donde ambos comparten una llave secreta para iniciar dicha autenticación, siendo el cliente el dispositivo móvil que desea ser autentificado y el AP (también conocido como "responder") el que recibirá dicha petición. El cliente, envía una trama (management frame) indicando que el método a usar es de llave compartida. Al recibir el AP esta trama, enviará una nueva con los 128 Bytes de texto para ser usado como desafío. Estos Bytes se generan por el PRNG (Pseudo-Random Number Generator) usando dicha llave y un vector de inicialización (IV – Initialization Vector). Una vez recibida esta segunda trama por el cliente, se copia el contenido del desafío en el cuerpo de una nueva trama, que a su vez es encriptada con WEP usando la llave compartida mas un nuevo vector de inicialización (esta vez es elegido por el cliente). Una vez realizado todo esto se envía al responder.
El Access Point al recibir esta trama procede a:

a) Des-encriptarla.
b) Comprobar si el CRC es válido.
c) Verificar la validez del desafío.

Una vez realizado este proceso de manera satisfactoria, el AP autentifica al cliente. Una vez completado este paso, se realiza de manera inversa. De esta manera se produce una autenticación mutua y el cliente es registrado en la red.

Sus vulnerabilidades: Mediante un analizador de red, es fácil obtener los datos necesarios para recrear tramas válidas y *engañar* al Access Point al que se desea conectar. Capturando

el segundo mensaje, obtendríamos el *texto desafío* aleatorio en texto plano y con el tercer mensaje el mismo texto pero ya encriptado y el vector de inicialización.

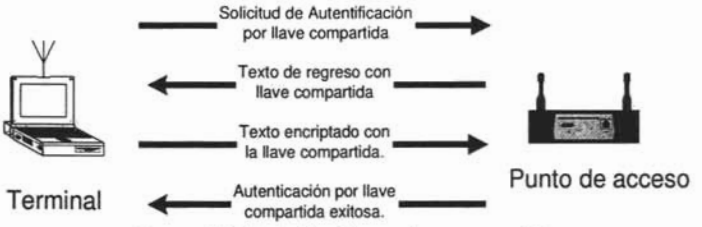


Figura 2-23.Autenticación por llave compartida.

2.4.2 WEP (Wired Equivalent Privacy).

WEP (*Wired Equivalent Privacy*, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11 [2]. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. A continuación las principales características de WEP:
WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.
El algoritmo de encriptación de WEP es el siguiente:

1) Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).
2) Se concatena la clave secreta a continuación del IV formado el *seed*.

3) El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del *seed,* de la misma longitud que los bits obtenidos en el punto 1.
4) Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5) Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el *seed* y con ello podrá generar el *keystream.* Realizando el XOR entre los datos recibidos y el *keystream* se obtendrá el mensaje sin cifrar (datos y CRC-32). A continuación se comprobara que el CRC-32 es correcto.

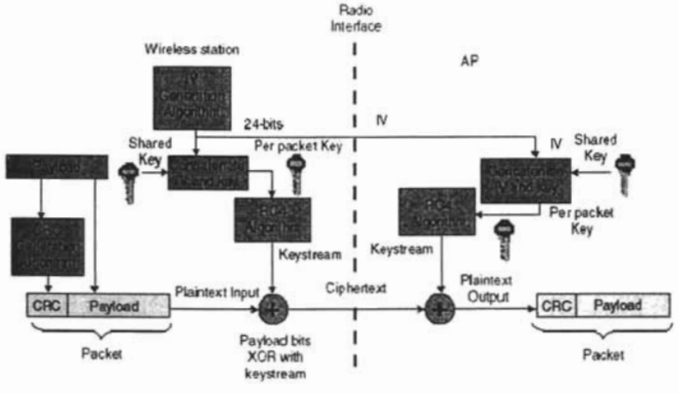


Figura 2-24. WEP.

2.4.3 WPA (WiFI Protected Access).

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.
WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.
WPA incluye las siguientes tecnologías:

- **IEEE 802.1X**. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de *puerto*, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service*) . Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).
- **EAP**. EAP, definido en la RFC 2284, es el *protocolo de autentificación extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (*EAP over LAN*) .
- **TKIP** (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama .
- **MIC** (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas.

WPA puede funcionar en dos modos:

- **Con servidor AAA, RADIUS normalmente**. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- **Con clave inicial compartida (PSK).** Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

2.4.4. WPA2 (IEEE 802.11i)

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mediados de 2004. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2.
Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.
WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto

es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.
Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.
Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

CAPÍTULO 3
HERRAMIENTAS DE CONFIGURACION Y MONITOREO DE UNA RED INALÁMBRICA WIFI.

3.1 Configuración de una red LAN inalámbrica.

Con el avance en la tecnología, los dispositivos Ethernet del tipo inalámbrico se han vuelto cada vez más comunes y accesibles al público. Su configuración, igualmente, se ha reducido a ser casi parecida a la configuración de dispositivos Ethernet, pero en este caso, podemos configurar diferentes recursos de red, como la ID de red, la frecuencia, etc.

Nota: Para implementar nuestra red inalámbrica, utilizamos un Adaptador de Red LAN Inalámbrica, marca Aironet Modelo 4800 tipo PCMCIA y un punto de acceso 3COM.

3.1.1 Preparativos para la instalación.

Se necesita la siguiente información para la correcta configuración de nuestra red:
El nombre de nuestro cliente inalámbrico
EL SSID (Service Set Indentifier) de la red.
La dirección IP, la mascara de red, a puerta de enlace así como el DNS. Y en su caso el usuario y el password de la cuenta de red.

Otro punto importante y que en muchas veces no se considera, es la colocación de nuestra computadora, ya que al utilizar un dispositivo de radio, este es susceptible a obstrucciones en la señal y a fuentes de interferencia, que pueden reducir nuestra capacidad de transmisión o recepción de datos. Por lo tanto es necesario colocar al adaptador en un área donde se eviten estos problemas.

Esta configuración es aplicable a la versión del kernel 2.4.20-8 y posteriores.

Controladores.

Los controladores son programas que permite la comunicación de la computadora con el dispositivo, y estos son cargados cada vez que el sistema se carga o cuando es activado el dispositivo, es por eso que es muy importante verificar si se tienen cargados estos programas en nuestro sistema. La ultimas versiones de Red Hat (a partir de la versión 7.2) ya tienen activado, un paquete de control y configuración para tarjetas PCMCIA y PC Cards que incluye un conjunto de módulos que se cargan en el kernel, controladores para

cada tarjeta específica, y un demonio (cardmgr) que controla las tarjetas, habilitando y cargando los controladores según se insertan o extraen las tarjetas.

etc/pcmcia/ vi config

y se despliega lo siguiente:

```
# PCMCIA Card Configuration Database
# config 1.154 2001/01/05 00:03:17 (David
Hinds)
# config.opts is now included at the very end
# Device driver definitions
device "airo_cs"
  class "network" module "airo_cs"
```

En caso de no encontrarse el modulo necesario, es necesario conseguir el archivo rpm necesario (kernel-pcmcia_cs) Ya habiendo verificado, la presencia del modulo necesario, lo que hacemos es insertar nuestra tarjeta.

Inserción de la tarjeta

El adaptador en un extremo cuenta con un conector PCMCIA de 68 pines, al ser insertada, el sistema detecta automáticamente el dispositivo inalámbrico; el encargado de monitorizar los estados de los sockets, es el demonio cardmgr, lo que hace es que cuando detecta la tarjeta carga los controladores necesarios y corre los scripts necesarios a nivel usuario en respuesta a las inserciones y extracciones de las tarjetas. Este graba sus acciones en el registro del sistema, y usa pitidos para señalar cambios en el estado de las tarjetas. Los tonos de los pitidos indican el éxito o fracaso de un paso de la configuración en particular. Por lo tanto, al insertar el adaptador nos podemos encontrar en los siguientes casos:

Dos pitidos agudos indican que la tarjeta fue identificada y configurada correctamente
Un pitido agudo seguido de un pitido grave indica que la tarjeta fue identificada, pero no pudo ser configurada por alguna razón.
Un pitido grave indica que la tarjeta no pudo ser identificada.

Para observar los mensajes de error al insertar una tarjeta, se puede inspeccionar con el editor vi el archivo de mensajes en el log:

vi /var/log/messages

El demonio cardmgr configura las tarjetas basadas en una base de datos de tipos de tarjetas conocidas almacenadas en /etc/pcmcia/config.

Otra herramienta, para comprobar el estado del socket o ver como esta configurado y en su caso alterar su configuración, es cardctl; sin embargo nosotros nada mas queremos ver la información de nuestra tarjeta, por lo tanto utilizamos la herramienta cardctl ident.

```
Socket 0:
product info: "Aironet", "PC4800"
manfid: 0x015f, 0x0007
function: 6 (network)
```

Ahora, para verificar que el adaptador ha sido cargado correctamente y que ha sido dada de alta como una interfase de red, utilizamos la herramienta ifconfig, en general se utiliza para ver o modificar el estado de una interfase de red. Las interfaces de red tipo Ethernet normalmente tiene nombres como eth0, eth1 y así sucesivamente, entonces, cuando se detecta una tarjeta Ethernet, le será asignado el primer nombre de interfase que este libre, en ese instante cardmgr ejecutara el script /etc/pcmcia/ network para configurar la interfase, la cual normalmente lee las configuraciones de red de /etc/pcmcia/network.opts. Los scripts *network*, y *network.opts* serán ejecutados sólo cuando su tarjeta Ethernet esté presente.

```
                    #ifconfig -a
eth0    Link encap:Ethernet  HWaddr 00:40:96:27:EF:A5
        inet    addr:192.168.27.161          Bcast:192.168.27.255
Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:8 dropped:0 overruns:0 carrier:8
        collisions:0 txqueuelen:100
        RX bytes:0 (0.0 b)  TX bytes:384 (384.0 b)
        Interrupt:3 Base address:0x100
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:41606 errors:0 dropped:0 overruns:0 frame:0
        TX packets:41606 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:2842011 (2.7 Mb)  TX bytes:2842011 (2.7 Mb)
```

Posteriormente configuramos el archivo network.opts. Cuando el archivo /etc/init.d/pcmcia corre, vemos que ejecuta el comando./network start ethx. Esto no quiere decir que el archivo etc/init.d/network se ejecute, si no que en vez de eso, se ejecuta etc/init.d/pcmcia/network comienza a correr. El problema radica que por default etc/pcmcia/network no hace nada. Es por eso que es necesario editarlo y configurarlo de acuerdo a nuestros parámetros de red.

```
[root@localhost root]# vi /etc/pcmcia/network.opts
```

```
# The address format is "scheme,socket,instance,hwaddr".
#
# Note: the "network address" here is NOT the same as the IP address.
# See the Networking HOWTO.  In short, the network address is the IP
# address masked by the netmask.
#
case "$ADDRESS" in
*,*,*,00:40:96:27:EC:80)
    INFO="Sample private network setup"
    # Transceiver selection, for some cards -- see 'man ifport'
    #IF_PORT="auto"
    # Use BOOTP (via /sbin/bootpc, or /sbin/pump)? (y/n)
    BOOTP="n"
    # Use DHCP (via /sbin/dhcpcd, /sbin/dhclient, or /sbin/pump)? (y/n)
    DHCP="n"
    # If you need to explicitly specify a hostname for DHCP requests
    #DHCP_HOSTNAME="192.168.0.1"
    # Host's IP address, netmask, network address, broadcast address
    [redacted]="192.168.0.100"
    NETMASK="255.255.255.0"
    NETWORK="192.168.0.0"
    BROADCAST="192.168.0.255"
    # Gateway address for static routing
    GATEWAY="192.168.0.1"
    ## Things to add to /etc/resolv.conf for this interface
    #DOMAIN=""
    #SEARCH=""
    DNS_1="192.168.27.201"
    DNS_2=""
    #DNS_3=""
```

Figura 3-1. Archivo network.opts.

Y se despliega la siguiente información. (el archivo ya ha sido editado con nuestros parámetros).
En este momento la configuración esta lista, para que el adaptador de red funcione correctamente. Por ultimo volvemos a arrancar la red, así como el manejador de la PCMCIA

3.2 Wireless Tools.

Su objetivo es brindar una interfase simple que permite al usuario manipular y establecer los parámetros para cualquier dispositivo de red inalámbrica (excluidos radios amateur, tecnología celular e infrarrojos) de una manera uniforme y estándar. Además de tener otras utilidades como la configuración, la generación de estadísticas, etc.
Estas se componen de tres partes: una interfaz de usuario, que se compone de una serie de herramientas para manipular dichas extensiones. La segunda consiste en la modificación del kernel para soportar y definir dichas extensiones y por ultimo, la tercera parte, es la interfaz de hardware, representado por cada controlador de dispositivos de red. Es importante recalcar que cada controlador debe soportar las wireless extensions para poder entablar el dialogo con el respectivo hardware.
Para todos aquellos controladores que son soportados, las Wireless Extensions permiten cambiar los parámetros en tiempo real, o pueden ser cargados a la hora se reiniciar el equipo o por la inserción de la tarjeta a través de scripts de inicialización (depende de la distribución de Linux).
Estas herramientas permiten diagnosticar varios problemas (configuración, encriptación, etc.) así como el monitorear el enlace, lo cual es fundamental para poder implementar una red con éxito.

3.2.1 Iwconfig

Iwconfig es una herramienta para interfaces de red inalámbricas que sirve para configurar ciertos parámetros de la capa de acceso al medio (MAC), además de mostrar datos estadísticos del medio. Estos parámetros y estadísticas dependen del equipo que se esté utilizando (tarjetas PCI, PCMCIA), ya que cada controlador solo proveerá algunos de esos datos y el rango puede variar entre equipo y equipo.

Parámetros utilizados en iwconfig

Para poder establecer una comunicación correcta y eficiente es necesario preestablecer ciertos parámetros de la capa de acceso, tales como la frecuencia a la que se desea transmitir y recibir, la tasa de transmisión, potencia de transmisión etc. La manera de establecer los parámetros es llamar a la herramienta, indicar la interfaz inalámbrica, el parámetro a configurar y las opciones del parámetro:

Ejemplo:
iwconfig [interfaz] [parámetro {opciones}]

Los parámetros que se pueden configurar con la herramienta iwconfig son los siguientes:

- essid .- Sirve para establecer la ESSID (Enhaced Service Set ID). La ESSID se utiliza para identificar células que son parte de la misma red virtual.
  Ejemplo:
  iwconfig eth1 essid any
  iwconfig eth1 essid "Mi Red"
- freq/channel .- Sirve para establecer la frecuencia de operación o el canal en el dispositivo.
- Sens.- Establece la mínima sensibilidad, esto es, el nivel mínimo de señal para el cual se puede lograr la recepción de un paquete. Las señales menores a dicho nivel no son recibidas.
- Mode.- Establece el modo de operación del dispositivo, que depende de la topología de la red. El modo puede ser Ad-hoc ó managed (infraestructura).

Otros parámetros que se pueden establecer son: MAC address de un punto de acceso, velocidad de transmisión de bits, tamaño de paquetes fragmentados, claves de encriptado, potencia de transmisión, tiempo para retransmitir paquetes, entre otras.

Desplegado

Para cada dispositivo que soporta las wireless extensions, iwconfig desplegará el nombre del protocolo de MAC utilizado , el ESSID (Nombre de la red), la NWID, la frecuencia (o canales), la sensibilidad, el modo de operación, la dirección del Punto de acceso, la tasa de transferencia, el RTS de encendido, fragmentación mínima, la clave de encriptado, y la configuración del manejo de potencia (dependiendo de la disponibilidad en el equipo).

Previamente se explicó el significado de dichos parámetros. Si la etiqueta del bit rate está seguida de un '=', significa que el valor del parámetro es fijo y forzado a dicho valor, si está seguido de ':', implica sólo el valor actual (dispositivo en modo automático normal).

Si existe el archivo /proc/net/wireless, iwconfig también desplegará su contenido (calidad del enlace, nivel de la señal, nivel del ruido, paquetes no desencriptados, paquetes perdidos por operaciones no válidas, etc.).

3.2.2 Iwspy

Esta herramienta del paquete wireless extensions sirve para listar todas las direcciones disponibles en una interfaz de red inalámbrica y así poder saber información acerca de la calidad del enlace de cada una. Esta información se encuentra en /proc/net/wireless: quality of the link, signal strength y noise level.
La información es actualizada cada vez que un nuevo paquete es recibido, de modo que cada dirección en la lista agrega información en el controlador.
Cabe mencionar que esta función sólo trabaja para nodos que son parte de las células inalámbricas actuales.

Es posible establecer hasta 8 direcciones.

- DNSNAME I IPADDR.- Establece una dirección IP, o en algunos casos un nombre de DNS (utilizando un asignador de nombres). Como el hardware funciona con direcciones de hardware, iwspy traduce esta dirección IP a través del ARP. En algunos casos, esta dirección tal vez no se encuentre en el caché del ARP e iwspy fallará. En esos casos, realice un ping a esta dirección/nombre y pruebe de nuevo.
- HWADDR.- Establece la dirección de hardware (MAC). La dirección MAC no es traducida ni checada como las IP y debe contener dos puntos (:) para que sea reconocida como dirección de hardware.
- +.- Agrega nuevas direcciones al final de la lista actual en lugar de remplazarlas. La lista de direcciones es única por cada dispositivo, así que se recomienda a los usuarios utilizar esta opción para evitar conflictos.
- Off.- Retira la lista actual de direcciones e inhabilita la función espía.

3.2.3 Iwpriv

Esta herramienta se puede considerar un complemento a la herramienta *iwconfig*. Iwpriv manipula y establece parámetros para cada controlador en especifico. Si ponemos a iwpriv sin ningún argumento este nos despliega la lista de todos los comandos disponibles para cada interfase, así como los parámetros que estos requieren.

Su sintaxis es la siguiente:

```
iwpriv [interfase]
iwpriv interfase comando [parámetros]
```

```
iwpriv interface --all
iwpriv interface roam {on,off}
iwpriv interface port {ad-hoc,managed,N}
```

Cuando llamamos a iwpriv interface roam, podemos habilitar o deshabilitar el roaming, si es soportado (setroam). A su vez con el parámetro port podemos leer y/o configurar el tipo de puerto (gport_type, sport_type, get_port or set_port).

```
iwpriv eth0 gethisto
```

3.2.4 Iwlist

Es utilizado para desplegar una lista de parámetros de la interfaz de red inalámbrica que no es desplegada por el iwconfig.

- Freq/channel .- Enlista las frecuencias disponibles en el dispositivo y el numero de canales definidos.
- Ap/accesspoint .- Enlista los puntos de acceso disponibles y de ser posible la calidad del link. (Función obsoleta)
- Scan .- Enlista los puntos de acceso y células tipo Ad-hoc dentro del rango, y de manera opcional puede desplegar información de estas (ESSID, Frecuencias, etc.). Depende del tipo de adaptador cliente.
- Rate/bit.- Enlista las velocidades de transmisión soportadas por el dispositivo.
- Key/enc .- Enlista el tamaño de llave de encriptación soportada y despliega todas las llaves de encriptación disponibles en el dispositivo.
- Power .- Enlista los distintos modos y atributos de la administración de energía del dispositivo.

Su sintaxis es:

```
iwlist interfase freq
iwlist interfase ap
iwlist interfase scan
iwlist interfase rate
iwlist interfase key
iwlist interfase power
iwlist interfase txpower
iwlist interfase retry
iwlist --help
iwlist --version
```

3.3 /PROC

/PROC es un sistema de pseudo archivos que da información y estadísticas del estado actual del sistema. Estas entradas actúan como archivos, por lo tanto podemos extraer los datos con cualquier visor de archivos como vi o cat. El stack de red en Linux usa una estructura (struct device – estructura del dispositivo) para llevar un seguimiento de cada dispositivo del sistema. La primera parte de esta estructura esta estandarizado, y contiene parámetros (p.e. direcciòn IP) y llamadas al sistema (callbacks). A esa estructura se le añadió otra llamada al sistema llamada get_wireless_stats para así obtener las estadísticas en el archivo /proc/net/wireless. Cuando esta entrada /proc es leída, esta llama al respectivo callback para todos los dispositivos presentes en el sistema y despliega la información. Entonces cuando es llamada el get_wireless_stats regresa una estructura llamada structiw_statistics que contiene todos los campos desplegados en la entrada /proc.

3.3.1 /proc/net/wireless

Este pseudo archivo esta diseñado para dar estadísticas especificas de cada interfaz inalámbrica en el sistema.
La información que se despliega es:

- Status .- Indica el estado presente. Es información que depende del dispositivo.
- Quality-link (Calidad del enlace) .-Muestra la calidad en general del enlace.
- Quality-level .- Muestra la potencia de la señal en el receptor. Sirve para rastrear y evitar áreas con sombra.
- Quality–noise (Calidad del ruido) .- Indica el nivel de silencio (es decir sin paquetes) en el receptor.
- Discarded- nwid .- No. de paquetes que han sido descartados , debido a una ID de red invalida. Un valor alto de estos paquetes podría indicar un problema en la configuración del ID de red o la existencia de una red adyacente.
- Discarded-crypt.- numero de paquetes que no se pueden des-encriptar.
- Discarded- misc .- Sin uso.

La diferencia entre Quality-link y Quality-level radica en que el primero indica que tan buena es la recepción (porcentaje de paquetes recibidos correctamente) y el segundo que tan fuerte es la señal.

3.3.2 /proc/driver/aironet/ethx.

Cada vez que se inserta la tarjeta Aironet, se crea una interfase en /proc la cual permite que uno se pueda comunicar con la tarjeta directamente, sin utilizar programas de interfaz gràfica. Por lo tanto si nos vamos al directorio /proc/driver/aironet/ethx, donde x es el numero de la interfaz Ethernet vemos los siguientes archivos:

ESTA TESIS NO SALE
DE LA BIBLIOTECA

APList BSSList Config SSID Stats StatsDelta Status WepKey

APList
Contiene la lista de las direcciones MAC de los punto de acceso preferidos, es decir a los cuales queremos ser conectados.

Config
Podemos establecer gran numero de parámetros como el Modo, Activar el radio, establecer el nombre del nodo, el tipo de modo de ahorro de energía, el canal, la potencia de transmisión, etc.

Tabla 3-1. Parámetros archivo Config.

Parámetro	Valores	Descripción
Mode		Tipo de transmisión: Unicast, Multicast, Broadcast
Radio	ON –OFF	Permite prender o apagar el radio.
Nodename	Opcional	El nombre que utiliza el cliente para asociarse al punto de acceso
Powermode	CAM PSM	Establece el método que el cliente utilizara para ahorrar energía.
Data rates	2,5.5,11,22 Mbps	Velocidades de transmisión y recepción del cliente
Channel		
XmitPower	1,5,15,20,30,50 o 100mW	Máxima potencia a la cual el cliente puede transmitir. Depende del tipo de radio instalado así como las regulaciones de cada país.
LongRetryLimit	0-255	Especifica el No. de veces que un paquete no fragmentado será reenviado después que ha sido descartado por un error de transmisión.
ShortRetryLimit	0-255	Especifica el No. de veces que un paquete fragmentado será reenviado para ganar acceso, después de haber sido descartado.
RTSThreshold	0-2312	Especifica el tamaño mínimo del frame en bytes para comenzar a transmitir RTS/CTS
TXMSDULifetime	0-xFFFF	Especifica el tiempo máximo para intentar transmitir un paquete.
RXMSDULifetime	0-xFFFF	Tiempo máximo para la recepción de un paquete fragmentado
TXDiversity y RXDiversity	Left-right-both	Especifica el modo al cual la antena transmitirá y recibirá paquetes.
FragThreshold	256-312 (Impar)	Especifica el tamaño de los fragmentos en bytes
WEP	Open o shared key	Especifica el tipo de autentificación WEP
Modulation	BPSK – QPSK-CCK	Muestra el tipo de modulación utilizado dependiendo de la velocidad de transmisión.
Preamble	short-long	Establece la longitud del bit de sincronización

SSID

Enlista todas las SSID que serán utilizadas. Si la lista esta vacía, se podrá asociar a cualquier punto de acceso que detecte.

Status

Las principales características que despliega son:

Tabla 3-2. Parámetros del archivo Status.

Parámetro	Descripción
Device, Manufacturer, Firmware Version, Driver Version	Descripción, fabricante, versión del firmware y driver del adaptador cliente respectivamente
Bit rate	La velocidad a la cual se transmiten los datos
Signal Strenght	Valor entre 0-100%. Despliega la fuerza de la señal con la que son recibidos los paquetes
Signal Quality	Valor entre 0-8. Cuantifica la calidad de la señal
SSID	Muestra el SSID al que esta asociado el cliente
AP	Nombre del punto de acceso al que esta asociado el cliente

Stats/StatsDelta

Nos permite ver todas las estadísticas, que muestran como los datos son transmitidos y recibidos por el adaptador cliente. El archivo Stats da las estadísticas desde que la tarjeta fue encendida, por su parte StatsDelta da las estadísticas desde el momento en que se le dio el ultimo reset a la tarjeta. Este archivo despliega alrededor de 68 variables, de las cuales las mas importantes son:

Tabla 3-3. Parámetros del archivo Stats.

Parámetro	Descripción
RxOverrun	Despliega el No. de paquetes recibidos cuando este no tiene la capacidad de leer mensajes en el buffer. Sucede cuando el host no puede recibir los paquetes lo suficientemente rápido.
RxMacCrcErr	No. de paquetes que tienen encabezados PLCP validos pero tienen un error en le CRC
RxBeacon	No. de Beacons que fueron recibidos exitosamente.
TxBeacon	No. de Beacon que fueron transmitidos exitosamente (modo ad-hoc).
HostRxBytes	No. de bytes de datos recibidos exitosamente.
DupFram	No. de frames duplicados recibidos exitosamente
DefersNo.	No. de paquetes que se pueden transmitir inmediatamente sin ser retardados por un retardo en el protocolo o por detección de energía.
DefersProt	No. de paquetes que fueron retrasados debido al mal funcionamiento

	del protocolo.
DefersEngy	No. de paquetes que fueron retrasados por la detección de otra señal de RF. (interferencia)
RetryLong	No. de paquetes que fueron retransmitidos.
RetryShort	No. de RTS que fueron retransmitidos
MaxRetries	No. de paquetes que fallaron de ser transmitidos de manera exitosa después de haber agotado el número máximo de intentos.
NoAck	No. de paquetes transmitidos que no se recibieron sus correspondientes ACK
NoCts	No. de paquetes a los cuales no fue recibido su CTS como respuesta a un RTS.
RxAck	No. de paquetes transmitidos con su correspondiente ACK recibido exitosamente.
RxCts	No. de paquetes CTS recibidos en repuesta a un RTS.
TxAck	No.. De ACK que fueron transmitidos en respuesta una buena recepción de paquetes.
TxRts	No.. De RTS transmitidos exitosamente
TxCts	No. de CTS que fueron transmitidos en respuesta a un RTS recibido.
TxSinColl	No. de paquetes que fueron retransmitidos una sola vez debido a una colisión.
TxMulColl	No. de paquetes que fueron retransmitidos mas de una vez debido a múltiples colisiones.
SsidMismatch	No. de veces que un paquete fue recibido que no tenia el campo SSID correspondiente al suyo.
ApMismatch	No. de veces que un paquete fue recibido de un punto de acceso que no esta especificado pero tiene el mismo SSID.
RatesMismatch	No. de veces que un paquete fue recibido donde el campo en donde se indican las velocidades de transmisión soportadas no coinciden con las del radio.
AuthReject	No. de veces que el adaptador cliente trato de autentificarse a un punto de acceso y fue rechazado.
AuthTimeOut	No. de veces que un adaptador cliente trato de autentificarse a un punto de acceso pero fue imposible debido a que este no respondía lo suficientemente rápido
AssocReject	No. de veces que el adaptador cliente trato de asociarse a un punto de acceso pero fue rechazado.
AssocTimeOut	No. de veces que el adaptador cliente trato de asociarse a un punto de acceso pero fue imposible ya que ese no respondía rápidamente.
ElapsedUptime	Tiempo que el adaptador cliente ha estado prendido (seg.)
ElapsedSec	Tiempo transcurrido desde el ultimo reset al adaptador.

3.4 Otras herramientas.

3.4.1 Wlanctl-ng

Esta herramienta se incluye dentro del paquete de *linux-wlan* el cual ayuda al usuario para tener un manejo más avanzado de su controlador.

Una vez instalado, hay dos formas de configurar el wlanctl-ng: una es modificando el archivo wlan.conf que se encuentra en el directorio /etc/wlan. Ahí existen líneas de programa que se deben editar según se indica en el mismo archivo. La segunda forma es por medio de comandos en el shell. La forma de sintaxis de estos comandos es la siguiente:

wlanctl-ng interface lversión|comandos|mibs cmd cmdarg [cmdarg..]

A continuación se muestran una serie de ejemplos de los comandos más utilizados:

Comando de autodetección: Sirve para asociar al dispositivo con un AP deseado estableciendo como parámetros el SSID y el modo de autenticación:
$ wlanctl-ng wlan0 lnxreq_autojoin ssid=<SSID> authtype=Tipo
donde
wlan0: Interfaz de red inalámbrica.
Tipo: opensystem, sharedkey.
SSID: SSID de la red inalámbrica

- Establecimiento del canal: Establece uno de 14 posibles canales:
  $ wlanctl-ng wlan0 dot11req_mibset mibattribute= p2CnfOwnChannel=Valor
  (El valor debe estar en un rango de 1~14).
- Establecimiento del tiempo de RTS:
  $ wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11RTSThreshold=Valor
  (El valor debe estar en un rango de 0~2347)
- Establecimiento del tamaño de fragmento de paquetes:
  $ wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11FragmentThreshold =Valor
  (El valor debe estar en un rango de 256~2346)
- Establecimiento de la SSID:
  $ wlanctl-ng wlan0 dot11req_mibset mibattribute= p2CnfOwnSSID=<SSID>
- Establecimiento de la clave WEP:
  $ wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11WEPDefaultKeyID=<Indice de clave>
  $ wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11ExcludeUnencrypted=true
  $ wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11PrivacyInvoked=true
  $ wlanctl-ng wlan0 dot11req_mibset mibattribute=dot11WEPDefaultKey<Indice de clave>=xx:xx:xx..

*El indice de clave debe estar en un rango de 0 a 3
** xx:xx:xx... es la clave WEP en formato hexadecimal. El número de valores depende del formato WEP (5 para WEP64, 13 para WEP128, etc.).

Los cuatro comandos son necesarios para establecer una clave WEP. Después de establecer la información necesaria, se puede asociar a un AP con el siguiente comando:

```
$ wlanctl-ng wlan0 lnxreq_autojoin ssid=<SSID> authtype=sharedkey
```

Reconocimiento del Sitio: Con este comando se establecen parámetros para que se detecte alguna red inalámbrica:

```
$ wlanctl-ng wlan0 dot11req_scan bsstype=any bssid=00:00:00:00:00:00 \
scantype=both probedelay=0 channellist="01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:00"\
minchanneltime=200 maxchanneltime=1000 ssid=""
```

Esta herramienta es algo compleja por su modo de utilización y sólo se recomienda a usuarios avanzados.

3.4.2 KWi-Fi Manager

Esta es una herramienta gráfica creada para KDE que se basa en las *wireless tools* para desplegar cierta información de la red inalámbrica, además de poder configurar ciertos parámetros. La información que despliega en un primer plano es la velocidad de la conexión, nombre de la ESSID, dirección MAC del punto de acceso asociado, la ip del dispositivo inalámbrico, el número del canal en el que se está trabajando, el encriptado y la fuerza de la señal.

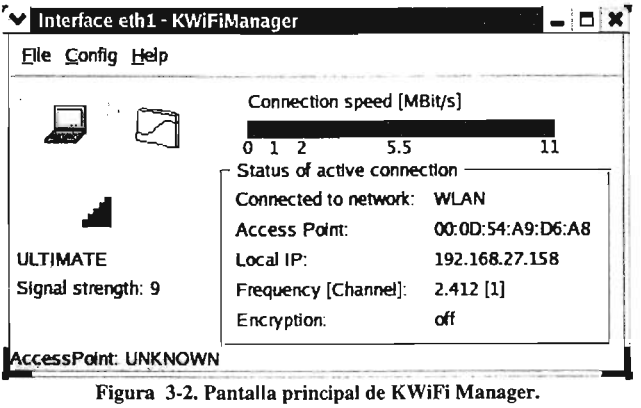


Figura 3-2. Pantalla principal de KWiFi Manager.

Además de ello despliega una gráfica algo ambigua sobre la relación señal a ruido de los datos recibidos.

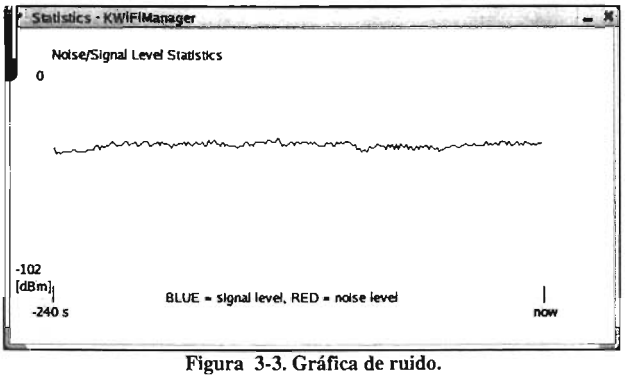


Figura 3-3. Gráfica de ruido.

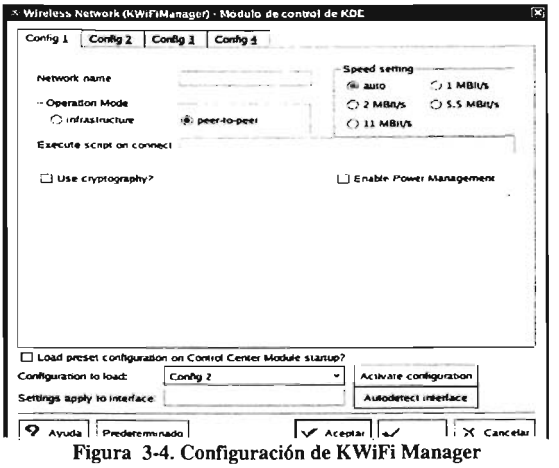


Figura 3-4. Configuración de KWiFi Manager

También es posible configurar algunas características por medio de la ficha *Config* en el menú principal. En dicho menú es posible tener hasta 4 tipos de perfiles de configuración diferentes donde se pueden establecer la SSID (Network name), el modo de operación, velocidad de transferencia, habilitar el manejo de potencia y ciertos controles para intentar detectar la interfaz automáticamente.
En general, Kwi-Fi Manager es una herramienta simple que sirve para darse una idea de la intensidad de la señal y conocer datos básicos. Si se desean saber más parámetros es recomendable utilizar otra herramienta

3.4.3 Cisco ACU Manager.

Esta herramienta gráfica sólo está disponible para interfaces de tarjetas pcmcia modelos *Aironet*. Esta herramienta permite configurar una red inalámbrica estableciendo parámetros como el SSID, dirección del AP, configurar el modo de utilización de energía, modo de

configuración, seguridad (WEP), velocidad de transmisión, tamaños de paquetes fragmentados, canal de frecuencia a utilizar, etc.

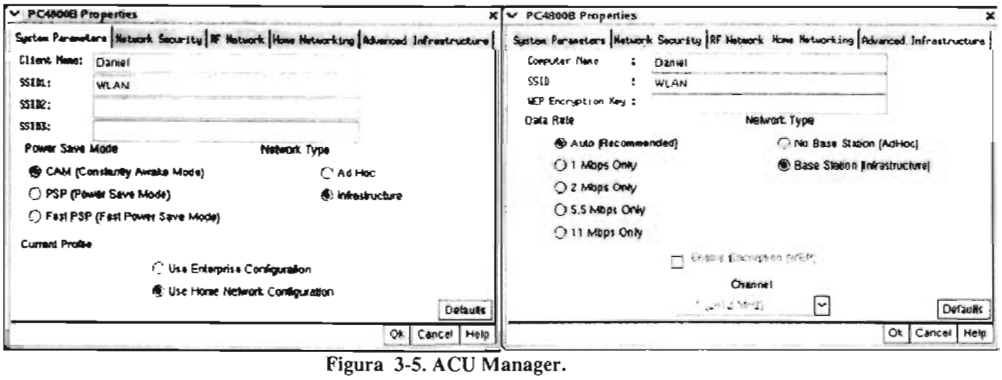


Figura 3-5. ACU Manager.

Además de configurar los parámetros, es posible utilizar esta herramienta para observar ciertos parámetros como el modo de autenticación, dirección MAC del dispositivo inalámbrico utilizado, potencia, frecuencia de trabajo, SSID y un indicador del nivel de señal.

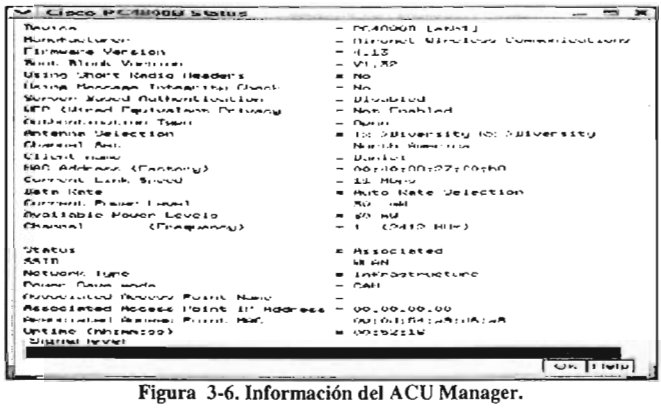


Figura 3-6. Información del ACU Manager.

Además de ello, se presentan ciertos datos estadísticos en tiempo real como paquetes RTS, CTS, paquetes recibidos correctamente, etc.

Esta herramienta es de las más completas y amigables, sin embargo el inconveniente es que no funciona más que para un tipo específico de tarjetas (una marca comercial) y por lo tanto se limita su utilización.

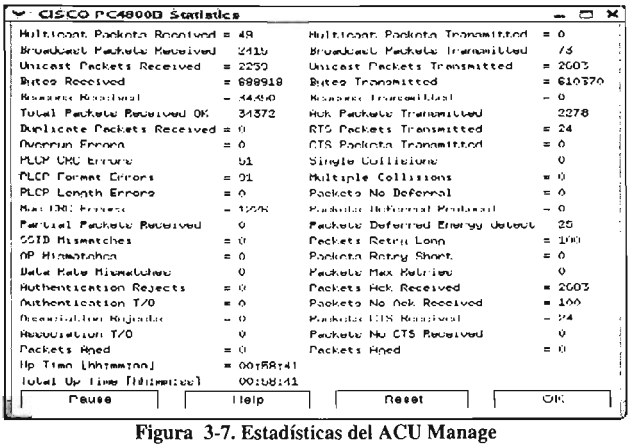


Figura 3-7. Estadísticas del ACU Manage

CAPÍTULO 4
HERRAMIENTA DE ADMINISTRACIÓN, MONITOREO Y CONTROL: "MONITOR WIFI".

4.1. Introducción.

A pesar de la existencia y rápido crecimiento en el numero de herramientas para la administración, monitoreo y control de redes inalámbricas 802.11 en el sistema operativo Linux; existe una clara deficiencia en herramientas en idioma español y que además permitan tener un panorama amplio del desempeño de la red: estadísticas en tiempo real y automatizadas, escaneo de puntos de acceso disponibles, información del host, etc. Para ello, es necesario el uso de dos o más herramientas en trabajo conjunto, añadiendo complejidad de uso y saturación de recursos del sistema, para brindar toda la información necesaria para el monitoreo de la red.

Monitor WiFI, surge ante esta necesidad de crear una herramienta de administración y monitoreo que cubra todas aquellas deficiencias. Monitor WiFI, permite al administrador de red o usuario en general poseer una herramienta de computo simple y adecuada para la administración y monitoreo de la red, sin dejar a un lado otras características no menos importantes como su facilidad de uso y configuración, su libre distribución y licencia, así como estar en idioma español.

Por lo tanto, Monitor WiFI, le permite al usuario monitorear y administrar su red, para así poder tomar decisiones de configuración de esta, y poder ser optimizada y obtener un mayor potencial en la transmisión de datos.

Monitor WiFI, fue desarrollado bajo la plataforma de Linux, por varias razones: primero, hasta su versión Red Hat 9, el sistema era tipo GPL, por lo tanto su distribución es gratuita y no es necesario el pago de licencias; en segunda, Linux permite el acceso a información mas detallada de las características, funcionamiento y desempeño de los dispositivos, en este caso la tarjeta inalámbrica, teniendo la posibilidad de extraerla y manipularla a través de archivos de texto, facilitando el diseño de herramientas y aplicaciones.

Monitor WiFI esta diseñado en dos partes o capas; la primera, que es transparente al usuario, consiste en la ejecución de comandos propios del sistema operativo Linux, que permiten seleccionar y filtrar la información, para después ser administrada en diferentes cajas de texto (llamada *TextBox*). La segunda parte, consiste en una interfaz gráfica de fácil uso, minimizando y optimizando al máximo, las configuraciones externas y las consultas respectivamente, para evitar sobrecarga al sistema, permitiendo al usuario visualizar de manera automática y organizada la información. Además, Monitor WiFI posee algunas

implementaciones y sugerencias para el control del sistema y permitir una correcta ejecución de este.

4.2 Objetivo.

Monitor WiFI tiene como objetivo ser una herramienta de simple y de fácil uso, gratuito y en idioma español, que permite el manejo y visualización de información necesaria para la administración, monitoreo y control de una red IEEE 802.b para tarjetas modelo Aironet 4800. Para el caso de otras tarjetas solo se tendrían algunas de las funciones de esta herramienta.

4.3 Ventajas.

- Facilitar el acceso en tiempo real de información del sistema, sin necesidad del uso de terminales o la memorización de comandos.
- Eliminar la dependencia de herramientas de marca propia (por ejemplo ACU Cisco), para la visualización de estadísticas del desempeño de la tarjeta de red inalámbrica.
- Contar con información rápida y oportuna del host, puntos de acceso, modo de transmisión, etc.

4.4 Alcances.

Automatización de la recopilación y filtrado de información específica, para su correcta administración y visualización en tiempo real, para el análisis del desempeño de la transmisión de una tarjeta de red inalámbrica.

4.5 Requisitos Mínimos de Software y Hardware para la Correcta ejecución de Monitor WiFI.

El equipo en el cual se quiera instalar la Herramienta debe de tener las siguientes características:

- Procesador Pentium III o superior.
- Mínimo 50 Mb. libres en disco duro.
- Monitor VGA o SUPER VGA.
- Tarjeta inalámbrica Marca Aironet Modelo 4800.
- Conexión de red vía Punto de acceso.
- Sistema Operativo Red Hat V. 9 (Kernel 2.4. 20-8).
- Wireless Tools Versión 25.
- Controlador para la tarjeta Marca Aironet Modelo 4800.

De manera adicional, el usuario de esta herramienta, necesita tener una cuenta de administrador, es decir, tipo "root".

4.6 Descripción de configuraciones especiales, Software de Desarrollo Utilizado y Requerimientos Técnicos.

Para posterior desarrollo y actualización de esta aplicación, es necesario:

- Glade V.2 o posteriores.
- Cualquier editor de textos (emacs, gedit, vi, etc.).
- Acceso a la terminal Bash.
- Conocimiento de lenguaje de programación C.
- Conocimientos de lenguajes orientados a eventos.

Es necesario recalcar, que para el correcto funcionamiento de este programa, la tarjeta inalámbrica debe tener asociado el nombre y el numero de interfaz ***eth0***. *(Véase Apéndice 1).*

4.7 GLADE V. 2

Monitor WiFI, forma parte de las herramientas GST (Gnome System Tools), ya que como hemos mencionado, permiten gestionar el sistema de manera eficaz desde una interfaz gráfica. El diseño de este tipo de herramientas, del tipo GST, se realiza de tal manera que el trabajo a bajo nivel con el sistema no complique el desarrollo de las interfaces gráficas.

En nuestro caso se decidió utilizar ***Glade,*** por dos razones: la primera, es GPL y la segunda, es que hace uso de las librerías GTK+, lo cual permite desarrollar de manera flexible y rápida interfaces gráficas para Linux y por ultimo, es que Glade al permitir la creación de la interfaz gráfica de manera visual, y solo dedicarte al desarrollo del código inherente de la herramienta.

El funcionamiento muy general de Glade es el siguiente: esta herramienta es separada en dos partes, un backend que puede ser desarrollado en Perl, Python o C (en el caso de Monitor WiFI se uso el lenguaje C) y que trabaja e interactúa con el sistema y que entrega un fichero XML a la interfaz gráfica. Las modificaciones desde la interfaz gráfica se comunican de nuevo al backend utilizando XML. El backend analiza los cambios y se encarga de aplicarlos al sistema. La interfaz gráfica utiliza este XML para mostrar la información necesaria al usuario desde la interfaz gráfica creada con GLADE y C.

Rápidamente veremos el entorno de desarrollo de Glade; Glade cuenta con 3 ventanas principales:

Tabla 4-1. Ventanas del programa Glade

Ventana principal	*Paleta de Widgets.*	*Editor de Propiedades*
Muestra los widgets que se van añadiendo a la aplicación.	Nos permite seleccionar que elementos se agregaran a la aplicación.	Nos permite editar las características al widget, así como la asignación de eventos.

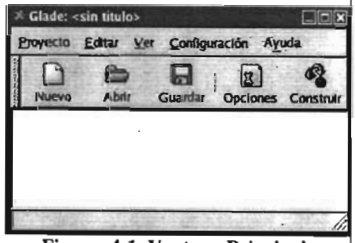


Figura 4-1. Ventana Principal

Figura 4-2. Paleta de widgets

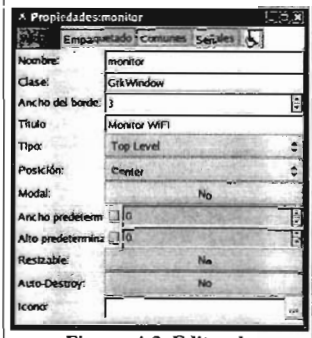


Figura 4-3. Editor de propiedades

Cuando se termina de diseñar la aplicación, el proyecto se debe guardar y generar su código. Glade genera muchos archivos, pero los que más nos interesa y podemos modificar, son callbacks.c y main.c.

Es importante recalcar la importancia del archivo callbacks.c, ya que ahí es donde están todos los prototipos de las funciones, correspondientes a los eventos de cada widget.

Por ejemplo:
Si generamos un botón, llamado *salir*, y queremos que cuando se apriete realiza alguna función, se genera el siguiente prototipo:

```
on_boton_salir_clicked()
{
Líneas de código;
}
```

4.8 Comandos del sistema.

Como mencionamos, la herramienta Monitor wifi, se compone de dos partes, una interfaz gráfica, que fue diseñada con GLADE, y la otra parte que consiste en la selección y filtrado de la información.

Monitor WiFI, utiliza las siguientes herramientas de Unix-Linux para obtener información de las características, configuración de red y transmisión, estatus, asociación a punto de acceso, escaneo de puntos de acceso disponibles y estadísticas de la tarjeta de red inalámbrica Aironet 4800:

1. *Wireless Tools Versión*
   Se usaron los comandos
   - Iwconfig.- Para configuración, información del Punto de acceso y estatus. (Véase Capitulo 3).
   - Iwlist.- Para el escaneo de punto de acceso disponibles. (Véase Capitulo 3).
2. *Ipconfig*.- Configuración y estadísticas. (Véase Capitulo 3).
3. *Cardctl ident*.- Es un comando que nos permite identificar características de hardware de la tarjeta inalámbrica.
4. *Hostname y whoami* - Para los nombres del usuario y máquina.
5. *Archivo Proc*.- Generado por el controlador airo.cs. Utilizado para obtener las estadísticas secundarias. (Véase Capitulo 3).

Para el filtrado de la información:

1. *Grep* . - Busca en ficheros o en la entrada estándar líneas que contengan alguna coincidencia con la expresión regular que se le señale. Por defecto, solo se listarán las líneas coincidentes.
2. *Awk*.- Es un lenguaje de programación que permite modificar archivos, buscar palabras, etc. Esta herramienta dispone de características internas para descomponer líneas en campos y compara estos campos con patrones que se especifiquen. Por lo tanto su función, es buscar líneas en ficheros que coincidan con ciertos patrones, y cuando en una línea se encuentra dicho patrón, AWK realiza las acciones especificadas para dicho patrón sobre dicha línea. AWK sigue realizando el procesamiento de las líneas de entrada de esta forma hasta que se llega al final del fichero.
3. *Cut* .- Es una herramienta que selecciona porciones de cada línea de un archivo o de la entrada estándar por default, y las despliega estas en la salida estándar.

En conjunto estas herramientas permitieron la selección de la información, para poder administrarla y ser desplegada en la aplicación gráfica.

4.9 Diagrama de los procesos del sistema.

Una vez que conocemos la manera en que se realizo la interfaz grafica, veamos un panorama general del funcionamiento de la herramienta Monitor wifi.

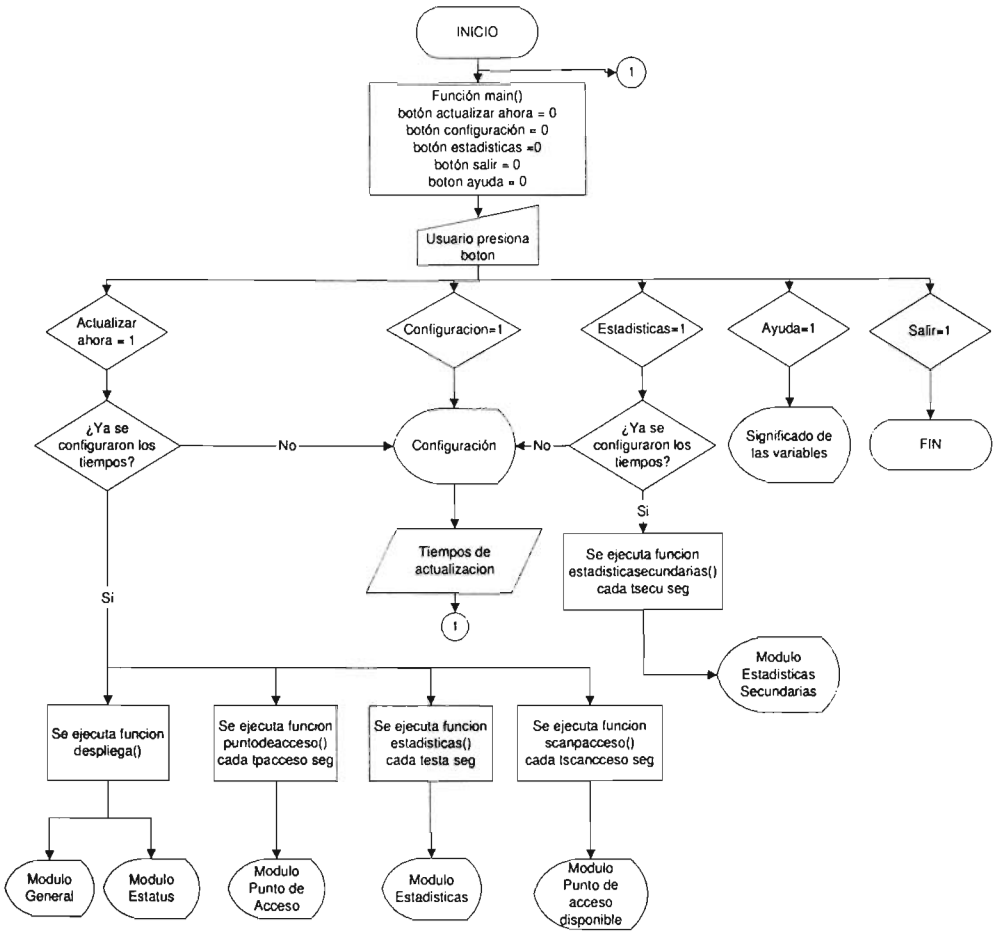


Figura 4-4. Diagrama de Flujo de Monitor WiFI.

4.10 Administración y despliegue de la información.

A continuación mostraremos una platilla general de la programación, para la generación de ventanas, botones y funciones utilizadas para el despliegue de información, utilizada en Monitor WiFI.

- ***Para la creación de ventanas.***

```
GtkWidget *ventana;
ventana = create_ventana();
gtk_widget_show(ventana);
```

Se declara el tipo de objeto, en este caso un widget, después se crea, y por ultimo se muestra el widget..

- ***Para los eventos relacionados a los botones.***

```
void
on_boton_clicked  (GtkButton     *button, gpointer       user_data)
{
// Código a ejecutar
}
```

Este es el prototipo de la función, que indica que debe de hacer el botón en cuanto sea accionado, en "Codigo a ejecutar", puedes ser cualquier subprograma, en lenguaje C o Gtk.

- ***Para la creación y despliegue de información (Cajas de texto).***

```
//HOST
//Se borra el contenido de  la caja de texto
target = lookup_widget (GTK_WIDGET(button), "thost");
borrar = gtk_text_view_get_buffer( GTK_TEXT_VIEW(target));
gtk_text_buffer_set_text (borrar, " ",-1);
 system("whoamilawk '{printf $1}'>/home/monitor/host.txt");
fichero=fopen("/home/monitor/host.txt","r");
  if (fichero == NULL)
    { perror ("NO se puede abrir HOST");
    }
//Leemos
fgets(aux,20,fichero);
target = lookup_widget (GTK_WIDGET(button), "thost");
buffer= gtk_text_view_get_buffer( GTK_TEXT_VIEW(target));
gtk_text_buffer_insert_at_cursor( buffer, aux, strlen(aux));
fclose(fichero);
printf("exec\n");
//TERMINA HOST
```

Para este caso, el orden del proceso es:

- Borrar cualquier contenido de la caja de texto.
- Después seleccionar y filtrar la información.
- Se coloca la información en la caja de texto.

Veremos algunos de los comandos utilizados:

- lookup_widget(): nos devuelve un apuntador hacia el widget existente.
- gtk_text_view_get_buffer: Como la caja de texto solo es un visor (GtkTextView), debemos de obtener como un tipo buffer (GtkTextBuffer), para así poder manipular el texto.
- gtk_text_buffer_set_text: Pone el buffer del argumento dentro de la caja de texto.
- System: Hace llamadas al sistema.
- gtk_text_buffer_insert_at_cursor: utiliza la posición actual del cursor, como el punto de inserción.

- ***Para salir de la herramienta Monitor WiFI.***

//Salir
gtk_main_quit();
Simplemente se sale del ciclo principal, y termina del programa.

4.11 Módulos de la Herramienta Monitor WiFI

La herramienta fue dividida en 5 secciones diferentes, en la cual cada una de ellas muestra información relacionada al modulo que le corresponde. Esto se hizo con la finalidad de generar un entorno más amigable y administrado de la información recopilada.

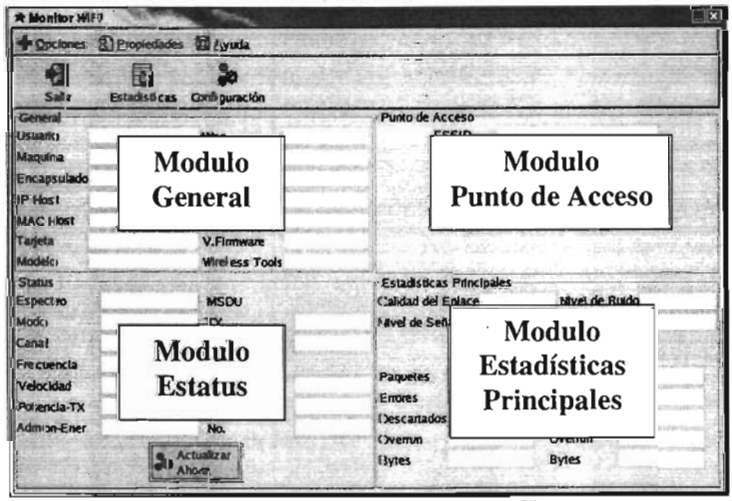


Figura 4-5. Módulos de Monitor WiFI.

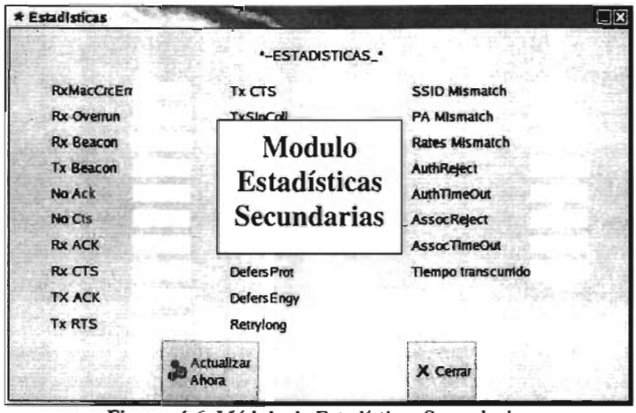


Figura 4-6. Módulo de Estadísticas Secundarias

4.11.1 Modulo General.

Este módulo se activa al presionar el botón "Actualizar ahora" muestra información general del entorno: Usuario, tarjeta, y condiciones de transmisión.

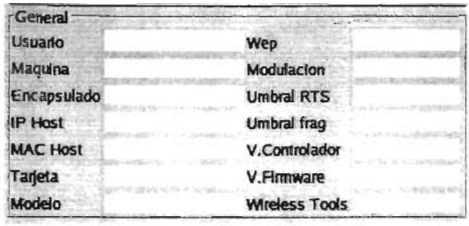


Figura 4-7. Modulo General.

4.11.2 Módulo Estatus.

Se activa al presionar el botón "Actualizar ahora" y muestra el estatus y características de transmisión en capa física de los datos de la tarjeta inalámbrica.

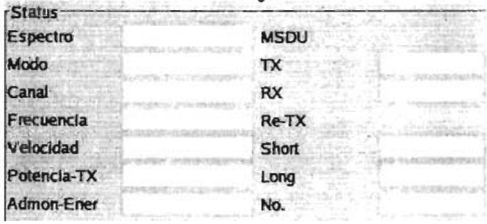


Figura 4-8. Módulo Estatus.

4.11.3 Modulo Punto de Acceso.

Se activa al presionar el botón "Actualizar ahora" y muestra toda aquella información relacionada al punto de acceso al cual esta asociado la tarjeta inalámbrica. Además, tiene la capacidad de escanear todos aquellos puntos de acceso disponibles dentro del área de cobertura de la tarjeta inalámbrica.

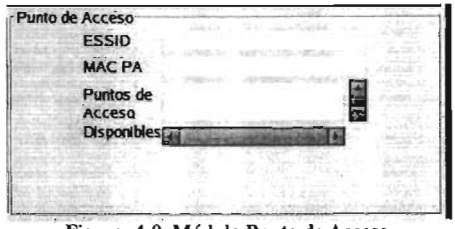


Figura 4-9. Módulo Punto de Acceso.

4.11.4 Modulo Estadísticas Principales.

Se activa al presionar el botón "Actualizar ahora" y muestra las estadísticas de transmisión y recepción de los datos. Así como también, las características del enlace de RF, entre la tarjeta inalámbrica y el punto de acceso al que esta asociado.

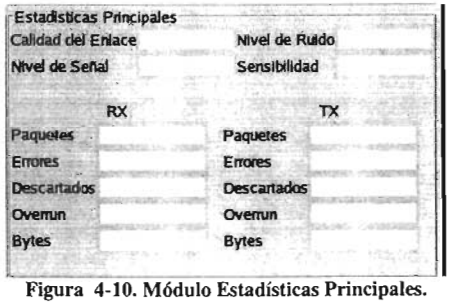


Figura 4-10. Módulo Estadísticas Principales.

4.11.5 Modulo Estadísticas Secundarias.

Se ejecuta al desplegar el botón "Estadísticas" dentro del menú de herramientas. Muestra todas aquellas estadísticas generadas por el controlador airo.cs. Estas estadísticas son un poco mas detalladas que las anteriores, ya que permiten ver si existen errores de protocolo, velocidad, etc.

Figura 4-11. Módulo Estadísticas Secundarias.

Nota: Para mayor referencia de cada una de estas variables, acuda a la Ayuda y a Significado de las variables; esto dentro de la herramienta Monitor WiFI.

4.12 Configuración.

Para poder comenzar a utilizar la herramienta Monitor WiFI, es necesario configurar los tiempos de actualización de los Módulos Estadísticas, Punto de Acceso y Estadísticas Secundarias. Esto quiere decir, que le vamos a decir al software cada cuando va a actualizar la información que se despliega en pantalla. La elección es libre, y dependiendo de las necesidades del usuario, así como las características del hardware del sistema (procesador, memoria RAM) es como debe configurarlos; sin embargo existen algunas restricciones, ya que tiempos demasiado bajos, hacen que la herramienta se sature y no se ejecute correctamente.

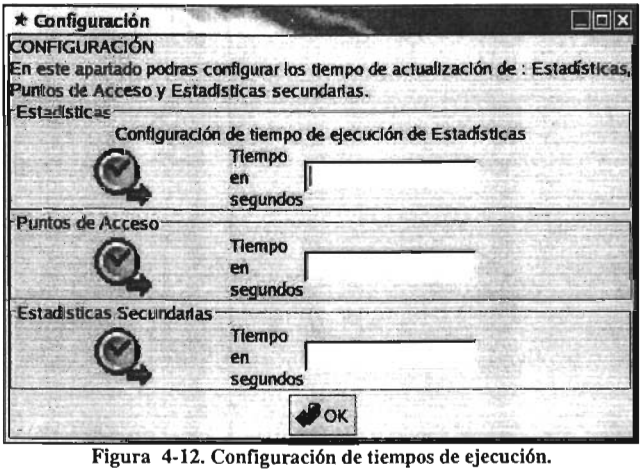


Figura 4-12. Configuración de tiempos de ejecución.

En caso de olvidar configurar los tiempos, la herramienta le mostrara una advertencia de la necesidad de configurar estos tiempos.

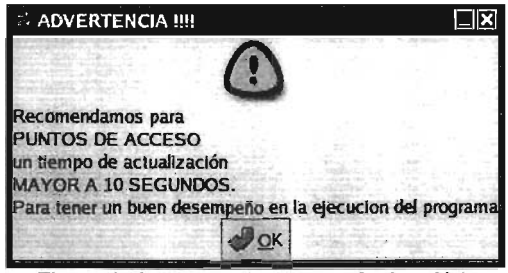


Figura 4-13. Advertencia (Tiempos de ejecución).

Nota: Los tiempos de ejecución en muchas ocasiones depende de varios factores como el tipo y velocidad del procesador, la cantidad de memoria RAM etc. De la maquina en que se este ejecutando el programa.

4.13 Ayuda.

Se accede a través del menú ayuda y en el icono significado de las variables. Monitor WiFI ofrece una ayuda completamente en español, en donde se muestra el significado de cada una de las variables. Estas variables se encuentran ordenadas en orden alfabético, para una rápida localización.

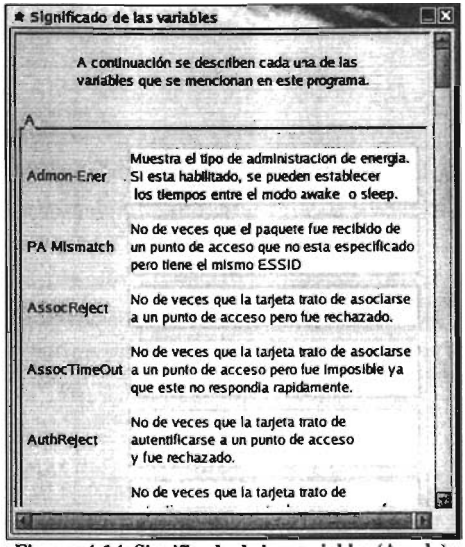


Figura 4-14. Significado de las variables (Ayuda).

4.14 Advertencias.

Monitor WiFi, provee al usuario de ciertas advertencias, que le permiten saber que existe un error ya sea en la configuración o ejecución de esta.

4.14.1 Ausencia de la interfaz eth0.

Esta se presenta, cuando se presenta uno o ambos de los siguientes casos:

- La ausencia de una tarjeta inalámbrica marca Aironet, insertada en la ranura correspondiente. Acción a realizar: Insertar la tarjeta o checas si esta dada de alta dicha interfaz.
- La tarjeta inalámbrica, no tiene asignado el nombre de interfaz eth0. Acción a realizar: Checar su configuración de red y realizar los cambios pertinentes.

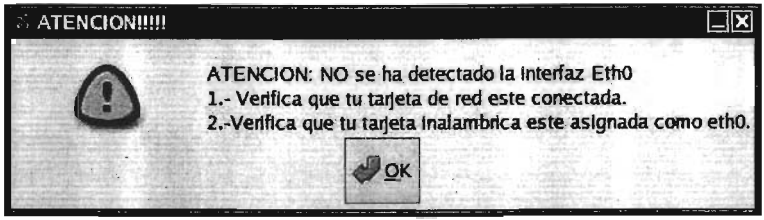


Figura 4-15. Advertencia (Interfaz eth0).

CAPÍTULO 5
CARACTERIZACIÓN DE UNA RED IEEE 802.11.

5.1 Introducción.

A continuación mostramos las pruebas realizadas para la caracterización del comportamiento del canal de radio, para poder planificar correctamente la red y asegurar una buena cobertura y desempeño de las tarjetas y red inalámbricas haciendo uso de la herramienta *Monitor WiFI.*

En este caso solo realizamos pruebas en interiores (Indoors), a lo cual nos enfrentamos a dos problemas, el primero son aquellos problemas inherentes al tipo de propagación de la banda de los 2.4 Ghz y segundo, que al estar en este tipo de entornos complican la propagación de las ondas de radio y además cualquier modificación en el entorno (Muebles, personas, etc.), generan nuevas zonas de sombra, limitando la cobertura del servicio. Los diferentes obstáculos que encuentran las ondas a su paso crean atenuaciones y/o reflexiones dificultando una buena planificación de la red.

Las pruebas se realizaron en el Piso 3, del edificio del Valdez Vallejo de la División de Ingeniería Eléctrica en el Departamento de Telecomunicaciones. El piso tiene en general una distribución compleja, es decir que esta segmentado y ocupado por laboratorios, cubículos, etc. Estas pruebas se dividen en dos grupos: la primera, consiste en medir el alcance de cobertura de la tarjeta Aironet 4800, que permitirá implementar una red de área local en la zona. y la segunda, consiste en pruebas de desempeño de la tarjeta, que nos permiten definir las características de operación de esta tarjeta.

Los parámetros a medir fueron Velocidad, Calidad de link, Potencia de la señal, así como el numero de errores.

5.2 Equipo de las pruebas.

Hardware

- Punto de acceso inalámbrico marca 3com Office Connect 11Mbps
- Nodo 1, corresponde a una PC Portátil DELL Intel Celeron (Nodo Móvil).
- Nodo 2, corresponde a una PC Portátil Toshiba Pentium III.(Nodo fijo).
- Tarjeta inalámbricas marca Aironet Modelo 4800 a 11Mbps

Software.

- Nodo 1 . Posee un sistema operativo Windows Millenium, e instalada la herramienta Cisco Aironet Utilities.

- Nodo 2, posee un sistema operativo Linux Red Hat v. 9 e instalada la herramienta de monitoreo Monitor WiFI.
- Tarjetas Inalámbricas. Versión del firmware 4.13.

5.3 Prueba de Cobertura.

Para esta prueba, solo consideramos los espacios interiores (pruebas Indoor), y dos tipos de arquitectura Infraestructura y Ad-hoc.

5.3.1 Infraestructura.

5.3.1.1 Descripción de la prueba.

Consiste en que el Nodo 1, envía paquetes que son recibidos por el Punto de Acceso. El Punto de acceso sirve como servidor y escucha constantemente en espera de paquetes de datos del Nodo 1, el cual envía paquetes de datos con la herramienta ***ping (Véase Apéndice 4).***

El Nodo 1, se colocó en 5 puntos distintos del piso 3 del edificio, en donde se registro para cada intervalo la velocidad de transmisión, Calidad del link y Potencia de la señal, todo esto con el uso de la herramienta Monitor WiFI.

5.3.1.2 Arquitectura.

A continuación se muestra un diagrama de la arquitectura utilizada para las pruebas.

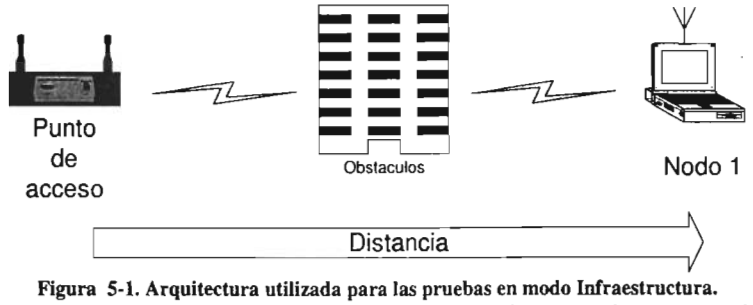


Figura 5-1. Arquitectura utilizada para las pruebas en modo Infraestructura.

En la figura anterior, los obstáculos, simulan todas aquellas paredes, marcos de metal, ventanas, etc., que separan a los nodos y que ocasionan atenuación en la recepción de la señal.

5.3.1.3. Toma de lecturas.

Comenzamos con una distancia inicial de 0 m, y se fue alejando al Nodo 1 del Punto de Acceso, y se tomaron lecturas en los distintos puntos del piso.

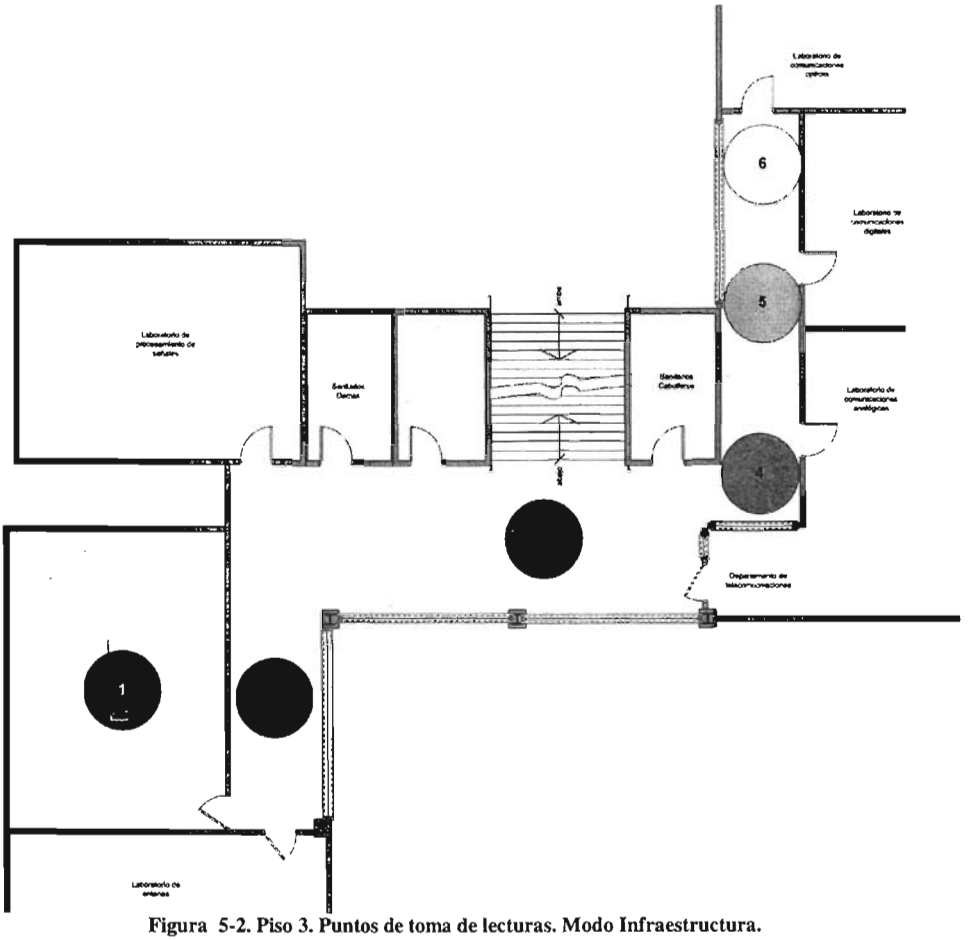


Figura 5-2. Piso 3. Puntos de toma de lecturas. Modo Infraestructura.

5.3.2 Ad-hoc.

5.3.2.1. Descripción de la prueba.

El Nodo 1 y Nodo 2, son configurados en Modo Ad-hoc, de tal manera que entre estos forman una sola célula, permitiendo intercambiar información de manera directa sin el uso de punto de acceso.

La prueba consiste en que el Nodo 2, envía paquetes que son recibidos por el Nodo 1. El Nodo 1 funciona como servidor y escucha constantemente en espera de paquetes de datos del Nodo 2, el cual envía paquetes de datos con la herramienta ***ping (Véase Apéndice 4).***

El Nodo 1, se colocó en 5 puntos distintos del piso 3 del edificio, en donde se registro para cada intervalo la velocidad de transmisión, Calidad del link y Potencia de la señal, todo esto con el uso de la herramienta Monitor WiFI.

5.3.2.2. Arquitectura.

A continuación se muestra un diagrama de la arquitectura utilizada para las pruebas.

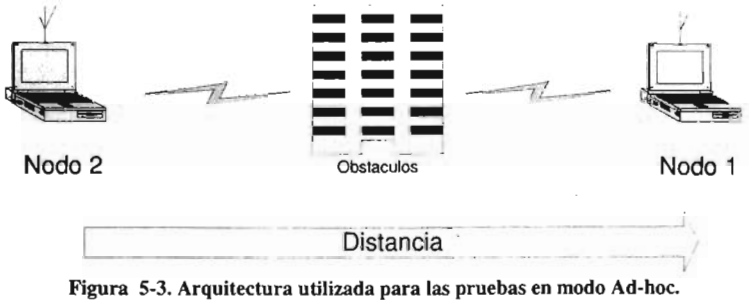


Figura 5-3. Arquitectura utilizada para las pruebas en modo Ad-hoc.

5.3.2.3. Toma de lecturas.

Comenzamos con una distancia inicial de 0 m, y se fue alejando al Nodo 1 del Nodo 2, tomando en cada punto las lecturas necesarias.

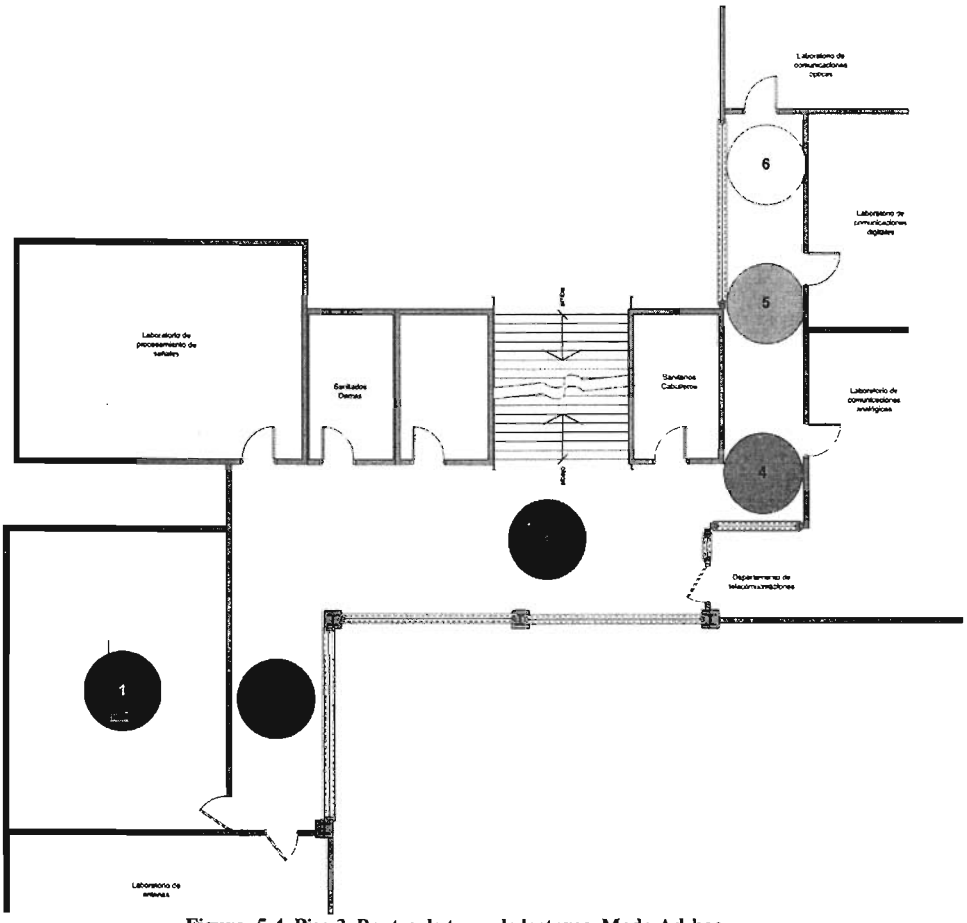


Figura 5-4. Piso 3. Puntos de toma de lecturas. Modo Ad-hoc.

En esta figura se muestran los puntos de toma de lecturas, y podemos apreciar, también, que cada circulo de acuerdo a su tonalidad, representa la intensidad de la señal.

5.3.3 Análisis de datos.

Los datos obtenidos fueron:

Tabla 5-1. Datos de la prueba de cobertura en modo Infraestructura.

Punto de lectura	*Velocidad de transmisión.*[1]	*Interferencia.*	*Potencia de la señal(dBm).*	*Potencia de la señal (nW).*
1	11	20%	-34	398.1
2	11	10%	-45	31.62
3	11	30%	-56	2.51
4	11	10%	-69	0.125
5[2]	11	5%	-75	0.031
6	Se pierde asociación con el punto de acceso. No se reciben datos.			

Tabla 5-2. Datos obtenidos de la prueba de cobertura en modo Ad-hoc.

Punto de lectura	*Velocidad de transmisión.*[1]	*Interferencia.*	*Potencia de la señal(dBm).*	*Potencia de la señal (nW).*
1	11	70%	-42	63
2	11	50%	-59	1.25
3	11	30%	-75	0.0316
4	11	40%	-86	0.0025
5[2]	2	10%	-90	.0001
6	Se pierde asociación con la célula. No se reciben datos.			

Nota 1. La velocidad de transmisión se mantiene fija, ya que la tarjeta inalámbrica transmite a esa velocidad de manera predefinida.

Nota 2. Este es el ultimo punto donde se tienen lecturas.

5.3.3.1 Calidad del link .

Con este parámetro podemos ver, el nivel de interferencia conforma aumenta la distancia entre nodos y la presencia de obstáculos.

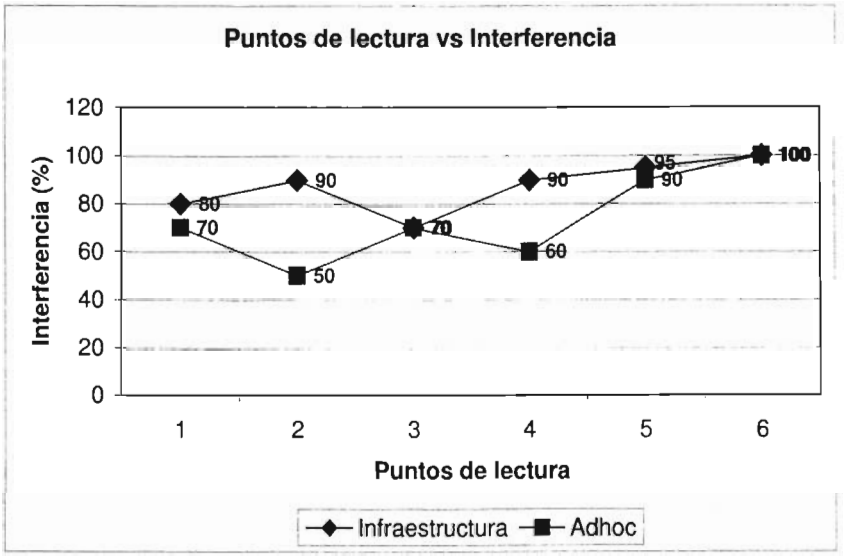


Figura 5-5. Gráfica. Puntos de lectura vs Interferencia.

5.3.3.2 Potencia de la señal.

En este apartado, podemos verificar, que conforme el Nodo 1 se aleja del punto de acceso y Nodo 2, la potencia de la señal disminuye considerablemente.

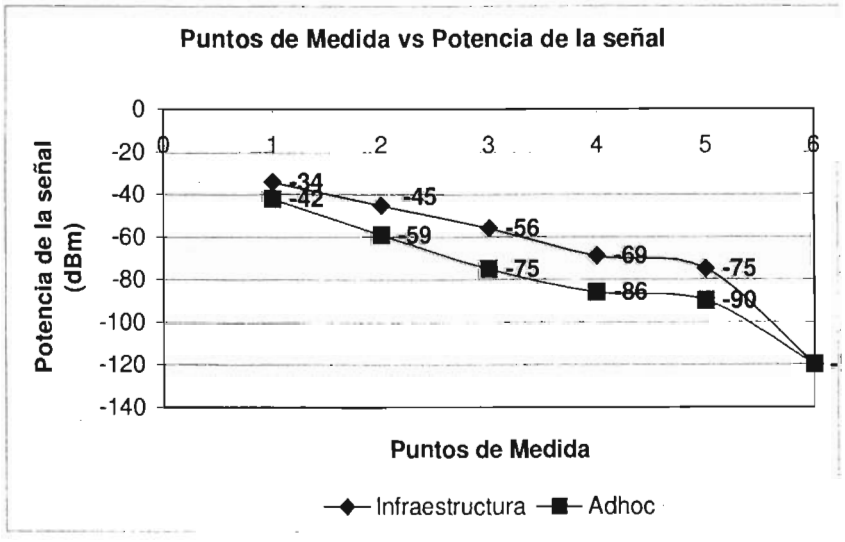


Figura 5-6. Gráfica. Puntos de Medida vs Potencia de la señal (dBm).

5.3.3.3 Análisis .

Claramente se observa, que conforme el Nodo 1 (Nodo móvil), se aleja los niveles de interferencia y atenuación se incrementan considerablemente, sin embargo , se nota que en la arquitectura Ad-hoc, los niveles de interferencia son menores, pero la atenuación es mayor. Sin embargo, vemos que este no es lineal, si no que tiene puntos de inflexión, esto lo podemos asociar a zonas de reflexión, si notamos es en los puntos 3 y 4, donde existen muchos marcos metálicos. (Obsérvese figuras 5-2 y 5-4).

Por lo tanto podemos decir:

- Que a mayor distancia y más obstáculos, mayor interferencia y atenuación
- Se obtiene un nivel mínimo de interferencia y atenuación a los 0 m, teniendo línea de vista entre los nodos.
- La mayor atenuación se presenta en el punto numero 6, ya que no hay recepción de datos, ni asociación al punto de acceso y la célula.
- Vemos que a partir del punto 2, existe una considerable atenuación, debido principalmente a los obstáculos presentes.

5.4 Prueba de desempeño de la red IEEE 802.11(Calidad de servicio)

Para esta prueba se utilizo la arquitectura de Infraestructura, y se utilizo la red de Internet para bajar un archivo de considerable magnitud y evaluar el numero de errores y determinar el desempeño de la red.

5.4.1 Descripción de la prueba.

El Nodo 1, se fue moviendo en distintos puntos del piso del edificio y en cada uno de ellos , se descargo un archivo de 37.8Mb. Se evaluaron , con la ayuda de la herramienta Monitor WiFI, el numero de errores, y se verifico en que punto existen un mayor numero de estos. En cada punto de tomaron 3 lecturas diferentes.

5.4.2 Arquitectura.

A continuación mostramos la disposición de los elementos para esta prueba.

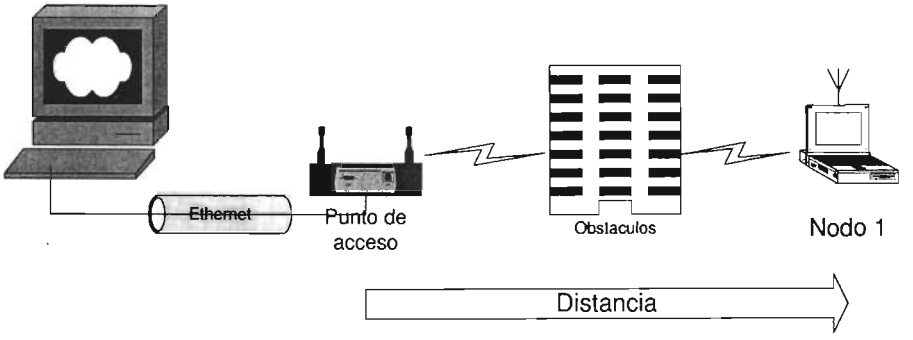


Figura 5-7. Arquitectura utilizada para las pruebas de desempeño.

5.4.3 Toma de lecturas.

A continuación se muestran los puntos de lectura, para esta prueba.

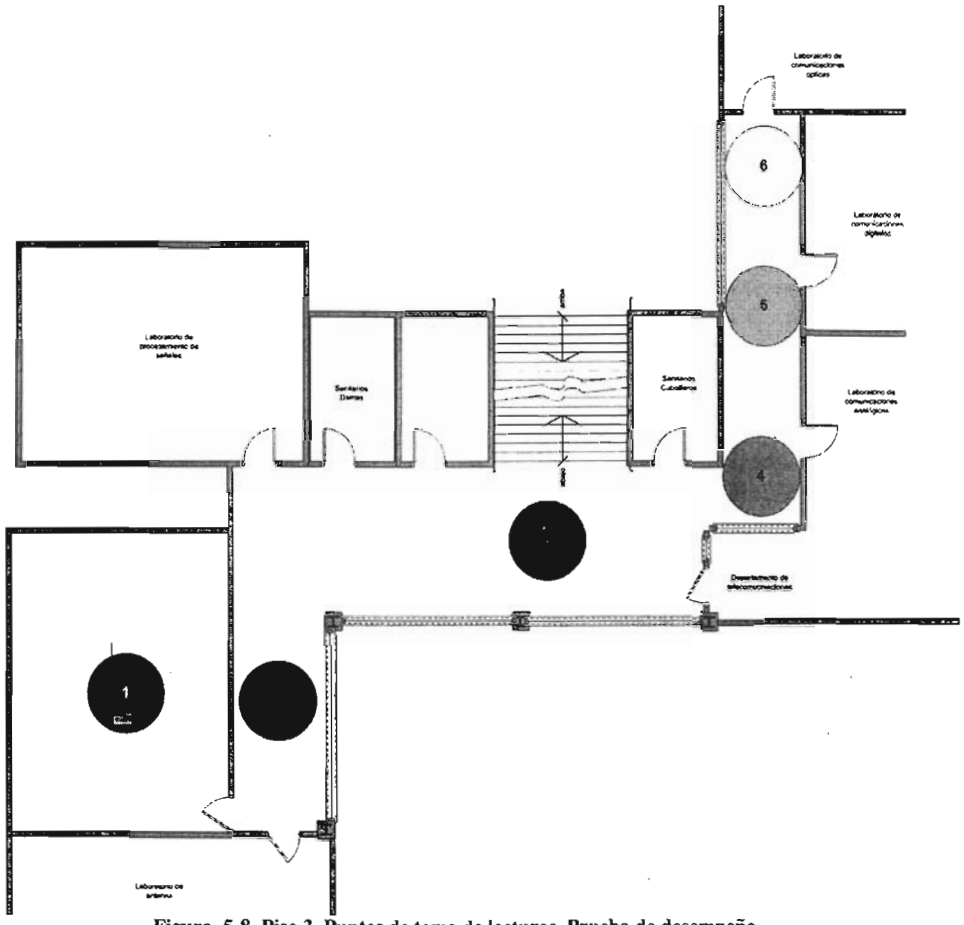


Figura 5-8. Piso 3. Puntos de toma de lecturas. Prueba de desempeño.

5.4.4 Datos.

A continuación mostramos los datos obtenidos en los puntos de lectura.

Tabla 5-3. Datos de la prueba de desempeño.

Punto de lectura	*No. de errores promedio*	*Velocidad de transmisión Promedio (Kbps)*	*Potencia de la señal.(dBm)*	*Tiempo de descarga Promedio (min)*
1	*1072*	122	-45	5:09
2	2438	110	-50	5:53
3	5345	86	-63	7:28
4	13392	60	-74	10:19
5	52208	39.5	-80	16:33

5.4.5 Análisis de datos.

A continuación mostramos las gráficas

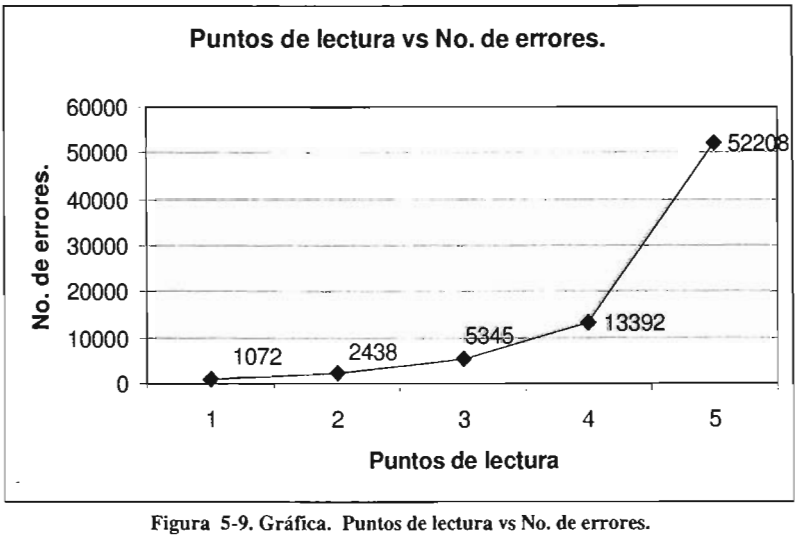


Figura 5-9. Gráfica. Puntos de lectura vs No. de errores.

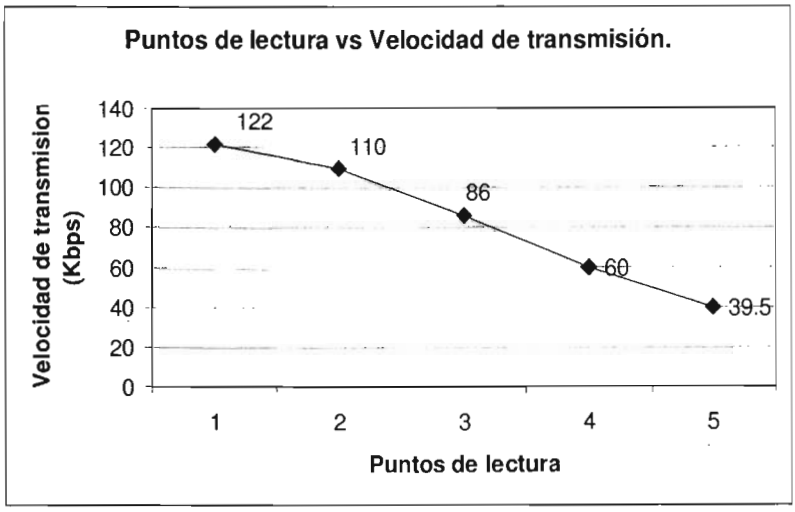


Figura 5-10. Gráfica. Puntos de lectura vs Velocidad de transmisión.

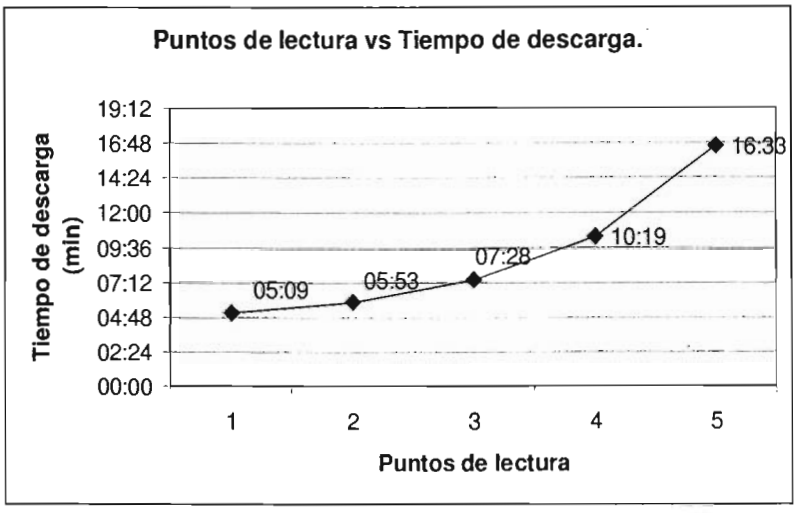


Figura 5-11. Gráfica . Puntos de lectura vs Tiempo de descarga.

De las anteriores gráficas podemos concluir lo siguiente:

Existe una relación directa , entre la distancia y el desempeño de una red inalámbrica. Ya que al comparar a velocidad de transmisión en cada punto , esta baja considerablemente, lo cual repercute directamente en le tiempo de descarga que aumenta en cada punto.
Además observamos que entre mas distancia, la potencia de la señal disminuye, y el numero de errores se incrementa considerablemente.

Entonces podemos decir que el punto máximo a la cual la red trabaja de manera eficiente es el punto 3.

Todos los datos recopilados, sirven para planear una futura disposición de puntos de acceso en el piso de telecomunicaciones. A lo cual sugerimos la siguiente:

Colocar puntos de acceso entre el punto 2 y 3 y un punto de acceso en el punto 4 para así lograr cobertura a todos los cubículos y laboratorios de este piso.

CAPÍTULO 6
CONCLUSIONES.

Las redes inalámbricas de área local (WLAN) han alcanzado gran popularidad y han extendido su uso a muchos campos como educación, medicina, etc. Esto, es debido a las grandes virtudes que ofrece en comparación a otras tecnologías de datos (HiPERLAN, HomeRF, etc.)

La tecnología WLAN es muy flexible ya que permite adaptarse a diferentes topologías y/o arquitecturas, hasta la posibilidad de roaming, de acuerdo a las necesidades y características del entorno; su configuración e incorporación de mas terminales es relativamente sencilla.

Otra de las ventajas, que prepondera por mucho en comparación de otras tecnologías es el sistema de ahorro de energía que posee, permitiendo a las terminales mayor tiempo de vida de sus baterías reflejándose en mayor movilidad para el usuario.

La banda de trabajo, es de libre utilización por lo que no requiere autorización o pagos excesivos, abaratando así los costos del equipo y permitiendo que un mayor número de usuarios tengan acceso a esta tecnología; sin embargo hay que recalcar que a pesar de esto, las redes WLAN coexisten con diferentes tecnologías, existiendo así, interferencias que deterioran la calidad del enlace.

Además, cada vez existen mayor variedad de dispositivos de red de distintas marcas y precios permitiendo una mayor interconexión e interacción entre equipos con diferentes características que van desde la oficina hasta el hogar. Sin embargo, todavía, existen mucho puntos en contra, por ejemplo, la interoperabilidad entre dispositivos de distintas marcas todavía no es total, limitando su expansión comercial.

Hablando en términos de velocidades, el estándar IEEE 802.11 todavía tiene un camino largo que recorrer para poder competir con las redes alámbricas, ya que solo ofrece velocidades de 1, 2, 5.5, 11 y 54 Mbps. en sus distintas modalidades del estándar. Además habrá que esperar por el ingreso en forma masiva del estándar IEEE 802.11g que tener velocidad de 54 Mbps, y además y quizá una de las cosas más importantes es su interoperabilidad con el estándar IEEE 802.11b el cual es el más adoptado hasta el momento.

En términos de transmisión de frames el IEEE 802.11 es de los más eficientes ya que permite la fragmentación de paquetes, haciendo más eficiente el uso de ancho de banda. Además ofrece otras características importantes como el uso de protocolo de supresión de colisiones, resolviendo así el problema de terminales ocultas.

Sin embargo una de las mayores desventajas de este tipo de redes, es la seguridad. El estándar por si solo ofrece soluciones políticas de seguridad muy débiles, fáciles de corromper, teniendo así que integrar otro tipo de tecnologías en seguridad haciendo que la

instalación dependiendo del grado de seguridad requerido se encarezca de manera significativa. La expectativa esta en la puesta en marcha del estándar IEEE 802.11 que cubrir todas aquellas deficiencias, y haciendo la transmisión de datos más segura y fiable.

En cuento a las herramientas de monitoreo estudiadas es claro la deficiencia de estas en el aspecto de facilidad de instalación, de uso y sobre todo de interpretación de la información.

Las WLAN tiene como futuro la interoperabilidad con las redes celulares, esto permitirá ampliar el área de cobertura y la transmisión de datos, así como la bondad de tener todos los servicios que cada una de estas tecnologías ofrece, haciéndose su uso más flexible, barata y eficiente.

Por lo tanto de las herramientas pudimos analizar, recopilamos algunas de las bondades y deficiencias que presentan cada una, los puntos más importantes que se destacaron fueron:

- *Cantidad y calidad de información.*-Algunas herramientas resultan muy poderosas, debido a la gran cantidad de información que proveen, y es tal, que permite un total monitoreo de la red ya sea en capa física o MAC, como son Wlanctl-ng y las Wireless Tools y el ACU CISCO, pero carecen de una interfaz que permitan visualizar de una manera ordenada, sencilla y amigable dicha información.

- *Ambiente gráfico.*- En contraparte, otras herramientas como KwifiManager, que poseen un ambiente gráfico que despliega la información de manera amigable y elegante, pero a su vez muy limitada, ya que se omiten varios parámetros importantes necesarios para un buen análisis de la red.

- *Facilidad de instalación y uso.*- Consideramos que en general es un problema el instalar este tipo de software debido a la plataforma en que trabajamos, pero ya con un poco de experiencia el uso y configuración de estas herramientas es relativamente sencillo.

A continuación mostramos una tabla comparativa con las herramientas analizadas:

Herramientas / Parámetros	*Ifconfig*	*Iwconfig*	*Iwlist*	*Iwspy*	*Iwpriv*	*/proc/driver /aironet*	*/proc/net/ wireless*	*Kwifiman ager*	*Wlang ng*	*xwconfig*	*ACU cisco*
Nombre- host	No	No	No	No	Dependen del fabricante y del driver de cada tarjeta	Si	No	No		Si	Si
IP - host	Si	No	No	No		No	No	Si		No	No
MAC - host	Si	No	Si	Si		No	No	No		No	No
MAC - AP	No	Si	Si	Si		No	No	Si		No	No
Tipo de acceso al medio	No	Si	No	No		No	No	No		No	No
ESSID	No	Si	No	No		Si	No	Si		Si	Si
Modo de operación	No	Si	No	No		Si	No	Si		SI	Si
Frecuencia de trabajo	No	Si	SI	No		Si	No	Si		No	Si

Herramientas / Parámetros	*Ifconfig*	*Iwconfig*	*Iwlist*	Iwspy	*Iwpriv*	*/proc/driver /aironet*	*/proc/net/ wireless*	*Kwifiman ager*	*Wlang ng*	*xwconfig*	*ACU cisco*
Canal	No	No	Si	No		Si	No	Si		No	Si
Velocidad de transmisión	No	Si	SI	No		Si	No	Si		No	Si
Potencia de transmisión	No	Si	Si	No		Si	No	No		No	Si
Umbral de sensibilidad	No	Si	No	No		Si	No	No		No	Si
Retrylimit	No	SI	Si	No		Si	No	No		No	Si
RTSthreshold	No	SI	No	No		Si	No	No		No	Si
Fragmentación	No	Si	No	No		Si	No	No		No	Si
Encriptación	No	Si	Si	No		Si	No	No		No	Si
Administración de energía	No	Si	Si	No		Si	No	Si		No	Si
Calidad del link	No	Si	No	Si		Si	No	Si		No	Si
Nivel de señal	No	Si	No	Si		Si		Si		No	Si
Nivel de ruido	No	Si	No	Si		Si	No	Si		No	Si
Paquetes RX y TX	Si	No	No	No		Si	Si	No		No	Si
Paquetes con error RX y TX	Si	No	No	No		Si	SI	No		No	Si
Paquetes despreciados RX y TX	Si	No	No	No		Si	Si	No		No	Si
Paquetes Overrun Rx y Tx	Si	No	No	No		Si	Si	No		No	Si
No. de bytes Rx y TX	Si	No	No	No		Si	Si	No		No	Si
Fragmentación	No	SI	No	No		Si	Si	No		No	Si
Rx invalid nwid	No	Si	No	No		Si	Si	No		No	Si
Rx invalid frag	No	Si	No	No		Si	Si	No		No	Si
Tx excessive retries	No	Si	No	No		Si	Si	No		No	Si
Invalid misc	No	Si	No	No		Si	Si	No		No	Si
Missed beacons	No	Si	No	No		Si	Si	No		No	Si
Colisiones	No	No	No	No		Si	No	No		No	Si

Nuestra herramienta "Monitor WiFi", intenta incluir todas las bondades de cada una de estas herramientas, ofreciendo un ambiente gráfico amigable y de sencilla configuración, presentando la información en un formato claro y conciso, dividiendo esta, en módulos que permite saber al usuario qué parámetros y unidades se está obteniendo de manera ordena y clasificada. En nuestra herramienta no incluimos indicadores gráficos ya que, aunque éstos dan una idea aproximada del estado de la red, nuestra herramienta está más enfocada a la obtención de datos precisos y exactos para los posibles programas de investigación.

Para ejemplificar el uso y posibilidades de nuestra herramienta, se realizaron pruebas de cobertura y desempeño de la red inalámbrica obteniendo los resultados del capitulo 5, y concluyendo lo siguiente:

Comparando el modo ad-hoc e infraestructura, se observa que conforme se aumenta la distancia entre terminales, aumenta la interferencia, siendo mayor en general en modo infraestructura; sin embargo, cabe mencionar que existía en el momento de la prueba la señal de otro punto de acceso ubicado en un piso inferior del edificio y que se sabe que estaba trabajando en el mismo canal de frecuencia que en el nuestro.

Así mismo observamos que la potencia de la señal decrece de manera exponencial, conforma aumenta la distancia. Destacando que la atenuación era menor en cada punto en el modo infraestructura, debido a que el punto de acceso transmite a una mayor potencia.

Por otro lado, observamos que conforme aumenta la distancia se presenta un mayor número de errores en los paquetes recibidos reflejándose, en un decremento y aumento cuasi-lineal de la velocidad de transmisión y tiempo de descarga respectivamente. Esto se debe a que al aumentar la distancia, disminuye la potencia, se incrementa el fenómeno de desvanecimiento y esparcimiento de la señal, por lo que el número de paquetes efectivos en la recepción son menores y tardan más tiempo de llegar desde el origen al destino.

Expectativas:

El presente trabajo servirá de base para futuros proyectos y tesis a nivel licenciatura, en el área de redes inalámbricas.

BIBLIOGRAFÍA

IEEE 802.11 system design
Prasad, N.R.;
Personal Wireless Communications, 2000 IEEE International Conference on , 17-20 Dec. 2000
Pages:490 – 494

WI-FI, Análisis, diagnostico y políticas públicas
Pérez Jorge, Redondo Juan, Ruano Vanesa, et. Al.
Grupo de Análisis y prospectiva del sector de las telecomunicaciones
Noviembre 2003

Wireless LAN Networking
White paper
US. Robotics

Arquitectura con redes Wi-Fi
Cimadevila López Enrique
Dealer World, Wireless Mundi

Redes inalámbricas y Móviles Avanzadas. IEEE 802.11 LAN Inalámbricas
Gómez Castellanos Javier
2003

Wireless Hotspots: Current Challenges and Future Directions
Balachandran, Geoffrey Paramvir Bahl

Investigation of the IEEE 802.11 medium access control (MAC) sublayer functions
Crow, B.P.; Widjaja, I.; Kim, J.G.; Sakai, P.;
INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies.
Proceedings IEEE ,Volume: 1 , 7-11 April 1997
Pages:126 - 133 vol.1

Wireless Community Networks
Jain Saurabh. ; Agrawal Dharm

Cordless Personal Communications
Dr. Walter H. W. Tuttlebee
Digital Cordless Technology, IEEE 1992
Pag 42-53

DECT the standard explained
DECT forum ,1997

Positioning of DECT in relation to other radio access technologies
Dect forum Junio 2002

MMAC activities on 5Ghz Band
Umehira Masahiro
NTT Network Service Systems Laboratories

2003 World Wide Wireless Communication Standards

PHILIPS

ZigBee Overview
Venkat Bahl , Zigbee Alliance
Septiembre , 2002.

Zigbee:"Wireless Control That simply Works"
Craig, Williams
ZMD América

Redes Inalámbricas
Alejandro Reguarti Ferri, Carmen Pérez Berenguer

Techno-economic evaluation of 3G & WLAN business case feasibility under varying conditions
Welling, I.; Harno, J.; Loizillon, F.; Stordahl, K.; Varoutas, D.;
Telecommunications, 2003. ICT 2003. 10th International Conference on ,Volume: 1 , 23 Feb.-1 March 2003
Pages:33 - 38 vol.1

IEEE 802.11 Wireless Local Area Networks
Crow, B.P.; Widjaja, I.; Kim, L.G.; Sakai, P.T.;
Communications Magazine, IEEE ,Volume: 35 , Issue: 9 , Sept. 1997
Pages:116 - 126

Análisis comparativo entre redes Lan, alámbrica e inalámbrica basada en el estándar IEEE 802.11.
Paola Pinelo Bolaños.
TESIS, facultad de Ingeniería, UNAM

Design of MAC protocols with fast Collision Resolutions for Wireless Local Area Networks.
Kwon, Younggoo,et.al.
IEEE Transactions of Wireless Communications, VOL 3 No 3 May 2004.

802.11a More Bandwidth Without the Wires,
Kapp Steve

On Spread Modulation Techniques Applied in IEEE 802.11 Wireless LAN Standard.
Boskovic Branimir, Milan Markovic

An Introduction to IEEE.11 Wireless LANs..
Saliga Stephen.
Aironet W.C. Inc

Nuevas tecnologías de transmisiones inalámbricas
F.Serrano
http://neutron.ing.ucv.ve/revista-e/No1/SERRANO2.htm

El Standard IEEE 802.11
http://www.arrakis.es/~sergilda/wlan/ieee408.htm#mac

Wifi
http://www.mundofree.com/juanpablo/xarxes/wifi.htm

Tecnologías de redes inalámbricas.
http://www.e-advento.com/tecnologia/wlan_intro.php

Home RF
http://www.wca.org/hp-negus/sld00 Re4.htm

Frequency Hopped Spread Spectrum (FHSS).
http://www.qsl.net/n9zia/wireless/fhss.html

Wireless Extension for Linux .
Tourrilhes Jean.
Linux Wireless LAN Howto, 1997. http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

Man pages : iwpriv, iwlist , ifconfig, iwspy, iwconfig, grep, cut, sed, awk.

How to setup a wireless card Under Red Hat 7.2.
http://jackal.dnsalias.com:8080/public/misc/wireless/wireless.html

Linux PCMCIA COMO: Uso y características.
http://www.insflug.org/COMOs/PCMCIA-Como/PCMCIA-Como-4.html

Instalación de la red inalámbrica en Debian GNU/Linux.
http://oasis.dit.upm.es/~cdc/wireless-debian.html

Glade GTK+ User Interface Builder
http://glade.gnome.org/

GTK+ programming with Glade
Ishan Chattopadhyaya
http://wingtk.sourceforge.net/ishan/glade.html

Grapbical Interface Development with Glade2
Rikke D. Giles
http://www.kplug.org/glade_tutorial/glade2_tutorial/glade2_introduction.html

Starting off in Glade/GTK+
Ishan Chattopadhyaya
http://www.geocities.com/ichattopadhyaya/linux/glade.htm

FAQ de Glade
http://tigre.aragon.unam.mx/m3d/glade_spanish.htm

Manual de Glade
http://tigre.aragon.unam.mx/m3d/glade/glade_manual.html

Mailing List Glade Usar Ximian
http://lists.ximian.com/mailman/listinfo/glade-users

Programación del entorno Gnome
Rodrigo Moya. Et al

El lenguaje de programación AWK /GWAK
Jesús Alberto Vidal Cortes
http://inicia.es/de/chube

Desarrollo de aplicaciones científicas con Glade
Francisco Domínguez Adame, 2003
http://valbuena.fis.ucm.es/~adame/programacion/index.html#manuales

Manual de UNIX
Jonathan Noel Tombs,et.al
1995

Alternative Networking Wireless Backgrounder
http://www.practicallynetworked.com/networking/alternative_net_wireless.htm

Introduction to de IEEE 802.11
http://www.intelligraphics.com/articles/80211_article.html

HIPERLAN 2
www.hiperlan2.com

DECT Web
www.dectweb.com

DECT
www.dect.org

ZigBee
www.zigbee.org

HomeRF Redes de datos
www.domotica.net/HomeRF.htm

HomeRF Overview
www.palowireless.com/homerf/homerf1.asp

Protocolos en seguridad de redes Inalámbricas.
Saulo Barajas
http://www.saulo.net/pub/inv/SegWiFi-art.htm

GTK Referente Manual
http://developer.gnome.org/doc/API/2.0/gtk/

Proyecto Acceso UMTS
Miguel Oliver, et.al.
2001
http://egotic.upf.edu/eGotic/WLAN/i2CAT-ctx-UMTS-UPC-010905.htm

Caracterización de la banda ISM a 2.4Ghz para la planificación de redes de área local inalámbricas IEEE 802.11
Miguel Oliver, et.al.
http://acimut.upf.es/moliver/OlE99b.pdf

Implementación de una red inalámbrica Bluetooth.
Rodríguez Calvachi Oscar
Tesis, Universidad del Valle, Santiago de Cali,
2003

Protocolos de seguridad en redes inalámbricas.
Barajas Saulo
Universidad Carlos III
Madrid , España.
http://www.saulo.net/pub/inv/SegWiFi-art.htm

Entendiendo las Wireless LAN.
KernelPanik Crew.
http://www.kernelpanik.org.

802.11:The security difference between b and i.
Brandon Brown.
IEEE Potencials.
Octubre - Noviembre 2003.

Risk Soluciones inalámbricas.
http://www.riskinformatica.com/content/documentacion/calculo.php

Comando Ping.
http://www.linux.cu/manual/basico-html/node91.html

Manual sobre el comando ping.
http://www.bossma.com/download/manuales/comando_ping.htm

Cisco Aironet 350 Series Client Adapters.
Cisco Systems, Inc. 2004.
http://www.cisco.com/global/MX/ps/cp/wrls/cac/index.shtml

3Com® OfficeConnect®
11 Mbps Wireless Access Point
3Com Corporation, 2004.
http://www.3com.com/prod/es_LA_AMER/detail.jsp?tab=features&sku=3CRWE41196

APÉNDICE 1. ESPECIFICACIONES DEL PUNTO DE ACCESO MARCA 3COM MODELO OFFICE CONNECT 11MBPS

Descripción	*Especificación*
Tasa de Velocidad soportada	1, 2, 5.5, y 11 Mbps
Estándar de Red	IEEE 802.11b
Puertos	Ethernet 10BASE-T 10/100
Banda de Frecuencia	2.4 to 2.4835 GHz
Medio Inalámbrico	DSSS, (Direct Sequence Spread Spectrum)
Modulación	DBPSK @1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 and 11 Mbps
Canales de Operación	Norte América: 11 ETSI: 13
Canales no sobrepuestos	Tres
Rango (típico)	Interior: 41m Exterior: 457 m
Sistemas Operativos Soportados	Windows 95, 98, NT 4.0, 2000, ME, XP
Longitud de Encriptación de Llave	40/64 y 128-bit
Indicadores de Estado	Estado del Enlace y Actividad del Enlace
Garantía	Limitada, por el tiempo de vida
Dimensiones (H x W x D)	24.4mm x 220mm x 135.4mm
Peso	592g
Temperatura Operativa	0° a 40°
Humedad Operativa Relativa	10 a 90% (no condensada)

APÉNDICE 2. ESPECIFICACIONES DE LA TARJETA INALÁMBRICA AIRONET MODELO 4800.

Descripción	*Especificación*
Tasa de Velocidad soportada	1, 2, 5.5, y 11 Mbps
Estándar de Red	IEEE 802.11b
Interfase de Sistema	PC Card (PCMCIA) Tipo II
Banda de Frecuencia	2.4 to 2.4897 GHz
Tipos de Arquitectura de red	Infraestructura y "ad hoc"
Medio Inalámbrico	DSSS, (Direct Sequence Spread Spectrum)
Protocolo de Acceso a Medios	CSMA/CA (Carrier sense multiple access with collision avoidance)
Modulación	DBPSK @1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 and 11 Mbps
Canales de Operación	Norte América: 11 ETSI: 13 Japón: 14
Canales no sobrepuestos	Tres
Sensibilidad de recepción	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm 11 Mbps: -85 dBm
Delay Spread	1 Mbps: 500 ns 2 Mbps: 400 ns 5.5 Mbps: 300 ns 11 Mbps: 140 ns
Configuraciones de poder de transmisión disponibles	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm) El poder de la configuración variará de acuerdo con las regulaciones individuales de los países
Rango (típico)	Interior: 130 ft (40m) @ 11 Mbps 350 ft (107m) @ 1 Mbps Exterior: 800 ft (244m) @ 11 Mbps 2000 ft (610m) @ 1 Mbps

Sistemas Operativos Soportados	Windows 95, 98, NT 4.0, 2000, ME, CE 2.0, CE 2.1, CE 3.0, Mac OS 9.x y Linux
Antena	dipoles diversos integrados
Longitud de Encriptación de Llave	128-bit
Tipo de Autenticación	EAP - Cisco Wireless
Indicadores de Estado	Estado del Enlace y Actividad del Enlace
Garantía	Limitada, por el tiempo de vida
Requerimientos de energía entrante	+5 VDC =/- 5%
Consumo de energía típico (con configuración de poder de transmisión de 100 mW)	Transmite: 450 mA Recive: 270 mA Sin trabajar: 15 mA
Dimensiones (H x W x D)	0.3 x 5.4 x 11.1 cm
Peso	45g
Temperatura Operativa	-30 to 70°C
Humedad Operativa Relativa	10 a 90% (no condensada)
Descripción	Especificación
Compatible con	Licencia de operación libre bajo FCC Parte 15 y que clasifica como dispositivo del tipo B; compatible con las regulaciones DOC; compatible con estándares ETS 300.328, FTZ 2100 y MPT 1349.

APÉNDICE 3
MANUAL DE USUARIO DE MONITOR WIFI.

Este es un pequeño manual que le guiara en el uso de Monitor WiFI.

Instalación de WiFI.

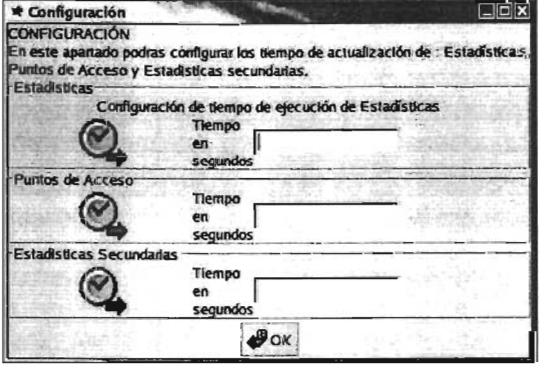
1. Debes tener cuenta de administrador (root)
2. Cambiar a la carpeta donde este Monitor WiFI, la carpeta se llama "telecom".
3. Desde la terminal, teclea "make clean"
4. Teclea "make". Si no te hace falta ninguna de las librerías estas listo para ingresar a Monitor WiFI.

Ingresar a Monitor WiFI.

1. Cambiar a la carpeta "xxx/telecom/src"
2. Teclea desde la terminal "./telecom".
3. En caso que no tengas tu tarjeta de red insertada, Monitor WiFI, te notificará por medio de una ventana, la necesidad de insertarla para su correcto funcionamiento.
4. En caso de que la tarjeta de red no tenga asignada el numero de interfaz de red "eth0", Monitor WiFI, te indicara que debes asignar el numero de eth0 a tu tarjeta de red (Véase Apéndice 5).
5. Sí, Monitor WiFI, no te ha desplegado ninguna ventana de avisos, estas listo para utilizar Monitor WiFI.

Configuración de Monitor WiFI.

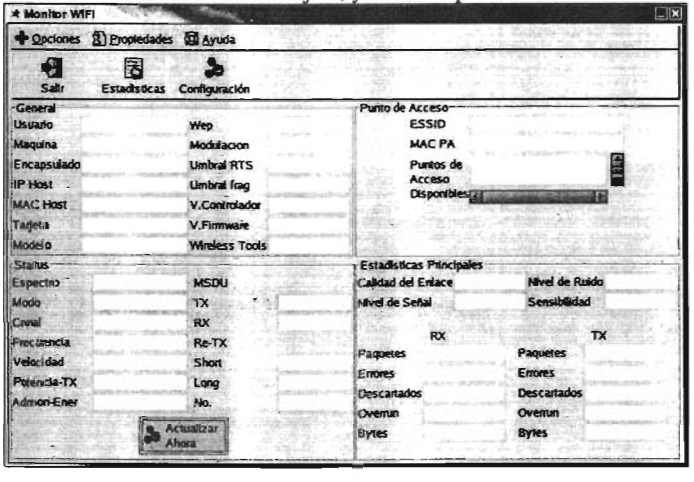
1. Antes de utilizar Monitor WiFI, necesitas configurar los tiempos en que la herramienta actualizará la información. Haz clic en el botón "Configuración". Te aparecerá la siguiente pantalla.



2. Aquí deberás ingresar los tiempos de actualización, de los cuales te sugerimos:
   Estadísticas > 3 segundos
   Punto de acceso > 14 segundos
   Estadísticas Secundarias > 3 segundos.
3. Una vez que has ingresado los tiempos en las respectivas cajas de texto, dale clic en OK. A partir de este momento estas listo para dar clic en el botón "Actualizar Ahora"
4. En caso de que hallas presionado el botón "Actualizar Ahora" sin haber configurado los tiempos de actualización, Monitor WiFI, sugerirá incrementar los tiempos de actualización para un correcto funcionamiento del software.

Uso de Monitor WiFI.

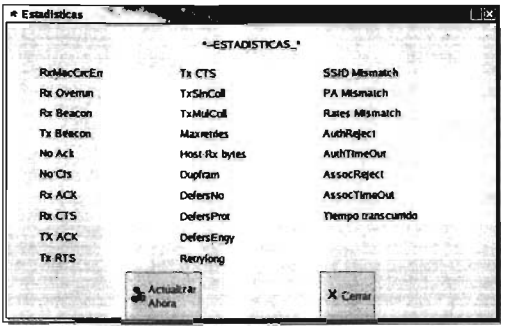
1. A partir de este momento, la ejecución de Monitor WiFI será automática, es decir que cada x tiempo (donde x es el tiempo que tu decidiste), actualizara la información relacionada con la tarjeta, y el desempeño de la red.



Estadísticas Secundarias.

1. Monitor WiFI, cuenta con un apartado de estadísticas secundarias, es decir que existe mayor información relacionada con el desempeño de la red, para ingresar tienes dos opciones, la primera es presionar el botón Estadísticas en la barra de herramientas, la segunda es presionar en la barra de menú "Propiedades" y posteriormente "Estadísticas".

2. Se abrirá una ventana como la que se muestra a continuación:



Para que comience a trabajar Monitor WiFI en su modulo Estadísticas Secundarias, presiona "Actualizar ahora". Esta ventana, puedes tenerla siempre abierta o en su caso puedes cerrarla dándole clic en "Cerrar". Si das cerrar, la próxima vez que vuelvas a abrir la ventana de Estadísticas Secundarias, deberás presionar el botón "Actualizar Ahora".

Ayuda de Monitor WiFI.

1. Monitor WiFI cuenta con una ventana de ayuda que te permite, consultar el significado de todas aquellas variables que están incluidas en la herramienta. Para acceder a esta ayuda, ve a la barra de menú y presiona "Ayuda" y después sitúate donde dice "Significado de las variables".
2. Las variables están dispuestas en orden alfabético, para un rápido acceso.
3. Para salir de ayuda, simplemente presiona la cruz de la esquina superior derecha y regresaras a la ventana principal de Monitor WiFI.

Salir de Monitor WiFI.

1. Para salir de Monitor WiFI, existen dos maneras: la primera es ir a la barra de herramientas y presionar el botón "Salir" o ir a la barra de menú y presionar "Opciones" y después presionar "Salir".

Para mayor información del funcionamiento, información y programación de esta herramienta, véase el Capitulo 4 "Herramienta de administración, monitoreo y control: "Monitor WiFI".

APÉNDICE 4. COMANDO PING.

Permite enviar paquetes ICMP (*Internet Control Message Protocol*) del tipo ECHO_REQUEST a otra computadora, con el objetivo de saber si esta es alcanzable a través de la red. Además muestra un resumen estadístico acerca del porciento de paquetes perdidos y las velocidades de transmisión. Este comando se ejecuta por defecto sostenidamente por lo que para interrumpirlo se debe hacer Ctrl-c.

Sintaxis: `ping [opciones] <máquina>`

Algunas opciones:

`-c <n>` :
envía n paquetes exactamente.

`-i <n>` :
espera n segundos entre los envíos.

`-s <n>` :
envía paquetes de n *bytes*. Se le suman los 8 *bytes* del *header* del paquete ICMP.

`-q` :
sólo despliega el sumario final.

-t :
solicita eco al host hasta ser interrumpido.

-a:
resuelve direcciones a nombres de host.

-n :
cantidad Cantidad de solicitudes de eco a enviar.

-l:
tamaño Tamaño del búfer de envíos.

-f:
no fragmentar el paquete.

-r :
cantidad Registrar la ruta para esta cantidad de saltos.

-s :
cantidad Registrar horarios para esta cantidad de saltos.

-j:
lista de hosts Ruta origen variable en la lista de host.

-k:
lista de hosts Ruta origen estricta en la lista de host.

-w:
Tiempo de espera agotado de respuesta en milisegundos

APÉNDICE 5.
NIVELES DE POTENCIA PERMITIDOS

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Americas (-A) (4 watts EIRP maximum)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	20
ETSI (-E) (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
Israel (-I) (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
China (-C) (10 mW EIRP maximum)	0	5
	2.2	5
	5.2	n/a
	6	n/a
	8.5	n/a
	12	n/a
	13.5	n/a
	21	n/a
Japan (-J) (10 mW/MHz EIRP maximum)	0	50
	2.2	30
	5.2	30
	6	30
	8.5	n/a
	12	n/a
	13.5	5
	21	n/a

APÉNDICE 6. ESTABLECER INTERFAZ INALÁMBRICA COMO ETH0.

El siguiente apéndice muestra uno de los varios pasos posibles a seguir para cambiar el nombre lógico de una interfaz de red inalámbrica. Este procedimiento es particularmente útil cuando se tienen dos o más interfaces dentro del equipo de cómputo.

Requisitos:
Contar con el sistema operativo Linux Red-Hat 8.0 o posterior
Tener permisos de administrador
Tener instalado el modo gráfico.

Pasos a seguir:

1. Dentro del menú de Red-Hat seleccione *herramientas del sistema.*
2. Seleccione *Control del dispositivo de red*
3. Es probable que tenga activada la interfaz de red LAN. Desactívela y posteriormente haga clic en *configurar.*
4. Dentro del menú, seleccione la ficha de *hardware.*
5. Seleccione el controlador actual de su interfaz LAN y haga click en *modificar.*
6. Dentro del submenú cambie el valor del campo de *Dispositivo* a otro diferente de eth0 (P.ej: eth1).
7. Haga clic en Ok.
8. En la ficha *dispositivos,* seleccione el dispositivo LAN y haga clic en Modificar.
9. Dentro del submenú en la ficha *General* cambie el campo de *sobrenombre* a eth1 (o el que haya elegido usted en el paso superior).
10. Haga clic en *ok.*
11. Dentro del menú principal de *configuración de red* haga clic en *Aplicar* y posteriormente en *cerrar.*
12. Nuevamente clic en *cerrar* y reinicie el equipo.
13. Al iniciar nuevamente, su interfaz LAN habrá cambiado de interfaz lógica por la que usted configuró mientras que la interfaz inalámbrica habrá tomado por orden la de eth0.

LISTA DE ABREVIATURAS Y ACRÓNIMOS.

ACK acknowledgment
AID association identifier
AP access point
ARQ automatic repeat request
ATIM announcement traffic indication message
BER bit error rate
BSA basic service area
BSS basic service set
BSSID basic service set identification
CCA clear channel assessment
CDMA code division multiple access
CF contention free
CFP contention-free period
CID connection identifier
CP contention period
CRC cyclic redundancy code
CS carrier sense
CSMA Carrier Sense Multiple Access
CSMA C/A carrier sense multiple access collision avoidance
CSMA C/D carrier sense multiple access collision detectance
CTS clear to send
CW contention window
DA destination address
DBPSK differential binary phase shift keying
DCE data communication equipment
DCF distributed coordination function
DCLA direct current level adjustment
DIFS distributed (coordination function) interframe space
DLL data link layer
Dp desensitization
DQPSK differential quadrature phase shift keying
DS distribution system
DSAP destination service access point
DSM distribution system medium
DSS distribution system service
DSSS direct sequence spread spectrum
DTIM delivery traffic indication message
ED energy detection
EIFS extended interframe space
EIRP equivalent isotropically radiated power
ERS extended rate set
ESA extended service area
ESS extended service set
FC frame control

FCS frame check sequence
FDMA frequency division multiple access
FEC Forward Error Correction
FER frame error ratio
FH frequency hopping
FHSS frequency-hopping spread spectrum
FIFO first in first out
GFSK Gaussian frequency shift keying
IBSS independent basic service set
ICV integrity check value
IDU interface data unit
IFS interframe space
IMp intermodulation protection
IR infrared
ISM industrial, scientific, and medical
IV initialization vector
LAN local area network
LME layer management entity
LRC long retry count
lsb least significant bit
LLC logical link control
MAC medium access control
MDF management-defined field
MIB management information base
MLME MAC sublayer management entity
MMPDU MAC management protocol data unit
MPDU MAC protocol data unit
msb most significant bit
MSDU MAC service data unit
N/A not applicable
NAV network allocation vector
NIC network interface cards
OSI open systems interconnection
PAN personal area network
PC point coordinator
PCF point coordination function
PDU protocol data unit
PHY physical (layer)
PHY-SAP physical layer service access point
PIFS point (coordination function) interframe space
PLCP physical layer convergence protocol
PLME physical layer management entity
PMD physical medium dependent
PMD-SAP physical medium dependent service access point
PN pseudo-noise (code sequence)
PPDU PLCP protocol data unit
ppm parts per million

PPM pulse position modulation
PRNG pseudo-random number generator
PS power save (mode)
PSDU PLCP SDU
RA receiver address
RADIUS remote authentification dial in user service
RF radio frequency
RSSI received signal strength indication
RTS request to send
RX receive or receiver
SA source address
SAP service access point
SDU service data unit
SFD start frame delimiter
SIFS short interframe space
Slot de tiempo Ranura de tiempo
SLRC station long retry count
SME station management entity
SMT station management
SQ signal quality (PN code correlation strength)
SRC short retry count
SS station service
SSAP source service access point
SSID service set identifier
SSRC station short retry count
STA station
TA transmitter address
TBTT target beacon transmission time
TDMA Time Division Multiple Access
TIM traffic indication map
TSF timing synchronization function
TU time unit
TX transmit or transmitter
TXE transmit enable
UCT unconditional transition
WAN wide area network
WAN wide area network
WDM wireless distribution media
WDS wireless distribution system
WEP wired equivalent privacy
WLAN wireless local area network
WM wireless medium