Universidad Nacional Autónoma de México

Facultad de Ingeniería

Comparación de los estándares IEEE 802.11 b y g.

Tesis que para obtener el título de

Ingeniero en Telecomunicaciones

Presenta:

Raúl Pulido Martínez.

Director de Tesis

Dr. Javier Gómez Castellanos.

Ciudad Universitaria, México, D. F.

Junio de 2006

Agradecimientos.

A mi madre, padre y abuelo (q.e.p.d.). Que me ayudaron, motivaron y sobre todo me mostraron la importancia de estudiar y siempre estuvieron cuando los necesité. A mis tíos Jaime y Raúl, así como a sus respectivas familias para quienes siempre me tomaron como a un hijo.

A Ana Elisa, Sergio, Carlos, Itiel, Eder y Paulina. A mis amigos de la facultad, con los que recorrí buena parte de mi carrera, Andrés, Enrique, Luís, Jordi, Hiromi, Jazmin, Jorge, Daniel, Cristian, Miguel Ángel, Everardo, Polo, Marcos Aurelio, Mauricio, Minerva, Sergio, Carlos, Alfredo, Oscar. A mis compañeros que conforman el laboratorio de redes y a todos mis demás amigos y amigas que me han acompañado durante toda mi educación, y que hicieron de la escuela un lugar agradable para estar.

A la UNAM, y a la Escuela Winston Churchill y a todos mis maestros, en especial a mi tutor de tesis el Doctor Javier Gómez, Dr. Víctor Rangel, Dr. Víctor García, Garduño, Dr. Miguel Moctezuma, Ing. Jesús Reyes, M.I. Raúl Lucido, Dr. Ismael Martínez, M.I. Lauro Santiago, Ing. Mario Ibarra, Ing. Juan Ocariz, Ing Pablo García, Dr. Neri Vela, y demás maestros que me mostraron el camino del conocimiento, y me enseñaron a poder aprender por mi cuenta, forzándome a dar lo mejor de mí para moldearme y prepararme para el mundo.

Al Ing Paco Sepúlveda y Arq Manuel García quienes me dieron la oportunidad de trabajar con ellos y haber sido pacientes durante el proceso de la elaboración de mi tesis.

Por último, siendo el más importante, a Dios, por darme la oportunidad de venir a este mundo, y proporcionarme las herramientas y oportunidades para poder llegar hasta aquí y continuar en este camino de vida e ir más lejos.

Índice

1. Capítulo 1 8
   1.1. Introducción. 8
   1.2. WLAN 8
      1.2.1. Wi-Fi 8
      1.2.2. Características principales 9
      1.2.3. Funcionamiento 9
      1.2.4. Configuraciones 10
      1.2.5. Seguridad 12
   1.3. Antecedentes e historia 13
      1.3.1. Sistemas inalámbricos de adquisición de datos. 14
      1.3.2. La migración a 2.4 GHz. 14
   1.4. Alcances en un futuro, Las redes inalámbricas en el siglo XXI 15
      1.4.1. Una visión personal 15
2. Capítulo 2 17
   2.1. El estándar IEEE 802.11 17
   2.2. La IR PHY 17
   2.3. Conceptos Básicos de la capa PHY 18
   2.4. Tipos de modulación de la capa PHY 19
   2.5. FHSS WLANs. 20
      2.5.1. PHSS PLCP 21
      2.5.2. Modulación FHSS PMD-GFSK 22
   2.6. DSSS WLAN 23
      2.6.1. 802.11 DSSS 24
   2.7. Las bases de DSSS 25
   2.8. 802.11b WLAN 27
      2.8.1. 802.11b HR-DSSS PLCP 27
   2.9. 802.11a WLANs 28
   2.10. 802.11a OFDM PLCP 29
      2.10.1. Bases del OFDM 30
   2.11. 802.11a OFDM PMD. 32
   2.12. 802.11j WLAN 33
   2.13. 802.11g WLAN 33
   2.14. 802.11g PLCP 34
      2.14.1. ERP-OFDM 35
      2.14.2. ERP-PBCC 35
      2.14.3. La interoperabilidad de las 802.11g y 802.11b 35
      2.14.4. CCA 35
   2.15. Modulación adaptiva 36
      2.15.1. En resumen. 37
3. Capítulo 3 38
   3.1. Retos del estándar 802.11. 38
      3.1.1. El problema de la estación oculta. 38
   3.2. La capa de enlace de datos. 38
      3.2.1. Frame 802.11 40
   3.3. Seguridad en las redes inalámbricas. 42
      3.3.1. Método 1: Filtrado de direcciones MAC 42

3.3.2. Método 2: Wired Equivalent Privacy (WEP) 43
3.3.3. Clave secreta..... 45
3.3.4. Método 3: Las VPN..... 46
3.3.5. Método 4: 802.1x..... 46
3.3.6. Método 5: WPA (WI-FI Protected Access)..... 50
3.4. ¿Qué significa la sopa de letras de estándares 802.11?..... 50
3.4.1. 802.11c..... 50
3.4.2. 802.11e..... 51
3.4.3. 802.11i..... 51
3.4.4. 802.11d..... 51
3.4.5. 802.11f..... 51
3.4.6. 802.11h..... 51
4. Capítulo 4..... 52
4.1. ¿Cuántas redes hay en el edificio Valdez Vallejo? 52
4.2. Evaluación..... 54
4.3. Elección de los parámetros a analizar..... 55
4.3.1. Iwconfig 55
4.3.2. Ifconfig..... 58
4.3.3. Resultados:..... 62
4.4. Colisiones..... 69
4.5. Nivel de la señal..... 70
4.5.1. Nivel de señal y thoughput..... 72
4.6. Transiciones de velocidades..... 73
4.7. Análisis por segundo..... 74
5. Capítulo 5..... 77
5.1. Análisis y Conclusiones..... 77
5.1.1. Resultados obtenidos: 77
5.1.3. Trabajos Futuros..... 78
5.1.4. 802.11a..... 78
5.1.5. El futuro 79
5.2. Comparativa:..... 80
5.3. Epílogo..... 81
6. Apéndices y Anexos..... 83
6.1. Glosario..... 83
6.2. Cómo generar las graficas en CivilCad, una mejora de Autocad..... 85
6.3. Localización de los puntos de pruebas 88
6.4. Atenuaciones e Interferencias..... 90
6.5. Especificaciones técnicas. 91
7. Bibliografía y referencias..... 95

Índice de Figuras.

Figura 1-1 Comunicación Peer-to-Peer o ad hoc 10
Figura 1-2 Cliente a AP 11
Figura 1-3 Configuración de una red con AP y EP 12
Figura 1-4 WLAN con antenas direccionales 12
Figura 1-5 AP en Nueva York en el 2004 16
Figura 2-1 Subcapas en el modelo de referencia OSI 18
Figura 2-2 Diagrama de estados del PLCP 19
Figura 2-3 Gráfica del salto en Frecuencia 20
Figura 2-4 FHSS PPDU 21
Figura 2-5 FHSS Scrambled PSDU 22
Figura 2-6 Dominio de la frecuencia de FSK 23
Figura 2-7 Canalización con DSSS 24
Figura 2-8 802.11 DSSS PPDU 24
Figura 2-9 Expansión de un bit con valor de 1 26
Figura 2-10 Expansión de un bit con valor de 0 26
Figura 2-11 PPDU corto de HR-DSSS 28
Figura 2-12 Formato del Frame PPDU 802.11a 29
Figura 2-13 Modulación OFDM 31
Figura 2-14 Formación del prefijo para el ciclo OFDM 32
Figura 2-15 Diagrama de bloques de un transmisor OFDM para 802.11a 32
Figura 2-16 Formato del PPDU largo y corto para CCK-OFDM 35
Figura 3-1 Problema de la estación oculta 38
Figura 3-2 El protocolo MAC 802.11 39
Figura 3-3 Frame 802.11 40
Figura 3-4 Estados de una estación de acuerdo a su relación con el AP 42
Figura 3-5 Funcionamiento del algoritmo WEP en modalidad de cifrado 44
Figura 3-6 Funcionamiento del algoritmo WEP en modalidad de descifrado. 45
Figura 3-7 Estructura de una VPN para acceso inalámbrico seguro 46
Figura 3-8 Arquitectura de un sistema de autentificación 802.1x 47
Figura 3-9 Diálogo EAPOL RADIUS 48
Figura 4-1 Tercera planta edificio Valdez Vallejo 60
Figura 4-2 Velocidades del AP 802.11b 62
Figura 4-3 Velocidades del AP 802.11g 63
Figura 4-4 Errores en 802.11b 67
Figura 4-5 Errores en 802.11g 67
Figura 4-6 Colisiones en 802.11b 70
Figura 4-7 Fuerza de la señal en 802.11b 71
Figura 4-8 Fuerza de la señal en 802.11g 72
Figura 4-9 Niveles de señal vs Throughput 73
Figura 4-10 Correlaciones entre Signal Level y Throughput 73
Figura 4-11 Análisis por segundo y cada 20 segundos 75

Figura 4-12 Cambios de nivel de señal en un mismo punto..... 75
Figura 4-13 Cambio de throughput en un mismo punto 76
Figura 6-1 Importar puntos..... 85
Figura 6-2 Triangulación entre puntos XYZ..... 86
Figura 6-3 Caja de diálogo de las curvas de nivel. 86
Figura 6-4 Curvas de nivel 87

Índice de Tablas.

Tabla 1 Patrón de salto. 21
Tabla 2 Filtro Gausiano 23
Tabla 3 Subcampo señal..... 25
Tabla 4 Subcampo señal. 27
Tabla 5 Subcampo servicio. 28
Tabla 6 Subcampo tasa de transmisión. 29
Tabla 7 Velocidades de datos. 33
Tabla 8 Tipo de modulación. 33
Tabla 9 Preámbulo de PPDU 34
Tabla 10 Preámbulo largo. 34
Tabla 11 Modulación adaptiva..... 36
Tabla 12 Características. 37
Tabla 13 Redes en el Valdez Vallejo..... 54
Tabla 14 Parámetros a medir 55
Tabla 15 Tasa de transmisión vs Througput en 802.11b 64
Tabla 16 Tasa de transmisión vs Througput en 802.11g 66
Tabla 17 Comparación de errores..... 69
Tabla 18 Transiciones en 802.11b 74
Tabla 19 Transiciones en 802.11g 74
Tabla 20 Comparativo de WECA 80

Presentación

Objetivo de la propuesta:

Con el paso del tiempo las redes inalámbricas han cobrado mayor importancia en el desarrollo de la vida diaria de las personas debido, principalmente, a la necesidad de estar comunicado desde cualquier lugar sin las limitantes de las conexiones alámbricas.

En este trabajo se hará una evaluación de las ventajas y desventajas que ofrecen los estándares 802.11b y 802.11g. Además se hará una revisión de los estándares 802.11 restantes con la finalidad de analizar sus posibilidades de aplicación en un futuro cercano.

Definición del problema

La *IEEE* ofrece varios estándares para redes locales inalámbricas. Esta tesis evaluará su desempeño y características de funcionamiento en un ambiente real de trabajo. Se espera que los resultados permitan evaluar y comparar dichos estándares para, finalmente, revisar el cumplimiento de sus especificaciones técnicas.

Método:

En el campo de prueba, el tercer piso del edificio Valdez Vallejo ubicado en la Facultad de Ingeniería de la UNAM, se realizará un mapeo del piso y se evaluará el comportamiento de los diferentes parámetros de la red, como la tasa de errores (BER), el radio de la señal a ruido y la velocidad de transmisión de datos, entre otros.

En primer lugar se obtendrá el plano del campo de prueba, se designarán los lugares para hacer el mapeo de los parámetros seleccionados de la red y finalmente se tomarán mediciones para conocer el número de veces que se realiza una transición de velocidad dentro de una misma sesión, con el fin de valorar la movilidad de dicha red.

Las mediciones se realizarán con herramientas que corren bajo el sistema operativo Linux, ya que ofrece mayor flexibilidad que Windows para la toma y procesamiento de la información.

Resultados esperados:

- Contar con un mayor conocimiento acerca del funcionamiento de las redes inalámbricas.
- Tener una caracterización de los estándares 802.11b y 802.11g en un ambiente real de trabajo.
- Determinar cuál es el estándar más conveniente para las diversas necesidades de funcionamiento de un ambiente real de trabajo.

1. Capítulo 1

En este capítulo se hará una revisión general de las redes inalámbricas que responden a las preguntas qué son las redes *WLAN,* cuáles es la perspectiva actual de las redes inalámbricas, cuáles son sus alcances para el futuro, etc.

1.1. Introducción.

En el pasado, la única manera de conectarse a las redes de comunicación era a través de cables. Ante la necesidad de desarrollar redes con mayor flexibilidad se realizaron investigaciones sobre posibles formas inalámbricas para la transmisión de datos, gracias a las cuales se llegó a la creación de estándares como el 802.11, desarrollado por la IEEE, que será tratado posteriormente con mayor detalle.

Utilizar sistemas basados en radio para transmitir datos a través del aire tiene ventajas como son el tener mayor movilidad, es decir, estar conectado en cualquier parte sin tener la limitante física del cable; su instalación es más sencilla ya que no requiere de ranuras y canaletas en las paredes y permite un entorno más estético en lugares como restaurantes, cafés y hogares. Sin embargo, también hay desventajas que deben considerarse.

En los últimos años se han desarrollado los dispositivos móviles (Laptops, PDA, etc.) así como las redes inalámbricas para diversas aplicaciones como el Bluetooth que se usa para distancias cortas, el Wi-Fi para distancias medias, el Wi-Max para redes metropolitanas y, para distancias muy grandes, redes satelitales. En esta tesis nos ocuparemos de analizar las WLAN.

1.2. WLAN

WLAN (*Wireless Local Area Network*) es un sistema de comunicación de datos inalámbrico flexible, frecuentemente utilizado como alternativa a las redes LAN cableadas o como una extensión de ésta. Utiliza tecnología de radiofrecuencia que permite a los usuarios una mayor movilidad ya que reduce el número de conexiones cableadas.

Las WLAN han ido adquiriendo importancia en los distintos campos de la industria que requieren una transmisión de información en tiempo real a una terminal central, como en manejo de almacenes, inventarios y manufacturación. También son muy populares en hogares, oficinas, aeropuertos, parques, ya que permite compartir un acceso a Internet entre varias computadoras.

1.2.1. Wi-Fi

Wi-Fi, es el acrónimo de *Wireless Fidelity*, un conjunto de estándares para redes inalámbricas WLAN, basado en las especificaciones IEEE 802.11.

Wi-Fi es una marca de la Wi-Fi Alliance, antes conocida como Wireless Ethernet Compatibility Alliance (WECA), organización comercial que prueba y certifica que los equipos cumplan los estándares IEEE 802.11x.

Wi-Fi alliance tiene como misión, certificar la interoperatividad y compatibilidad entre diferentes fabricantes de productos wireless bajo los estándares IEEE 802.11.

La WECA fue fundada por 3Com, Cisco, Intersil, Agere, Nokia y Symbol en agosto de 1999, bajo el compromiso de impulsar a nivel mundial la tecnología LAN inalámbrica bajo el estándar IEEE 802.11b. La lista de miembros se ha incrementado a más de doscientos.

WECA establece un procedimiento de certificación para garantizar la interoperatividad de los dispositivos entre fabricantes. Los productos que cuentan con el logo Wi-Fi, que actualmente suman más de dos mil, gozan de una garantía de interoperatividad.

1.2.2. Características principales

- Movilidad: permite transmitir información en tiempo real desde cualquier lugar de la organización, empresa, casa o negocio a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.
- Facilidad de instalación: al no requerir cables se evitan las obras civiles, lo cual proporciona un mejor aspecto, habitabilidad de los locales y reduce tiempos de instalación. El acceso es casi instantáneo, ya que el usuario sólo necesita el permiso para hacer uso de la red.
- Flexibilidad: las redes inalámbricas llegan donde el cable no puede, superando mayor número de obstáculos. Así, es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, plazas, parques de diversiones, reservas ecológicas, etc.

1.2.3. Funcionamiento

En el Punto de Acceso (*AP, Access Point*) WiFi se utilizan ondas de radio para llevar información de un punto a otro usando distintos tipos de modulación, sin necesidad de un medio físico guiado.

Si las ondas son transmitidas a distintas frecuencias de radio, pueden existir varias portadoras en igual tiempo y espacio sin que haya interferencia entre ellas. Para extraer los datos, el receptor se sitúa en la frecuencia portadora, ignorando las demás. En una configuración típica de WLAN, los puntos de acceso AP son los transductores de una red cableada a una inalámbrica. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de veinte metros hasta cientos de metros con antenas direccionales.

El punto de acceso es normalmente colocado en un lugar alto como el techo, pero podría colocarse en cualquier lugar si se obtiene la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores, quienes proporcionan una interfaz entre el sistema de operación de red del cliente (*NOS: Network Operating System*) y las ondas, mediante una antena.

La naturaleza de la conexión sin cable es transparente a las capa superiores del modelo OSI, después de la capa MAC.

1.2.4. Configuraciones

Existen configuraciones tan simples o complejas como se quiera. La más básica, es la llamada *Peer-to-Peer* o *ad hoc que* consiste en dos dispositivos equipados con tarjetas inalámbricas, donde sólo es necesario que ambos reciban suficiente señal de la otra tarjeta, y cada cliente tiene acceso a los recursos del otro. Este tipo de red ha sido bien acogida entre los dispositivos de juego.

Figura 1-1 Comunicación Peer-to-Peer o ad hoc

El BSS *(Basic Service Set*) está conformado por una agrupación de estaciones que se comunican entre sí. Un BSS es identificado con un BSSID (*Basic Service Set Identifier*), el cual es compartido por todas las estaciones que pertenecen a la agrupación.

Instalando un Punto de Acceso (AP) se puede duplicar el alcance al cuál los dispositivos pueden comunicarse, ya que el dispositivo se comunica con el AP y viceversa. El AP se puede conectar a una red cableada, actuar como mediador en el tráfico de la red y servir a varios clientes (que normalmente el límite es de cincuenta).

Figura 1-2 Cliente a AP

Los AP tienen un alcance finito y, como veremos en los experimentos, puede variar de gran manera según el lugar de uso. En zonas grandes es necesario usar más de un AP si se quiere una cobertura total. El objetivo es que el cliente se pueda mover sin perder conexión (*roaming*), lo cual consiste en que al moverse el usuario cambie de AP sin perder la conexión a la red.

Para resolver los problemas de cobertura, se pueden usar puntos de extensión EP con el fin de aumentar el número de puntos de acceso a la red, de modo que funcionan como AP pero no están cableados a la red externa. Los EP extienden la cobertura de la red retransmitiendo las señales de un cliente a un AP, o bien, a otro EP. También pueden encadenarse para pasar mensajes entre un AP y clientes lejanos de modo que se construye un "puente" entre ambos.

Figura 1-3 Configuración de una red con AP y EP

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: si se quiere una WLAN a otro edificio a 1Km de distancia, una solución puede ser instalar una antena direccional en cada edificio con línea de vista entre ellas. La antena del primer edificio está conectada a la red cableada mediante un AP, igualmente en el segundo edificio se conecta un AP, y se obtiene una conexión sin cable entre ambos.

Figura 1-4 WLAN con antenas direccionales

1.2.5. Seguridad

Uno de los problemas de este tipo de redes es que si no se tienen medidas de seguridad adecuadas, cualquier persona con una terminal inalámbrica podría comunicarse con un punto de acceso privado o escuchar una conversación. Dichas medidas van encaminadas en dos sentidos:

- El cifrado o encriptación de los datos que se transmiten. Tópico en el cual se están realizando diversas investigaciones, ya que se ha conseguido desencriptar los sistemas considerados inicialmente.
- La autentificación entre los diversos usuarios de la red. Se ha tomado como base el protocolo de verificación EAP (*Extesible Authentication Protocol*), que es bastante flexible y permite el uso de diferentes algoritmos de autenticación.

1.3. Antecedentes e historia

Aunque las WLAN se conoce como una tecnología de redes, no debemos olvidar que se tata de una tecnología de radio, por tanto su historia se remonta más de un siglo atrás.

Así como la tecnología de radiodifusión es el fundamento de LAN inalámbrica,del mismo modo, los primeros trabajos en electromagnética representan los fundamentos de la radio. El teórico escocés James Clerk Maxwell impulsó por primera vez la noción de las ondas electromagnéticas en 1864 al postular que éstas provienen de un cambio en la dirección de la energía eléctrica.

Basándose en esto, el alemán Heinrich Hertz desarrolló, en la década de 1880, un equipo que envió y recibió ondas electromagnéticas a través del aire. Este equipo era capaz de incrementar el número de ondas que se producían en un periodo determinado, así como su frecuencia y su velocidad de cambio u oscilación.

Guglielmo Marconi tomó estos primeros trabajos para crear una aplicación práctica. Aunque su nombre siempre estará vinculado con el de la radio, la primera aplicación fue pionera de la transmisión de datos. Después Marconi sintetizo su trabajo con el de Samuel Morse, ganando cada vez mas alcance. Obtuvo su primera patente en 1896 y después fundó la Wireless Telegraph and Signal Company Limited. Hacia 1898 el equipo telegráfico de Marconi se usaba para las comunicaciones entre barcos y tierra firme, después entre Francia e Inglaterra y más tarde a través del Océano Atlántico.

Thomas Edison estuvo detrás de los primeros sistemas inalámbricos que se desplegaron en Estados Unidos, cuestión que lo llevo a crear General Electric, donde trabajó con Nicola Tesla, quien después fue reconocido como uno de los inventores de la radio.

Toda la teoría fue llevada a la práctica en menos de una década, desde la comprobación del concepto hasta la comercialización en forma de una compañía multinacional. Marconi y otras personas como David Sarnoff, Alexande Popov, Lee De Forest y Reginald Fessenden, realizaron avances adicionales que marcaron el inicio de la época dorada de la radio.

En 1923 el gobierno americano tuvo que dividir las frecuencias para 11 años mas tarde crear la FCC.

Hedy Lamarr – nativa de Austria - era una estrella de cine muy conocida, que poseía un intelecto agudo y una repulsión hacia los nazis, contrajo nupcias con un traficante de armas de su país natal, con lo cual obtuvo experiencia que le ayudo a formar ideas para la innovación de la radio en Europa. Junto con George Antheil, un prestigiado compositor, crearon un sistema para emitir comunicaciones de radio de banda angosta a través de una banda ancha en el espectro de frecuencia. Lo cual se usaría para guiar torpedos hacia sus blancos de una manera que fuera menos susceptible a la técnica de obstrucción de frecuencias o al espionaje. Esto se realizó logrando que la frecuencia utilizada para comunicarse se cambiara de un canal al siguiente siguiendo un modelo predeterminado y coordinado. Lo cual forzaba a bloquear todo el espectro o a conocer el patrón de saltos para bloquear

la comunicación. La patente resultante, fue premiada el 11 de agosto de 1942, fue el primer sistema de espectro extendido, el número de saltos de estos eran 88, el número de teclas del piano.

No obstante que las transmisiones eran ideales para propósitos militares, también lo eran para el uso privado sin licencia. El espectro es una tecnología muy útil y accesible que puede tener un máximo aprovechamiento.

1.3.1. Sistemas inalámbricos de adquisición de datos.

Los primeros sistemas que realmente mostraron semejanzas con las LAN inalámbricas actuales aparecieron en 1981 por la necesidad de recorrer sin cable los puntos de venta y almacenamiento y no tener que esperar hasta el final de la jornada para conocer la información.

Los precursores de las WLAN eran sistemas de comunicación punto a multipunto, los usuarios no competían, por el contrario, compartían el espectro, basándose en el sistema remoto de área amplia ALOHANET, el cual no es sólo el precursor de las LAN inalámbricas, sino que también es la base de la tecnología de área local cableada predominante Ethernet.

En 1985 cambia la regulación en la parte 15 de la FCC, quedando el uso del espectro extendido para aplicaciones comerciales. En este mismo año los sistemas de adquisición de datos integraron el radio a la terminal.

En 1988 fue introducido al mercado el primer sistema comercial basado en la tecnología Secuencia Directa en el espectro extendido DSSS, estos sistemas operaban en banda de los 900 MHz que no requerían licencia para su uso. Debido a su cercanía con la banda de los celulares americanos se pudieron usar los mismos componentes. Estos sistemas de DSSS que no requerían de licencias fueron el blanco de aplicaciones diversas lo que ayudo a desarrollar las redes inalámbricas.

1.3.2. La migración a 2.4 GHz.

No obstante que la operación de la banda de 900 MHz se proporcionó para infraestructura común en Australia, Canadá y USA, estaba limitada solo a estos países. Al reunirse diversos representantes de las partes interesadas como Telxon, NCR, Proxim Technology y Symbol Technologies, emitieron una solicitud de autorización de proyecto al IEEE, a fin de que se creara un estándar de interoperabilidad para las LAN inalámbricas. Puesto que el IEEE es un comité internacional se inclina el grupo recién creado por la banda de los 2.4 GHz y rechaza la de los 900 MHz.

1.4. Alcances en un futuro, Las redes inalámbricas en el siglo XXI

Es difícil predecir un futuro ya que, en este mar de cambios, se dan a conocer inventos todos los días: computadoras que son más rápidas y cuentan con más memoria, celulares más poderosos que las PDA recientes e incluso que las Laptop de pocos años atrás. En este mundo tan cambiante es difícil saber qué le espera a esta tecnología. Las redes WiFI seguirán evolucionando, actualmente en el mercado hay algunas que dicen ir a 108 Mbps, e irán aumentando en velocidad, pero también en densidad.

Hoy en día el crecimiento de la banda ancha en los hogares y oficinas, nos es nada despreciable en las principales ciudades, aunque en nuestro país no ha sido tan grande como se esperaba. Por menos de 100 dólares uno puede instalar su red inalámbrica, evitándose los problemas de cablear, agujerear, ranurar superficies. Con la popularidad creciente de los dispositivos móviles que se conectan al Internet, resulta bastante conveniente y económico tener un AP en casa.

Antes, el conjunto de dispositivos móviles consistía solamente en Laptops con una autonomía de energía limitada y ausencia de tarjeta inalámbrica integrada. Ahora el conjunto consiste en:

- Laptops, con tarjeta de red inalámbrica integrada y más autonomía energética.
- Video juegos portátiles, como el PSP que traen integrado una tarjeta de red 802.11.
- Las PDA con tarjeta de red, o sus variantes de menor costo.
- Nuevos celulares como el Nokia 9500, listos para conectarse a la red inalámbrica local.
- Dispositivos para la automatización de la casa (Domótica).

Por todo lo anterior se vuelve más necesario tener nuestra propia WLAN. Desafortunadamente dicha demanda esta produciendo saturación en el espectro electromagnético, por la acumulación de redes inalámbricas instaladas, provocando en algunos casos su falla, situación que no se resolverá a menos que hagamos algo al respecto.

1.4.1. Una visión personal

Cuando hay tantas redes Wi-Fi, éstas terminan anulándose a sí mismas y dañan el funcionamiento de cualquier dispositivo portátil. Si lográramos un proyecto de Internet público en México, con la participación de todos, lograríamos un área de cobertura muy grande, que permitiría que todos accediéramos a éste servicio desde cualquier punto de la ciudad.

Además, podríamos hablar desde cualquier lugar por medio de la red de Internet, en vez de recurrir a la costosa red celular, con lo cual podríamos conectarnos en todo momento. Incluso se complementaría muy bien con las redes celulares de 3g que próximamente instalarán las compañías celulares y con las redes WIMAX; por lo que ninguna red sustituiría a la otra, si no que por el contrario, cada una tomaría su lugar en la red mundial, y se mantendrían disponibles permanentemente. Lo anterior ayudaría a pensar en una gran variedad de servicios y oportunidades de negocios que podrían crearse en unos años e incrementarían la productividad del país.

Como se observa en la figura 1-6, en Manhattan hay demasiadas redes 802.11. Si se unieran lograrían una gran cobertura; pero si todos cierran sus redes, éstas disminuirán su velocidad de transmisión y alcance.

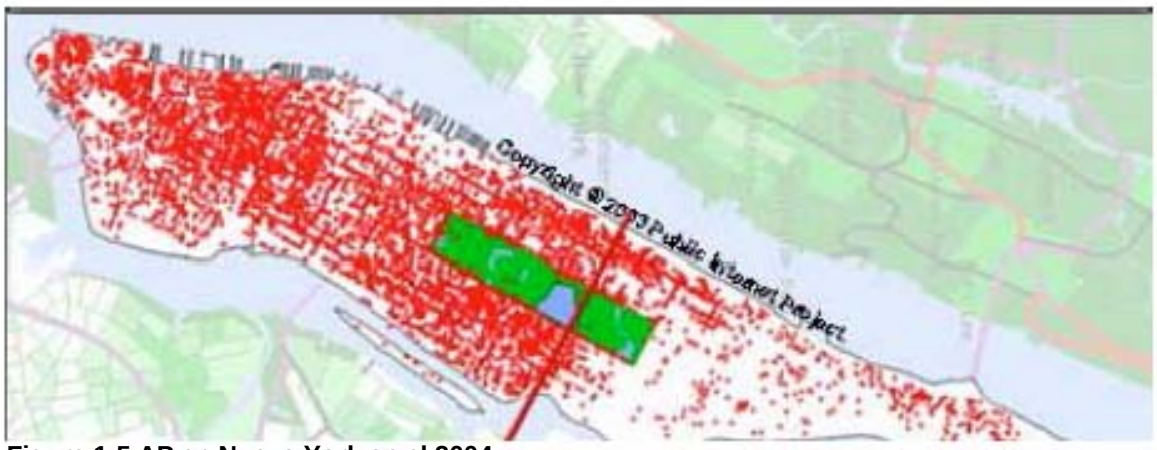


Figura 1-5 AP en Nueva York en el 2004

2. Capítulo 2

En esté capítulo se expone un poco de la historia de IEEE 802.11 y del modelo de referencia OSI, para identificar el tiempo en que se sitúa nuestro estándar por analizar. También contiene una explicación de la capa física con sus distintas variantes y modulaciones utilizadas.

2.1. El estándar IEEE 802.11

La ratificación en 1999 del 802.11a y 802.11b, transformó las redes inalámbricas, de ser una solución de código de barras pasó a una solución de acceso a redes portátil, barata y con Interoperabilidad.

La ausencia de cables en una conexión a red permite a sus usuarios tener la libertad de movimiento que no se tenía con las redes Ethernet. La estandarización y principalmente el uso de frecuencias sin licencia, debido a lo costoso y tardado que resulta obtenerlas, ha sido fundamental para su desarrollo. Finalmente ambos elementos han sido fundamentales para el rápido establecimiento de esta tecnología.

El estándar 802.11 define diferentes tecnologías de la capa física (PHY) para ser utilizados con la capa 802.11 MAC.

- El 802.11 2.4 GHz usa frequency hopping PHY.
- El 802.11 2.4 GHz usa direct sequencing PHY.
- El 802.11b 2.4 GHz usa direct sequencing PHY.
- El 802.11a 5 GHz usa Orthogonal Frequency Division Multiplexing (OFDM) PHY.
- El 802.11g 2.4 GHz usa extended rate physical (ERP) layer.

La capa física es el principal diferenciador de las variedades existentes de estándares.

2.2. La IR PHY

La capa IR PHY esta incluida en las especificaciones de las redes 802.11. La cual esta basada en los rayos infrarrojos (IR) en lugar de las ondas de radio. Esto implica ventajas en aspectos como, lo económico que resultan los puertos IR en comparación con los transmisores de radio.

IR es muy tolerante a la interferencia de RF ya que operan en frecuencias totalmente distintas. Además, debido a que los rayos infrarrojos no están regulados, no es necesario preocuparse por investigar y cumplir con las directivas de las distintas organizaciones alrededor del mundo.

La seguridad se centra en tener un control sobre los intentos no autorizados de acceso a la red. La luz puede ser confinada a un cuarto con sólo cerrar la puerta. Las redes basadas en IR pueden ofrecer algunas ventajas como flexibilidad y movilidad, pero con algunas deficiencias de seguridad. La principal dificultad de IR es que la dispersión de los techos disminuye el alcance y por consiguiente su rango es más corto.

Sin embargo, ningún producto ha sido creado con base en la IR PHY. Las laptops que cuentan con un puerto infrarrojo cumplen con el estándar IrDA pero no con el 802.11. Si algún día existen productos basados en la IR PHY, la capa MAC estará lista para comunicarse con ellos.

2.3. Conceptos Básicos de la capa PHY

El 802.11 PHY, esencialmente, provee un mecanismo de transmisión hacia la capa MAC, y soporta funciones adicionales como la identificación del estado inalámbrico y su notificación a la MAC.

El grupo 802.11 ha desarrollado avances en ambas capas manteniendo la interfase. La independencia entre la capa PHY y la capa MAC es lo que ha permitido la adición de estándares con mayor velocidad de datos, ya que se trata de la misma capa MAC.

La capa física 802.11 tiene 2 subcapas:

- PLCP, Physical Layer Convergence Procedure.
- PMD, Physical Medium Dependant.

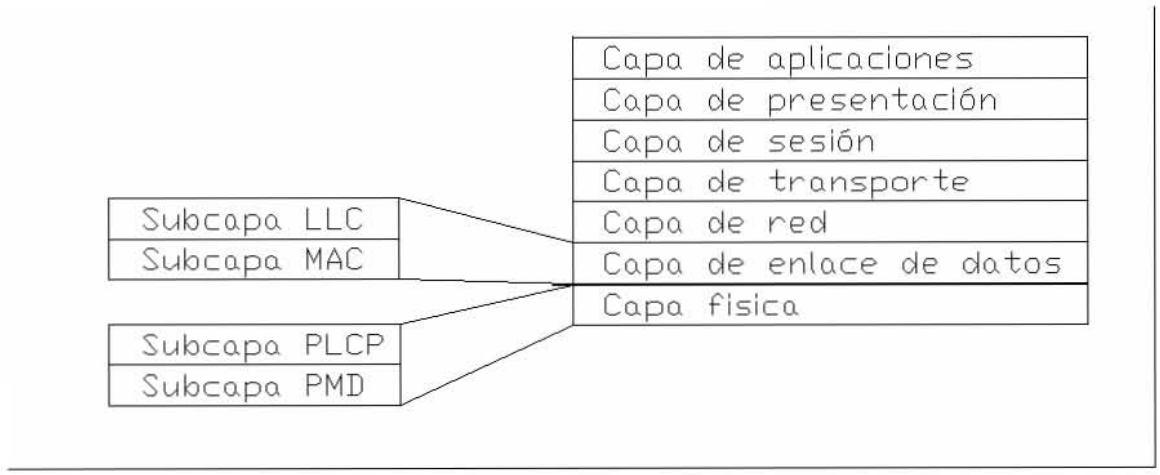


Figura 2-1 Subcapas en el modelo de referencia OSI

La PLCP es básicamente una capa de “hand shaken” que permite transferir unidades de datos del protocolo MAC (MPDUs) entre las estaciones MAC sobre la PMD, lo cual es el método de transmisión y recepción de datos a través de un medio inalámbrico. Se puede pensar en la PMD como una función de servicio de

transmisión interconectada a través de la PLCP. Las subcapas PLCP y PMD varían en los diferentes estándares 802.11.

Todas las PLCPs, sin importar el tipo de 802.11, tienen datos primitivos que proveen la interfase para transferir los octetos de datos entre la MAC y la PMD. Además cuentan con primitivas que le permiten a la MAC comunicarle a la PHY cuándo comenzar la transmisión y también, ser informada cuando la transmisión ha sido completada. Del lado del receptor, las primitivas PLCP de la PHY a la MAC le indican cuándo se debe iniciar la transmisión de otra estación y el momento en que la transmisión esta completa. Para soportar la función de asegurar el canal despejado (CCA), todas las PLCPs proveen el mecanismo para que la MAC resetee el mecanismo de PHY CCA y para que la PHY reporte el estatus actual del medio inalámbrico.

En general, las PLCPs operan de acuerdo al diagrama de estados que se muestra adelante (*figura 2-2).* Su estado de operación básico es el procedimiento del sensado de la portadora / aseguramiento de canal despejado (CS/CCA).

Este procedimiento detecta el comienzo de la señal de una estación diferente y determina cuándo el canal está vació para transmitir. Al recibir una solicitud de inicio de Tx se realiza la conversión al estado transmisor, el PMD cambia de recibir a transmitir, y se manda la unidad de datos del protocolo PLCP (PPDU). Entonces, se manda a Tx End y se regresa al estado CA/CCA. El PLCP invoca el estado "recibiendo" cuando el procedimiento CS/CCA detecta el preámbulo de la PLCP y una cabecera válida de PLCP. Si el PLCP detecta un error, se le indica a la MAC y se inicia el procedimiento de CS/CCA (Carrier Sense / Clear Channel Assessment).

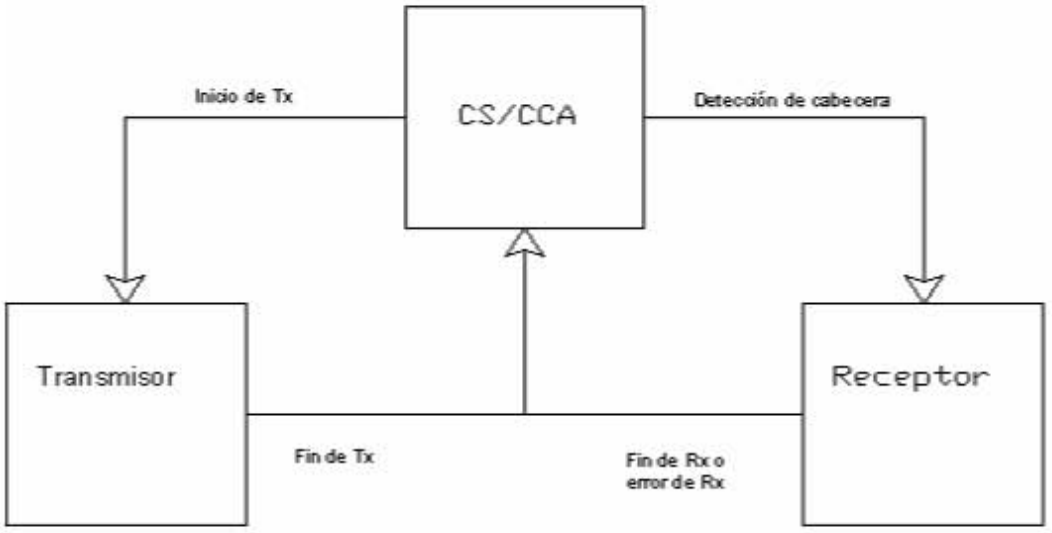


Figura 2-2 Diagrama de estados del PLCP

2.4. Tipos de modulación de la capa PHY

IEEE 802.11 señala dos posibles opciones para la elección de la capa física:

- 2.4 GHz frequency hopping spread spectrum (FHSS).
- 2.4 GHz direct sequence spread spectrum (DSSS).

Como se puede observar ambas operan en los 2.4 GHz, donde la FCC aloja los 82 MHz del espectro destinado en Estados Unidos a la banda para uso Industrial, Medico y Científico (ISM). Cada PHY tiene su propia subcapa PLCP y PMD.

2.5. FHSS WLANs.

FHSS WLANs (acrónimo de *Frequency hopping spread spectrum* / saltos de frecuencia de espectro disperso) soporta velocidades de datos de 1 y 2 Mbps. Como su nombre lo dice, es una técnica de modulación de espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia síncronamente con el transmisor (*figura 2-3*). Los dispositivos FHSS dividen el espectro en 79 canales independientes. Para Norteamérica y Europa de los 2.402 a los 2.480 GHz. Cada uno de los canales es de 1MHz de ancho, por lo que las FHSS WLAN usan un relativamente rápido símbolo de 1MHz y saltan alrededor de los 79 canales a una velocidad mucho mas baja.

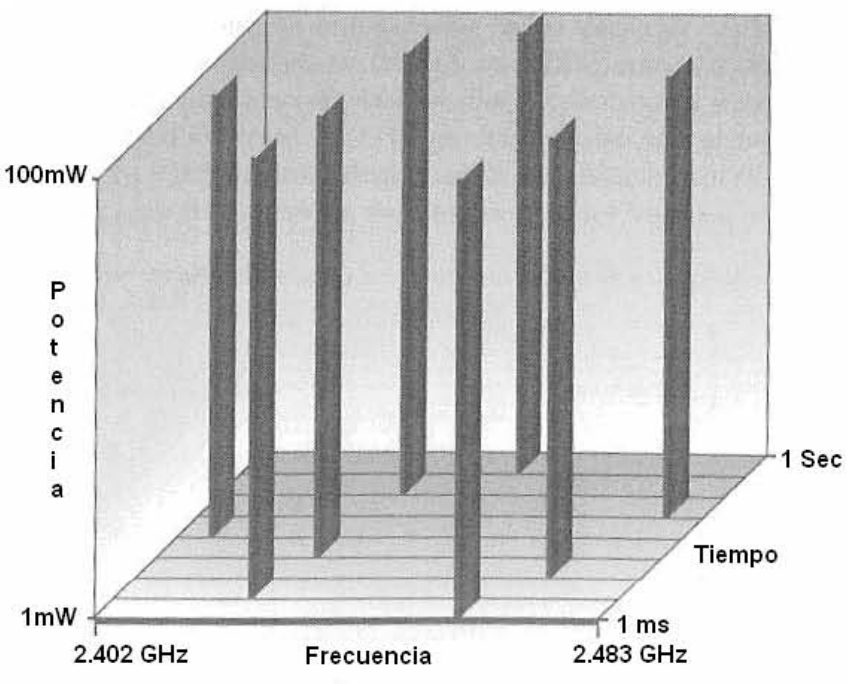


Figura 2-3 Gráfica del salto en Frecuencia

Es necesario que la secuencia de salto sea de al menos una tasa de 2.5 veces por segundo y deba contener un mínimo de seis canales (6 MHz). Para minimizar las colisiones entre las áreas traslapadas de cobertura, las posibles secuencias de

saltos pueden ser divididas en tres formas de saltos, 26 para Norte América y la mayoría de Europa, cabe hacer notar que es de 4 para Japón, 9 para España y 11 para Francia. Sólo se pondrá los patrones de salto más común para Norte América y la mayoría de Europa.

Config	*Patrón de salto*
1	*0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75.*
2	*1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61, 64, 67, 70, 73, 76.*
3	*2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 71, 72, 77.*

Tabla 1 Patrón de salto.

En esencia, los patrones de salto nos dan un camino, con al menos 6 MHz, para cuando se consideren sistemas multiceldas y así disminuir la probabilidad de colisión. El hecho de que en países como Japón, España y Francia se tenga una cadena mas corta se debe a que cuentan con la menor banda otorgada para aplicaciones ISM en los 2.4 GHz.

2.5.1. PHSS PLCP

Después de que la capa MAC pasa el frame MAC, también conocido como unidad de dato PLCP (PSDU), la subcapa PLCP aumenta dos campos al inicio de la transmisión para formar el frame PPDU. (*Figura 2-4*)

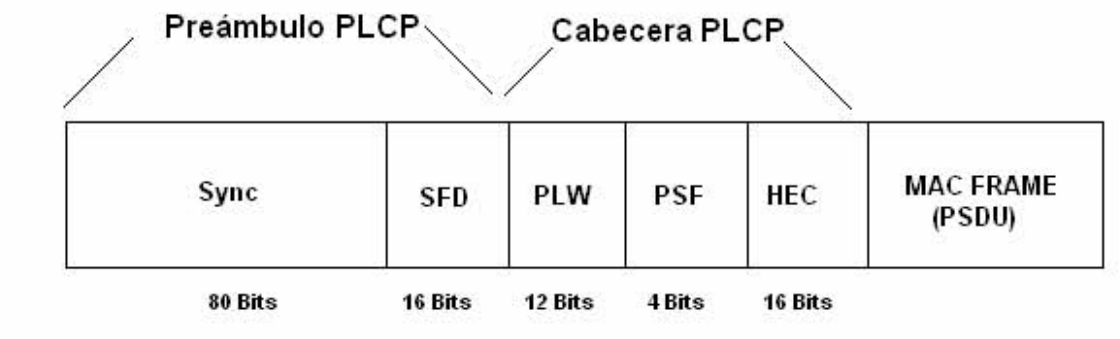


Figura 2-4 FHSS PPDU

El preámbulo de PLCP tiene dos subcampos:

- El subcampo de sincronización de 80 bits de longitud, que consiste en una cadena que alterna 0 y 1 empezando por el 0.
- El subcampo SFD (*Start Frame Delimiter*), es una cadena especifica de 16 bits de longitud (0000 1100 1011 1101) que le da el tiempo de inicio a la estación receptora.

La cabecera de PLCP contiene tres subcampos:

- El PLW (PSDU *Lenght Word*), de doce bits que nos da la longitud del campo MAC en octetos.
- El PSF (PLCP *Signal Field*), de cuatro bits de longitud que indica la velocidad de datos del frame.
- HEC (*Header Error Control*) Es un control de errores diseñado por la ITU-T para que, por medio del CRC-16, el transmisor genere la suma y el receptor la use para identificar errores en los datos recibidos del PLW y PSF.

El MAC Frame o PSDU pasa a un proceso llamado “scrambled”, que consiste en la inserción de bits de relleno cada 32 símbolos para acabar con cualquier problema de polarización o componente de corriente directa que afecte nuestros procesos sucesivos de modulación. (*Figura 2-5*)

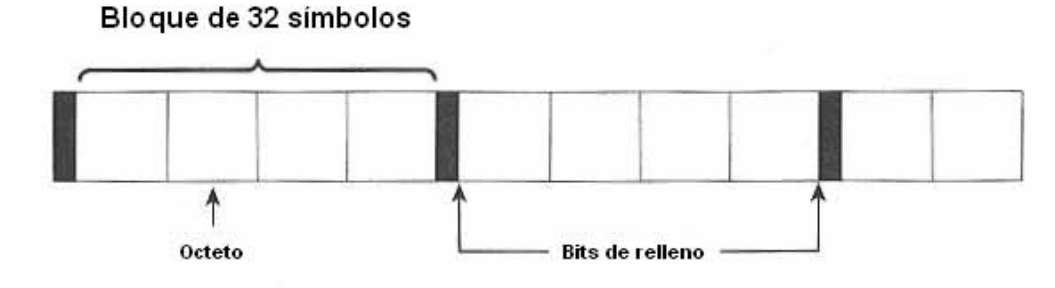


Figura 2-5 FHSS Scrambled PSDU

2.5.2. Modulación FHSS PMD-GFSK

El PLCP convierte el *frame* en una cadena de datos binarios que pasan a la capa PMD, la subcapa FHSS PMD modula esta cadena de datos usando GFSK (*Gaussian frequency shift keying*). En este punto es preciso recordar que FSK representa cada símbolo con una frecuencia distinta, por ejemplo:

Para 0 un valor de f1

Para 1 un valor de f2

Normalmente no se transmiten en frecuencia absoluta, más bien, se hacen relativas a una frecuencia portadora. (*Figura 2-6*)

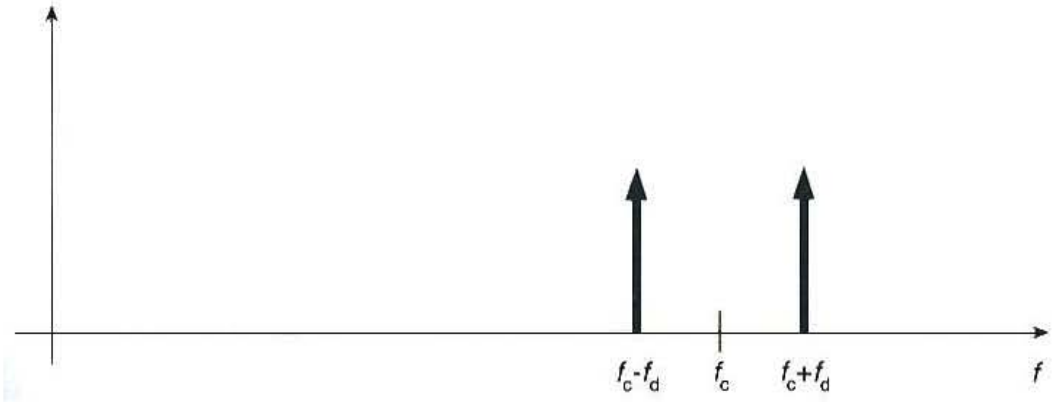


Figura 2-6 Dominio de la frecuencia de FSK

Donde:

F1=fc-fd

F2=fc+fd

Para GFSK se utiliza un filtro Gausiano. El estándar 802.11 especifica que debe ser de al menos110 kHz la frecuencia de desviación (fd). Para usar 2Mbps se usa 4GFSK porque modula dos bits al mismo tiempo, usando dos desviaciones de frecuencia.

Símbolo	*Frecuencia*
10	*fc+fd2*
11	*fc+fd1*
01	*fc+fd1*
00	*fc+fd2*

Tabla 2 Filtro Gausiano

2.6. DSSS WLAN

DSSS (acrónimo de *Direct Sequence Spread Spectrum* / Secuencia directa de espectro disperso), que consiste en otra de las especificaciones de la capa física 802.11. Como fue definida en 1997, la DSSS soportaba tasas de 1 y 2 Mbps. En 1999, el grupo de trabajo ratificó el estándar 802.11b para soportar tasas de 5.5 y 11 Mbps.

DSSS WLANs, usa canales de 22 MHz, permitiendo a varias WLANs operar en la misma área de cobertura. En Norte América y la mayor parte de Europa esto permite tres canales que no se empalman en el rango de frecuencia de los 2.4 a los 2.483 GHz. (*Figura 2-7*)

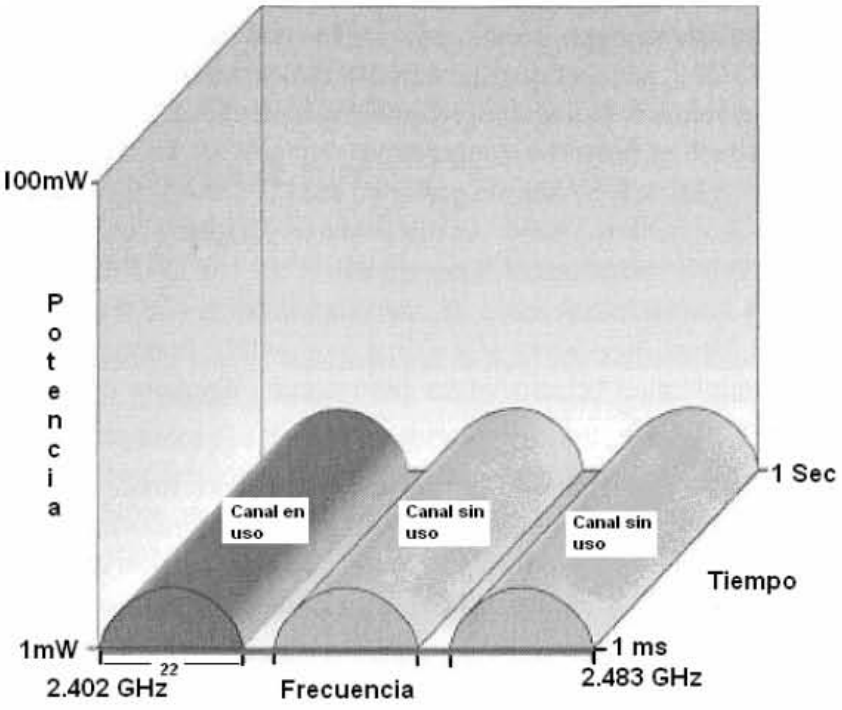


Figura 2-7 Canalización con DSSS

2.6.1. 802.11 DSSS

Al igual que la subcapa PLCP de FHSS, la PLCP de 802.11 DSSS adiciona dos campos al *frame* MAC para formar el PPDU, el preámbulo y el encabezado. (*Figura 2-8*)

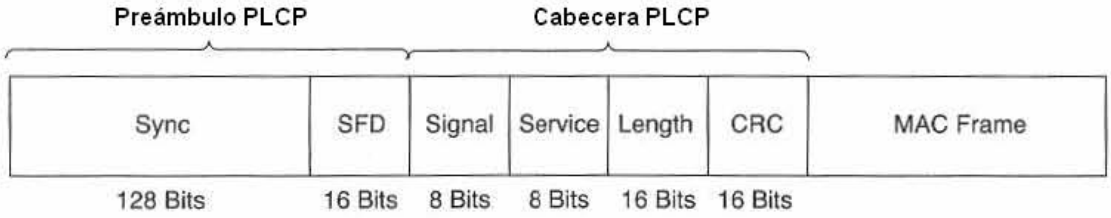


Figura 2-8 802.11 DSSS PPDU

El preámbulo PLCP contiene dos subcampos:

- SYNC: subcampo de sincronización que consiste en una cadena de 128 bits de unos.
- SFD: es una cadena específica 0xF3A0 de 16 bits de longitud, para proveer el tiempo a la estación receptora.

La cabecera de PLCP contiene cuatro subcampos:

- Señal: tiene una longitud de 8 bits y especifica la modulación y tasa de transmisión.

Señal	*Tasa de transmisión*
0x0A	*1 Mbps*
0x14	*2 Mbps*

Tabla 3 Subcampo señal

- Servicio: tiene 8 bits de longitud y es un campo reservado para futuras adecuaciones.
- Longitud: este subcampo de 16 bits de longitud, contiene el número de microsegundos en un rango de $2^{16} – 1$, requerido para transmitir la porción del MAC.
- El CRC: con 16 bits, esta encargado de efectuar la suma para que el receptor verifique si llegó bien la información.

El PLCP convierte el *frame* en una secuencia de bits que pasa a la capa PMD. El preámbulo siempre se transmite a 1 Mbps y el resto a la velocidad asignada en el subcampo de Señal.

- Se usa DBPSL (*Differential binary phase shift keying*) para una operación a 1 Mbps.
- Se usa DQPSK (*Differential quadrature phase shift keying*) para una operación a 2 Mbps.

2.7. Las bases de DSSS

La técnica del espectro disperso emplea una modulación que requiere una mayor cantidad de ancho de banda del espectro, que el necesario para comunicar la información a una tasa de transmisión mucho más baja. Cada bit es remplazado o extendido por un código de expandimiento, como si se codificara. Debido a que la información es extendida en muchos bits de información, se tiene la ventaja de poder operar con una condición muy baja de relación de señal a ruido (SNR), aceptar interferencia y baja potencia de transmisión.

Con DSSS la señal transmitida es multiplicada por una secuencia de expansión, que conocen tanto el transmisor como el receptor. WLAN DSSS codifica la información, toma una cadena de datos de 1 Mbps de la capa de comunicación de estos y la convierte en un “chip” de 11 MHz.

La secuencia de expansión de chipping o de Barrer convierte los bits de datos en “chips”, cada uno de 11 bits con valor de uno: (*Figura 2-9*)

- Un 1 se convierte en 11111111111
- Un 0 se convierte en 00000000000

Así, al bit expandido se le aplica una operación XOR con la secuencia de extendido, dando como resultado “chips” que son mapeados a símbolos modulados. (*Figura 2-10*)

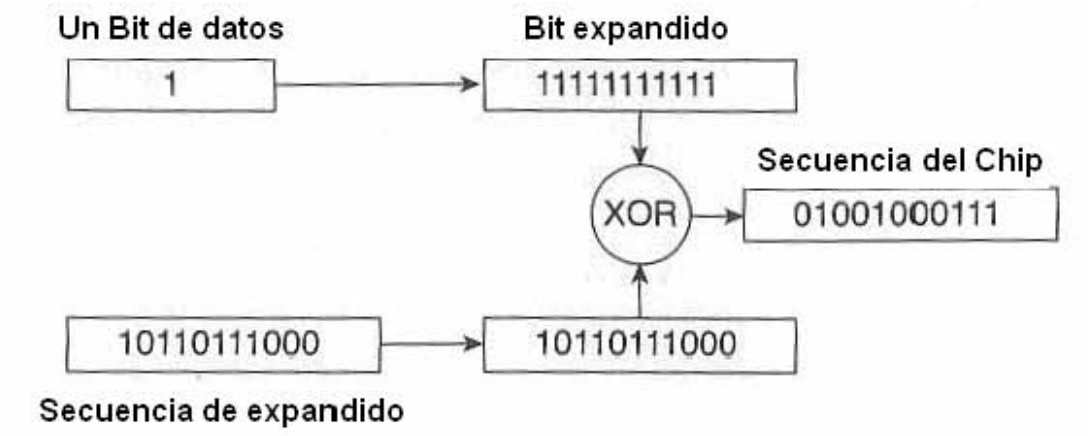


Figura 2-9 Expansión de un bit con valor de 1

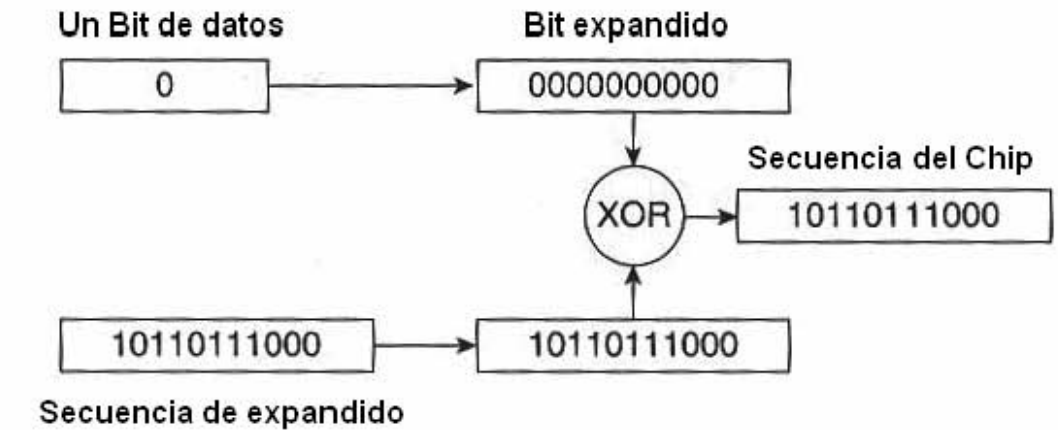


Figura 2-10 Expansión de un bit con valor de 0

Se podría pensar que es conveniente que las WLAN incrementen su uso del ancho de banda de 1 Mbps a 11 Mbps. Ello se explica porque el chip de datos de 11 bits representa solo un bit. La utilidad de esto se ve al suponer que el “chip” es transmitido a través de un medio inalámbrico durante la transmisión, y a veces las interferencias ocurren en algunas de las frecuencias de los canales.

Gracias a que la transmisión se extendió a través de un canal de 22 MHz de ancho de banda sólo algunos “chips” de la secuencia fueron impactados por la interferencia. En este caso, el receptor es capaz de reconstruir la secuencia original examinando los “chips” recibidos, a diferencia del proceso de mandar sólo los bits necesarios donde, ante la pérdida por interferencia se requiere de una retransmisión. El usar DSSS nos permite incrementar el *througput* y reducir la latencia.

En el caso de una modulación de 1 Mbps se usa DBSPK, para alcanzar velocidades de 2 Mbps se emplea DQPSK, ambas resultan en una tasa de 11 MHz símbolos, pero la DQPSK contiene dos “chips” a diferencia de la DBPSK que sólo cuenta con un “chip”.

2.8. 802.11b WLAN

La revisión del 802.11b en 1999 introdujo el HR-DSSS (*High rate DSSS*), que permite a las WLAN alcanzar velocidades de datos de hasta 5.5 y 11 Mbps en la banda ISM de los 2.4 GHz, usando CCK (*complementary code keying*) o PBCC (*packet binary convolutional coding*). HR-DSSS emplea la misma señalización que DSSS con un ancho de banda de 22 MHz y da 11 canales disponibles, de los cuales 3 no se empalman en la banda de los 2.4 GHz.

2.8.1. 802.11b HR-DSSS PLCP

La subcapa PLCP para HR-DSSS tiene 2 tipos de *frame* PPDU, uno corto y otro largo. El preámbulo y la cabecera en el 802.11b HR-DSSS largo, siempre son transmitidos a 1 Mbps para mantener la compatibilidad con DSSS. Incluso HR-DSSS es igual a DSSS PLCP, pero cuenta con extensiones para soportar tasas mayores de datos.

Estas extensiones son:

- El subcampo de señal tiene las siguientes adiciones:

Señal	*Tasa de transmisión*
0x37	*5.5 Mbps*
0x6E	*11 Mbps*

Tabla 4 Subcampo señal.

- El subcampo de servicio define los bits reservados, de la siguiente manera:

BIT	Nombre	*Decodificación*
B2	Reloj encadenado	*0=no encadenado*

		1=Frecuencia de transmisión y símbolos del reloj encadenados.
B3	Selección de modulación	*0=CCK, 1=PBCC*
B7	*Extensión de longitud*	*Se deja al campo de longitud*

Tabla 5 Subcampo servicio.

- El subcampo de longitud continúa dando el número de microsegundos para transmitir el PSDU.

El PLCP PPDU corto proporciona una manera de minimizar el tiempo de espera mientras el transmisor y el receptor se comunican adecuadamente. El encabezado 802.11b HR-DSSS corto usa el mismo preámbulo, cabecera y formato PSDU, pero la cabecera PLCP es enviada a 2 Mbps para transmitir el PSDU a 2, 5.5 y 11 Mbps. Los subcampos que se modifican son los siguientes. (*Figura 2-11*)

- El campo de sincronización: acortado de 128 a 56 bits de longitud y consiste en una cadena de ceros.
- El campo SFD: de 16 bits de longitud. Tiene la función de indicar el inicio del *frame* y señalar el uso de cabeceras cortas o largas. Con cabeceras cortas, los 16 bits son transmitidos en orden inverso, por lo que se transmite 0x05CF en lugar de 0xF3A0.

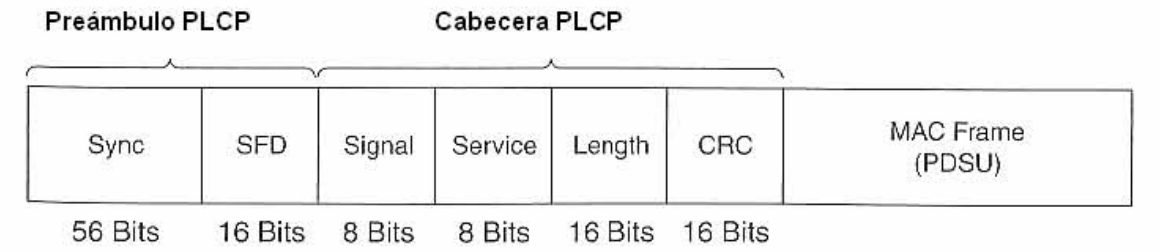


Figura 2-11 PPDU corto de HR-DSSS

Con el mismo procedimiento que lleva a cabo la capa 802.11 PHY, la PLCP convierte la unidad entera de PPDU para llevarla a la PMD. En ésta, los diferentes subcampos son enviados a la tasa de transmisión adecuada con la técnica de modulación de CCK o PBCC.

2.9. 802.11a WLANs

En 1999 el 802.11b introdujo la HR-DSSS, al mismo tiempo que la 802.11a introducía la OFDM PHY (*Orthogonal Frequency Division Multiplexing* / Multiplexación por división de frecuencias ortogonales) para la banda de los 5GHz. Ésta obliga a tasas de datos 24 Mbps y opcionales de 54 Mbps. En la banda (U-

NII) de los 5.15 a 5.35 GHz, 5.25 a 5.35 GHz y 5.725 a 5.825 GHz. 802.11a utiliza canales de 20 MHz y define 4 canales para cada una de las 3 bandas U-NII.

2.10. 802.11a OFDM PLCP

La subcapa PLCP para la capa física 802.11a, tiene un único PPDU formato, el cual es el siguiente: (*Figura 2-12*)

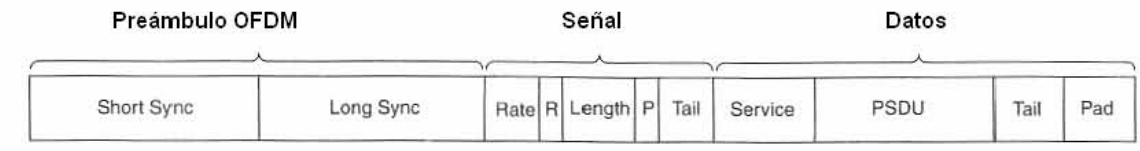


Figura 2-12 Formato del Frame PPDU 802.11a

Tres piezas básicas componen al PPDU:

- Preámbulo OFDM
- Señal
- Datos

El preámbulo OFDM consiste en pequeñas y largas señales de sincronización. El receptor usa un control de ganancia automática (AGC), tiempo y estimación del *offset* de frecuencias.

La parte de señal tiene 5 subcampos.

- El subcampo de Tasa de transmisión de 4 bits, especifica la tasa de transmisión de datos de acuerdo con la siguiente tabla:

R1-R4	Tasa (Mbps)
1101	6
1111	9
0101	12
0111	18
1001	24
1011	36
0001	48
0011	54

Tabla 6 Subcampo tasa de transmisión.

- El bit R, reservado para usos futuros.

- El campo de longitud, consiste en un entero de 12 bits no signados que especifica el número de octetos del PSDU.
- El bit P, es un non de paridad para los 17 bits usados en los anteriores.
- Signal Tail, el cual da 6 ceros no codificados.

El campo de Datos contiene 4 subcampos:

- El subcampo de servicio, nos da 7 bits de 0, seguido por 7 bits reservados, que en ese momento se ponen a 0. Este subcampo permite al receptor sincronizar su descodificador.
- El subcampo PSDU, contiene la información que va a ser transmitida.
- El subcampo Tail, remplaza los seis últimos ceros codificados con ceros no codificados, para reiniciar la memoria del codificador convolucional.
- El subcampo de PAD, adiciona el número de bits necesarios para alcanzar el número apropiado para codificar en OFDM.

2.10.1. Bases del OFDM

El multiplexado en división de frecuencia (FDM) es una tecnología que transmite múltiples señales simultáneamente sobre un mismo canal de comunicación, un cable o el aire. Cada señal viaja en su propia frecuencia dada por la portadora, que a su vez es modulada por la información.

Cuando se lleva este espaciamiento a frecuencias ortogonales entre sí, se evita que los demoduladores vean otra frecuencia que no sea la suya (*Figura 2-13*). En la frecuencia central de la sub-portadora las demás sub-portadoras son cero, de aquí su ortagonalidad.

Los beneficios de OFDM son alta eficacia espectral, resistencia a la interferencia de RF, baja distorsión por multitrayectorias. Lo anterior es muy útil porque en un escenario de transmisión típico existen muchas multitrayectorias.

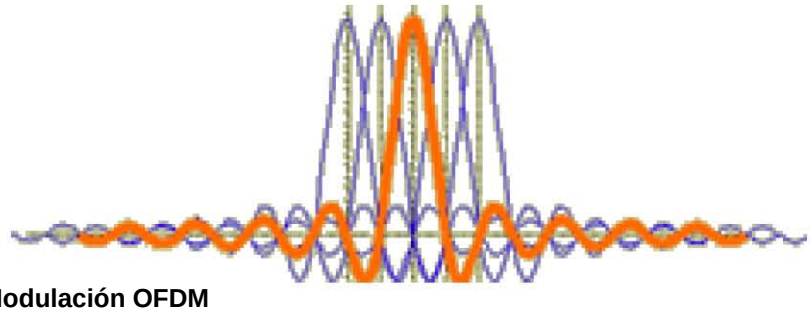


Figura 2-13 Modulación OFDM

OFDM es parte de una familia de modulación multicanal, inventada para enviar datos bajo una severa interferencia ínter simbólica. En el caso de QPSK donde se transmiten dos símbolos consecutivos, conforme estos símbolos viajan a través del medio de entrega, del transmisor al receptor, estos símbolos experimentan distorsión y varias partes de la señal pueden sufrir retrasos. Si estos retrasos son lo suficientemente largos, el primer símbolo puede empalmar en tiempo al segundo, llamándose a esto interferencia Intersimbólica (ISI).

El retraso en tiempo de la recepción desde la primera instancia de la señal hasta la última se conoce como "*delay spread*" (esparcimiento del retardo) del canal. También se puede pensar en esto, como la cantidad de tiempo en la que el primer símbolo se empalma con el segundo. Tradicionalmente los diseñadores trataban al ISI de dos maneras: empleando símbolos que son lo suficientemente largos para ser decodificados correctamente en presencia del ISI o ecualizando para acabar con la distorsión causada por la ISI.

Este método limita la tasa de símbolos a algo menos que el ancho de banda del canal, la cual es inversamente proporcional al "delay spread". Ya que el ancho de banda del canal se incrementa, se puede aumentar la tasa de símbolos, alcanzando finalmente una tasa alta de datos. El método de ecualizar usualmente requiere métodos muy caros así como complicados para realizar dicho procedimiento en el canal y para maximizar el uso del ancho de banda.

La modulación multicanal toma un enfoque totalmente distinto. El canal se parte en pequeños canales independientes, paralelos u ortogonales para transmitir señales de banda angosta con bajas tasas de transmisión, las cuales son moduladas en el dominio de la frecuencia por subportadoras independientes, esto es similar al proceso de modulación FHSS con la apropiada subportadora, si se divide el canal en N subcanales independientes.

Para un ancho de banda de canal, cuanto más largo el N que se escoja más largo será el periodo del símbolo y más estrecho el subcanal y si estos últimos se llevan en número al infinito el ISI se va a cero.

Una herramienta muy útil para construir estos símbolos independientes es la transformada rápida de Fourier (FFT), que es una eficiente implementación de la transformada discreta de Fourier (DFT) y puede ser convertida al dominio del tiempo a la frecuencia y viceversa.

En el dominio de la frecuencia se generan símbolos N 4-QAM (*Quadrature Amplitude Modulation*) que son convertidos al dominio del tiempo usando la transformada inversa rápida de Fourier (IFFT), esto se logra haciendo el tamaño de la FFT una potencia de 2 que permite una simple y eficiente implementación. Por esta razón los sistemas OFDM usualmente escogen a N como una potencia de 2.

Para permitir el proceso de recibir la señal, ésta debe ser una convolución circular de la entrada del canal. Lo anterior es el proceso matemático de pasar una señal a través del canal y determinar la salida. Para asegurar esta propiedad, se debe tomar la representación en el dominio del tiempo de un símbolo OFTM y crear un prefijo cíclico repitiendo el final de las muestras en el principio. (*Figura 2-14*)

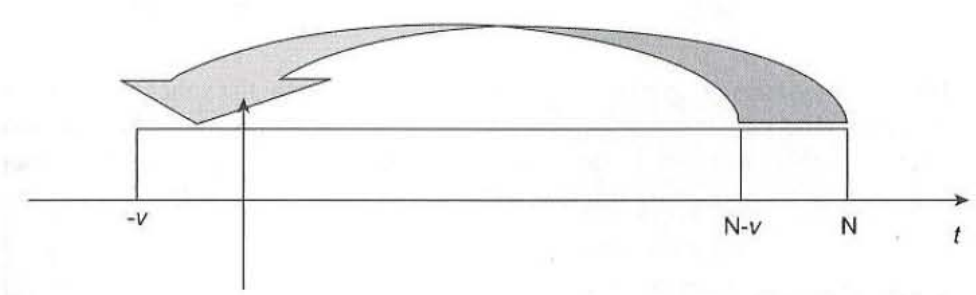


Figura 2-14 Formación del prefijo para el ciclo OFDM

N es el tamaño de la FFT en uso.

V es la longitud del ciclo.

2.11. 802.11a OFDM PMD.

Para transmitir en OFDM se usa el siguiente esquema de bloques:(*Figura 2-15*)

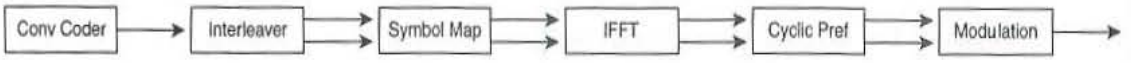


Figura 2-15 Diagrama de bloques de un transmisor OFDM para 802.11a

Dependiendo del tipo de modulación que se escoja se pueden obtener las siguientes velocidades de datos:

Tasa de datos (Mbps)	Constelación	Tasa de convolución de codificación	Bits codificados por subporadora	Bits codificados por símbolo OFDM	Bits de datos por símbolo OFDM
6	BPSK	½	1	48	24

9	BPSK	¾	1	48	36
12	QPSK	½	2	96	48
18	QPSK	¾	2	96	72
24	16-QAM	½	4	192	96
36	16-QAM	¾	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	¾	6	288	216

Tabla 7 Velocidades de datos.

Hay que recordar que la modulación QAM codifica la información en amplitud y fase de la sinusoidal. 16-QAM tiene 4 niveles de amplitud, mientras que 64-QAM tiene 8 niveles, por lo que se puede pensar en la fase para determinar 2 bits, como en QPSK y en la amplitud para determinar 2 o 3 bits.

Por último, para asegurarse de que todas las tasas de transmisión estadísticamente tengan la misma potencia, las multiplicamos por un factor de escala según el tipo de modulación.

Tipo de modulación	Factor de escala
BPSK	1
QPSK	1/sqrt(2)
16-QAM	1/sqrt(10)
64-QAM	1/sqrt(42)

Tabla 8 Tipo de modulación.

2.12. 802.11j WLAN

La 802.11j es una enmienda para permitir la interoperabilidad de las redes de área local con las redes de área metropolitanas, esto se logra al operar en la banda de los 4**.**9 GHz. En Japón, la numeración de los canales va del 240 al 255 en incrementos de 5 MHz cada uno.

2.13. 802.11g WLAN

El estándar 802.11g aprobado en junio del 2003, introduce la ERP para prestar soportes de tasas de datos de hasta 54 Mbps en la banda ISM de los 2.4 GHz, toma prestada las técnicas de modulación OFDM utilizadas en el 802.11a, y provee una total compatibilidad con 802.11b, gracias a que los dispositivos 802.11g, pueden caer a tasas de datos comparadas con la velocidad de la 802.11b.

Tres esquemas de modulación fueron definidos: ERP-ORFM, ERP-PBCC y DSSS-OFDM. El ERP-OFDM específicamente provee mecanismos para 6, 9, 12, 18, 24, 36, 48, 54 Mbps, con las tasas de datos 6, 12 y 24 obligatorias y las de 1, 2, 5,5 y 11 Mbps. El estándar permite el modo de modulación PBCC a 22 y 33 Mbps y es una opción de DSSS-OFDM a 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

2.14. 802.11g PLCP

El estándar 802.11g define cinco formatos de PPDU: 1) preámbulo largo, 2) preámbulo corto, 3) ERP-OFDM, 4) Largo de DSSS-OFDM, y 5) corto de DSSS-OFDM. Únicamente es obligatorio soportar los primeros tres, los dos restantes son opcionales.

Tipo de preámbulo	Tasas de datos soportados / interoperabilidad
Largo	1, 2, 5.5 y 11 Mbps DSSS-OFDM a todas las tasas de OFDM ERP-PBCC a todas las tasas de ERP-PBCC
Corto	2, 5.5 y 11 Mbps DSSS-OFDM a todas las tasas de OFDM ERP-PBCC a todas las tasas de ERP-PBCC
ERP-OFDM	ERP-OFDM a todas las tasas
Largo DSSS-OFDM	DSSS-OFDM a todas las tasas
Corto DSSS-OFDM	DSSS-OFDM a todas las tasas

Tabla 9 Preámbulo de PPDU

El preámbulo largo usa el mismo preámbulo que está definido en HR-DSSS pero con el campo de servicio modificado.

Bit	Nombre	Decodificación
B0	Reservado	0
B1	Reservado	0
B2	Encadenamiento de reloj	0=no encadenado 1=El reloj y la frecuencia de transmisión están encadenados.
B3	Selección de modulación	0=no ERP-PBCC 1=ERP-PBCC
B4	Reservado	0
B5	Extensión de la longitud	Para ERP-PBCC
B6	Extensión de la longitud	Para ERP-PBCC
B7	Extensión de la longitud	Para PBCC

Tabla 10 Preámbulo largo.

El formato para el CCK-OFDM largo y corto es el siguiente: (*Figura 2-16*)

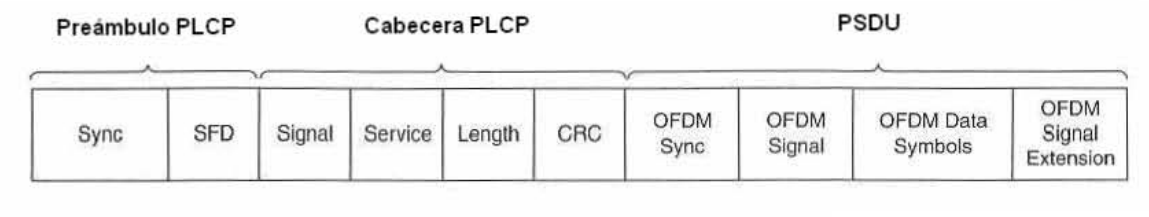


Figura 2-16 Formato del PPDU largo y corto para CCK-OFDM

Similar al preámbulo largo de DSSS-OFDM, el corto DSSS-OFDM del formato PPDU usa el del HR-DSSS y una cabecera que se transmite a 2 Mbps.

2.14.1. ERP-OFDM

El ERP-OFDM nos ofrece un mecanismo para usar una tasa de datos del 802.11a en una banda ISM de manera que sea compatible con DSSS y HR-DSSS. Además de utilizar la modulación 802.11a OFDM bajo la frecuencia de los 2.4 GHz, ERP-OFDM exige que en la transmisión de la frecuencia central y la del reloj de símbolos, éstas se encuentren encadenadas en el mismo oscilador.

2.14.2. ERP-PBCC

Las tasas de datos de 22 y 33 Mbps e PBCC usan los mismos mecanismos que las más bajas de 5.5 y 11 Mbps PBCC, pero con 8-PSK en lugar de QPSK y BPSK para obtener 22 Mbps. Los 33 Mmbps se alcanzan usando un reloj de 16.5 MHz en lugar de uno de 11 MHz.

2.14.3. La interoperabilidad de las 802.11g y 802.11b

La parte clave de las 802.11g es extender la tasa de datos hasta 54 Mbps en la banda de los 2.4 GHz, asegurando compatibilidad con los viejos dispositivos de 802.11b. En un ambiente donde sólo operan dispositivos 802.11g, todas las transmisiones son llevadas a cabo en la velocidad más alta de datos disponible. Sin embargo, al introducir un dispositivo 802.11b, la información de las cabeceras necesita transmitirse a una menor velocidad para que los dispositivos 802.11b puedan entender. Lo anterior es el costo de la interoperabilidad de los sistemas 802.11b y 802.11g.

2.14.4. CCA

Los diferentes estándares 802.11 definen cinco modos de CCA para ser usados en la banda de frecuencia de los 2.4 GHz.

- Detección de la energía basada en la decisión de CCA de detectar energía en el umbral.

- Sensado de la portadora basado en la decisión de CCA acerca de que una señal 802.11 fue detectada.
- Sensado de la portadora con detección de energía de los dos modos anteriores.
- Sensado de la portadora con reporte por un tiempo de que el medio es ocioso si no se ha detectado una señal 802.11 en 3.65 milisegundos.
- Tasa extendida en PHY de detección y censado de la energía.

La utilización de al menos un proceso de estos cinco es obligatorio.

2.15. Modulación adaptiva

Diferentes órdenes de modulación permiten mandar mayores cantidades de bits por símbolo y por lo tanto alcanzar *troughputs* más altos o mejorar la eficacia espectral. Sin embargo, se debe tomar en cuenta que al utilizar una técnica de modulación como 64-QAM, es requerida una mejor relación señal a ruido (SNRs) como protección ante cualquier interferencia y para mantener baja la tasa de errores (BER).

El uso de modulación adaptiva permite a un sistema inalámbrico escoger el orden más alto de modulación, dependiendo de las condiciones del canal. Conforme nos alejemos del AP se necesitará una modulación de menor orden, y por el contrario, al acercarnos se usará una de mayor orden. Además, el uso de modulación adaptiva nos permite vencer el desvanecimiento y otras interferencias.

Tasa de Datos. Mbps	**Tipo de transmission.**	**Tipo de modulación.**	**Radio de Bits**
1	***DSSS***	***BPSK***	***Chip de 11 bits***
2	***DSSS***	***QPSK***	***Chip de 11 bits***
6	***OFDM***	***BPSK***	***1/2***
9	***OFDM***	***BPSK3***	***3/4***
12	***OFDM***	***QPSK***	***1/2***
18	***OFDM***	***QPSK1***	***3/4***
24	***OFDM***	***16QAM***	***1/2***
36	***OFDM***	***16QAM***	***3/4***
48	***OFDM***	***64QAM***	***2/3***
54	***OFDM***	***64QAM***	***3/4***

Tabla 11 Modulación adaptiva.

2.15.1. En resumen.

La siguiente tabla resume las diferentes tecnologías utilizadas en la capa física. A pesar de que la FHSS experimentó una gran adopción al principio, ahora es más común encontrar la DSSS y la HR-DSSS, así como las basadas en OFMD que también son de gran uso.

Características	802.11 FHSS	802.11 DSSS	802.11 HR-DSSS	802.11a OFDM	802.11g ERP	802.11j
Banda de frecuencia (GHz)	2.4	2.4	2.4	5	2.4	4.9
Máxima tasa de datos (Mbps)	2	2	11	54	54	54
Modulación	QPSK	GFSK	CCK	OFDM	OFDM	OFDM

Tabla 12 Características.

3. Capítulo 3

En este capítulo se estudiará la capa de enlace de datos, los retos del estándar 802.11 y los avances de los grupos de tarea. Además, se retoma el importante tema de la seguridad en las redes inalámbricas y las opciones existentes.

3.1. Retos del estándar 802.11.

Uno de los aspectos más interesantes de este estándar es que la propagación de señales inalámbricas se realiza en un medio menos confiable que el de una red cableada. Dicho medio tiene una forma irregular, es muy difícil limitarlo aunque tal vez una manera de hacerlo es controlando la intensidad de emisión de las señales, y resulta muy complicado conocer con certeza sus dimensiones como en el caso de las redes cableadas donde ésta es visible y palpable.

Adicionalmente, las señales son altamente susceptibles de interactuar con otras que transitan al mismo tiempo en este medio, dicha interferencia puede provocar la pérdida parcial o total de la información original que porta cada señal.

3.1.1. El problema de la estación oculta.

Un reto más es el problema de la “estación oculta” (*Figura 3-1*), dónde H1 y H2 tienen visibilidad del AP pero no son visibles entre sí. El problema consiste en que al transmitir simultáneamente H1 y H2 hacia AP es posible que se genere una interferencia que impida la comunicación durante el intervalo de tiempo que dure esta operación.

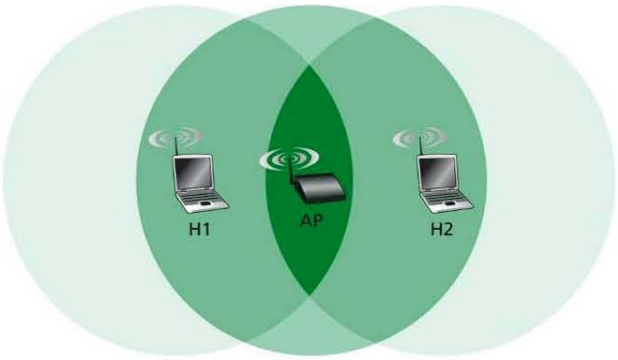


Figura 3-1 Problema de la estación oculta

3.2. La capa de enlace de datos.

La capa de enlace de datos se divide en dos subcapas: la MAC (*Medium access control*) y la LLC (*Logical Link Control*). El estándar 802.11 utiliza la capa MAC 802.11, mientras que la capa LLC requiere el 802.2 o *ethernet*, lo anterior permite que tanto *ethernet* y *wireless* ofrezcan la misma interfase a la capa de red.

El protocolo MAC 802.11 funciona de forma similar al protocolo MAC 802.3 (*Ethernet*). Ambos tienen en común que son CSMA (*Carrier Sense Multiple Access*), es decir, revisan el canal antes de trasmitir y se abstienen de hacerlo cuando detectan el canal ocupado. La diferencia entre ambos radica en la forma como las estaciones se dan cuenta de que el canal se encuentra ocupado, el 802.3 emplea la técnica de detección de colisiones (CD), esto es, que escucha el canal y simultáneamente se empieza a transmitir, si el canal está desocupado la transmisión finaliza en buen término y éste se libera pero si está ocupado se detecta la colisión y aborta la transmisión. Por su parte, 802.11 evita las colisiones (CA, *Collision Avoidance*) ya que no puede detectarlas a causa del problema de la estación oculta.

El protocolo MAC (*Figura 3-2*) indica que una estación que necesita transmitir debe escuchar el canal. Si está libre, la estación espera un corto periodo de tiempo DIFS (*Distributed Inter-frame Space*) y luego envía un RTS (*Request to Send*) al destino. Si el canal está ocupado, la estación genera un contador de valor inicial aleatorio que, en cuanto percibe un estado ocioso comienza a disminuir hasta que de nuevo se encuentre ocupado.

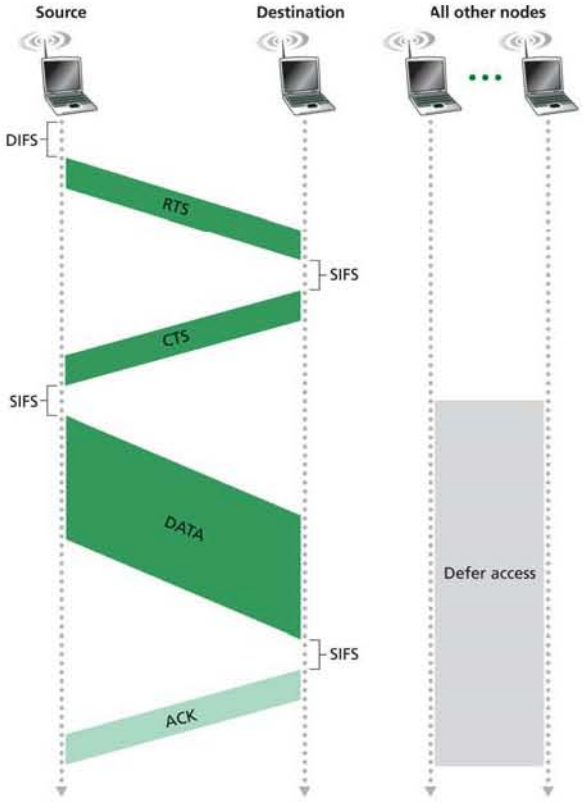


Figura 3-2 El protocolo MAC 802.11

Una vez que se vence el contador, la estación trasmite el RTS que es una petición al destino para reservar el canal todo el tiempo que requiera el envío de datos. A

continuación el destino responde con un CTS (*Clear to Send*) que es la confirmación de la reserva que será escuchada por todas las estaciones dentro de su rango de alcance, y de esta manera elimina el inconveniente de la estación oculta. El destino usualmente es AP y su recepción se lleva a cabo en todas las estaciones del BSS.

Una vez que la estación origen recibe el CTS, ésta espera un corto periodo de tiempo (SIFS, *Short Inter-frame space*) para asegurar que las demás estaciones lo escucharon. Luego, transmite los datos y espera que el destino envíe el *acknowledgement (*ACK*)* precedido por un intervalo SIFS. Después de esto, el canal queda listo para que otra estación lo use apegándose al protocolo MAC.

A nivel de la capa MAC 802.11, existen *Ackowledgements (*ACKs) que únicamente son similares, a los de la capa de transporte, en la filosofía de trabajo sobre la pérdida o daño de datos a causa del medio y fenómenos como la interferencia.

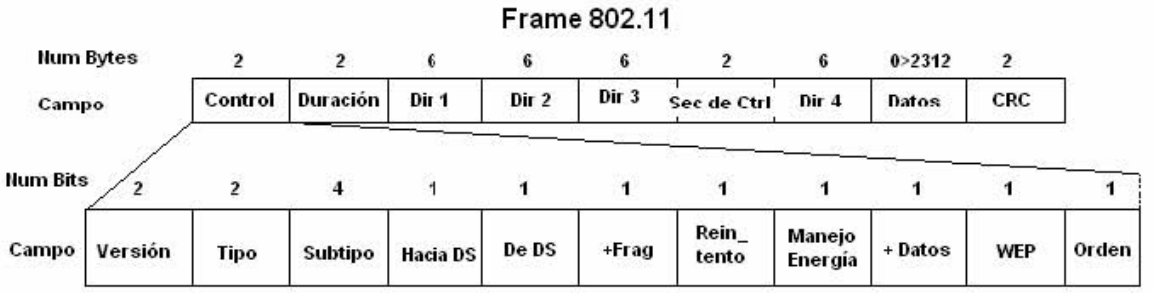


Figura 3-3 Frame 802.11

3.2.1. Frame 802.11

El campo de control de la trama (*frame control*) es importante porque determina el tipo de datos que contiene lo demás del *frame*. Su primer componente (2 bits) corresponde a la versión del protocolo, actualmente 0b00. Vale la pena mencionar que los campos se transmiten en el orden como van apareciendo en el papel (de izquierda a derecha) pero sus valores se encuentran invertidos, es decir, el *bit* más significativo de los campos está a la derecha y el de menor valor a la izquierda.

En el campo de datos va la información. El tipo y subtipo definen la clase de información que contiene la trama. La siguiente tabla relaciona los más relevantes:

Tipo	**Subtipo**
Administración (00)	Solicitud/Respuesta de Asociación
	Solicitud/Respuesta de Reasociación
	Solicitud/Respuesta de *Probe*
	Beacon
	Desasociación
	Autentificación / Desautentificación

Control (01)	RTS
	CTS
	ACK
Data (10)	Data + …
	Null Data

Por ejemplo, si aparece ‘10’ en el campo Tipo es porque se trata de un *frame* de control, ya que el valor del campo debe leerse de derecha a izquierda, el 1 está en la posición menos significativa por estar más a la izquierda y el 0 se encuentra en la posición de la derecha, la más significativa.

La AP tiene conocimiento del estado gracias al campo *Null Data* generalmente requerido por las estaciones para informar de los cambios en su manejo de energía, como es el paso a un estado de ahorro que consiste en la interface que apaga temporalmente algunas de sus partes y lo índica encendiendo el *bit* “manejo de energía” en el *Frame* Control. Cuando una estación entra en dicho estado, la AP puede almacenar los *frames* que provienen del BS y para registrarlo debe encender el *bit* “más datos”.

El campo duración contiene el tiempo estimado en microsegundos, durante el cual, el canal permanecerá ocupado por la transmisión en curso.

El campo control de secuencia se divide en dos partes: una de 4 bits de número de fragmento y otra de 12 bits de número de secuencia. Su función principal es descartar los *frames* duplicados y fragmentar las tramas muy grandes provenientes de la capa superior (capa de red), de forma muy similar a lo que hace el protocolo IP, esto se realiza para que la capa de enlace maneje el control de flujo de los datos provenientes de la superior.

Cuando se va a retransmitir un *frame* y el receptor no lo ha reconocido de esa manera, se enciende el *bit* de “reintento” en el campo de control y se envía. A cada *frame* recibido de la capa del nivel superior (red) se le asigna un número de secuencia, según el orden de llegada, que aumenta de *frame* en *frame* a menos que se trate de una retransmisión o que requiera ser fragmentado. En este último caso, todos los fragmentos comparten el mismo número de secuencia y difieren en el de fragmento ya que, a medida que se van transmitiendo, al primero le corresponde el cero y para los siguientes irá en ascenso hasta 0x0F máximo. Para saber cuándo se ha recibido el último fragmento, basta revisar el undécimo *bit* del campo *frame* control que indica si deben esperarse más o si se trataba del último para el número de secuencia que indica el campo.

La carga de datos es la información que se encapsula de los datos recibidos de la capa superior, pero cuando se trata de un *frame* de administración o control se el término se refiere a las opciones de tipo-subtipo que ahí se indican.

El tamaño máximo de la carga es de 2304 octetos de datos procedentes de la capa superior (Red), sin embargo, se habla de un tamaño máximo de campo de

2312 octetos con el fin de acomodar el *overhead* WEP en caso de que se encuentre en uso.

Finalmente, está el campo Control de Redundancia Cíclica (CRC) que se calcula en todas las estaciones que procesan el *frame* a partir de los demás campos que lo conforman, comparándolo con el valor actual. Si el resultado del cálculo coincide con el valor actual, entonces, hay una alta probabilidad de que el contenido de la trama no se haya dañado en su paso por el medio.

3.3. Seguridad en las redes inalámbricas.

3.3.1. Método 1: Filtrado de direcciones MAC

Los filtros *Media Access Control* (MAC) son un mecanismo de seguridad en la capa de enlace, que permiten asociarse al AP mediante la definición de una lista de direcciones físicas (MAC) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso, las cuales son únicas y autentifican el equipo. Si una estación intenta asociarse con una MAC que no se encuentra en la lista, será denegada la solicitud manteniéndola al margen del BSS y negándole la posibilidad de usufructuar los servicios ofrecidos por la red.

Para que una estación pueda hacer uso de los servicios de la WLAN de Infraestructura, es necesario lograr el equivalente a “conectar el cable” en una red cableada. Lo primero que hace la estación es ubicar la AP, luego, solicita la autentificación que ésta puede conceder o denegar de acuerdo a los filtros y medidas de seguridad con las que cuente, por ejemplo WEP, Radius, etc. Una vez autenticada, procede a solicitar su asociación. (*Figura3-4*)

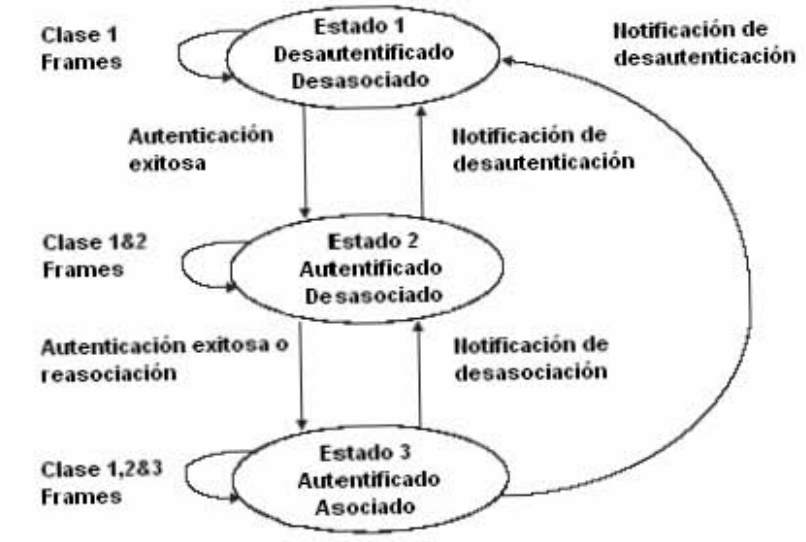


Figura 3-4 Estados de una estación de acuerdo a su relación con el AP

Si la dirección MAC de la estación solicitante no está filtrada, el proceso se inicia con el *frame* “solicitud de autentificación” y continúa con la respuesta de la AP. Después, la estación solicitante ya autentificada, demanda la asociación y si la petición fue concedida recibe el código 0x00. En este momento la estación alcanza el estado 3 de la relación con la AP (ver figura 3-4), obteniendo así, acceso a todos los servicios de la red que se verán en *frames* posteriores donde se realiza una transacción con el servidor DHCP.

La ventaja de este método consiste en la sencillez para utilizarla en redes caseras o pequeñas. Sin embargo, posee las siguientes desventajas para las redes medianas y grandes:

- No escala bien, cada vez que se desea autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Si se manejan varios puntos o equipos la situación se torna inmanejable
- El formato de una dirección MAC no es amigable, como su escritura es de 6 *bytes* en hexagesimal se pueden cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante, empleando un *sniffer*, puede pasarse por cliente válido mediante la captura de direcciones MAC de tarjetas matriculadas en la red, y luego asignándolas a la tarjeta de su computador con programas como AirJack6 o WellenReiter.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. Cuando el elemento hurtado es un punto de acceso, el problema es más serio porque el contiene toda la tabla de direcciones válidas en su memoria de configuración.
- Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida porque no prevé ningún mecanismo de cifrado.

3.3.2. Método 2: Wired Equivalent Privacy (WEP)

El algoritmo WEP10 forma parte de la especificación 802.11 y se diseñó con el fin de proteger, mediante un cifrado, los datos que se transmiten en una conexión inalámbrica. WEP opera a nivel dos del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas. Cifra de la siguiente manera: (*Figura 3-5*)

- A la trama en claro se le computa un código de integridad (Integrity *Check Value,* ICV) mediante el algoritmo CRC-32. El ICV se concatena con la trama y más tarde es empleado por el receptor para comprobar si la trama ha sido alterada durante el transporte.
- Se escoge una clave secreta compartida entre emisor y receptor, que puede poseer 40 ó 128 bits, para cifrar las tramas. Si todas las veces se empleara la misma clave, dos de éstas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave

secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits, que cambia con cada trama.

• La concatenación de la clave secreta y el IV, conocida como semilla, se emplea como entrada de un generador RC4 de números seudo- aleatorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria, o cifra de flujo, tan larga como se desee a partir de la semilla y del mismo tamaño de la trama a cifrar más 32 bits para cubrir su longitud y el ICV.

• Se hace un XOR, *bit* por *bit* de la trama con la secuencia de clave, para obtener como resultado la trama cifrada.

• El IV y la trama se transmiten juntos.

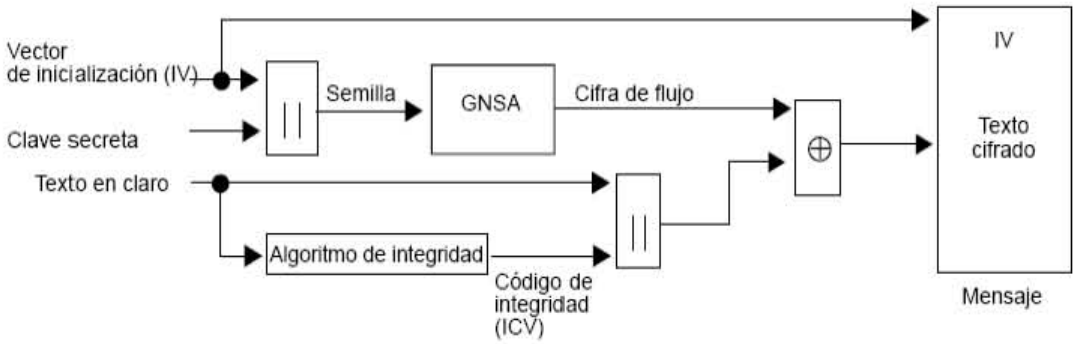


Figura 3-5 Funcionamiento del algoritmo WEP en modalidad de cifrado

En el receptor se lleva a cabo el proceso de descifrado: (*Figura 3-6*)

• Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.

• Un generador RC4 produce la cifra de flujo a partir de la semilla. Si ésta coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la utilizada en el proceso de comunicación.

• Se efectúa un XOR, *bit* por *bit* de la cifra de flujo y la trama del cifrado, para obtener la trama en claro y el ICV.

• A la trama en claro se le aplica el algoritmo CRC-32 para conseguir un segundo ICV que se compara con el recibido.

• La trama se acepta si los dos ICV son iguales, de lo contrario, se rechaza.

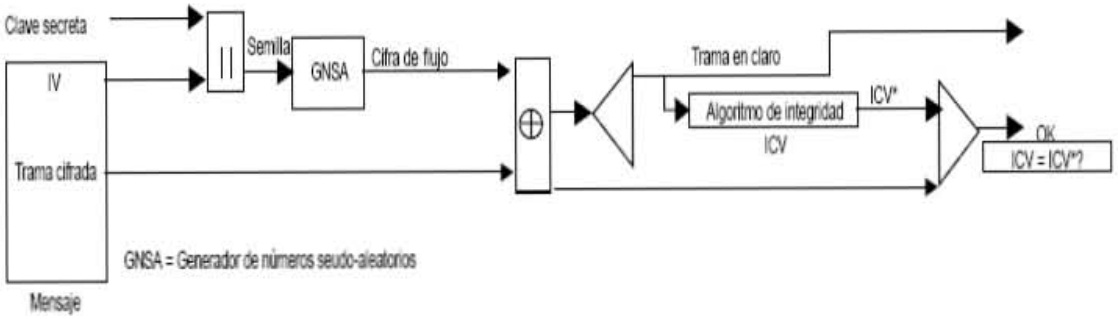


Figura 3-6 Funcionamiento del algoritmo WEP en modalidad de descifrado.

3.3.3. Clave secreta

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen razones para no considerar seguro a WEP en el manejo de la mayoría de las aplicaciones:

- La mayoría de las instalaciones emplea WEP con claves de cifrado estáticas, es decir, se configura una clave en el punto de acceso y nunca o rara vez se cambia. Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.
- El IV que se utiliza tiene una longitud insuficiente de 24 bits. Dado que cada trama se cifra con un IV diferente, es cuestión de tiempo, que se agote el espacio de 224 IV distintos. Esto no es problemático en una red casera, pero en una con mucho tráfico se puede agotar el espacio en 5 horas aproximadamente. Si el atacante logra conseguir dos tramas con un IV idéntico, puede efectuar un XOR entre ellas y, mediante un ataque estadístico, obtener los textos en claro de ambas tramas. Con éstos y su respectivo texto cifrado se puede obtener la cifra de flujo y una vez conociendo el funcionamiento del algoritmo RC4 se puede obtener la clave secreta para descifrar toda la conversación.
- WEP no ofrece servicio de autentificación ni del cliente o de la red, basta con que el equipo móvil y el punto de acceso compartan una clave WEP para que la comunicación pueda llevarse a cabo.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack que consiste en una serie de *scripts* escritos en lenguaje Perl, diseñados para analizar un archivo de captura de paquetes de un *sniffer*. La herramienta AirSnort9 realiza lo mismo pero es más fácil de utilizar debido a que

integra las funciones de *sniffer*, realiza una captura pasiva de paquetes para romperla cuando ha adquirido los datos suficientes.

3.3.4. Método 3: Las VPN

Las *Virtual Private Network (*VPN) emplean tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de *hardware* inalámbrico y superan las limitaciones de WEP.

Al configurar una red inalámbrica utilizando las VPN se debe tener en cuenta que se trata de una red insegura, sin embargo, los riesgos pueden disminuirse instalando la parte que maneja el acceso inalámbrico de manera aislada del resto de la red. Se logra, utilizando una lista de acceso adecuada en un enrutador o, en caso del switching, agrupando todos los puertos de acceso inalámbrico en una VLAN, con la cual únicamente se permite el acceso del cliente inalámbrico a los servidores de autorización y autentificación de la VPN. (*Figura 3-7*)

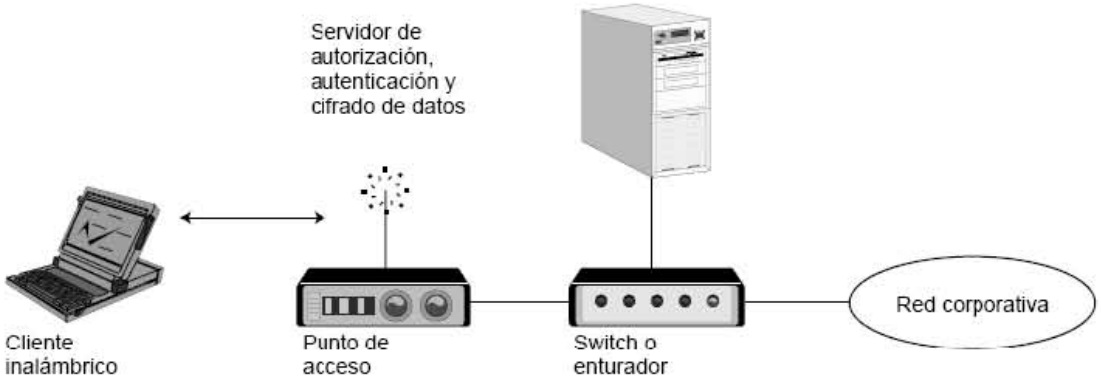


Figura 3-7 Estructura de una VPN para acceso inalámbrico seguro

El acceso completo se realiza cuando ha sido debidamente autorizado y autentificado por los servidores de VPN que además se encargan de cifrar el tráfico desde y hacia dichos clientes. Los datos se cifran en un nivel superior del modelo OSI, por lo tanto no es necesario emplear WEP en este esquema.

3.3.5. Método 4: 802.1x

802.1x es un protocolo de control de acceso y autentificación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. Inicialmente fue creado por la IEEE para uso en redes de área local cableadas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058.

Estos servidores fueron creados inicialmente para autentificar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autentificación en las LAN.

El protocolo 802.1x involucra tres participantes: (*Figura 3-8*)

- El suplicante o equipo del cliente que desea conectarse con la red.
- El servidor de autorización/autentificación que contiene toda la información necesaria para determinar cuáles equipos y/o usuarios están tienen permitido acceder a la red.
- El autenticador, es el equipo de red (switch, enrutador, servidor de acceso remoto) que recibe la conexión del suplicante y le permite el acceso cuando el servidor de autentificación lo autoriza. Es un intermediario entre ambos elementos. (*Figura 3-8*)

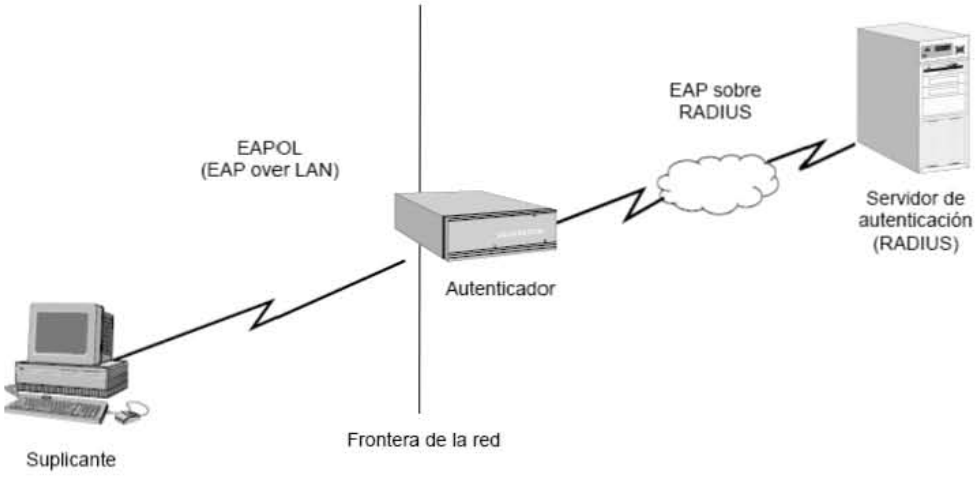


Figura 3-8 Arquitectura de un sistema de autentificación 802.1x

La autentificación del cliente se lleva a cabo mediante el protocolo *Extensible Authentication Protocol (EAP*) y el servicio RADIUS, de la siguiente manera: (*Figura 3-9*)

- El proceso inicia, en el caso de la red alámbrica, cuando la estación de trabajo se enciende y activa su interfaz de red, mientras que en la red inalámbrica, es al enlazarse o asociase con un punto de acceso. En ese momento la interfaz de red tiene bloqueado el acceso de tráfico normal y lo único que admite es el *EAP over LAN* (EAPOL) para la autentificación.
- La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso.
- El autenticador envía un mensaje EAP-Request/Identity solicitando que la estación se identifique con un mensaje EAP-Response/Identity que será

transmitido al servidor de autentificación en la forma de mensaje RADIUS-Access-Request.

• El autenticador envía un mensaje EAP-Request al cliente para informarle del RADIUS Acces-Challenge enviado por el servidor de autentificación, el cual describe el desafío a resolver, que puede ser desde introducir una contraseña hasta realizar funciones criptográficas.

• El cliente da respuesta al desafío con un mensaje EAP-Response (Credentials) y el autenticador lo reenvía al servidor en la forma RADIUS-Access-Response.

• Si responde correctamente, el servidor envía al autenticador un mensaje RADIUS-Access-Accept con la autorización de acceso y la información inicial necesaria para que efectúe la apertura del puerto e informe al cliente con un mensaje EAP-Succes.

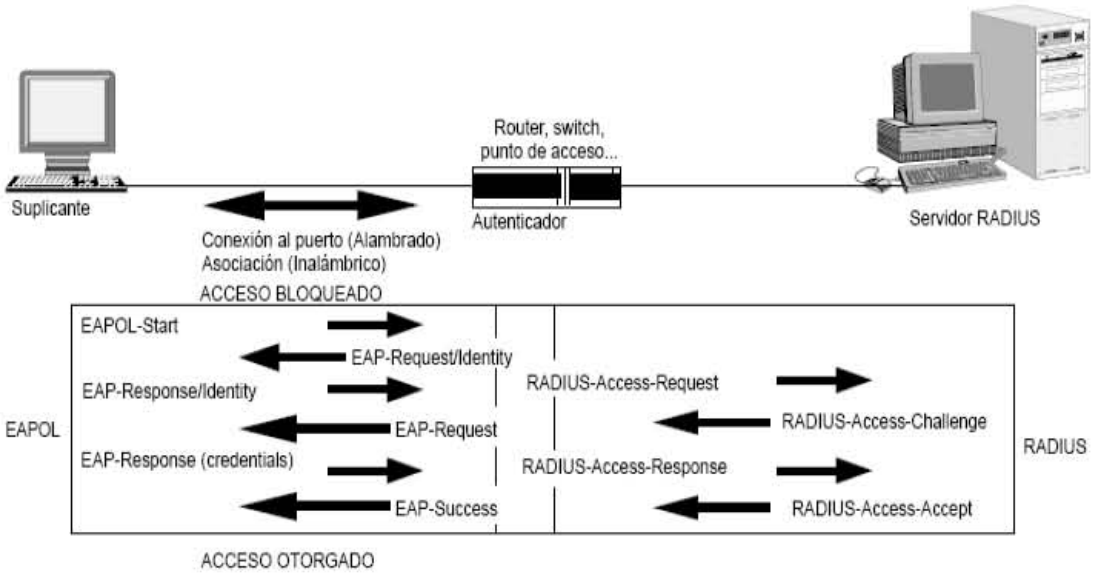


Figura 3-9 Diálogo EAPOL RADIUS

En el acceso inalámbrico, el servidor RADIUS despacha el mensaje RADIUS-Access-Accept con un juego de claves WEP entre el cliente y el punto de acceso, éstas cambian periódicamente para evitar un ataque de “rompimiento”.

Existen variantes del protocolo EAP según la modalidad de autentificación que se emplee. Se puede hablar de dos grupos distintos: los que cuentan con certificados de seguridad y los que utilizan contraseñas.

Con certificados de seguridad son las siguientes:

• EAP-TLS: requiere de instalación de certificados en los clientes y en el servidor para que la autentificación sea fuerte y mutua, soporta el uso de claves dinámicas para WEP. La sesión de autentificación entre el cliente y

el autenticador se cifra empleando el protocolo *Transparent Layer Substrate* (TLS).

• EAP-TTLS: Desarrollada por Funk Software y Certicom, proporciona servicios similares a EAP-TLS, la diferencia consiste en el certificado del servidor que requiere para la instalación. Así se garantiza la autentificación fuerte del servidor por parte del cliente, y éste la obtiene cuando se establece la sesión TLS con el método PAP, CHAP, MS-CHAP o MS-CHAP v2.

• PEAP: Desarrollado por Microsoft, Cisco y RSA Security, se parece al funcionamiento de EAPTTLS en que únicamente requiere un certificado de seguridad en el servidor. Provee protección a métodos antiguos de EAP mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

El empleo de certificados también trae consigo varias desventajas, como:

• La administración de los certificados de seguridad puede ser costosa y complicada especialmente en los esquemas que requieren dos, para clientes y el servidor. Se pueden comprar con una autoridad de certificación (CA) conocida o montar una CA propia.

• El diálogo de autentificación es largo y vuelve lento el proceso, esto es molesto para usuarios que se reautentifican con mucha frecuencia, a causa del movimiento y del cambio de un punto de acceso a otro, entre otras.

• La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalarlo en la Terminal del usuario pero si es robada y era el único nivel de seguridad, entonces hay una situación de gran riesgo. Otra opción es llevar el certificado en una tarjeta inteligente (*smart card*) para leerla en todas las terminales con el hardware adicional instalado.

Las variantes de EAP que utilizan contraseñas son las siguientes:

• EAP-MD5: Emplea un nombre de usuario y una contraseña para la autentificación, se transmite cifrada con el algoritmo MD5 pero es susceptible a ataques de diccionario, esto es cifrar múltiples contraseñas con MD5 hasta encontrar una que coincida. Además el cliente no tiene manera de autenticar el servidor y el esquema no es capaz de generar claves WEP dinámicas. Por lo anterior, EAP-MD5 ha caído en desuso.

• LEAP: Esta variante es propietaria de Cisco, emplea un esquema con nombre de usuario y contraseña; soporta claves dinámicas y por tratarse de una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco y el servidor RADIUS compatible con LEAP.

• EAP-SPEKE: Variante que emplea el método *Simple Password-authenticated Exponential Key Exchange* (SPEKE), permite verificar que tanto cliente como servidor comparten una información secreta, una contraseña, a través de un medio inseguro. El método es muy seguro, aun

con contraseñas cortas, ofrece protección contra ataques de diccionario y servicio de autentificación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método fuerte y sencillo.

3.3.6. Método 5: WPA (WI-FI Protected Access)

WPA14 es un estándar propuesto por los miembros de la Wi-Fi Alliance que reúne a los grandes fabricantes de dispositivos para WLAN, en colaboración con la IEEE. Mejoró los algoritmos de cifrado de trama, de los datos y de generación de los IVs con respecto a la WEP. Su propuesta de mecanismo de autentificación consiste en el nuevo protocolo de cifrado Temporary Key Integrity Protocol (TKIP) que cambia cada cierto tiempo la clave compartida entre el punto de acceso y el cliente para evitar ataques que permitan revelarla y emplea 802.1x y EAP.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

• Modalidad de red empresarial: para operar necesita que la red cuente con un servidor RADIUS para suministrar las claves compartidas que cifran los datos. El punto de acceso emplea 802.1x y EAP para la autentificación.

• Modalidad de red casera o Pre-Shared Key (PSK): WPA opera cuando no se dispone de un servidor RADIUS. La seguridad es garantizada por TKIP. Introduce una contraseña compartida en el punto de acceso y los dispositivos móviles, ambos tienen que coincidir para lograr la conexión. Se recomienda que las contraseñas sean de veinte caracteres o más porque se ha comprobado que WPA es vulnerable a los ataques de diccionario cuando son cortas. La norma WPA data de abril de 2003, a finales de ese año, su cumplimiento se volvió obligatorio entre todos los miembros de la Wi-Fi Alliance, para que todo equipo de red inalámbrica que porte el sello “Wi-Fi Certified” se actualice por software y cumpla con la especificación WPA.

3.4. ¿Qué significa la sopa de letras de estándares 802.11?

Los grupos de tareas (*task groups*) del grupo de trabajo del 802.11 están encargados de mejorar sus partes. Cada letra corresponde a un Standard o revisión, por ejemplo, el grupo de tarea b fue responsable del 802.11b y así cada uno de los grupos en sus diferentes estándares. Ya que en los capítulos anteriores se ha explicado el 802.11, 802.11a, 802.11b, 802.11j y 802.11g a continuación solamente se tratará el 802.11c, 802.11e, 802.11i, 802.11d. 802.11f y el 802.11h.

3.4.1. 802.11c.

Proporciona la información necesaria para asegurar la correcta operación de los *Bridge*. Los propósitos de este proyecto completado son parte del estándar IEEE 802.11 c. Sus inventores lo requieren para desarrollar access ponts (AP).

Actualmente no despierta mucho interés en los usuarios e instaladores de redes inalámbricas.

3.4.2. 802.11e

Su objetivo es proporcionar soporte de Calidad de Servicio (QoS) para aplicaciones de redes LAN. Se empleará para los estándares físicos a, b y g de 802.11 con la finalidad de otorgar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.

3.4.3. 802.11i

Se refiere al tema de la seguridad que es el objetivo mas frecuente del estándar 802.11. Se aplicará a los estándares físicos a, b y g de 802.11. Proporciona una alternativa a la Privacidad Equivalente Cableada (WEP) con nuevos métodos de encriptación y procedimientos de autentificación. IEEE 802.1x constituye una parte clave de este estándar.

3.4.4. 802.11d

Constituye un complemento al nivel de control de Acceso al Medio (MAC) en 802.11. Busca el uso a escala mundial de las redes WLAN del estándar 802.11. Permite a los puntos de acceso comunicar información acerca de los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

3.4.5. 802.11f

Su objetivo es lograr la interoperabilidad de Puntos de Acceso (AP) dentro de una red WLAN multiproveedor. Cuando el usuario se mueve de un punto de acceso a otro, el estándar define el registro de AP dentro de la red y el intercambio de información entre ellos.

3.4.6. 802.11h

Busca cumplir los reglamentos europeos para redes WLAN a 5 GHz que demandan un control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio, en el punto de acceso, para reducir al mínimo la interferencia con otros sistemas, particularmente el radar.

4. Capítulo 4

En este capítulo se evalúa el desempeño de los estándares a, b, y g que actualmente se comercializan. Se explica la metodología de la tesis y las pruebas que se realizaron para medir los diferentes parámetros de velocidad, BER, relación señal a ruido (SNR), entre otros. Esto se llevó a cabo en el tercer piso del edificio Valdez Vallejo con la finalidad de mapear el desempeño de los distintos estándares, así como graficar y analizar los resultados de Movilidad WI FI que consiste en los cambios de velocidad en una sesión.

4.1. ¿Cuántas redes hay en el edificio Valdez Vallejo?

Como primer paso de este análisis se estudiará el entorno de nuestro lugar de pruebas, para tener un mejor conocimiento del campo de trabajo.

Red		**Planta baja**	**Primer piso**	**Segundo piso**	**Tercer piso**	**Laboratorio**
1	**Essid**	RPM	RPM	RPM	RPM	RPM
	Canal	11	11	11	11	11
	Señal dBm	-90	-89	-90	-80	-23
	Encriptación	No	No	No	No	No
	Max Vel	54 Mb/s	54 Mb/s	54 Mb/s	54 Mb/s	54 Mb/s
2	**Essid**	mobilelan	Mobilelan	Mobilelan	mobilelan	Mobilelan
	Canal	6	6	6	6	6
	Señal dBm	-86	-85	-86	-72	-43
	Encriptación	Si	Si	Si	Si	Si
	Max Vel	11 Mb/s	11 Mb/s	11 Mb/s	11 Mb/s	11 Mb/s
3	**Essid**	mobilelan2	mobilelan2	mobilelan2	mobilelan2	mobilelan2
	Canal	6	6	6	6	6
	Señal dBm	-84	-82	-79	-62	-88
	Encriptación	Si	Si	Si	Si	Si
	Max Vel	11 Mb/s	11 Mb/s	11 Mb/s	11 Mb/s	11 Mb/s

4	**Essid**	Control	Control	Control	Control	Control
	Canal	6	6	6	6	6
	Señal dBm	-81	-82	-85	-73	-90
	Encriptación	Si	Si	Si	Si	Si
	Max Vel	54 Mb/s	54 Mb/s	54 Mb/s	54 Mb/s	54 Mb/s
5	**Essid**	RoboCupFi-linksys	RoboCupFi-linksys	RoboCupFi-linksys	My Wireless Network A	
	Canal	6	6	6	10	
	Señal dBm	-88	-86	-87	-87	
	Encriptación	No	No	No	No	
	Max Vel	54 Mb/s	54 Mb/s	54 Mb/s	54 Mb/s	
6	**Essid**	Lmsr	Lmsr	Lmsr	Diedimei1G	
	Canal	11	11	11	1	
	Señal dBm	-84	-83	-83	-67	
	Encriptación	Si	Si	Si	No	
	Max Vel	22 Mb/s	22 Mb/s	22 Mb/s	54 Mb/s	
7	**Essid**	lab_sistemas	lab_sistemas	diedimei1G	lab_sistemas	
	Canal	6	6	1	6	
	Señal dBm	-91	-91	-57	-95	
	Encriptación	No	No	No	No	
	Max Vel	54 Mb/s	54 Mb/s	54 Mb/s	54 Mb/s	
8	**Essid**	diedimei1G	diedimei1G	diedimei2G		
	Canal	1	1	1		
	Señal dBm	-76	-73	-88		
	Encriptación	No	No	Si		
	Max Vel	54 Mb/s	54 Mb/s	54 Mb/s		
9	**Essid**	My Wi – Net	diedimei2G			
	Canal	10	1			
	Señal dBm	-75	-81			
	Encriptación	no	Si			
	Max Vel	54 Mb/s	54 Mb/s			

10	**Essid**	diedimei2G				
	Canal	1				
	Señal dBm	-78				
	Encriptación	si				
	Max Vel	54 Mb/s				

Tabla 13 Redes en el Valdez Vallejo

Se encontró que hay bastantes redes inalámbricas en este edificio, sobre todo cerca de las ventanas donde salen y entran las señales, aunque muchas veces se trataba de unos cuantos paquetes que nada más informan de su presencia pero no nos permiten conectarnos.

La tabla anterior muestra que casi la mitad de las redes detectadas tienen algún tipo de encriptación y la otra podría estar filtrada por MAC. Ambos casos se registraron como ruido en esta investigación.

Algo que sirve en gran medida para mejorar el desempeño de nuestra red es tratar de usar los canales menos saturados y entonces tener una disminución de interferencias. Se observó que los programas de configuración dan por default el canal 1 o el 6, pero si queremos identificar el que más nos conviene para nuestra red, debemos evitar los dados por los programas, o mejor aún, hacer una sencilla exploración del sitio.

4.2. Evaluación

Se decidió comparar las redes inalámbricas en el tercer piso del edificio Valdez Vallejo por tratarse de un ambiente de trabajo cotidiano, contrario a los ambientes ideales donde los fabricantes prueban el desempeño de sus productos.

Se comenzó el experimento utilizando varias herramientas propietarias del fabricante de las tarjetas inalámbricas, no se tuvo éxito porque Windows no permite modificar los programas y sólo proporciona la información esencial sobre la red.

Después se intentó con Lindows pero el Kernerl no soportaba la plataforma G. Una vez que empezó a trabajar en Linux, se configuró la tarjeta inalámbrica 802.11 b 3com para ver los parámetros que se iban a medir en la investigación.

Después de hacer todas las mediciones con la tarjeta 802.11b, se instaló un AP 802.11g para hacer las pruebas con la tarjeta 802.11g.

Desafortunadamente no se consiguió un AP 802.11a, ni tarjeta, lo cual hubiera sido muy conveniente para ver el verdadero desempeño. La 802.11a tiene la ventaja de operar en una frecuencia más despejada, pero también cuenta con la gran desventaja de que a mayor frecuencia mayor atenuación y por lo tanto menor alcance.

Parámetro a medir	Unidades
Tasa de transmisión	Mbps
Throughput	Mbps
Nivel de la señal	dBm
Transiciones	Transiciones / hora
Colisiones	Colisiones / segundo

Tabla 14 Parámetros a medir

4.3. Elección de los parámetros a analizar.

Cuando se teclea en la línea de comandos iwconfig, dependiendo del dispositivo utilizado será los parámetros y las estadísticas obtenidas, cada tipo de driver dará sólo algunas dependiendo del hardware que soporte. En nuestra investigación se obtuvo lo siguiente:

4.3.1. Iwconfig

```
eth1      IEEE 802.11-DS  ESSID:"mobilelan"
          Mode:Managed  Frequency:2.412GHz  Access Point:
00:0D:54:A9:D6:A8
          Bit Rate:11Mb/s   Tx-Power=15 dBm   Sensitivity=0/65535
          Retry limit:16   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:8/10  Signal level:-40 dBm  Noise level:-256 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:4  Invalid misc:1143   Missed beacon:0

wifi0     IEEE 802.11-DS  ESSID:"mobilelan"
          Mode:Managed  Frequency:2.412GHz  Access Point:
00:0D:54:A9:D6:A8
          Bit Rate:11Mb/s   Tx-Power=15 dBm   Sensitivity=0/65535
          Retry limit:16   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:8/10  Signal level:-40 dBm  Noise level:-256 dBm
```

```
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:4  Invalid misc:1143   Missed beacon:0

eth0      Link encap:Ethernet  HWaddr 00:06:1B:D5:A2:EB
          inet addr:192.168.27.124  Bcast:192.168.27.255
Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:11
```

Con esta información se observan los parámetros útiles y los innecesarios para evaluar el desempeño de la red inalámbrica. La información se divide en tipos de tarjetas de red.

A continuación se muestra el tipo de conexión y su nombre de red.

```
eth1      IEEE 802.11-DS  ESSID:"mobilelan"
          Mode:Managed  Frequency:2.412GHz  Access Point:
00:0D:54:A9:D6:A8
          Bit Rate:11Mb/s   Tx-Power=15 dBm   Sensitivity=0/65535
          Retry limit:16   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:8/10  Signal level:-40 dBm  Noise level:-256 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:4  Invalid misc:1143   Missed beacon:0
```

La herramienta Iwconfig nos muestra los siguiente:

- Essid: da el nombre de la red y verifica que estemos conectados.
- Nwid / domain: proporciona el identificador de la red o dominio, se requiere para diferenciar todas las redes vecinas que comparten el mismo medio e identificar nodos pertenecientes a la misma célula.
- Nick name: asigna un sobrenombre a la estación, por ejemplo **“**mi nodo**”** para Linux.

- Mode: da la forma de operación del dispositivo dependiendo de la topología de la red y puede ser AD-Hoc si no hay AP o Managed. En esta investigación su función es verificar que estemos en modo Manged.
- Freq / Channel: informa el número de canal del dispositivo cuando los valores están debajo de mil, y la frecuencia de operación en Hz con los que están por encima..
- AP: indica a que AP se está conectando y si es posible informa la dirección física. Verificar que estemos usando el AP que se va a examinar. Cuando la calidad de la señal es muy baja el driver busca otro punto de acceso o se queda, dependiendo de su configuración.
- Bit rate: da a conocer la velocidad a la que se está transmitiendo.
- Txpower: muestra la potencia de transmisión para tarjetas que soportan múltiples, puede estar en W o dbm. Su función es informativa.
- Sens: (sensitividad), significa el nivel mas bajo de señal para el cual se hará un intento de la recepción del paquete. Éste parámetro se define de acuerdo al nivel de ruido que se tenga y sirve para evitar recibir ruido de fondo. En este proyecto no se configuró para eliminar el ruido de fondo porque se quizo detectar el máximo alcance de la señal, se utilizó con un carácter informativo.
- Retry: este parámetro puede ser puesto en intentos o en segundos usando el subfijo “m” o “u”. El hecho de que la mayoría de las tarjetas tienen retrasmisión de la MAC permite configurar el comportamiento del mecanismo. Para nuestros fines se dejó en 16.
- Rts threshold. umbral del RTS. RTS / CTS. Adiciona un “*handshake*” o verificación de que el canal está libre antes de iniciar la transmisión de cada paquete. Esto agranda la cabecera pero ayuda a mejorar el desempeño en caso de tener muchos nodos ocultos o activos. En este trabajo se puso en apagado debido a que se quizo el mejor desempeño de la red además de que no presentó un tráfico excesivo.
- Fragmentation threshold, es el umbral de fragmentación que permite dividir un paquete IP en muchos fragmentos pequeños antes de transmitirlos en el medio, esto agranda la cabecera pero en ambientes de mucho ruido reduce los problemas de errores. Para esta tesis se manejó apagado porque se trabajó en un ambiente de poco ruido.
- Encryption key: se usa para modificar la encriptación y aumentar la seguridad. Para poner la llave o clave hay que hacerlo en hexagesimal o en ASCII con el prefijo ”s”. En este caso se usó el enlace sin encriptación.
- Power management: puede manipular los parámetros de control de potencia y ahorrar energía, por ejemplo poniendo el tiempo entre despertar y empezar a transmitir, fijarlo para volver a dormir, o recibir paquetes multicast o unicast y entonces despertar. En la investigación se dejó apagado este parámetro.

- Link quality: se trata de la calidad del enlace, puede estar basado en el nivel de contención, en la interferencia, las tasas de errores de *bits* o *frames*, la calidad de la señal recibida, el tiempo de sincronización o en algún otro parámetro del hardware. Este es un valor adicional y depende únicamente del driver y del hardware.
- Signal level: (nivel de la señal), informa la fuerza con la que llega la señal, por lo regular esta en dBm.
- Noise level: (nivel de ruido), indica el nivel de ruido de fondo cuando ningún paquete es transmitido, está en dBm.
- Rx invalid nwin: indica el número de paquetes recibidos con un diferente NWID o ESSID, sirve para detectar problemas con redes cercanas. Usáremos este parámetro para las estadísticas.
- Rx invalid crypt: consiste en el número de paquetes que el hardware no pudo desencriptar. Sirve para ver problemas con la configuración de la encriptación. Este parámetro no se utilizó porque no se encriptó la información.
- Rx invalid frag: es el número de paquetes que el sistema no pudo re ensamblar adecuadamente. No se usó en esta investigación porque nose fragmentaron los paquetes.
- Tx excessive retries: número de paquetes que el hardware falló en entregar. La mayoría de los protocolos MAC lo intentan varias veces antes de darse por vencidos. Aquí no se utilizó porque puede variar por distintas razones.
- Invalid misc: se trata de otros paquetes perdidos en relación con una operación inalámbrica. En este proyecto no se utilizó porque puede haber muchas razones.
- Missed beacon: número de *beacons* de otra célula o AP que se han perdido. Éstos son mandados en intervalos regulares para mantener la coordinación con la célula o el AP, su pérdida usualmente indica que estamos fuera de rango.

Continuamos nuestro proyecto tecleando ifconfig para obtener más indicadores del funcionamiento de la red. Esto fue lo obtenido:

4.3.2. Ifconfig

```
eth1      Link encap:Ethernet  HWaddr 00:40:96:27:EF:A5
          inet       addr:192.168.27.131             Bcast:192.168.27.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25418 errors:2580 dropped:0 overruns:0 frame:2580
          TX packets:11584 errors:4 dropped:0 overruns:0 carrier:4
```

```
          collisions:903 txqueuelen:1000
          RX bytes:33597591 (32.0 Mb)  TX bytes:668992 (653.3 Kb)
          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:6585 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6585 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:693382 (677.1 Kb)  TX bytes:693382 (677.1 Kb)

wifi0      Link encap:UNSPEC  HWaddr 00-40-96-27-EF-A5-00-00-00-00-00-00-
00-00-00-00
          inet       addr:192.168.27.132             Bcast:192.168.27.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:2312  Metric:1
          RX packets:25418 errors:2580 dropped:0 overruns:0 frame:2580
          TX packets:11584 errors:4 dropped:0 overruns:0 carrier:4
          collisions:903 txqueuelen:100
          RX bytes:33597591 (32.0 Mb)  TX bytes:668992 (653.3 Kb)
          Interrupt:3 Base address:0x100
```

Al igual que iwconfig, ifconfig nos sirve para configurar y monitorear los parámetros de la interface de red, así como asignarle una dirección o configurar sus parámetros. Se tienen las siguientes opciones disponibles.

- HWaddr: nos da la dirección física del dispositivo.
- Inet addr: da la dirección IP, la, Broadcast y la máscara de red.
- Paquetes recibidos: total, errores, descartados, desbordados, y frames.
- Paquetes transmitidos: total, errores, descartados, desbordados, portadores, colisiones, en cola para transmitir.
- *Bytes* recibidos
- *Bytes* transmitidos.
- Interrupciones.
- Dirección base.

La velocidad de transmisión se midió con el número de *bytes* enviados en un determinado intervalo de tiempo, sin importar las variaciones de velocidad.

Sobre un plano actualizado del tercer piso del edificio Valdez Vallejo se eligieron los puntos representativos a medir que se utilizaron en todo el proyecto.

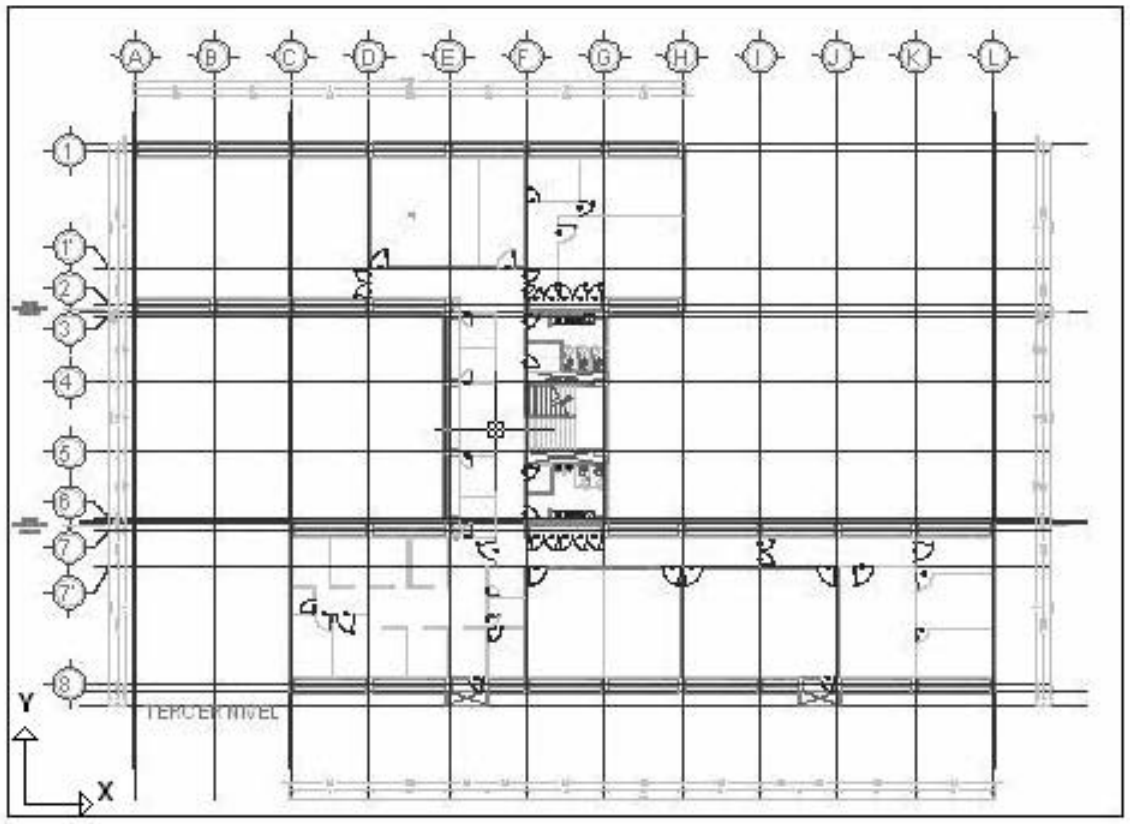


Figura 4-1 Tercera planta edificio Valdez Vallejo

Para guardar constantemente la vasta información obtenida se automatizó el proceso de guardar utilizando el signo “mayor que” de la manera comando>archivo de texto, las veces que fuera necesario. Este comando también sirvió para enviarla a un archivo de texto. Otros comandos de gran ayuda fueron “sleep” que hace una pausa de los segundo que escojamos, y el comando “date” que proporciona la fecha y hora con la que se verificó que todo funcionara bien.

Se ejecutó el archivo seis veces en todos los puntos ha estudiar para obtener cinco muestras, la media y la desviación estándar. Los datos obtenidos se almacenaron en el archivo hope.exe, donde todo se crea en prueba.txt y se le va adicionando información cada 20 segundos.

```
date > prueba.txt
iwconfig >> prueba.txt
ifconfig >> prueba.txt
sleep 20
date >> prueba.txt
iwconfig >> prueba.txt
ifconfig >> prueba.txt
sleep 20
date >> prueba.txt
iwconfig >> prueba.txt
ifconfig >> prueba.txt
sleep 20
date >> prueba.txt
iwconfig >> prueba.txt
ifconfig >> prueba.txt
sleep 20
date >> prueba.txt
iwconfig >> prueba.txt
ifconfig >> prueba.txt
sleep 20
date >> prueba.txt
iwconfig >> prueba.txt
ifconfig >> prueba.txt
```

Posteriormente se realiza una medición más detallada para monitorear cada momento, se escanearon las redes existentes en nuestro edificio de pruebas y se midió el número de transiciones de velocidad que realizaron las personas.

4.3.3. Resultados:

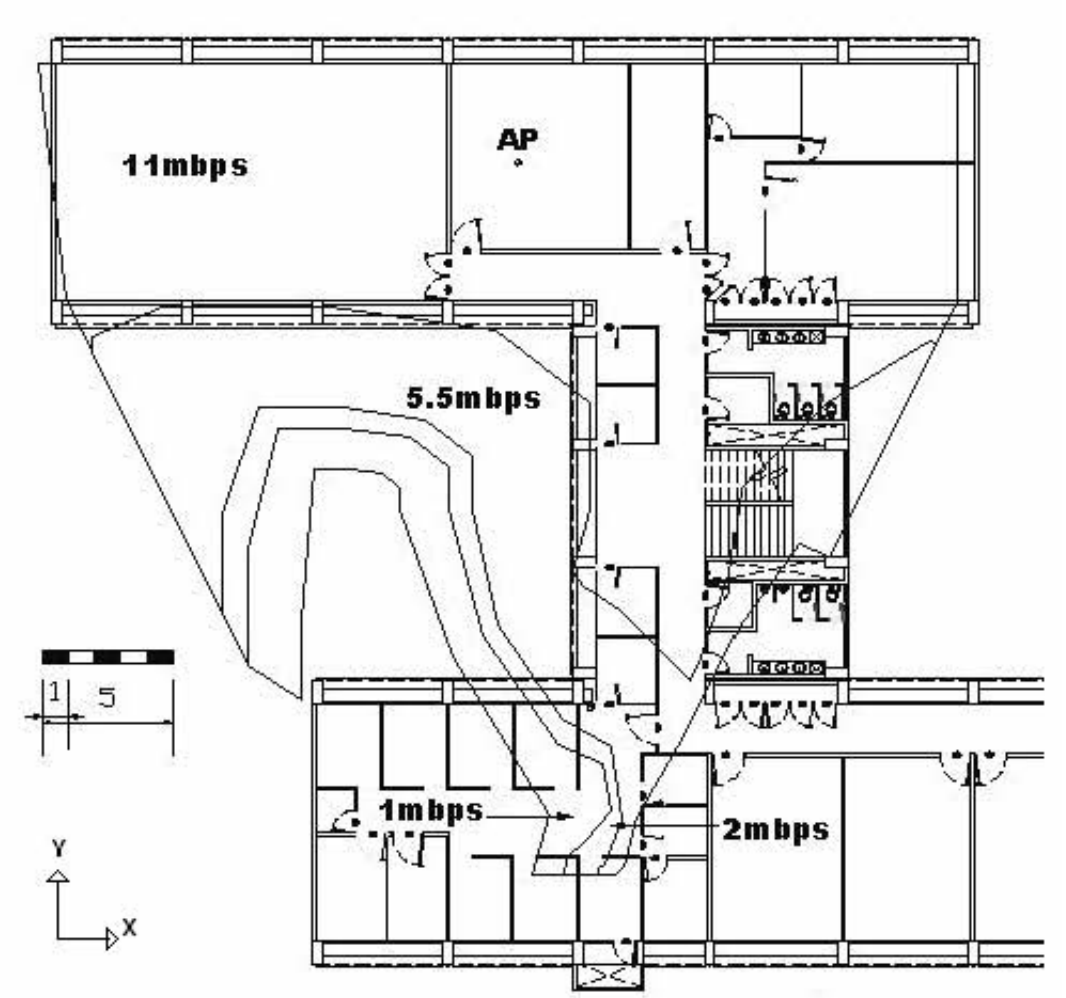


Figura 4-2 Velocidades del AP 802.11b

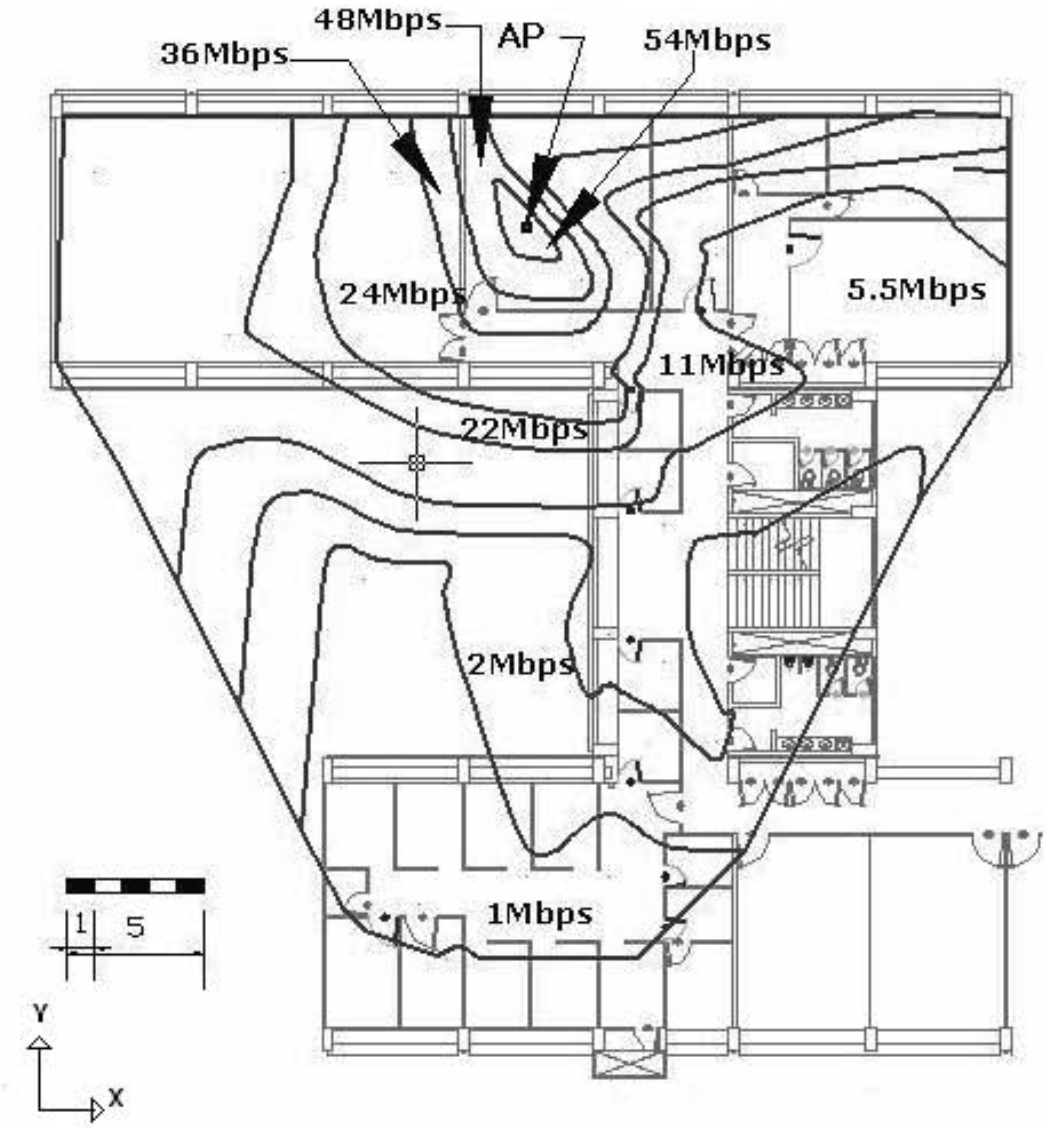


Figura 4-3 Velocidades del AP 802.11g

A continuación se analizó la tasa de transmisión en cada punto para ver su velocidad real.

Distancia al AP [m]	Tasa de transmisión [mbps]	Throughput [mbps]	Desviación estándar	Porcentaje
0.0	11	4.44	0.71	40%
2.8	11	4.42	1.22	40%
4.5	11	4.05	0.26	37%
5.4	11	4.95	0.49	45%
5.8	11	4.50	0.26	41%
6.7	11	4.65	0.15	42%

6.4	11	4.83	0.58	44%
18.4	11	3.28	0.64	30%
17.7	11	3.87	0.42	35%
9.2	11	3.79	0.96	34%
11.7	11	3.38	0.82	31%
7.1	11	2.51	0.69	23%
17.7	11	3.97	0.37	36%
17.5	11	3.69	0.77	34%
12.6	11	4.22	0.88	38%
7.8	11	3.94	0.52	36%
12.1	11	3.69	0.71	34%
15.3	11	3.48	0.48	32%
16.8	11	2.40	0.43	22%
20.2	11	2.27	0.77	21%
13.6	11	2.06	0.46	19%
19.3	11	2.93	0.20	27%
15.3	11	1.17	0.23	11%
15.8	11	1.10	0.23	10%
16.4	5.5	0.15	0.06	3%
23.5	5.5	0.24	0.06	4%
24.2	2	0.51	0.05	25%
27.3	5.5	0.25	0.15	4%
24.0	2	0.68	0.17	34%
27.2	0	0.00	0.00	
26.7	1	0.54	0.07	54%
25.3	1	0.54	0.07	54%
26.0	1	0.10	0.09	10%
24.4	0	0.00	0.00	

Tabla 15 Tasa de transmisión vs Througput en 802.11b

En el mejor de los casos del estándar 802.11b su desempeño alcanzó el 54%, esta claro que existen encabezados pero no fueron significativos porque se mandó información continuamente y se obtuvo un buen tamaño promedio de frame, 1482 en 802.11b y 1511 bytes en 802.11g, ya que el máximo es de 2334. Esto nos indica que se mandaron a un 63% y 64% del tamaño máximo con una eficacia de datos respecto a la cabecera del 97%, algo que resulta bastante respetable. En el peor de los casos cayó a un tres por ciento. Estas distancias están en línea recta

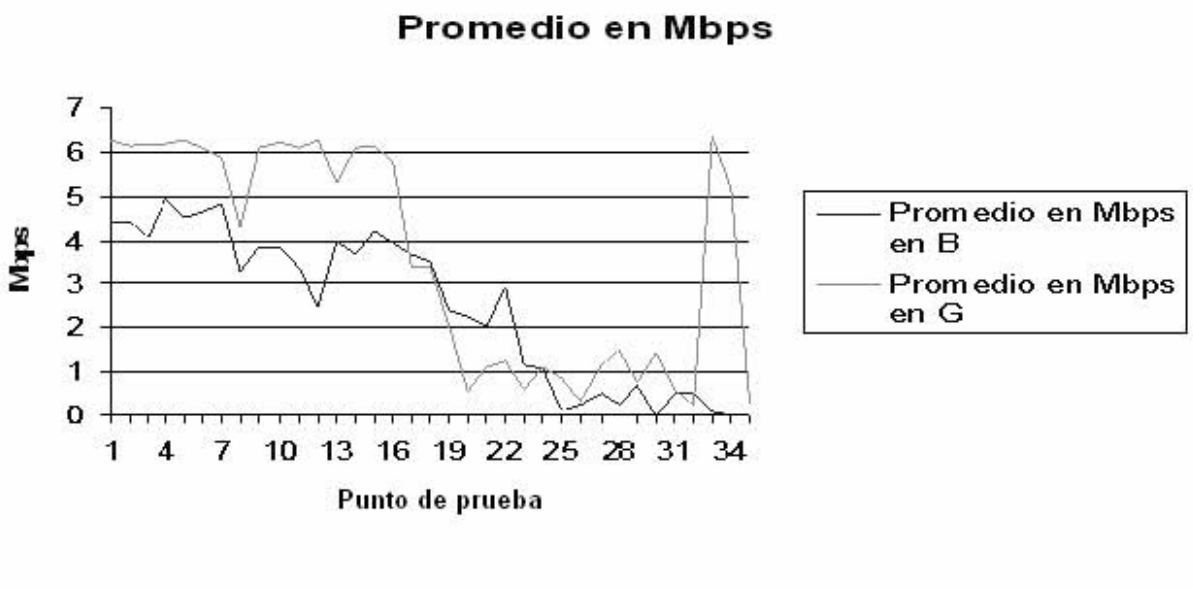
desde el AP y presentan diferentes tipos de materiales que atenúan la señal de distinta manera.

Distancia al AP [m]	Tasa de transmisión [mbps]	Throughput [mbps]	Desviación estándar	Porcentaje
0.0	54	6.3	2.21	12%
2.8	48	6.1	2.72	13%
4.5	48	6.2	1.80	13%
5.4	36	6.2	1.37	17%
5.8	36	6.2	0.52	17%
6.7	36	6.1	3.45	17%
6.4	36	5.9	2.28	16%
18.4	24	4.3	0.19	18%
17.7	24	6.1	2.81	25%
9.2	24	6.2	1.48	26%
11.7	24	6.1	3.07	25%
7.1	12	6.2	0.91	52%
17.7	12	5.3	0.14	44%
17.5	18	6.1	0.41	34%
12.6	12	6.1	2.67	51%
7.8	18	5.8	1.18	32%
12.1	12	3.4	1.10	28%
15.3	12	3.4	1.27	28%
16.8	12	2.0	0.07	17%
20.2	11	0.6	0.27	5%
13.6	11	1.1	0.64	10%
22.1	11	1.3	0.22	11%
15.3	5	0.6	0.17	13%
15.8	5	1.1	0.50	23%
16.4	6	0.9	0.19	14%
23.5	5	0.4	0.17	7%
24.2	2	1.2	0.09	60%
27.3	5	1.5	0.35	31%
24.0	5	0.8	0.26	15%
27.2	11	1.4	0.08	13%
26.7	1	0.6	0.32	61%

25.3	2	0.2	0.07	12%
26.0	2	6.4	1.53	318%
24.4	5	5.2	3.86	103%
14.3	2	0.3	0.43	15%

Tabla 16 Tasa de transmisión vs Througput en 802.11g

El mejor desempeño fue en la velocidad más lenta con un 318%, pero el dato no es confiable ya que existía una modulación para 5Mbps y el driver lo reconoció de 2Mbps, el desempeño registrado cada 20 segundos fue variable y pudo haber cambios de transmisión que no se detectaron, además se presenció una ráfaga que disparó los resultados. El peor caso se da en la velocidad más alta de transmisión con un 12% pese a los 54Mbps que se marcaban.



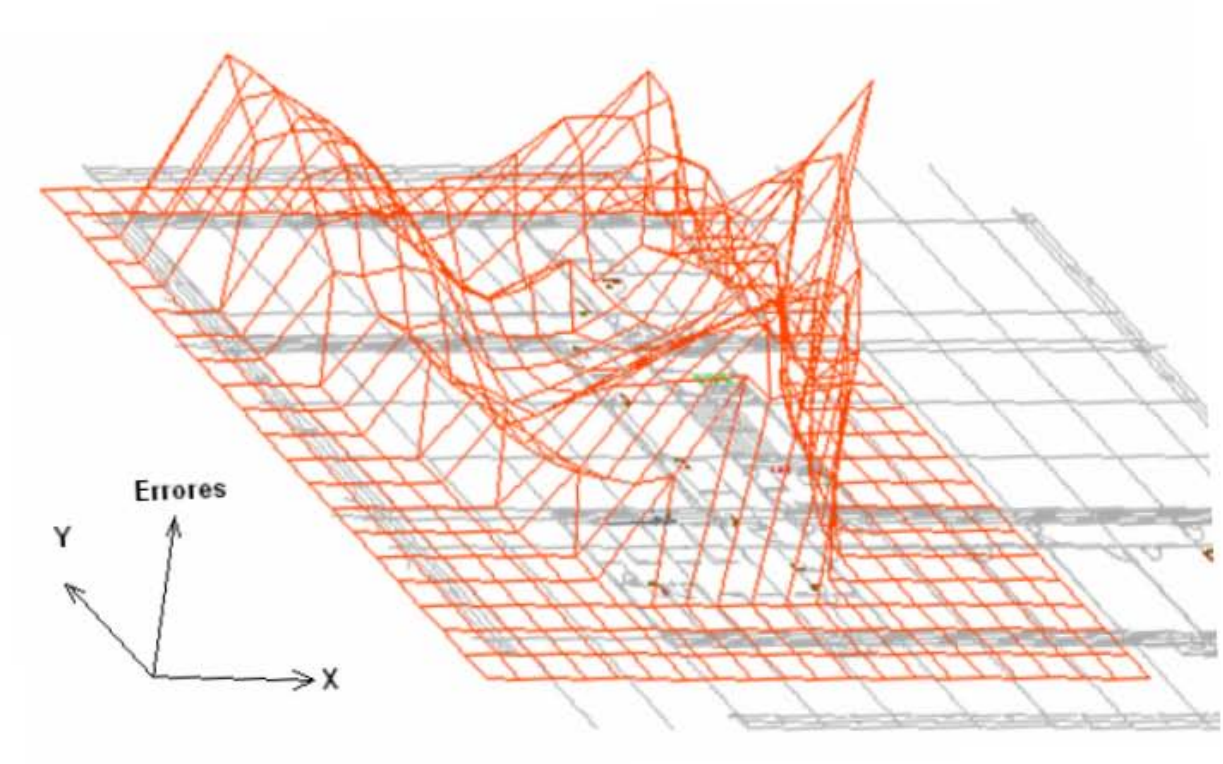


Figura 4-4 Errores en 802.11b

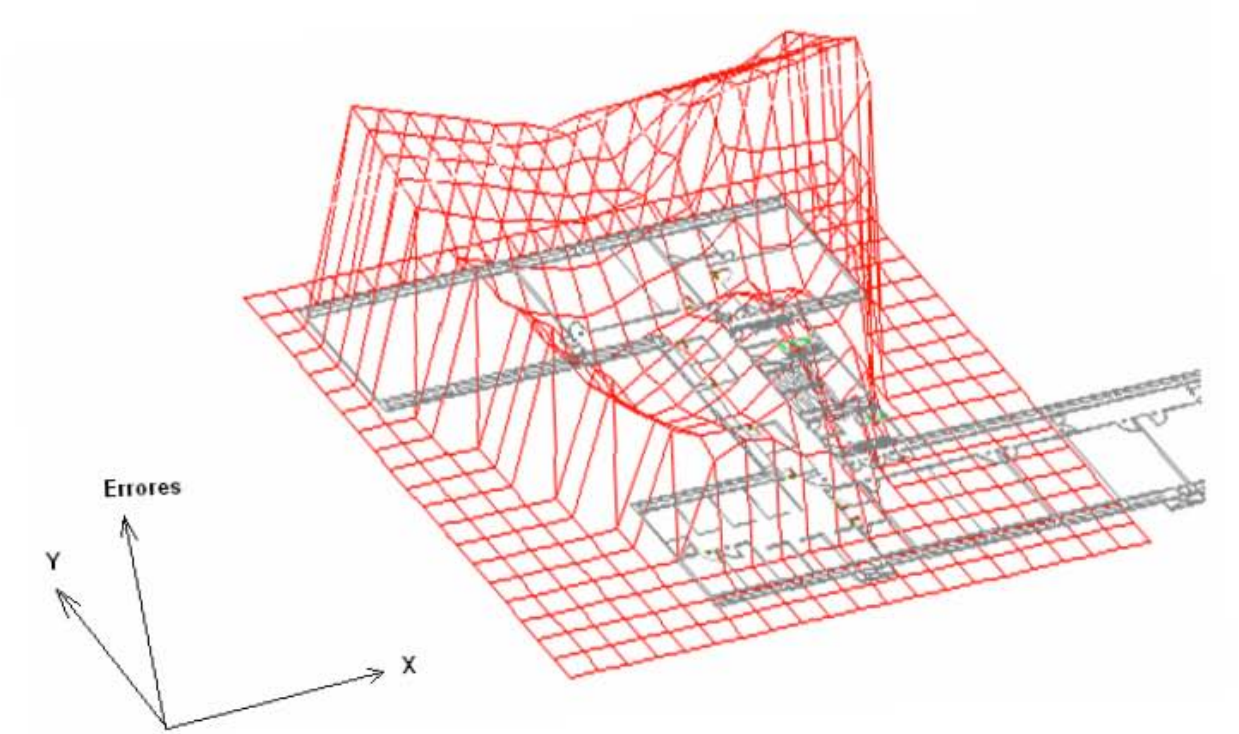


Figura 4-5 Errores en 802.11g

Punto	Errores/s recibidos en 802.11b	Errores/s recibidos en 802.11g	Diferencia G-B
1	0.4	92.9	92.5
2	0.8	76.8	76.0
3	14.4	80.6	66.2
4	45.4	87.1	41.7
5	18.5	79.9	61.4
6	15.3	95.9	80.7
7	21.1	96.4	75.3
8	104.8	132.2	27.4
9	57.6	116.2	58.6
10	69.9	106.4	36.6
11	82.0	104.4	22.3
12	128.9	121.6	**-7.3**
13	18.4	152.4	134.0
14	54.3	110.9	56.6
15	17.3	85.7	68.4
16	34.0	140.2	106.2
17	45.6	62.5	17.0
18	74.1	80.7	6.6
19	130.4	69.9	-60.4
20	142.4	26.7	**-115.7**
21	163.4	26.8	**-136.6**
22	98.1	64.1	**-34.1**
23	218.7	63.8	**-154.9**
24	188.2	39.5	**-148.7**
25	34.2	61.4	27.2
26	80.6	35.2	**-45.5**
27	149.6	79.5	**-70.1**
28	29.5	19.1	**-10.5**
29	165.2	60.0	**-105.2**
30	0.0	64.4	64.3

31	115.8	49.5	**-66.3**
32	115.8	63.1	**-52.7**
33	33.9	64.0	30.1
34	0.0	25.5	25.5
35	0.0	20.3	20.3
Total	**2468.5**	**2655.4**	**186.9**

Tabla 17 Comparación de errores

Los errores en 802.11b y en 802.11g al final se comportaron de una manera similar, lo extraño es que el primero tuvo una tasa de paquetes con errores muy bajos en las cercanías del AP y en la parte media se dispararon. El segundo,, en las cercanías presentó una tasa de errores muy grande que fue disminuyendo conforme se alejaba. En los últimos puntos hay demasiados errores pero el estándar 802.11b, no presentó transmisión de información en esta zona.

4.4. Colisiones

El comportamiento de las coaliciones está relacionado con la forma de la estructura (*figura 4-6*) porque pueden aumentar cuando hay rebotes en las paredes. Cuando se experimentó en la estatua del Ing. Valdez Vallejo las coaliciones disminuyeron porque sólo llegan unos cuantos paquetes con poco tráfico. Desafortunadamente no se pudo realizar este análisis con el 802.11g, ya que el driver para Linux indicaba cero, ya que no soportaba esta función.

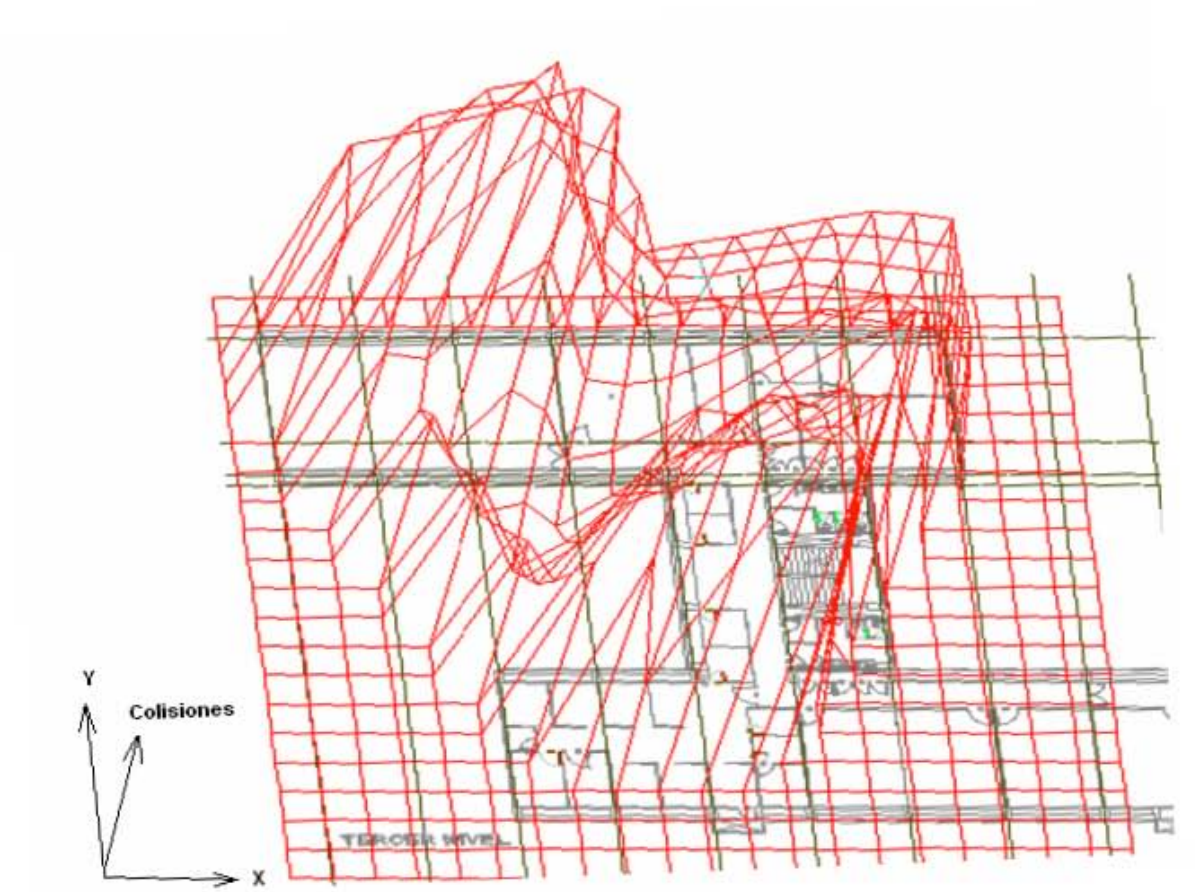


Figura 4-6 Colisiones en 802.11b

4.5. Nivel de la señal.

La señal se midió con la escala logarítmica dbm. El ruido se comportó en el orden -94 a -97 dbm, con un máximo de 97 dBm en la escalera. Las redes se comportan como ruido en los pisos inferiores porque no se puede completar la recepción. El promedio en todos los pisos fue 95 dBm. La comunicación se pierde cuando la intensidad de la señal llega a niveles muy cercanos al ruido. Al tomar mediciones después de la frontera de la zona con capacidad de transmisión se obtuvo un valor de ruido de -90dbm insuficiente para comunicarse.

En la aplicación de ambos estándares se observó un comportamiento similar debido a que la información se transmite por medio de ondas electromagnéticas que les es indiferente de que estándar son, sin embargo si quién las transmite, con qué antena, en qué frecuencia, por qué medio y a qué receptor. (Figuras 4-7 y 4-8)

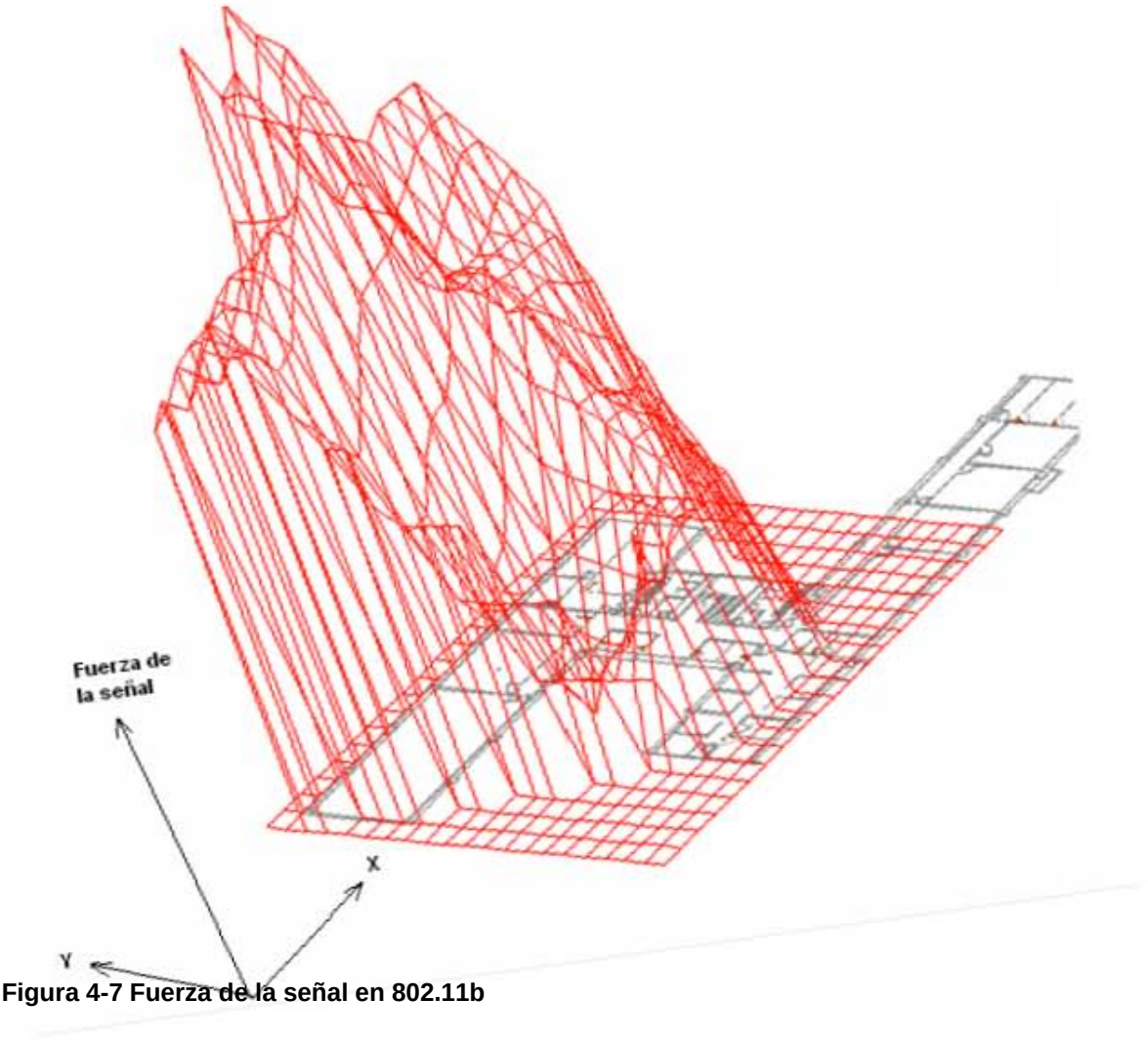


Figura 4-7 Fuerza de la señal en 802.11b

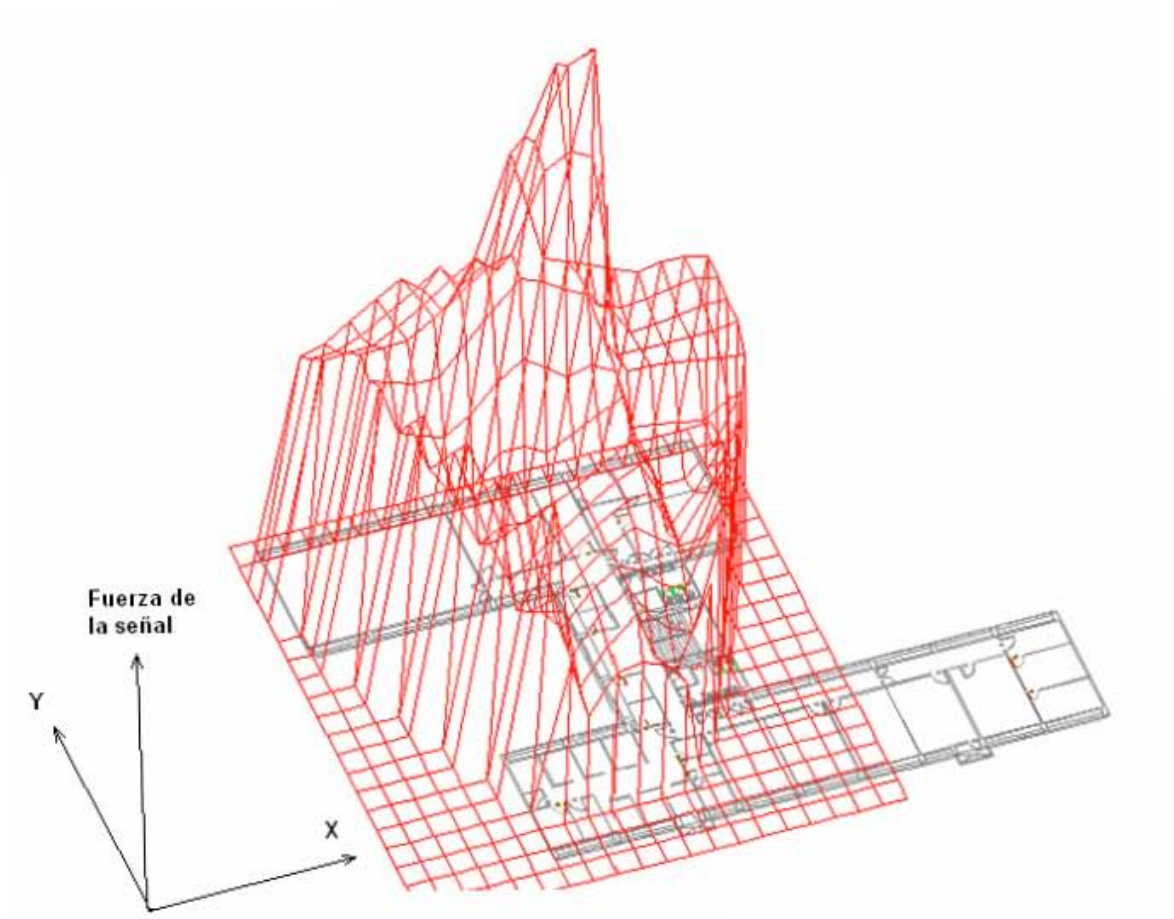


Figura 4-8 Fuerza de la señal en 802.11g

4.5.1. Nivel de señal y thoughput.

Entre la intensidad de la señal y el throughput, especialmente en 802.11b existe una fuerte correlación, como era de esperarse, porque trabajan en la misma frecuencia y tienen atenuaciones similares frente a los distintos materiales. Donde hay intensidad de la señal se tiene comunicación con el AP. La correlación no es de 1 debido a que en momentos en que más se utiliza el AP tal vez es mejor buscar otra opción como la que promueve el 802.11k con sus transiciones de estaciones base para tratar de equilibrar el desempeño de todos los AP, y no sólo decidir por la intensidad de señal.

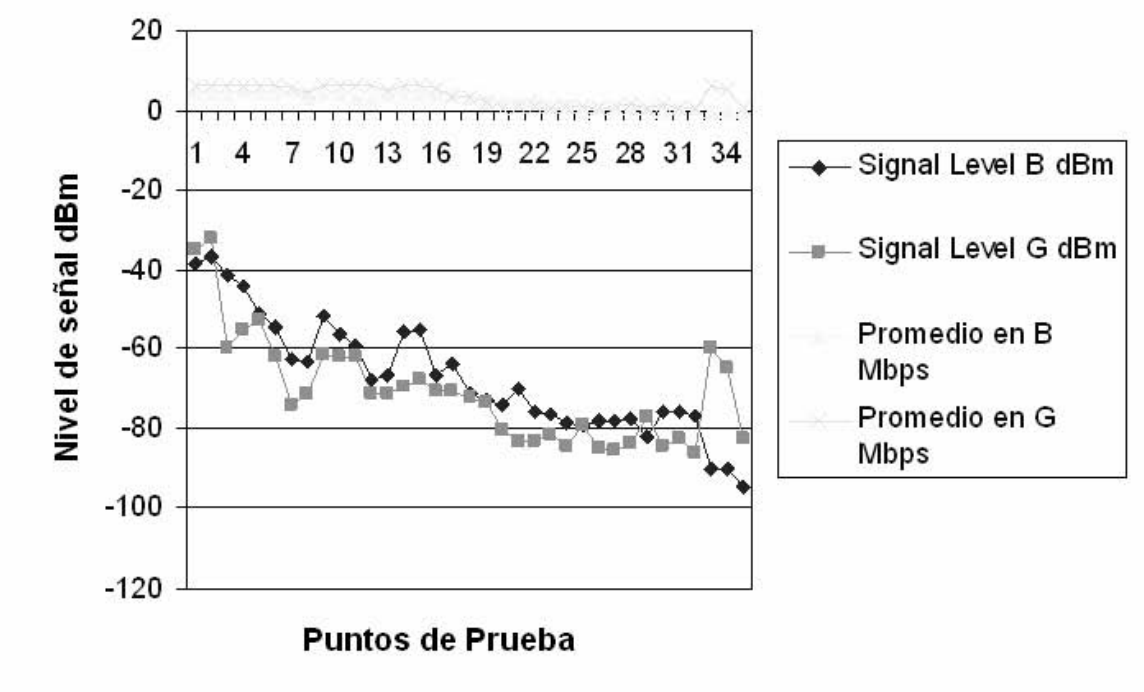


Figura 4-9 Niveles de señal vs Throughput

Correlación	Signal Level 802.11b	Signal Level 802.11g	Throughput 802.11b	Throughput 802.11g
Signal Level 802.11b	NA	0.7963077	0.86206014	NA
Signal Level 802.11g	0.7963077	NA	NA	0.7963077
Throughput 802.11b	0.86206014	NA	NA	0.73947046
Throughput 802.11g	NA	0.7963077	0.86206014	NA

Figura 4-10 Correlaciones entre Signal Level y Throughput

4.6. Transiciones de velocidades

Se hizo un muestreo de las veces que las personas cambian de una velocidad a otra. Los casos de usuarios de laptop fueron escasos por tratarse de un aparato incómodo para estar en movimiento. LA relevancia de esto es que cada vez es mayor el porcentaje de dispositivos que tienen 802.11 como los PDAs, los aparatos para juegos, los teléfonos que tienen conectividad de datos a través de este estándar y no sólo de Edge, GPRS, o EVDO. Los usuarios de estos dispositivos tienen necesidad de cambiar de una velocidad a otra, y

probablemente de un AP a otro, esto en un futuro nos permitirá hacer llamadas de VOIP desde los celulares, lo cual se trata de una las ideas que 802.11r ya se encuentra desarrollando.

Durante una hora se analizó el comportamiento de las personas en el Valdéz Vallejo en un momento en la que no había clases y el flujo de gente era moderado.

Velocidades **[mbps]**	Transiciones por hora
54	0
48	10
36	12
24	14
22	14
11	25
5.5	42
2	15
1	6

Tabla 18 Transiciones en 802.11b

Velocidades	Transiciones por hora
11	4º
5.5	15
2	6
1	5

Tabla 19 Transiciones en 802.11g

4.7. Análisis por segundo

Se probó un punto y se comparó su versión larga con la corta con una toma de datos cada veinte segundo para, finalmente, observar un comportamiento similar entre ambas versiones. Se graficó la intensidad de la señal en los dos casos:

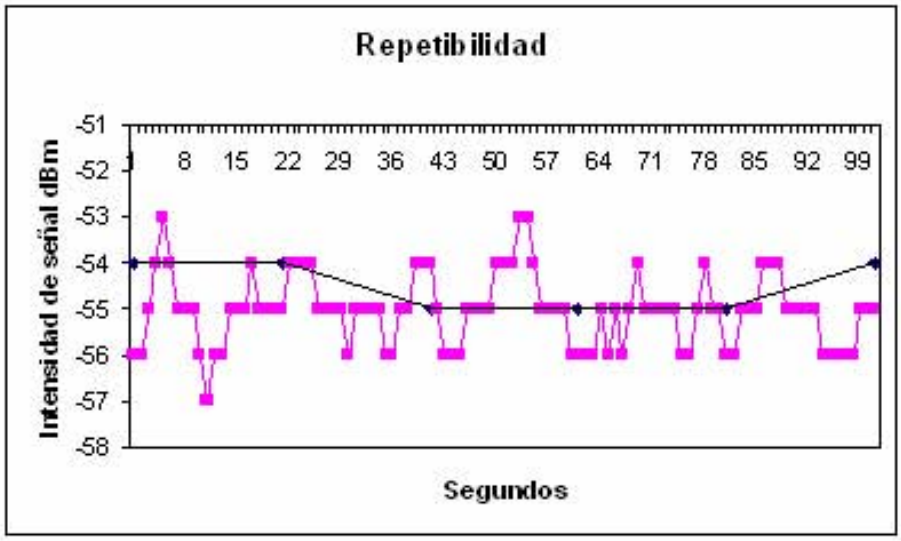


Figura 4-11 Análisis por segundo y cada 20 segundos

El promedio de la toma de datos cada 20 segundos fue -54.5 y -55.029703 cuando se hizo por segundo, ambas son muy similares y la primera puede ser representativa de la segunda para no perdernos en un mar de datos e información.

Se realizaron pruebas 12 veces en un punto para observar el problema de la repetibilidad en los experimentos. Los resultados mostraron diferencias de comportamiento porque las condiciones del medio no son las mismas, pero resultaron bastante parecidos como para establecer datos modelo. (*Figura 4-14 y 4-15*)

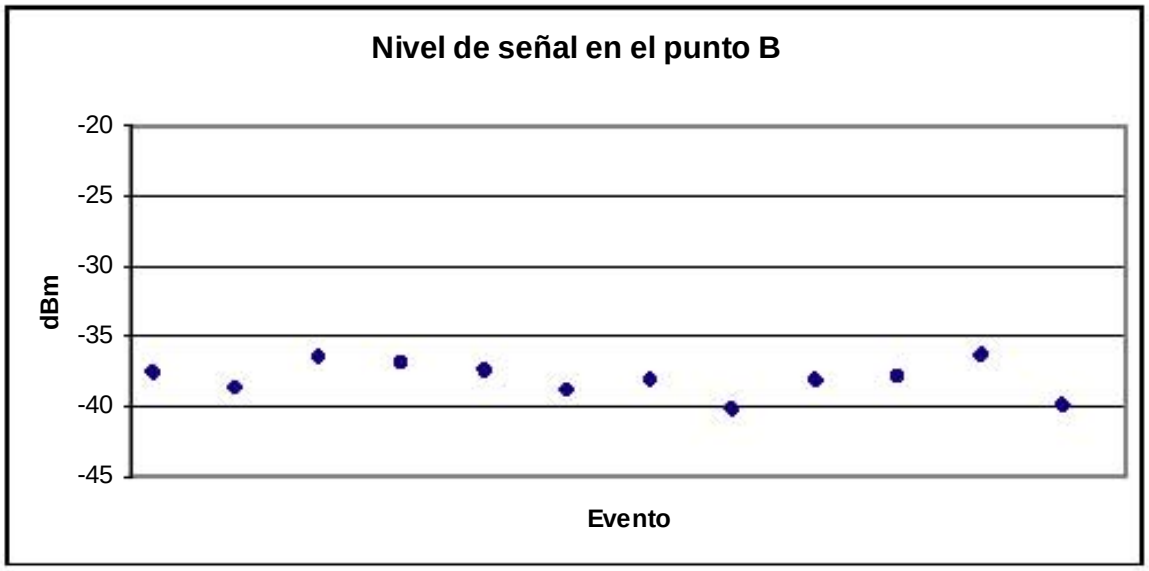


Figura 4-12 Cambios de nivel de señal en un mismo punto

Promedio=-37.9583333, Desviación estándar=1.23679898

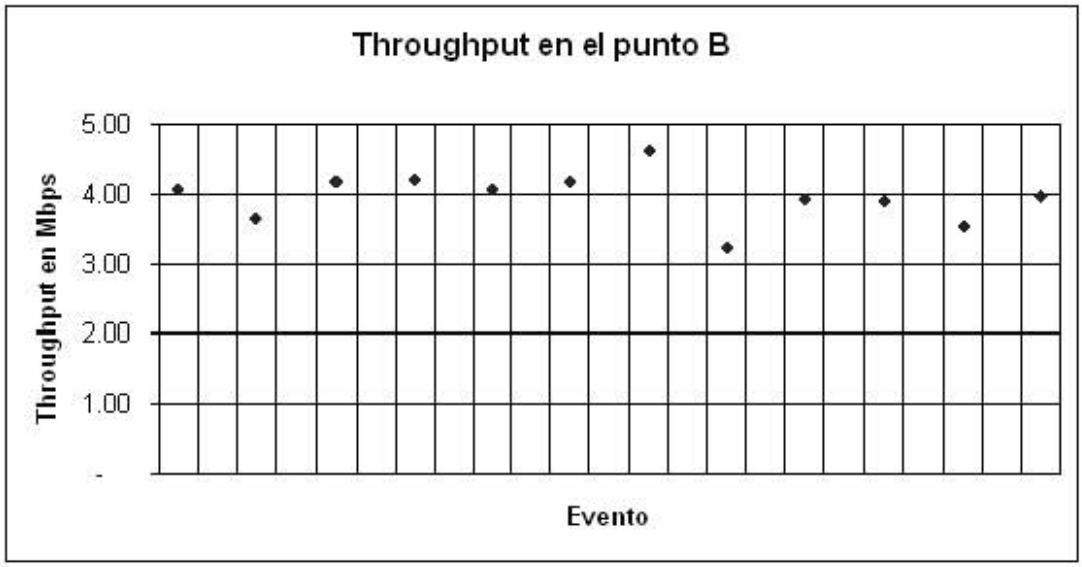


Figura 4-13 Cambio de throughput en un mismo punto

Promedio 3.953 Mbps, Desviación estándar=0.36

5. Capítulo 5

5.1. Análisis y Conclusiones.

En este trabajo se evaluó las ventajas y desventajas que ofrecen los estándares 802.11b y 802.11g. Además de revisar los estándares 802.11 restantes con la finalidad de analizar sus posibilidades de aplicación en un futuro cercano.

5.1.1. Resultados obtenidos:

- Se cuenta con un mayor conocimiento acerca del funcionamiento de las redes inalámbricas.
- Se tiene caracterizado de los estándares 802.11b y 802.11g en un ambiente real de trabajo en este caso el tercer piso del Valdez Vallejo.

Al hacer un comparativo entre las velocidades se hizo evidente que el estándar 802.11g en algunos casos presenta mejores registros así como un área más amplia de cobertura pero su desempeño no es cinco veces más rápido, como lo maneja su marketing. Incluso el desempeño del 802.11b llegó a superarlo ya que trabajaba con 11 Mbps mientras que el 802.11g se encontraba en el área de 5.5 Mbps, esto tal vez se debe al comportamiento inadecuado que puede presentar la tarjeta o el driver que además en su versión para Linux muchas veces no cuenta con soporte técnico del fabricante.

En teoría no deberían existir éstas diferencias porque el estándar 802.11g lo que adiciona es un tipo de modulación de OFDM mediante la capa ERP que supuestamente le permite funcionar a muy alta velocidad. Se logró un aumento de velocidad de más del 50% que dista mucho del 500% que se promociona. Tal vez ello se logre en un campo libre de interferencias o dentro de una cámara anecoica, pero no en la realidad.

Ante la necesidad de seleccionar una nueva tarjeta, recomiendo ampliamente el estándar 802.11g por ser mejor en varios aspectos, actualmente su diferencia en precio es casi nula y las que solamente eran para 802.11b ya están casi descontinuados. Sin embargo, no recomiendo cambiar el AP y la tarjeta del estándar versión “b” por el “g” ya que las diferencias en el desempeño no son tan grandes como para pensar en remplazar todo el hardware, más aún, sería inconveniente si la mayoría de nuestras salidas a la nube del Internet no superan 1Mbps.

Por lo tanto, es conveniente recurrir a una tarjeta del 802.11g para asegurar la interoperabilidad con 802.11b y de preferencia que sea compatible con 802.11a.

5.1.2. Aportaciones:

- Comparativo en un ambiente real de trabajo de los estándares 802.11b y 802.11g.
- Recomendación de cambiar a 802.11g solo para nuevas tarjetas.
- Creación de literatura en español sobre redes inalámbricas.
- Falta de normalización de la calidad de las tarjetas WI-FI. Por lo que se recomienda una Norma Mexicana.

Estando en contacto con diversas tarjetas de red inalámbrica se observó que el desempeño varía de una a otra a pesar de que cumplen con el estándar 802.11x y de estar certificadas por Wi-Fi. Algunas detectan redes que se encuentran muy alejadas mientras que otras, por el contrario, identifican muy pocas. En cuanto a la intensidad de la señal también hay diferencias, algunas tienen una señal al 100% y otras, estando en el mismo punto, del 80% o 70%.

Se puede deducir que los fabricantes de tarjetas de red no siempre cumplen con los procesos de certificación de calidad del producto y además su publicidad exagera dichas cualidades. Se recomienda acudir a las marcas conocidas que, aunque pueden ser más costosas, garantizan el cumplimiento del desempeño anunciado. Debido al constante crecimiento de las redes inalámbricas yo recomendaría una Norma Mexicana para asegurar la interoperabilidad de los dispositivos, así como su calidad.

5.1.3. Trabajos Futuros.

Ante el constante avance de las redes inalámbricas podría hacerse el siguiente paso de esta investigación usando 802.11a y los nuevos 802.11n.

Comparación de diferentes tarjetas de red para ver la calidad de los dispositivos.

5.1.4. 802.11a

Respecto a 802.11a, aunque no se pudo incluir en las pruebas, tampoco lo recomiendo porque, aunque trabaja en una banda con poca saturación, permite un mayor número de usuarios en un mismo cuarto, esta tiene más atenuación y su costo es mayor. Tanto 802.11a como 802.11g operan a 54Mbps, pero el triunfo se lo lleva 802.11g por su capacidad de compatibilidad con 802.11b.

5.1.5. El futuro

Tal vez en un futuro valdría la pena pensar en cambiar a estándares como el MIMO que ofrece más alcance y 108Mbps, pero como protocolo propietario sólo tendrá ese gran desempeño con los dispositivos de dicho fabricante.

Se perfila un nuevo estándar inalámbrico, el 802.11n en cuya página electrónica se informa que podría alcanzar los 600Mbps. Está fechado para principios del 2007 aunque ya se empiezan a vender productos pre-n que dicen alcanzar velocidades de 108Mbps, aunque éstos aún no están estandarizados. Para ello se está trabajando en dos frentes:

El primero es *WorldWide Spectrum Efficiency* (WWiSE) apoyado por Texas Instruments, Broadcom, Conexant, STMicro, Airgo y Bermai. Los partidarios de WWiSE creen que 802.11n necesita ser capaz de usar el canal con 20Mhz de ancho, el mismo que 802.11b y 802.11g, a fin de que no siga los pasos del menos conocido 802.11a, que se despoja de la compatibilidad con estándares anteriores a cambio de velocidades mayores.

Al emplear, WWiSE se debería poder alcanzar velocidades de hasta 540Mbps empleando *Multiple Input, Multiple Output* (MIMO), el actualmente utilizado *Orthogonal Frequency Division Multiplexing* (OFDM) o una serie de antenas 4x4 y un canal de 40Mhz de ancho.

Gracias a la compatibilidad con anchos de canal de 20Mhz, la tecnología sería capaz de retroceder a una tecnología más lenta cuando sea usado en países que prohíban el uso de los 40Mhz del canal.

El segundo frente de 802.11n consiste en TGn Sync, fundado por Agere Systems y apoyado por Cisco, Intel, Nokia, Nortel, Philips, Sony y otros. Como WWiSE, TGn Sync planea usar el canal de 40Mhz y la tecnología MIMO para alcanzar una velocidad real de alrededor de 175Mbps y velocidades teóricas rozando los 600Mbps.

Esperemos el logro de un nuevo estándar 802.11 en el que sólo pueda escogerse un estándar con la opción de mantener o eliminar la compatibilidad con los estándares anteriores. Esto evita tener que comprar nuevas tarjetas con el inconveniente de que cada vez los dispositivos portátiles son más pequeños y en muchas ocasiones ya han eliminado el puerto PCMCIA. No es conveniente utilizar muchos estándares porque la dificultad de elección se incrementa y entonces es necesario investigar si se cuenta con red inalámbrica y si es compatible con la que se tiene.

5.2. Comparativa:

La certificadora de Wi-Fi hace el siguiente comparativo:

¿Cuál escoger? A vs B vs G Tabla comparativa de tecnologías inalámbricas			
Estándar Inalámbrico	802.11b	802.11ª	802.11g
Popularidad	Alta	Baja	Media
Velocidad	11Mbps	54Mbps	54mbps
Costo relativo	Económica	Cara	Medio Económica
Frecuencia	2.4Ghz	5Ghz	2.4Ghz
Alcance	30.48m – 45.72m	7.62m – 22.86m	30.48m – 45.72m
Acceso publico	Existe un gran número de “hotspots”, en aeropuertos, hoteles, campus, restaurantes y áreas públicas.	Prácticamente no existen	Compatible con los “hotspots” de 802.11b, además de que se espera que se vayan cambiando a 802.11g
Compatibilidad	Es el de mayor adopción.	Incompatible con 802.11b y 802.11g	Compatible con 802.11b y 802.11g, incompatible con 802.11ª
Principales ventajas	Precio bajo	Soporta más usuarios por cuarto.	Mayor valor por un 10% más de precio tenemos hasta 5 veces más de velocidad
	Excelente rango de señal	No es afectada por interferencias de dispositivos 2.4Ghz	Compatible con los hotspots de 802.11b
	La cobertura penetra la mayoría de las paredes.	Puede coexistir con redes B y G	Excelente rango de señal
	Trabaja con hotspots públicos.	La cobertura se limita a un solo cuarto.	La cobertura penetra la mayoría de las paredes.

Tabla 20 Comparativo de WECA

Prácticamente podría decir que el estándar 802.11g cumple casi con todo, funcionó bastante bien ya que la señal sí penetró la mayoría de las paredes, tuvo un buen rango de alcance en línea recta de más de 26 metros, aunque lo ideal son 45m pero en condiciones óptimas. La prueba se hizo en un ambiente real de trabajo con paredes, columnas, ventanas, etc. Únicamente hubo diferencias entre las velocidades asignadas por sus fabricantes y las mediciones inferiores alcanzadas en esta investigación, lo cual puede explicarse al concebir los datos proporcionados por los fabricantes como resultados ideales.

Es importante considerar que hablar de datos ideales nos plantea un problema para determinar lo que podría ocurrir en la realidad, por ejemplo, para determinar la velocidad de una red inalámbrica es necesario considerar la velocidad del procesador, la cantidad de memoria disponible en ese momento, el número de tareas en espera, esto duplicado ya que se usa una computadora suplicante y el servidor al que le solicitamos la información, más los problemas que pueden existir en un medio cambiante, para que finalmente la velocidad real diste de la expectativa teórica.

5.3. Epílogo

El desarrollo de las redes inalámbricas representa el siguiente escalón en la tecnología de redes al permitir dotar de nuevas posibilidades a las redes convencionales. Las principales capacidades de las tecnologías inalámbricas aumentan la movilidad y la flexibilidad en las redes, para el correcto desarrollo de estas características es necesario que existan las terminales móviles (portátiles, PDAs, video juegos, reproductores musicales, teléfonos) que deben ser los principales beneficiarios de estas tecnologías. De modo que el desarrollo de las WLAN irá ligado al del mercado de dichas terminales. Con el aumento de las redes inalámbricas aumentará la diversidad de dispositivos.

El progresivo abaratamiento de las computadoras, incluidas las laptop, facilitan la expansión de las redes domésticas e inalámbricas que en un futuro se convertirán en algo normal en las casas debido a la facilidad con que se instalan y la capacidad de interconexión con otros dispositivos pertenecientes al campo de la domótica. Una red inalámbrica será cada vez más indispensable en las casas y oficinas para el control de luces, persianas, ventanas, cortinas, enchufes así como en climatización automática, vigilancia calefacción, refrigeración y la gestión óptima de la energía. Sería muy engorroso y problemático cablear todo.

IPV6, apoyándose en redes inalámbricas, proporcionará direcciones para cada uno de los dispositivos y será muy fácil controlarlos a distancia. Esto significa que el avance de la tecnología debe ser en conjunto y las redes inalámbricas no son la excepción.

Respecto a la elección de tecnología es recomendable la 802.11g, si se va a adquirir un nuevo dispositivo y si no esperar hasta la siguiente tecnología, recordar siempre buscar que haya interoperabilidad entre los equipos, ya que eso nos permite ir amortizando la inversión y no tenerla que hacer de golpe.

Por último hay que hacer notar que las redes 802.11 no consisten en una competencia de las redes por cables, más bien se complementan, una nunca podrá sustituir a otra o ser mejor respecto a las demás, cada una tendrá que ir tomando su lugar en el mercado de las telecomunicaciones dependiendo de las necesidades de cada uno de los usuarios.

Esperemos que se puedan seguir implementando las nuevas tecnologías en México y que la Cofetel les asigne frecuencias de uso sin licencia que le darán mayor competitividad al país.

6. Apéndices y Anexos.

6.1. Glosario.

AP Punto de acceso
La mayoría de las redes 802.11, llamadas redes de infraestructuras, utilizan una pieza básica de hardware llamada punto de acceso, y todos los equipos de la red se comunican a través de ese dispositivo. Un punto de acceso actúa como una especia de estación central que gestiona toda la información que se envía a través de los equipos.

Ad hoc
Redes que utilizan comunicación directa de equipo a equipo. Las redes ad hoc hacen posible que los equipos "hablen" (envíen información) de manera directa de uno a otro.
Para que funcione una red ad hoc, todos los equipos de la red tienen que tener instalada una tarjeta de red inalámbrica que tiene que configurar (instaladas en cada uno de los equipos que conforman la red) en modo Ad Hoc.

DHCP
DHCP (Protocolo de Configuración dinámica de Host)

Dirección IP
La dirección IP (Protocolo de Internet) de un ordenador es la serie de números con las que se identifica un equipo y es algo parecido a: 192.168.0.99-cuatro grupos de cifras divididos por periodos.

Latencia
La Latencia es el tiempo que tarda un equipo en iniciar una descarga (o cualquier otro tipo de información requerida).

PCI
La interconexión de componentes periféricos (PCI) y la USB (Universal Serial Bus) son las dos formas de las que dispone para conectar equipo a su ordenador.

PCMCIA Tarjeta de PC
La Asociación Internacional de Tarjetas de memoria para Ordenadores personales (PCMCIA) ha desarrollado la tarjeta PCMCIA, por lo general denominada tarjeta PC. Tiene más o menos el tamaño de una tarjeta de crédito, por lo general es la tarjeta en la que se realiza la conexión de red del portátil.

USB
El Puerto USB (Universal Serial Bus) es la alternativa a la interconexión de componentes periféricos (PCI). Todos los equipos de una red tienen que disponer de la tarjeta de red adecuada para poder comunicarse dentro de la red. Por lo general pueden obtener el tipo adecuado de tarjeta para su red en cualquiera de las clases de USB o PCI.

WEP
El estándar de Privacidad equivalente a la del cable (WEP) es el parámetro que se utilizaba antes para la seguridad y la protección de información en las redes inalámbricas. El estándar que se utiliza actualmente es el de WPA, que es más sólido pero todavía hay dispositivos que no ofrecen soporte para él.

WPA
El Acceso Protegido Wi-Fi (WPA) es el estándar actual para la protección de información y seguridad en las redes inalámbricas. De este modo se evita que usuarios no autorizados se conecten a su red.

6.2. Cómo generar las graficas en CivilCad, una mejora de Autocad.

Curvas de nivel.

Antes de generar curvas de nivel debe de producirse una triangulación entre los puntos “X”, “Y” y “Z” para que sea posible calcular por interpolación las curvas de nivel a los intervalos especificados. A continuación se describe el procedimiento mediante un ejercicio para ilustrar más claramente estos conceptos.

1. Una vez teniendo el dibujo en Autocad y los datos a graficar en un archivo de texto, del menú del módulo seleccione la rutina para importar puntos, al hacerlo aparecerá la siguiente caja de diálogo:

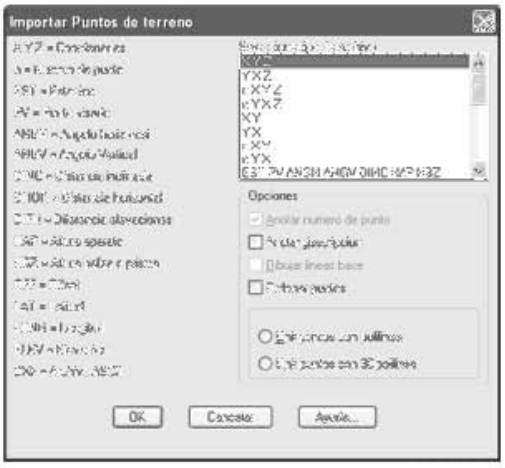


Figura 6-1 Importar puntos

2. Seleccione el tipo de archivo “X”, “Y” y “Z”, luego “*OK*”.

3. Al desaparecer la caja de diálogo aparecerá otra donde deberá seleccionar el archivo PUNTOS.DAT localizado en el directorio CivilCAD (normalmente C:\CivilCAD). Después de un breve momento aparecerán los puntos dibujados en pantalla.

4. Defina el área de trabajo con la rutina para insertar margen. Seleccione el tamaño D, escala 1:1000. Al insertar el margen se establecen los factores de escala para conversión de altura de texto y líneas, además del área efectiva de impresión.

5. Active la rutina para generar triangulación de terreno y seleccione los puntos dibujados. (*figura 6-2*).

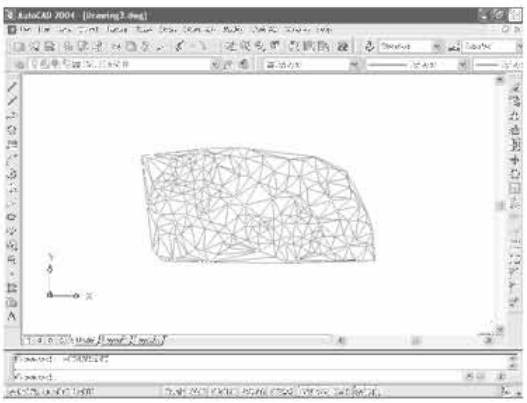


Figura 6-2 Triangulación entre puntos XYZ

6. Seleccione “generar curvas de nivel” del menú principal aceptando los valores que aparecen en la caja de diálogo correspondiente (*figura. 6-3*). Al de desaparecer la caja de diálogo, seleccione la triangulación generada. NOTA: Se pueden seleccionar las triangulaciones por medio de una ventana de selección sin importar que se incluyan otros objetos porque el programa filtra de la selección los objetos válidos.

7. Active la rutina correspondiente para anotar la elevación en las curvas gruesas.

Figura 6-3 Caja de diálogo de las curvas de nivel.

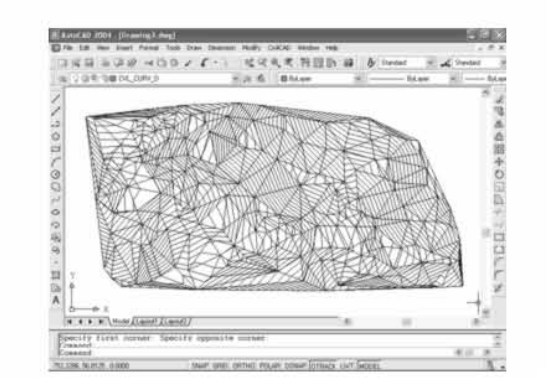


Figura 6-4 Curvas de nivel

El módulo de altimetría toma en cuenta sólo las triangulaciones al calcular los perfiles, secciones y volúmenes, por lo que las curvas de nivel se producen sólo para información de proyecto. Si se desea producir curvas más estéticas se puede especificar un grado de curvatura desde 0 hasta 10, aunque el tiempo de procesamiento aumentará proporcionalmente.

6.3. Localización de los puntos de pruebas

Punto a, laboratorio mesa de la esquina junto al servidor.

Punto b, contraesquina del laboratorio.

Punto c, Esquina junto a la ventana y el lab del Ing. Ibarra.

Punto d, Junto a la ventana y lab de EM, puerta abierta.

Punto e, En la otra esquina de la ventana junto a la columna.

Punto f, En el lab, EM, en la primera columna, 1m ventana, 3m pizarrón.

Punto g, En el lab EM, esquina 1.5m x 1.5m esquina al circuito.

Punto h, En el lab EM, en la esquina a la facultad, a 1.5 x 1.5m.

Punto i, en el centro de el lab EM.

Punto j, en el bote de basura, esquina afuera del Cubículo del Ing. Ibarra y procesamiento.

Punto k, en el lab de procesamiento, a 1.5 m de la puerta, pegado a la pared.

Punto l, en el lab de procesamiento, en la esquina de curso de matlab, no hay cuarto al otro lado.

Punto m, en el lab, que esta al lado de procesamiento 1x1m de la esquina al circuito.

Punto n, en el lab, que esta al lado del procesamiento, a 1m de la puerta de pasillo.

Punto o, en la esquina del primer cubículo, frente a los racks.

Punto p, en la contra esquina, en el cubículo 2, a 1 m de la escalera.

Punto q, en la puerta de cubículo 3, junto a la ventana.

Punto r, en la contra columna del cubículo 3.

Punto s, afuera del baño de hombrd.

Punto t, en el cuarto escalón la escalera pegado al barandal 30 cm del suelo.

Punto u, del otro lado de la sep edificio, buzón.

Punto v, del lado central escalera quinto escalón.

Punto w, en la escalera centro 7 escalones abajo -10cm.

Punto x, en la escalera 9 escalones abajo -50 cm frontera se apaga.

Punto y, en las oficinas esquina, adentro puerta, encima archivero.

Punto z, en las oficinas, escritorio secretaria 2m de la columna.

Punto 1, en la esquina afuera del cubículo del Dr. García Garduño.

Punto 2, en la contra pared, afuera del cubículo del Dr. Moctezuma.
Punto 3, en la esquina, afuera del cubículo del Ing. Ibarra.
Punto 4, afuera del cubículo del Dr. Xavier.
Punto 5, afuera de cubículo del Ing. Jesús Reyes.
Punto 6, cuartito llaves, pegado hacia el ap, 40 cm de la pared.
Valdez, En la pb junto al monumento al Ing. Valdez Vallejo.

6.4. Atenuaciones e Interferencias

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales. La inspección del sitio nos ayudará a identificar los elementos que afecten negativamente a la señal inalámbrica.

Material	**Ejemplo**	**Atenuaciones**
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia / Niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metal	Vigas, armarios	Muy Alta

Debido a que las redes inalámbricas operan en un espectro de frecuencias utilizado por otras tecnologías, pueden existir interferencias que afecten negativamente el rendimiento

Las tecnologías que pueden producir interferencias son las siguientes:

- Bluetooth
- Hornos Microondas
- Algunos teléfonos inalámbricos
- Otras redes WLAN

6.5. Especificaciones técnicas.

3Com® 11a/b/g Wireless PC Card with XJACK® Antenna

Data Sheet

• Provides universal, complete access to IEEE 802.11a, 802.11b, and 802.11g wireless networks.

• Supports the latest, most effective authentication techniques and simplifies management.

• Help keeps wireless transmissions private.

Complete 802.11 Standards Support

Universal, high-speed wireless networking has just been made practical. This single card supports all three existing IEEE 802.11 networking standards—11a, 11b, and 11g—so you can connect to any existing Wi-Fi wireless network. This flexibility lets you stay connected, no matter what wireless environment you're in. And Wi-Fi certification helps ensure interoperability with Wi-Fi-certified products from other vendors.

Secure

3Com® offers one of the most robust suites of standards-based security on the market today. To protect against unwanted network access, the PC Card supports the next generation wireless security standard—Wi-Fi Protected Access (WPA),

802.1x authentication, and EAP-TLS, PEAP, and EAP-TTLS authentication protocols. To protect wireless data, the PC Card supports the MD5 algorithm and 128-bit AES (Advanced Encryption Standard) encryption and WEP (Wireless Equivalent Privacy) RC4 40/60-bit, 128-bit and 154-bit shared-key encryption.

Performance and Reliability

Notebook users can access network resources, the Internet, and e-mail at speeds up to 108 Mpbs in turbo mode*, ideal for multimedia applications. The PC Card also offers a host of features that ensure reliable wireless connections, excellent speeds, and seamless roaming.

Easy to Set Up and Use

Setup and operation are extraordinarily easy, making this card an intelligent choice for busy mobile users. You can create profiles with specific wireless LAN settings for each place you travel—just click the proper profile and you are configured for connection. And 3Com's patented XJACK extends for excellent reception then tucks safely away for traveling.

Specifications Standards Conformance Wi-Fi

IEEE 802.11a

IEEE 802.11b

IEEE 802.11g

System Requirements

Notebook PC with an available Type II or III 32-bit or PC Card slot (3.3V)

Notebook PC must be running Windows XP/ 2000/98SE/ME

Computer slot type

Type II 32-bit PC Card (3.3 V)

Drivers/Supported Operating Systems

NDIS 5: 2000, 98 SE. ME

NDIS 5.1: Windows XP

Receive Sensitivity

802.11a

54 Mbps – -70 dBm

48 Mbps – -71 dBm

36 Mbps – -78 dBm

24 Mbps – -81 dBm

18 Mbps – -83 dBm

12 Mbps – -85 dBm

9 Mbps – -86 dBm

6 Mbps – -87 dBm

802.11g

54 Mbps – -69 dBm

48 Mbps – -70 dBm

36 Mbps – -74 dBm

24 Mbps – -80 dBm

18 Mbps – -82 dBm

12 Mbps – -84 dBm

9 Mbps – -86 dBm

6 Mbps – -87 dBm

802.11b

11 Mbps – -86 dBm

5.5 Mbps – -88 dBm

2 Mbps – -91 dBm

1 Mbps – -93 dBm

Transmit Power

802.11b/g: 17 dBm

802.11a: 16 dBm

LED Indicators

Link

Activity

Dimensions

With extended antenna:

11.3 cm (4.4 in) x 5.4 cm (2.1 in) x 0.5 cm (0.2 in)

With retracted antenna:

8.6 cm (3.4 in) x 5.4 cm (2.1 in) x 0.5 cm (0.2 in)

Operating Voltage

3.0V—3.6V

Data Rates Supported

54, 48, 36, 24, 18, 12, 9, and 6 Mbps (802.11a/g)

11, 5.5, 2, and 1 Mbps (802.11b)

Frequency Bands

2.4-2.4835 GHz (802.11b/g)

5.150—5.825 GHz (802.11a)

Modulation Technique

DSSS (Direct Sequence Spread Spectrum)

Media Access Protocol

CSMA/CA

Security

WPA, AES 128-bit encryption, 40/64-bit, 128-bit, and 154-bit WEP encryption 802.1x authentication, EAP-MD5, EAP-TLS,

EAP-TTLS, PEAP, MD5

Environmental Range

Operating temperature:

0° to 50°C (32° to 122°F)

Regulatory/Agency Approvals

Safety: UL/CSA 60950, EN/IEC 60950

Radio: FCC Part 15.247 and 15.407, RSS-210,

EN 300 328-2, draft EN 301 893

EMC: FCC Part 15 Subpart B, EN 301 489-17

SAR: FCC OET Bulletin 65, RSS-102, EN 50371

Cisco Airones PC4800

Full Specifications

Network Adapter Features	
Adapter Type	Network adapter
Form Factor	Plug-in module
Data Transfer Rate	11 Mbps 5.5 Mbps 2 Mbps 1 Mbps
Frequency Band	2.4 GHz
Interface Type	PC Card
Wireless	Yes
Data Link Protocol	Ethernet

General Product Info	
Manufacturer Part No.	AIR-PC4800-RF

7. Bibliografía y referencias.

ROSHAN, LEARY. 802.11 Wireless LAN Fundamentals, A practical guide to understanig, designing, and operating 802.11 WLANs. Cisco Press**.** Usa, 2005.

GAST y Mathew S. 802.11 Wireless Networks, The Definitive Guide. Ed. O´Reilly. USA, 2003.

BERROCAL, CÓRDOBA, LAVERDE, ORTIZ y Puentes, Diana. Evasión de filtros MAC en redes 802.11. Diana, México 2002.

Evasión de filtros MAC en redes 802.11. Berrocal Camilo, Córdoba Jonathan, Laverde Ricardo, Ortiz Diego, Puentes Diana.

CWNA Certified Wireless Network Administrator Official Study Guide. Mc Graw Hill Planet 3 Wireless Planet Osborne.

REID, Neil. 802.11 (Wi-Fi) Manual de Redes Inalámbricas. Mc Graw Hill. México 2003.

RAY, John. Aprendiendo Linux en 10 minutos. Ed. Prentice may. España, 2000.

http://www.poynting.co.za

http://www.proxim.com

http://www.elpais.es

http://www.conexiones.net

http://www.uah.es (Universidad de Alcalá de Henares)

http://www.multipoint.com.ar

http://www.hiperlan2.com

http://www.zonabluetooth.com

http://www.ericsson.com

http://www.okeda.com.ar

http://www.arrakis.es/~sergilda/wlan/quees.html

http://www.wi-fiplanet.com/columns/article.php/947661

http://en.wikipedia.org/wiki/IEEE_802.11r

http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm

http://www.linux-magazine.es/issue/05/CriptoWep.pdf

http://news.com.com/2061-10801_3-6028894.html

http://www.microsoft.com/spain/windowsxp/using/networking/getstarted/glossary.mspx

Estándares de la IEEE

Se bajaron de:

http://standards.ieee.org/getieee802/

IEEE 802.11, 1999 Edition (ISO/IEC 8802-11: 1999) IEEE Standards for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Network

IEEE 802.11a-1999 (8802-11:1999/Amd 1:2000(E)), IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band

IEEE 802.11b-1999 Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band

802.11b-1999/Cor1-2001, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 2: Higher-speed Physical Layer (PHY) extension in the 2.4 GHz band—Corrigendum1

IEEE 802.11g-2003 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band

IEEE 802.11i-2004 Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003). IEEE Standard for Information technology--Telecommunications and information exchange between system--Local and metropolitan area networks. Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements