



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

“Proyecto para la implementación de una red inalámbrica”

Tesis
Que para obtener el título de:
Ingeniero Mecánico Electricista

Presenta

Miriam Carrada Hernández

Director de Tesis: Raúl Barrón Vera.

México, D.F., 2005



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

**[PROYECTO
PARA LA
IMPLEMENTACIÓN
DE UNA** **red
inalámbrica]**

Miriam Carrada Hernández



Al motor que impulsa mi vida, me guía y acompaña siempre: mi familia



Siempre he tenido la certeza de que lo más difícil de escribir es empezar, pues ninguna idea que cruza la mente parece lo suficientemente buena o sustancial, pero una vez que esta etapa ha sido superada, y una idea aparece para iluminar el papel, las palabras fluyen rápidamente.

La verdad es que me costó más escribir los agradecimientos que la propia tesis, pues quería encontrar las palabras exactas para expresar mi agradecimiento y mi especial sentir por todas y cada una de las personas que me han acompañado en el desarrollo de esta tesis y a lo largo de este camino que he recorrido.

Gracias a:

Dios, por darme una vida privilegiada, una familia, un hogar, por demostrarme muchas veces que cuida de mí; por permitirme vivir y por todas las bendiciones que me ha dado.

Mis papás por su cariño incondicional, por toda una vida de cuidados y dedicación, por su comprensión y su ejemplo.

Mi hermanita, por ser mi brazo derecho e izquierdo, mi guía, mi mejor amiga, mi compañera de vida, mi conciencia y mi inseparable; por los años vividos y los que nos faltan por vivir...

Abuelita Celia por todo su amor, su alegría y sus ganas de vivir...

Tía Reyna, tío Migue, tía Chelo y mis primitos por su dulce compañía, todo su cariño y por hacer de mi infancia una etapa muy feliz.

Mis tíos y primos por su cariño, compañía y el valor de la familia.

Roberto Viveros por hacer de mi "estancia" en ASA una experiencia muy placentera e inolvidable, por brindarme sus buenos consejos y su amistad.

Aeropuertos y Servicios Auxiliares, por abrirme las puertas para hacer mi servicio social, y darme la oportunidad de conocer y convivir con gente maravillosa: Juanito, Ricardo, Alfredo y Normita por su ayuda, cariño y apoyo.

Amabel, por su ayuda, colaboración y amistad.

Omarcito B. por todos sus sabios consejos, su colaboración, su compañía, su apoyo, por hacer de mi tiempo de "becaria" una muy grata experiencia, sobre todo por ser el único que se detuvo a explicarme mis dudas y tuvo la paciencia de enseñarme.

Mis compañeros por los buenos y malos momentos que convivimos juntos, y por brindarme su amistad

Kika por toda su energía positiva, su cariño y su alegría.

Joquín, por su simpatía, sus buenas conversaciones en el Messenger, y sus ganas de participar.

Jesús Olea por sus INNUMERABLES aportaciones a esta tesis, su tiempo, su paciencia, sus sugerencias, por ayudarme a concretar la idea y llevarla a cabo.

Ing. Moisés Hernández por brindarme la oportunidad de desarrollar el proyecto en Cuautitlán, por su ayuda y generosidad.

A José Salinas Chávez, Rubén Salinas Chávez y Ernesto Torres, por su mano de obra y su buena voluntad

Ing. Mandujano por su paciencia y comprensión.

A la Universidad Nacional Autónoma de México, por la educación recibida.

A todos mis profesores por todos los conocimientos heredados, Luna, Margarito, Cerecedo, Reyes Solís, Villanueva, Teresa; en especial al Ing. Ulises Mavridis por el valor de la ética profesional.

A mi asesor de tesis, el Ing. Barrón, por su tiempo, su paciencia y su ayuda para que pudiera concluir esta tesis.

A todos GRACIAS, por su comprensión, su tiempo, su amistad, sus regaños, sus observaciones, su compañerismo, por hacer con todo esto la persona que soy ahora y darle sentido a mi vida.



TEMARIO

INTRODUCCIÓN	11
Capítulo I – ANTECEDENTES	13
I.1 ¿Qué es una red?	16
I.2 Redes LAN	16
I.2.1 Topologías	16
a) Bus	16
b) Estrella	17
I.2.2 Medios de Transmisión.	18
a) Cable UTP	18
b) Fibra óptica monomodo y multimodo	18
c) Cableado Estructurado	20
I.2.3 Tecnología Ethernet	22
a) Fast Ethernet	22
c) Gigabit Ethernet	24
I.2.4 Arquitecturas	26
a) Redes cliente/servidor	26
b) Redes de igual a igual	26
I.3 Redes WAN	27
I.3.1 Tecnologías de transmisión	29
a) ISDN o RDSI	29
b) Frame Relay	30
c) PPP	32
d) HDLC	33
1.4 Modelo de Referencia OSI	34
Capítulo II - TECNOLOGÍAS INALÁMBRICAS	37
II.1 ¿Qué es una red inalámbrica?	39
II.1.1 Características de una red inalámbrica	40
a) Flexibilidad	41
b) Movilidad	41
c) Escalabilidad	42
d) Frecuencias libres de licencia	42
II.2 Componentes de una red inalámbrica	43
II.2.1 AP	43
II.2.2 Tarjetas inalámbricas	44
II.2.3 Antenas	46
a) Tipos de antenas	47
II.3 Estándares para redes inalámbricas	51
II.3.1 Wi-Fi	52
a) 802.11a	56
b) 802.11b	59
c) 802.11g	62
II.3.2 Bluetooth	64
II.3.3 Otros estándares	68
a) Home RF	68
b) Hiper LAN	70

II.3.4 Tabla comparativa de los estándares inalámbricos	74
II.4 WLAN	75
II.4.1 Topologías	75
a) BSS (Ad-hoc)	75
b) IBSS (Infraestructura)	76
c) ESS	76
II.4.2 Técnicas de propagación	77
a) Espectro extendido de salto de frecuencia (FHSS)	78
b) Espectro extendido de secuencia directa (DSSS)	79
c) Multiplexión por división ortogonal de frecuencia (OFDM)	80
II.4.3 Tipos de modulación	81
a) BPSK	81
b) QPSK	82
c) CCK	83
d) QAM	83
II.5 Seguridad	85
II.5.1 Autenticación	86
II.5.2 Control de acceso por filtrado de direcciones MAC	87
II.5.3 WEP	87
II.5.4 Autenticación 802.1X	89
II.5.5 802.11i	91
a) AES	91
b) TKIP	91
c) WPA	92
II.5.6 Ataques comunes	92
Capítulo III – APLICACIONES	93
III.1 Hidden Villa Ranch	98
III.2 Alvear Palace Hotel	99
III.3 Florida Hospital	99
III.4 Aeropuerto de Sydney	100
III.5 Aeropuertos y Servicios Auxiliares	101
Capítulo IV – PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA	107
IV.1 Objetivo del proyecto	109
IV.2 Diseño del proyecto	109
IV.2.1 Cronograma de actividades	110
IV.2.2 Propuesta de solución	111
a) Evaluación del sitio	111
IV.2.3 Pruebas de propagación	120
a) Prueba 1	121
b) Prueba 2	127
c) Prueba 3	134
d) Prueba 4	141
IV.2.4. Carta de aceptación del proyecto.	148
IV.3 Planeación	149
IV.3.1 Selección del hardware	149



TEMARIO

IV.4 Ejecución	158
IV.4.1 Instalación	158
a) Instalación de antena	158
b) Instalación de cableado	160
c) Instalación de equipo	163
IV.4.2 Configuración	164
IV.4.3 Pruebas	165
a) Site Survey	165
- Prueba interior de la biblioteca planta alta	165
- Prueba exterior de la explanada	172
b) Pruebas de conexión	179
IV.4.4 Cierre	180
CONCLUSIONES	183
GLOSARIO	184
BIBLIOGRAFÍA	190

Las necesidades actuales y el continuo avance tecnológico, ha impulsado el desarrollo de nuevas tecnologías que permiten un mejor uso y utilización de las tecnologías de información.

En la actualidad se manejan esquemas de redes alámbricas, las cuales se encuentran diseñadas con base a ciertas topologías establecidas que permiten un mejor funcionamiento de acuerdo a las necesidades de la empresa u organismo que la utiliza, es por esta razón que se da una breve descripción en el primer capítulo, de estas topologías que permiten el diseño de redes de datos, las cuales se utilizan también para la implementación de redes inalámbricas.

En el segundo capítulo vemos que las redes inalámbricas ofrecen comunicar a los usuarios de computadoras sin la necesidad de estar ligados físicamente a un nodo de red mediante un cable, es decir, brindan un esquema de movilidad lo que da al usuario una gran gama de beneficios como el poder desplazarse con un equipo portátil fuera de su oficina y tener disponible siempre los servicios que le otorga una red de datos. Otro de los beneficios es la facilidad de realizar cambios en la ubicación física de equipo de cómputo, ya que ahora pueden realizarse con mayor frecuencia sin representar un incremento en los costos derivados de la nueva instalación de red, así como la desinstalación de la red anterior.

Para la implementación de una red inalámbrica, es necesario seguir algún estándar de los muchos que existen ya que esto nos permitirá realizar una conexión confiable. En el presente trabajo abordaremos principalmente el de Wi-Fi y revisaremos brevemente otros estándares para poder identificar los alcances y beneficios de cada uno de ellos.

Debido a que la mayoría de las redes inalámbricas están conectadas a una red cableada y que los equipos operan en bandas sin licencia (bandas que pueden operarse sin necesidad de permisos especiales otorgados por el gobierno) es necesario tener en cuenta los aspectos básicos de seguridad para proteger la información que viaja a través de las ondas de radio.

En el tercer capítulo abordaremos las principales aplicaciones de las tecnologías inalámbricas, su uso en diferentes áreas y mostraremos algunos casos reales en los que se haya utilizado la tecnología inalámbrica, por ejemplo, en un hospital para tener siempre actualizado y al instante el historial de un paciente; en un almacén para facilitar la captura de inventarios y tener en control todo lo que ahí se guarde, etc. Las aplicaciones son muchas y todas brindan a los usuarios mayor disponibilidad de la información para ofrecer un mejor rendimiento.

Puesto que hemos revisado los conceptos teóricos básicos que comprenden a una red inalámbrica, en el cuarto capítulo se elabora un proyecto para implementar una red inalámbrica en la FES Cuautitlán con el fin de definir los pasos básicos que se deben seguir para diseñar e implementar una red inalámbrica y ver de manera práctica una de las muchas aplicaciones de este tipo de redes.



[ANTECEDENTES]

■ I.1 [¿Qué es una red?]

Una red en general es el conjunto de personas, objetos u órganos conectados entre sí que se relacionan para realizar algún servicio u operación.

Todos hemos utilizado una red alguna vez, al usar el teléfono o al enviar un paquete, claro que no eran redes de computadoras, pero con estos ejemplos podemos entender el propósito de cualquier red, el cual es enlazar objetos similares para que trabajen en conjunto siguiendo ciertas reglas.

Una red de datos puede definirse como dos o más computadoras conectadas por medio de un cable para poder intercambiar información. [Lowe, 2001]

El objetivo de una red es asegurar la entrega de información de manera confiable, es decir, sin ningún daño en los datos, al lugar que la haya solicitado.

Las redes surgen por la necesidad de intercambiar información. En un principio las empresas compraban computadoras y dejaban que estas existieran como dispositivos aislados, cuando alguien necesitaba imprimir copiaba su información en un disquete y caminaba al sitio donde se encontrara conectada la impresora, a este medio de comunicación se le llamó "sneakernet", este sistema tenía muchas deficiencias, fue por eso que se ideó una forma de conectar electrónicamente a las computadoras para poder suprimir este método rudimentario de comunicarse.

El propósito de construir una red es el de aumentar la eficiencia de una empresa, y facilitar el trabajo de los usuarios de la red, además que las redes ayudan a tener un mejor control de la información pues esta puede ser respaldada en diferentes computadoras y no solo en una.

Los primeros dispositivos que se necesitan para formar una red son las computadoras e impresoras, a continuación se describen brevemente los principales elementos que conforman una red [Hayden, 1999]:

- Estación de trabajo: computadora en la que trabaja el usuario.
- Servidor: computadora con mayor capacidad que comparte sus recursos con otras computadoras.
- Impresora de red: impresora en la cual puede imprimir más de un usuario.
- Hub: dispositivo que sirve como punto de conexión para otros dispositivos
- Ruteadores y Puentes: dispositivos que transfieren datos entre las redes

■ 1.2 [Redes LAN]

Una red de área local o LAN (Local Area Network) es una agrupación de computadoras enlazadas. Las redes LAN son capaces de conectar todas las estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos ubicados dentro de un mismo edificio.

“Las redes LAN permitieron a muchos usuarios en un área geográfica relativamente pequeña intercambiar archivos y mensajes así como el acceso compartido a recursos y aplicaciones; además de la comunicación con otros usuarios vía correo electrónico.”¹

La principal característica de las redes LAN es que son redes de datos de alta velocidad con bajo nivel de errores que abarcan un área geográfica relativamente pequeña. Manejan anchos de banda de 10 y 100Mbps, 1Gbps y actualmente 10Gbps.

Son las redes más sencillas, pero no por eso son, necesariamente las más pequeñas o simples. Usualmente son redes privadas, que sirven para que las computadoras de una empresa compartan un medio de transmisión común.

■ 1.2.1 [Topologías]

Existen diferentes definiciones sobre topología: “Una topología es la forma en la cual se organizan las computadoras dentro de cualquier red de transmisión de datos”², otros dicen que una topología es simplemente la organización física de los equipos [Habraken, 1999].

Una topología define la manera en que los dispositivos de red se encuentran organizados, no sólo en su conexión física sino también su arquitectura lógica; esto es que los dispositivos pueden no estar organizados físicamente en esta configuración pero si trabajar como si lo estuvieran.

Las topologías básicas más utilizadas para las redes LAN Ethernet son las siguientes:

a) Bus

La topología de bus es la más sencilla de todas. Consiste en que todos los equipos están conectados de forma directa a un único medio de transmisión compartido o bus. Todos los dispositivos están en espera y escuchan el medio.

Cuando un equipo desea transmitir su información se asegura de que nadie más este transmitiendo y entonces envía su información, esta se propaga a lo largo del bus, es decir, todas las estaciones reciben la información hasta que llega a su destino.

Las principales ventajas de esta tecnología son la facilidad para añadir o quitar equipos de la red, si algún equipo llega a fallar esto no afecta a todos los demás y la red puede seguir trabajando.

¹ DOWES, Kevin. *Internetworking Technologies Handbook*. 38

² SÁNCHEZ, Jesús. *Redes: iniciación y referencia*. 7

El problema existe cuando ocurre alguna falla en el bus, ya que las estaciones pierden contacto con algunas o todas las demás estaciones haciendo que la red deje de funcionar.

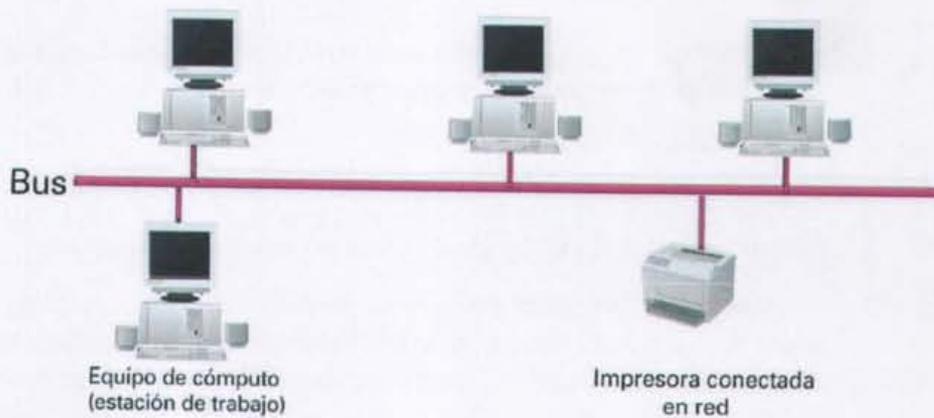


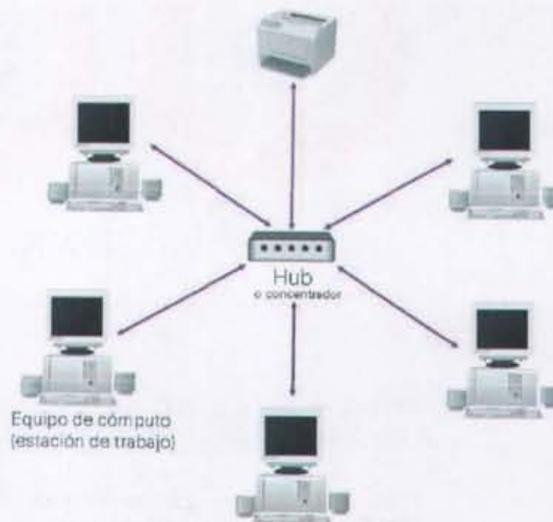
Figura I.1 Topología de Bus

b) Estrella

Esta topología consiste en conectar todos los dispositivos o estaciones de trabajo por medio de un hub o concentrador, el cual está ubicado al centro de la red. El hub es el encargado de administrar la comunicación entre los equipos, ya que toma la decisión de que estación puede transmitir, pero al igual que el bus las estaciones escuchan el medio para saber cuando pueden transmitir.

Este tipo de conexión es fácil de expandir, ya que se pueden agregar equipos fácilmente, aunque la red esté operando sin causar fallas en la misma. Cuando ocurre alguna falla en uno de los equipos esto no afecta al resto de la red, por lo cual es fácil detectar donde existe algún problema.

La principal desventaja de esta topología es cuando falla el hub, pues por ser el punto central de la red esta deja de funcionar.



I.2 Topología en estrella



■ 1.2.2 [Medios de transmisión]

Los medios de transmisión utilizados actualmente, para conectar a las redes de datos debido a sus características, son principalmente el cable UTP y la Fibra óptica.

a) Cable UTP o par trenzado

Consiste en dos filamentos de hilo de cobre girados uno sobre otro. Un cable se forma de un número de pares trenzados agrupado y encerrado en una funda protectora.

Los giros en el cable sirven para cancelar el ruido eléctrico que pudiera originarse en los pares adyacentes o por alguna fuente externa como pueden ser los transformadores, los motores, etc. que estén operando cerca del cable. Cuando existe alguna corriente eléctrica sobre un cable se generará un campo electromagnético, al trenzar los cables lo que se logra es cancelar los campos magnéticos de cada uno, debido a que son iguales y opuestos, lo mismo se logra con las cargas capacitivas.

b) Fibra óptica monomodo y multimodo

La fibra óptica está formada por un cilindro de vidrio extremadamente delgado llamado Núcleo, que se encuentra envuelto por una capa concéntrica de vidrio o Revestimiento y una capa exterior llamada buffer. El núcleo lleva la luz, "el revestimiento proporciona la diferencia en el índice de refracción, necesario para la reflexión total interna de la luz a través del núcleo. El revestimiento tiene un índice de refracción menor al del núcleo."³ Y el buffer sirve para proteger tanto al revestimiento como al núcleo de algún daño.

Los núcleos grandes propagan diferentes modos (o trayectorias) a diferentes velocidades. Los núcleos pequeños pueden propagar un solo modo.



Figura 1.3 Tipos de fibra y tamaños de los núcleos

Las fibras ópticas transportan señales digitales en forma de pulsos modulados de luz, son buenas para transmisiones de alta velocidad, ya que casi no presentan atenuación dando como resultado una señal muy pura. Las fibras son de menor tamaño y peso que el cable UTP y están diseñadas para aplicaciones de mayor ancho de banda.

³ TRUNET, ADC. Sistemas de cableado estructurado.



La luz se propaga a través del núcleo debido a múltiples reflexiones que se originan con respecto al revestimiento; para que la luz pueda propagarse debe entrar con un ángulo respecto al eje de la fibra.

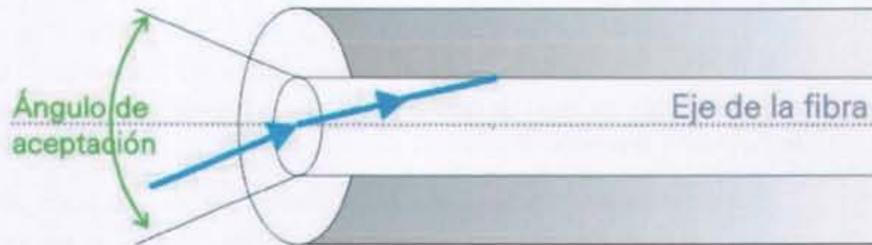


Figura 1.4 Ángulo de aceptación. (La luz debe entrar por este ángulo para pueda viajar a través del núcleo)

La luz puede viajar a lo largo del filamento monomodo y multimodo.

La fibra monomodo (Singlemode) SM, permite que un solo rayo de luz se propague a través de la fibra. Ya que solo un rayo de luz se utiliza, no existe una dispersión modal en la fibra, lo que le da un mayor ancho de banda.

19

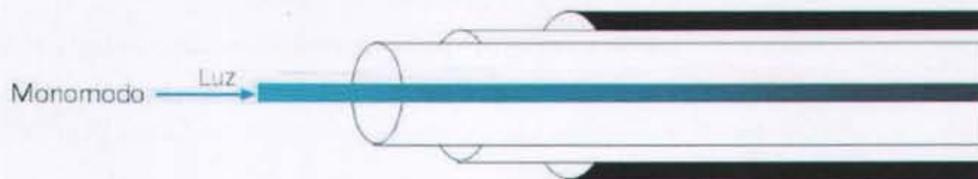


Figura 1.5. Fibra óptica monomodo

"La fibra multimodo (Multiplemode) MM permite que múltiples rayos de luz se propaguen a través de la fibra. Debido a que estos rayos de luz entran en la fibra a diferentes ángulos, llegarán al final de la fibra en diferentes tiempos. Esta característica es conocida como dispersión modal. La dispersión modal limita el ancho de banda y las distancias que pueden utilizarse en fibras multimodo"⁴

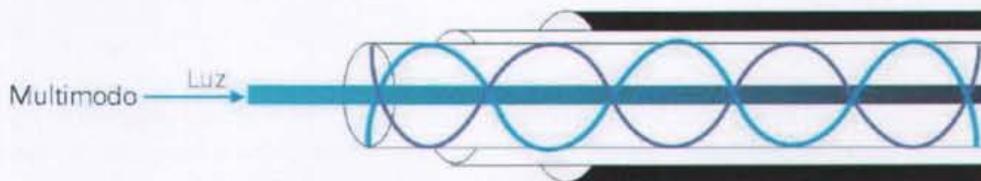


Figura 1.6 Fibra óptica multimodo

⁴ DOWES, Kevin. *op. cit.* 127

c) Cableado Estructurado

El cableado estructurado es un sistema integral conformado por los dispositivos que componen el canal de transmisión, cuya finalidad es garantizar que la transmisión y recepción de los bits sea completada correctamente, sin errores. Para que esto se lleve a cabo es necesario que los componentes estén sintonizados, para así tener un camino recto por el cual pase la información. Cuando se tienen diferentes componentes que no se integran adecuadamente, tenemos un camino irregular que originará cuellos de botella, y retardo en la transmisión y recepción de información.

Es recomendable que todos los componentes de un sistema de cableado sean de la misma marca ya que tendrán las mismas características y se puede garantizar así su integración.

El cableado estructurado se divide, de acuerdo al tipo de materiales que utilizan, en categorías. Fue a la categoría 5 a la que se le dio el nombre de cableado estructurado, pero existen otras categorías⁵

- **Categoría 1.** Cable telefónico UTP tradicional que transporta solo voz.
- **Categoría 2.** Certifica el cable UTP utilizado para la transmisión de datos hasta 4Mbps.
- **Categoría 3.** Certifica el cable UTP para transmisiones de datos de hasta 10Mbps. La distancia máxima entre repetidores es de 100mts. Se utilizaban cable y conectores UTP de menos de 100Mhz. Soportaba Ethernet a 10Mbps, y Arc Net a 2Mbps
- **Categoría 4.** Certifica el cable UTP para transmisiones de datos de hasta 16Mbps.
- **Categoría 5.** Soporta tecnologías inferiores y Fast Ethernet. La velocidad máxima de transferencia es de 100Mbps. Los materiales que se utilizan son Cable UTP y conectores Categoría 5 de 100Mhz.
- **Categoría 5e.** La velocidad máxima de transferencia es de 155Mbps. Soporta tecnologías inferiores y ATM. Los conectores y materiales que se utilizan deben soportar 150Mhz.
- **Categoría 6.** Soporta hasta Gigabit Ethernet y las tecnologías inferiores. Se puede utilizar cable y conectores de Categoría 6 y/o Fibra óptica. La velocidad máxima de transferencia es de 1Gbps. La distancia máxima entre repetidores para la fibra óptica es de 1Km en fibra multimodo y 2Km en fibra monomodo.

Los parámetros eléctricos que KRONE [2001] considera, para evaluar las características de los cables UTP son principalmente los siguientes:

- **Atenuación:** es la pérdida de potencia de la señal transmitida a lo largo de un cable. A mayor atenuación menor señal se tiene en el receptor. Se mide en decibeles (dB)* y se expresa como un valor negativo. La atenuación esta determinada por la construcción del cable, la longitud y frecuencias de la señal enviada. Para minimizar la atenuación se deben revisar las longitudes del cable y la terminación de los conectores.

⁵ BRAIN. [Cableado estructurado.htm](#)

* Decibel [dB]: unidad utilizada para medir el cambio de intensidad de una señal $10 \log \frac{\text{Señal Transmitida}}{\text{Señal original}}$

- **NEXT (paradiafonía):** Es el aislamiento de la interferencia o pérdida de diafonía. La diafonía, es la interferencia que se induce en un par por la influencia de los pares próximos. Se mide en dB y es la diferencia en amplitud entre la señal presente y la señal de diafonía. A mayor aislamiento de interferencia menor es el efecto de inducción. La diafonía se evita teniendo un mayor trenzado en los cables, pues esto cancela los campos de inducción.
- **ACR (Razón atenuación a diafonía):** es la diferencia entre NEXT y atenuación. Se mide en decibeles
- **PSNEXT (Power Sum NEXT):** es el resultado de la suma algebraica de los efectos de NEXT individuales en cada par a los otros 3 pares. Es un parámetro importante para evaluar los cables que soportan transmisiones a 4 pares.
- **SACR (Power Sum ACR):** se obtiene de la suma algebraica de los efectos ACR individuales en un par a los otros 3 pares.
- **RL (Pérdida de retorno):** es la suma de todas las señales reflejadas; es decir, es la razón de potencia de la señal transmitida con respecto a la potencia reflejada, (desde el panel de parcheo hasta el extremo del cable donde se origina la señal). El cambio de impedancia a lo largo del cable origina que parte de la señal sea reflejada.
- **SRL (Pérdida de retorno estructural):** originado por las variaciones en densidad e imperfecciones que tiene el cable. Se mide en dB.
- **ELFEXT (Equal Level Far End Crosstalk):** Se puede considerar como el ACR (Razón de atenuación diafonía) en el extremo lejano. Se obtiene restando la atenuación del par inducido al FEXT que esté par induce en los pares adyacentes.
- **PSELFEXT (Power Sum ELFEXT):** se deriva de una suma algebraica de los efectos ELFEXT individuales en cada par a los otros 3 pares.
- **Propagation Delay (Retardo de propagación):** es el tiempo requerido para que una señal se propague de un extremo a otro. Se mide en nanosegundos (η s). Esta es una de las principales razones para limitar la longitud del cableado.
- **Propagation delay skew (Sesgo de retardo de propagación):** es la diferencia de retardo de propagación entre el par más rápido y el par más lento en un cable UTP. Este parámetro es importante debido a que en tecnologías de alta velocidad un delay skew demasiado grande hará imposible recombinar la señal original en el receptor.
- **Impedancia:** es la oposición al flujo de la corriente; incluye los efectos de resistencia, capacitancia e inductancia. Para UTP tiene un valor de 100Ω
- **Pérdida de inserción (Insertion Loss):** es la pérdida que resulta de insertar un dispositivo en la línea, y es la diferencia de potencial que existe en la línea antes del dispositivo y después de él.

La tabla I.1 muestra las características del cable UTP categorías 5, 5e y 6.

Categoría	Velocidad	Ancho de Banda	
CAT 5	100Mbps	100MHz	Mejora las especificaciones para NEXT, PSELFEXT y Atenuación
CAT 5e	155Mbps	100MHz	ACR = 6.1 Pérdida de retorno = 10 Propagation Delay = 548
CAT 6	1Gbps	250MHz	ACR = 3.6 (presenta mejoras en ACR en comparación con la categoría 5e) Pérdida de retorno = 9 Propagation Delay = 547

Tabla I.1 Características del cable UTP

■ I.2.3 [Tecnología Ethernet]

Ethernet es la tecnología más utilizada en las redes LAN debido a que es muy flexible y de fácil implementación.

Utiliza para acceder al medio, el protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detect) Acceso múltiple con detección de portadora y detección de colisiones, lo cual significa que los nodos de la red escuchan hasta que el medio este libre. Si esta libre, el dispositivo envía su información, pero si hay mas de una computadora transmitiendo se produce una colisión. Al sensar las colisiones el dispositivo detiene la transmisión y espera un tiempo hasta que el medio este libre y vuelve a transmitir.

Las necesidades de proporcionar mayor velocidad a una red para aminorar el tráfico, impulsaron a diseñar versiones de Ethernet que pudiesen trabajar a velocidades mayores de 10Mbps; estas son: 100Mbps Ethernet conocida como Fast Ethernet y 1000Mbps Ethernet o Gigabit Ethernet.

a) FAST ETHERNET

Fast Ethernet es una extensión del estándar Ethernet que surgió debido a que algunas aplicaciones demandaban mayor velocidad en las redes LAN. Esta tecnología de alta velocidad ofrece un incremento en el ancho de banda tanto en las comunicaciones de los servidores como en las de los usuarios.

Fast Ethernet incrementa la velocidad diez veces más que 10Base T Ethernet.

Cuando se desarrolló Fast Ethernet surgieron dudas acerca del método de acceso a utilizar, pues algunos creían que un Ethernet más rápido no soportaría CSMA/CD, así que crearon dos estándares: 100Base T desarrollado por "Fast Ethernet Alliance" y 100VG-AnyLAN desarrollado por varias compañías, entre las cuales están IBM y Hewlett Packard que conformaron el "100VG-Any LAN Forum". La primera conservó el protocolo de Ethernet, CSMA/CD (Carrier Sense Multiple Access with Collision Detect) y la segunda utiliza un protocolo de demanda-prioridad que elimina las colisiones.

- 100 Base T

100Base T es una extensión del estándar original IEEE 802.3, pues conserva el formato de trama, el tamaño y el mecanismo de detección de errores. Además soporta el software y las aplicaciones que pudieran existir en una red que opera con Ethernet, por lo cual no es necesario ningún protocolo de traducción de datos entre ambos.

Existen tres tipos de medios sobre los cuales puede viajar Fast Ethernet: 100 Base TX, 100Base FX y 100Base T4. La tabla I.2 muestra las características principales de cada tipo de medio.

100Base TX	100Base FX	100Base T4
Cable UTP 2 pares, uno para transmitir y otro para detectar colisiones y recibir información	Fibra óptica 2 hilos o fibras Uno para transmitir y otro para detectar colisiones y recibir información	Cable UTP 4 pares Utiliza tres pares para transmitir y recibir, y otro para detectar colisiones
Diámetro máximo de la red: 200 metros	Diámetro máximo de la red: 400 metros	Diámetro máximo de la red: 200 metros
Máxima longitud del segmento: 100 metros	Máxima longitud del segmento: 400 metros	Máxima longitud del segmento: 100 metros

Tabla I.2 Características de los medios 100BaseTx, 100BaseFX y 100Base T4.

La principal diferencia entre 10Mbps Ethernet y 100Base T es la disminución en el diámetro máximo de la red el cual es de 205m.

La red 100Base T cuenta con una función llamada "autonegociación", la cual consiste en un proceso de negociación que permite a los diferentes dispositivos intercambiar información acerca de sus capacidades (velocidad), permitiendo ajustarse para trabajar juntos de una manera óptima y eficaz.

- 100VG-Any LAN

La segunda de las tecnologías que trabajan a 100Mbps es 100VG-Any LAN. Es completamente nueva y su método de acceso es más determinístico que CSMA/CD porque el hub controla el acceso a la red, además soporta tanto Ethernet como 16Mbps Token Ring.

100VG-Any LAN trabaja de la siguiente manera: cuando un dispositivo necesita transmitir envía una petición al hub (o switch); si la red está libre el hub acepta la petición y el dispositivo empieza a transmitir. Si se recibe más de una petición, el hub asigna un turno a cada petición.

Existen dos tipos de peticiones: de prioridad alta y de prioridad normal. Las peticiones de prioridad alta son aquellas sensibles al tiempo como las aplicaciones de videoconferencia, y son atendidas antes que las de prioridad normal.

100VG-Any LAN puede viajar a través de:

- 4 pares de cable UTP Categoría 3.
- 2 pares de cable UTP Categoría 4 o 5.
- STP y Fibra óptica.

Algunos fabricantes dicen que 100VG-Any LAN es un mejor protocolo para LAN's que transmiten grandes cantidades de datos sensibles al tiempo

"La siguiente tabla muestra una comparación entre 100Base T y 100VG-Any LAN."⁶

	100 Base T Fast Ethernet	100VG-Any LAN
Velocidad	100Mbps	100Mbps
Método de acceso	CSMA/CD	Demanda-prioridad
Tamaño de la trama	64 a 1500 bytes	64 a 16Kbytes
Servicios	Asíncrono	Asíncrono y sincrónico
Diámetro de la Red	205m	300m
Aplicación	Grupo de trabajo, Backbone y usuarios	Grupo de trabajo, Backbone y multimedia

Tabla I.3 Comparación entre 100BaseT y 100VG-Any LAN

b) GIGABIT ETHERNET

Gigabit Ethernet basado al igual que Fast Ethernet en la norma IEEE 802.3 incrementa la velocidad de Fast Ethernet 10 veces más hasta 1Gbps.

Gigabit Ethernet surge de la mezcla de dos tecnologías IEEE802.3 y ANSI X3TII Fibre Channel. Esto significa que este nuevo estándar toma las ventajas de la existente tecnología de la interfaz física de alta velocidad, mientras mantiene el formato de trama, la compatibilidad con el equipo instalado y el uso de full-duplex o half-duplex de IEEE 802.3. [Network Associates, 2002]

Existen cuatro diferentes medios de transmisión por los cuales puede viajar Gigabit Ethernet:

- Onda larga (LW -long wave) Láser sobre fibra monomodo y multimodo conocido como 1000Base LX.
- Onda Corta (SW-short wave) Láser sobre fibra multimodo conocido como 1000Base SX.
- 1000 Base CX que permite la transmisión sobre cable de cobre de 150Ω balanceado
- 1000 Base T 4 pares de cable UTP Categoría 5 con un máximo de 100m [Gigabit Ethernet Alliance, 1999]

⁶ CISCO. Technology Brief Fast Ethernet 100 Mbps Solution. 5

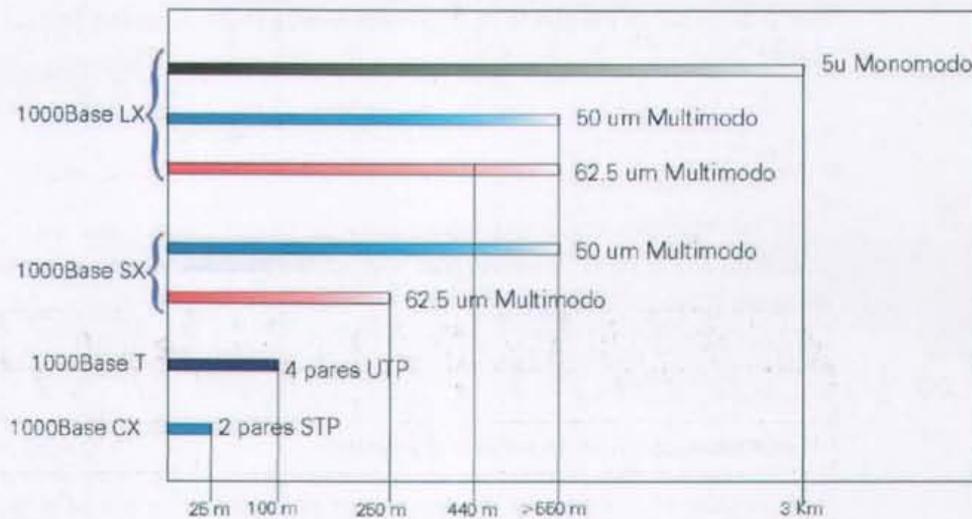


Figura I.7 Medios de Transmisión para Gigabit Ethernet

Los datos que son transmitidos a la 1000Mbps son "puestos en código" esto es, la información se modifica en el formato requerido de transmisión con el objetivo de mejorar la recuperación de el pulso de reloj, además que incrementa la posibilidad de detectar y corregir errores de transmisión o recepción y ayuda a distinguir bits de datos entre bits de control.

Transmisión Half-Duplex

Para la transmisión Half-duplex se utiliza CSMA/CD para asegurar que las estaciones puedan comunicarse por un solo alambre y que la recuperación de colisión se puede llevar a cabo. CSMA/CD se utiliza igual para Ethernet y Fast Ethernet.

Debido a que es un protocolo sensible a demoras es necesario crear un bit-budget o "presupuestador" por dominio de colisión, que se forma tomando el tiempo máximo de demora de la señal en varios componentes de la red como repetidores, el medio físico, etc. Su función principal es determinar la separación máxima entre dos estaciones finales sobre un segmento compartido.

Se necesita además agregar un "carrier extensión" que añade bits a la trama hasta que la trama encuentra el mínimo espacio de tiempo requerido para que la red pueda manejar las colisiones.

Ya que Gigabit Ethernet half-duplex presenta ineficiencia en el tamaño de la trama y además se necesita del carrier-extensión, se puede decir que la transmisión half-duplex no es efectiva para Gigabit Ethernet –

Transmisión Full-Duplex

Full duplex permite que el ancho de banda de las redes Ethernet y Fast Ethernet sea fácilmente y con bajo costo doblado de 10Mbps a 20Mbps y de 100Mbps a 200Mbps.

Se eliminan las colisiones en el alambre, por lo cual no se utiliza CSMA/CD como método de acceso.

Gigabit Ethernet se utiliza principalmente para incrementar el ancho de banda disponible entre el puerto de un switch y el puerto de otro switch o entre el del dispositivo terminal y el puerto de un switch.

■ 1.2.4 [Arquitecturas]

Son las relaciones lógicas que existen entre las computadoras y una red. Las computadoras pueden operar como cliente/servidor o de igual a igual sin importar la tecnología que se este utilizando. [Hayden, 1999]

a) Redes cliente/servidor

Los equipos se dividen en servidores y clientes.

Un servidor es una máquina que tiene mayor capacidad, en la que se centran los recursos a compartir de la red. Hay dos clases de servidores: dedicados y no dedicados. Los servidores no dedicados funcionan también como estaciones de trabajo.

Los clientes o estaciones de trabajo son máquinas menos poderosas en comparación con los servidores y se conectan a este a través de la red.

Algunos de los beneficios que se tienen al utilizar una red cliente/servidor es que:

- Ofrecen más seguridad contra accesos no autorizados a la información, ya que se pueden establecer controles estrictos y rigurosos en cuando al acceso a archivos.
- Las tareas de administración y supervisión se facilitan ya que la red está centralizada.
- Reducción significativa de las funciones de administración en los clientes
- Capacidad de asegurar y respaldar datos desde el servidor
- Actualización de antivirus y software a todos los equipos por medio del servidor.

Algunas desventajas son:

- Son más costosas de implementar que las de igual a igual, por el costo que tiene el servidor.
- Si el servidor se daña, la red deja de funcionar.

b) Redes de igual a igual

En esta red cualquier estación de trabajo puede ofrecer recursos a compartir, es decir, todas las estaciones de trabajo manejan algunas de las funciones de servidor.

Como no existe un servidor todas las computadoras pueden utilizarse como estaciones de trabajo.

Ventajas de una red de igual a igual:

- Fácil instalación y configuración
- Menor costo en comparación con las redes cliente/servidor



Desventajas:

- No es administrable, puesto que no tiene un control centralizado
- Es insegura ya que todos tienen acceso a la información sin restricción alguna.

Este tipo de red es apropiada para redes pequeñas entre 3 o 4 estaciones de trabajo.

■ 1.3 [Redes WAN]

"Cuando se desea realizar una conexión de larga distancia aparece un mundo totalmente nuevo en las comunicaciones de datos: las redes de área extensa"⁷

Una red de área amplia o extensa, WAN (Wide Area Network) es una red compuesta de muchas subredes o redes LAN que se encuentran dispersas geográficamente.

Las WAN se construyen principalmente cuando es importante que los usuarios puedan acceder a información común que se encuentra en otra ciudad, a lo largo de un país o al otro lado del mundo.

A diferencia de las LAN las WAN casi siempre utilizan routers (Ruteadores) y puentes para interconectarse, puesto que los puentes proporcionan menor control sobre el tráfico, los Ruteadores son la mejor opción para interconectar redes LAN

En una red LAN el equipo y el manejo del ancho de banda depende de cada empresa, pero para la realización de un enlace WAN en la mayoría de los casos es necesario contratar un proveedor de servicios de telecomunicación que proporcione los medios para enviar la información a larga distancia, pues requiere de una gran inversión económica el instalar cables de fibra óptica de larga distancia, realizar un enlace terrestre de microondas o lanzar un satélite propio.

Debido a que lo que se compra al proveedor de servicios es el ancho de banda existen diferentes tipos de conexiones para proporcionar mayor flexibilidad en la cantidad de ancho de banda

Enlaces Punto a Punto.

Un enlace punto a punto provee un solo camino de comunicaciones WAN preestablecidas por parte de un cliente a través de una red "transportadora", puede ser una compañía telefónica o una red remota. Este enlace también es conocido como línea arrendada o dedicada, porque el camino que se establece es permanente y fijo para cada red remota.

Normalmente las líneas arrendadas son líneas digitales, por lo que proveen un ancho de banda mayor y son menos susceptibles al ruido y la interferencia, además permiten diversas transmisiones que pueden incluir comunicación de voz y datos.

⁷ ZACKER, Craig. *Redes: Manual de Referencia*. 175

La compañía proveedora de servicios reserva enlaces punto a punto para el uso privado de algún cliente.



Figura 1.8 Enlace punto a punto

Comutación de circuitos.

En este tipo de conexión se establece un canal dedicado llamado circuito, entre dos puntos, el cual es mantenido y terminado por cada sesión de comunicación. Los datos viajan desde la fuente hasta el destino a través del camino que ha sido creado por una sesión en particular. [Habraken, 1999]

Normalmente estos tipos de circuitos son provistos por una compañía telefónica, pues opera como una llamada normal de teléfono, y el costo depende de que tan seguido se ha usado la línea para transferir información.

ISDN (Integrated Services Digital Network) es un ejemplo de tecnología WAN de circuitos conmutados.

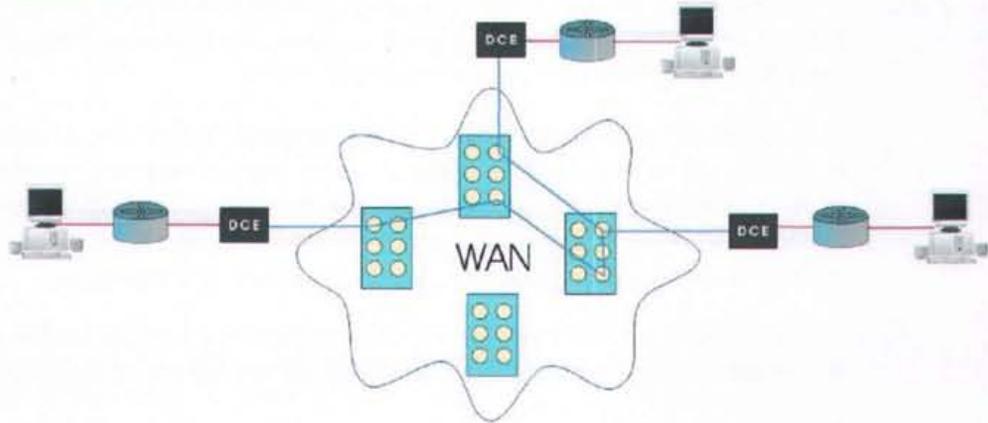


Figura 1.9 Conmutación de circuitos

Comutación de paquetes.

Este método de conmutación transmite datos divididos en pequeños paquetes, entre dos puntos enrutándolos a través de una red conmutada.

Con una sola conexión, un sitio de red puede proporcionar acceso a varios sitios remotos con solo utilizar diferentes rutas a través de la red, es decir, múltiples usuarios pueden compartir el mismo medio. Para que los dispositivos puedan compartir estos circuitos es necesario multiplexar la información a transmitir.



Cada paquete puede seguir diferentes rutas a través de la red WAN y al llegar a su destino el equipo receptor los reorganizará en el orden correcto.

ATM (Asynchronous Transfer Mode) y Frame Relay son ejemplos de tecnologías WAN que utilizan conmutación de paquetes.

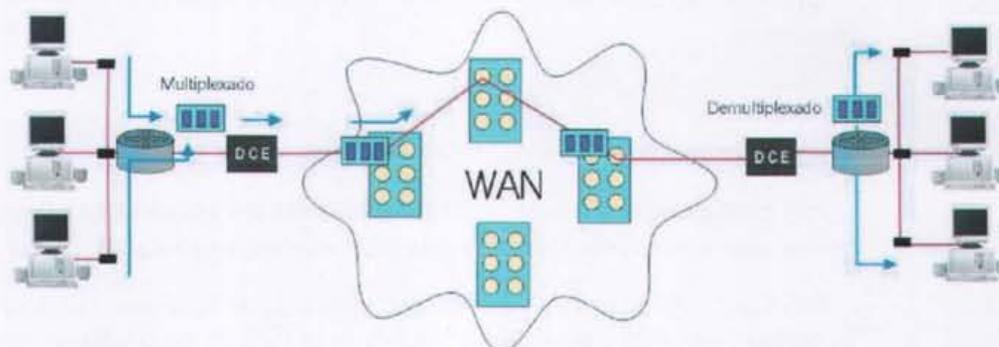


Figura I.10 Conmutación de paquetes

■ I.3.1 [Tecnologías de Transmisión]

Existen muchas tecnologías y protocolos que se pueden utilizar en las redes WAN. La elección de alguna tecnología depende de las necesidades de ancho de banda y tiempo de uso, así como de las diversas aplicaciones con las que se va a utilizar el enlace.

Las siguientes tecnologías y protocolos son los más utilizados para realizar un enlace WAN.

a) ISDN o RDSI

ISDN (Integrated Services Digital Network, por sus siglas en inglés) o RDSI (Red Digital de Servicios Integrados, por sus siglas en español), es una red de telecomunicaciones pública que permite transmitir voz, datos, texto, gráficos, música, video y otras fuentes a través de los cables telefónicos existentes.

RDSI fue creada con el fin de sustituir el sistema telefónico actual por un sistema digital; ahora es un medio alternativo para conexiones de banda ancha.

Se le conoce también como servicio de conmutación de circuitos, pues se establece un circuito punto a punto temporal entre dos sitios, similar a una llamada telefónica.

ISDN utiliza dos tipos de canales denominados: canales B (portadores) y D (delta). Los canales B son canales utilizados para transportar tráfico de voz y datos del usuario, mientras que el canal D se ocupa para transportar tráfico de control que le indica a la red que hacer (canal de señalización)

Existen dos tipos de servicio:

- **BRI (Basic Rate Interface)**

Interfaz de velocidad base o simplemente interfaz básica. También se le conoce como (2B+ D) puesto que la interfaz BRI está compuesta por 2 canales B de 64kbps y un canal D de 16kbps.

Un usuario BRI puede utilizar la misma línea para enviar datos y mantener una conversación al mismo tiempo.

- **PRI (Primary Rate Interface)**

Interfaz de velocidad primaria o Interfaz primaria.

Para Estados Unidos se le llama (23B+ D), pues consta de 23 canales B de 64kbps y un canal D de 64Kbps, con un ancho de banda total de 1.544Mbps diseñado para transmitir a través de un T1.

Para Europa, América Latina y Asia-Pacífico, PRI consta de 30 canales B de 64Kbps y un canal D de 64Kbps (30B + D), y se suministra a través de un canal E1 de 2.048Mbps [Nortel Networks, Training Program 1999]

“Una de las principales ventajas de ISDN es su capacidad de combinar el ancho de banda de varios canales”⁸ Los canales B se pueden sumar para una aplicación que requiera gran ancho de banda y luego ser reasignados para utilizarse en otras aplicaciones de menor ancho de banda.

A la combinación de canales B se le conoce como Multiplexión inversa, esta Multiplexión es automática ya que los dispositivos detectan el ancho de banda disponible y lo aplican para transmitir.

b) Frame Relay

Frame Relay es un protocolo WAN que proporciona transmisiones de alta velocidad con mayor flexibilidad y menor costo en comparación con otros servicios, pues asigna eficientemente el ancho de banda conforme a las necesidades y dependiendo de la disponibilidad.

Trabaja en las capas: física y de enlace de datos del modelo de referencia OSI, además tiene la capacidad de manejar diversos protocolos o diferentes tipos de tráfico, por ejemplo, voz, tráfico Intranet por IP, etc.

La red Frame Relay esta formada por dos tipos de equipos

- DTE (Data terminal equipment o equipo terminal de datos)
- y los DCE (Data circuit-terminating equipment o equipo de circuito de terminación de datos)

Entre los DTE se encuentran las computadoras personales, los routers y bridges, los dispositivos de acceso Frame Relay o FRAD (Frame Relay Access Devices, funcionan de interfaz entre la red local y la línea alquilada) El FRAD es el encargado de empaquetar en tramas la información de la LAN y trasmitirlas a través de la red.

⁸ Ibid. 192



El propósito de los equipos DCE es proveer sincronización y conmutación a la red como son los multiplexores T1/E1, los enrutadores de red y los switches.

Debido a que una red Frame Relay no es una sola conexión física entre 2 terminales, sino que se define una trayectoria lógica dentro de la red, se le representa como una nube.

Las trayectorias o conexiones lógicas reciben el nombre de circuitos virtuales (VC, virtual circuit).

"Un circuito virtual de tramas puede pasar a través de cualquier cantidad de nodos de red ubicados dentro de la nube Frame Relay"⁹

Existen dos tipos de circuitos virtuales:

- SVC (Switched Virtual Circuits) circuitos virtuales conmutados
- PVC (Permanent Virtual Circuits) circuitos virtuales permanentes

Los SVC son conexiones temporales creadas de forma dinámica, ya que se establecen cuando es necesario realizar una transferencia esporádica de datos entre dispositivos DTE a través de la red Frame Relay.

Esta conexión consta de 4 estados:

- 1) Se establece la llamada
- 2) Transferencia de datos
- 3) Desocupado (ocioso en espera)
- 4) Termina la llamada

Los PVC son conexiones permanentemente establecidas que se utilizan para transferencias frecuentes de datos a través de la red Frame Relay. Esta conexión siempre esta activa, independientemente de si existe tráfico o no para transmitir.

Consta de dos estados, pues no se requiere establecer una llamada ni terminarla, los estados que existen son los siguientes:

- 1) Transferencia de datos
- 2) Desocupado (en espera)

Para tener siempre garantizado un ancho de banda sin importar que la red Frame Relay se encuentre congestionada se establece con el proveedor de servicios una velocidad de información comprometida (CIR, comitted information rate).

Cada circuito virtual se divide en un ancho de banda garantizado (CIR) y un ancho de banda etiquetado como "entrega en base a la disponibilidad".

Entrega en base a la disponibilidad significa que si existe ancho de banda disponible los datos serán transmitidos, de no ser así serán marcados como DE (Discard Eligibility) elegible para descarte y serán descartados cuando exista una congestión en la red.

⁹ NORTEL Networks, *Training program, Module Frame Relay*, 19

c) PPP

PPP (Point to Point Protocol) o Protocolo Punto a Punto, se creó como un protocolo de encapsulación para transportar tráfico IP a través de enlaces punto a punto, así como “tener la posibilidad de multiplexar protocolos de nivel de red y admitir diversos protocolos de autenticación”¹⁰

PPP ayudó a solucionar los problemas de conectividad remota de Internet. PPP es el protocolo WAN más popular y más ampliamente utilizado porque ofrece las siguientes funciones:

- Control de la configuración del enlace de datos
- Proporciona asignación dinámica de direcciones IP
- Configuración de enlace y verificación de la calidad del enlace
- Detección de errores

Debido a esto PPP utiliza LCP (Link Control Protocol), Protocolo de control de enlace y una familia de NCP (Network Control Protocol) Protocolo de control de red para negociar la configuración de algunos parámetros.

Las partes principales que conforman al protocolo PPP en un enlace serial punto a punto son:

- Método de encapsulación de datagramas sobre enlaces seriales: PPP utiliza HDLC (High-Level Data Link Control).
- LCP para establecer, configurar y probar la conexión.
Existen tres tipos de tramas de LCP:
 - Tramas de establecimiento de enlace
 - Tramas de mantenimiento del enlace
 - Tramas de terminación del enlace.
- NCP para establecer y configurar diferentes protocolos de nivel de red.

Una sesión PPP está compuesta por los siguientes pasos:

1. Establecimiento de la conexión

Se envían paquetes LCP para configurar los parámetros y probar el enlace. La etapa de establecimiento de la conexión está completa cuando una trama de configuración y conocimiento ha sido enviada y recibida.

2. Determinación de la calidad del enlace (opcional)

LCP permite una opción para determinar la calidad del enlace. En esta fase se examina y determina si el enlace tiene calidad suficiente para utilizar protocolos de nivel de red.

3. Autenticación (opcional)

Aunque no se requiere, el sistema puede utilizar un protocolo de autenticación ya sea PAP (Password Authentication Protocol) Protocolo de autenticación de contraseña o CHAP (Challenge Handshake Authentication Protocol) Protocolo de autenticación Challenge Handshake.

¹⁰ ZACKER, *op.cit.* 403

4. Fase de protocolo de red

Inicia la negociación para la configuración de protocolos de nivel de red. Se envían los paquetes NCP. Por cada uno de los protocolos de nivel de red que se utilicen durante la sesión se realizara un procedimiento NCP independiente.

5. Cierre de sesión

LCP puede terminar el enlace en cualquier momento, ya sea por petición del usuario o por algún evento físico.

d) HDLC

HDLC (High-Level Data Link Control) es un protocolo derivado de SDLC (Synchronous Data Link Control), que especifica un formato de encapsulación de trama para enlaces de datos sincrónico orientado a la conexión. SDLC fue desarrollado inicialmente por IBM, algunos comités de estándares lo modificaron para crear los siguientes protocolos:

- ISO (International Organization Standard) creó HDLC
- CCITT modificó HDLC y creó LAP (Link Access Procedures) y LAPB (Link Access Procedure Balanced)
- IEEE modificó HDLC y creó IEEE 802.2

HDLC puede ser usado en conexiones punto a punto, punto a multipunto, transmisión half-duplex y full-duplex, redes de circuitos conmutados o de conmutación de paquetes. Debido a que HDLC no es compatible entre diversos vendedores, cada uno ha elegido su manera de implementarlo. CISCO lo ha implementado de la siguiente manera:

Este protocolo separa en dos tipos a los nodos de red: primarios y secundarios.

"Los nodos primarios son los encargados de controlar la operación de otras estaciones llamadas secundarias. Los nodos primarios encuestan en un orden determinado a los nodos secundarios, para que estos puedan transmitir su información".¹¹

Los nodos secundarios son aquellos que se encuentran controlados por los primarios, y pueden enviar su información solo si los nodos primarios lo autorizan.

HDLC soporta dos configuraciones de nodos.

- Punto a punto: la cual consiste en solo 2 nodos un nodo primario y un nodo secundario
- Multipunto: esta configuración incluye varios nodos secundarios y un solo nodo primario.

Los modos de transferencia que soporta HDLC son tres, SDLC a diferencia de HDLC solo utiliza un modo. "Los modos de transferencia son los siguientes:

- **NRM (Normal Response Mode) Modo de respuesta normal.** Este es el único modo utilizado por SDLC. Los nodos secundarios no pueden comunicarse con un nodo primario hasta que este último haya dado su permiso.

¹¹ DOWES, *op. cit.* 216

- ARM (Asynchronous Response Mode) Modo asincrono de respuesta. Aquí los nodos secundarios pueden iniciar la comunicación con un nodo primario sin recibir algún permiso o autorización.
- ABM (Asynchronous Balance Mode) Modo asincrono balanceado. En este modo existen unos nuevos nodos llamados combinados, los cuales pueden actuar tanto de nodos primarios como de nodos secundarios, dependiendo de la situación.

Este último modo de transferencia solo puede llevarse a cabo entre nodos que sean combinados. Cualquier estación puede iniciar la transmisión de datos sin permiso de alguna otra estación".¹²

■ I.4 [Modelo de Referencia OSI]

El modelo OSI (Open System Interconnection) es el principal modelo de referencia que existe para llevar a cabo comunicaciones de red, su objetivo es la interconexión de sistemas entre diferentes fabricantes tanto en hardware como en software.

La mayoría de los fabricantes se basan en él, pues es la mejor herramienta disponible para enseñar a los usuarios a utilizar sus productos y comprender como viaja la información a través de una red.

Los protocolos LAN funcionan en las 2 capas más bajas del modelo de referencia OSI, esto es en la capa física y en la de enlace de datos.

Esta conformado por 7 capas.



Figura I.11 Modelo de referencia OSI

¹² *ibid.* 220

Capa Física.

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas de comunicación de red. Convierte los bits en series de niveles de voltaje.

Capa Enlace de Datos.

La capa de enlace de datos permite la transferencia confiable de datos a través de un enlace físico. Se ocupa del direccionamiento físico, la topología de red, la notificación de errores (basado en la integridad del paquete), la secuencia de tramas y el control del flujo.

Esta capa esta dividida en dos subcapas que son:

- LLC (Logical Link Control)
- MAC (Media Access Control)

La subcapa LLC maneja comunicaciones entre dispositivos sobre un solo enlace de la red, soporta servicios sin conexión y orientados a la conexión usados por protocolos de capas superiores.

La subcapa MAC controla el protocolo de acceso al medio físico de la red, se encarga de definir un identificador único que permite a múltiples dispositivos identificarse uno del otro entre la capa de enlace de datos llamada Dirección MAC (MAC Address).

Capa de Red.

Esta capa provee funciones de ruteo para habilitar la combinación de múltiples enlaces de datos en una red. Soporta servicios tanto sin conexión, como orientados a la conexión de protocolos de las capas superiores. Forma los datagramas con el paquete, mas un encabezado, el cual contiene la dirección lógica de la red, información de ruteo y control de flujo.

Capa de Transporte.

Suministra un servicio de transporte de datos que aísla las capas superiores, además proporciona confiabilidad del transporte de datos.

Las funciones típicas de esta capa son: control del flujo, Multiplexión, manejo de circuitos virtuales (establece, mantiene y termina estos circuitos), recuperación y corrección de errores y segmentación.

En esta capa se encuentra el protocolo UDP (User Datagram Protocol) y TCP (Transmission Control Protocol).

Capa de Sesión.

Establece, maneja y termina sesiones de comunicación entre entidades de la capa de presentación. Sincroniza el dialogo entre las capas de presentación y administra el intercambio de datos. Además determina quien inicia la conversación y acuerda que servicios son los requeridos así como la duración de los mismos.

Ofrece alternativas para una eficiente transferencia de datos (clase de servicio).

Capa de Presentación.

Esta capa provee una variedad de funciones de codificación y conversión. Garantiza que la información que se envía desde la capa de aplicación de un sistema, pueda ser leída por la capa de aplicación de otro sistema; de ser necesario traduce entre varios formatos de datos utilizando un formato común.

Capa de Aplicación.

Esta es la capa más cercana al usuario, ya que el modelo OSI y el usuario interactúan con el software de aplicación. Difiere de otras capas debido a que no proporciona servicios a ninguna otra capa, sino a aplicaciones fuera del modelo OSI.

Establece y sincroniza acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.





TECNOLOGÍAS INALÁMBRICAS

■ II.1 [¿Qué es una red inalámbrica]

Para poder dar una definición de red inalámbrica debemos entender primero el concepto de "inalámbrico". Inalámbrico o wireless significa textualmente sin cables, pero se usa para describir a los sistemas de comunicaciones que utilizan ondas electromagnéticas como medio para transportar una señal a través del aire.

Por lo tanto, una red inalámbrica es aquella en la cual diversos equipos pueden comunicarse entre sí, sin la necesidad de estar conectados a algo con cables. [Brisbin, 2002]

Los hechos que dieron pauta al origen de la tecnología inalámbrica se remontan al año de 1857, cuando el físico norteamericano Samuel Morse (1791-1872) inventó el telégrafo eléctrico y un alfabeto par poder transmitir mensajes a largas distancias por medio de emisiones alternadas de una corriente eléctrica a través de un conductor metálico.

Después los estudios realizados por James C. Maxwell (1831-1879), quien formuló la teoría electromagnética, estableció que los campos eléctricos y magnéticos al interactuar, producían un nuevo tipo de energía llamada radiación, y determinó que las ondas tienen un carácter ondulatorio; y los estudios realizados por Heinrich R. Hertz (1857-1894) entre 1885 y 1889 para comprobar la existencia de las ondas electromagnéticas, impulsaron los experimentos sobre como producir este tipo de ondas y recibirlas.

Fue Guillermo Marconi (1874-1937) quien logró enviar señales en clave Morse sin necesidad de cables utilizando el telégrafo inalámbrico. Esto lo hizo apoyándose en las teorías de las ondas electromagnéticas para transmitir señales a través del espacio por medio de un aparato con un transmisor y un receptor con antena.

En junio de 1896 transmitió el primer mensaje radiotelegráfico a una distancia de 250m entre el emisor y el receptor, estando ambos separados por muros; al año siguiente logró realizar comunicaciones a distancia entre dos ciudades, y para 1901, logró entablar comunicación a través del Océano Atlántico. Muy pronto todos los barcos de guerra fueron provistos de aparatos de radiotelegrafía, y poco a poco se fue popularizando este sistema de comunicación.

"El primer tubo de vacío capaz de detectar electrónicamente ondas de radio fue inventado por Sir John Fleming en 1904. Dos años después Lee de Forest inventó una especie de triodo (un elemento de tres tubos de vacío) llamado audion que no sólo detectaba ondas de radio, sino también las amplificaba.

Los inicios de la Radio Frecuencia (RF) refiriéndonos a la transmisión de música y voz comenzaron en 1906, con el trabajo de Reginald H. Armstrong quien patentó el circuito para el receptor regenerador que hizo posible la recepción de radio de largo rango"¹³ En 1920 apareció la primer estación comercial de radio en Estados Unidos y el aparato radiofónico se popularizó rápidamente en todo el país.

¹³ OVELLET, *Building a Cisco Wireless LAN*. 33

Desde los primeros días de la radio, incontables mejoras y estudios ha traído aplicaciones más especializadas de comunicaciones inalámbricas. Algunos ejemplos son:

- Monitores de bebe: radios receptores y transmisores de rango limitado.
- Televisión satelital: permite el acceso a cientos de canales con buena calidad
- Control de sistemas caseros de entretenimiento: el control remoto del video casetera, los estéreos y la TV.
- Localizadores y teléfonos celulares
- Teléfonos inalámbricos: dispositivos de rango limitado para su uso en el hogar.
- Periféricos inalámbricos para computadora: por ejemplo teclados y Mouse inalámbricos o dispositivos para hacer inalámbrica una impresora
- Radios de dos vías: servicio de radio aficionados y para comunicaciones marítimas y militares
- WLANS: Dispositivos de radio inalámbricos para Redes LAN.

La evolución de las comunicaciones inalámbricas y la tecnología han dado paso al desarrollo de sistemas más especializados de telecomunicaciones como son:

- **GSM (Global System Mobile Communication) o Sistema Global para comunicación móvil;** es el sistema telefónico digital estándar más ampliamente usado en Europa y en otros países del mundo, que proporciona un servicio personal de comunicaciones de banda ancha.

- **EDGE (Enhanced Data Rates for GSM Evolution)** es una versión más rápida de GSM que habilita el envío de datos multimedia y otras aplicaciones de banda ancha a teléfonos móviles y a usuarios de computadoras.

- **I-mode:** es un servicio inalámbrico que opera en Japón desde 1999, Este sistema utiliza una red inalámbrica de paquetes y permite a los usuarios acceder a Internet y mandar mensajes cortos en su teléfono digital.

- **GPRS: (General Packet Radio Service) Servicio General de Radio Paquetes;** es un servicio de comunicaciones inalámbricas basado en paquetes que permite a los usuarios tener conexión continua a Internet, tomar parte en videoconferencias e interactuar con sitios Web multimedia.

- **UMTS (Universal Mobile Telecommunications System) Sistema Universal de Telecomunicaciones Móviles.** Este sistema soporta altas velocidades de transmisión de datos lo cual le permite prestar servicios multimedia interactivos y nuevas aplicaciones como servicios de videotelefonía)

■ II.1.1 [Características de una red inalámbrica]

Las redes inalámbricas se pueden dividir en dos categorías de acuerdo a sus características (el rango que alcanzan, la fuerza de su señal, el espectro que usan, etc.) en redes infrarrojas (IR) y redes de radiofrecuencias (RF).

Las redes de radiofrecuencia son comúnmente las más usadas.

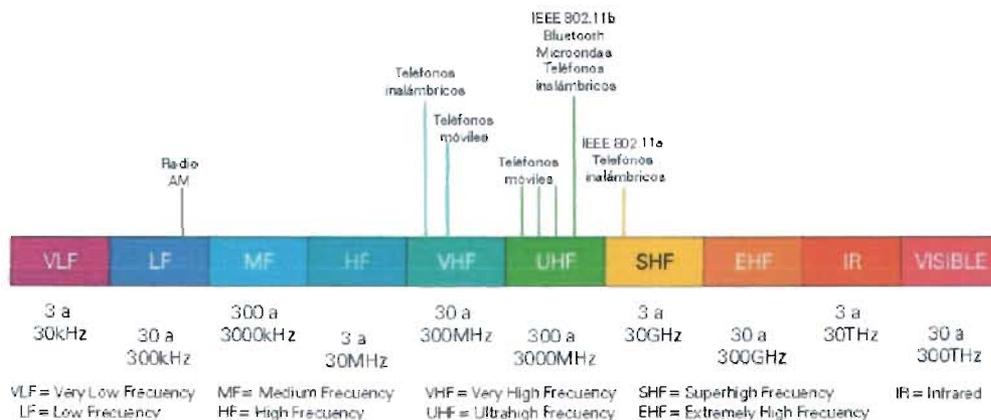


Figura II.1 Espectro radioeléctrico.

Las redes infrarrojas se encuentran justo por debajo del espectro de luz visible, y debido a que su señal no puede traspasar los objetos su aplicación no es tan amplia como las RF, pues deben tener siempre libre su línea de vista para poder llevar a cabo la comunicación. Aunque también se ocupan para aplicaciones más complejas, normalmente se ocupan para comunicaciones de corto rango como puede ser entre un PDA y una laptop o entre algunos teléfonos móviles.

Debido a que las redes inalámbricas RF utilizan frecuencias muy por debajo del espectro de luz visible y sus longitudes de onda permiten a la señal atravesar algunos objetos sólidos, tomaremos en cuenta solo a las redes de RF para su análisis.

"Por las características de las redes en sí mismas y las formas en que estas redes se usan para brindar un nuevo tipo de comunicación en lugares donde no existían antes"¹⁴ las redes inalámbricas se han vuelto más necesarias en lugares donde implementar una red cableada sea difícil. Las siguientes características muestran algunas de sus ventajas:

a) Flexibilidad

Debido a que no es necesario tener cables, se puede instalar una red en cualquier lugar, sobre todo en aquellos lugares de difícil acceso o donde no se pueda modificar la estructura original de un edificio (como es el caso de museos, edificios con valor histórico o construcciones muy antiguas). Ya que el despliegue de una red inalámbrica es muy rápido esto simplifica y facilita su instalación.

b) Movilidad

El poder compartir información sin tener una conexión física permite una mayor movilidad, pues los usuarios de la red no tienen que estar en un solo lugar (escritorio u oficina) para poder obtener la información que requieren.

Con las redes inalámbricas, pueden tener con ellos un dispositivo de mano, una laptop o un PDA y moverse a través de la empresa o área de trabajo y obtener la información en tiempo real en cualquier lugar.

¹⁴ BRISBIN, *Build your own Wi-Fi network*, 2



c) Escalabilidad

Se define como la capacidad de expandir una red después de la instalación inicial. Una red inalámbrica es muy escalable, pues no es necesario agregar mucha infraestructura para dar a nuevos usuarios servicio de red. Esto facilita el dar de alta usuarios, crear cedos temporales y el mover fácilmente la red a otro lugar.

d) Frecuencias libres de licencia

El espectro electromagnético se encuentra dividido en diversas bandas de frecuencia. La mayoría del espectro de frecuencia esta asignado a su uso con licencia; esto es que el portador de la licencia puede hacer uso exclusivo de ella con solo pagar una cuota y siguiendo las regulaciones necesarias para dicha banda.

Pero existen unas bandas que no requieren algún permiso en especial, estas son las frecuencias libres de licencia y reciben el nombre de ISM (Industrial Scientific and Medical) para los dominios regulados por la FCC (Federal Communications Commission) que es una agencia del Gobierno de Estados Unidos; o en el caso de México ICM (Industrial Científica y Medica).

Al principio la banda ISM estaba limitada a su uso por instrumentos científicos, médicos e industriales para la experimentación e investigación, pero después se asignó también a las redes inalámbricas (1985) y a otras aplicaciones.

Las bandas libres de licencia son las siguientes:

- 902 – 928MHz con 26MHz de ancho de banda
- 2.4 – 2.4835GHz con 83.5MHz de ancho de banda
- 5.725 – 5.875GHz con 125MHz de ancho de banda

La banda de 900MHz es usada comúnmente para los teléfonos inalámbricos y radioaficionados; también para las primeras redes inalámbricas.

La banda de 2.4GHz la utilizan los teléfonos inalámbricos, los hornos de microondas, Bluetooth y los sistemas 802.11, 802.11b y 802.11g y algunos radioaficionados.

La banda de 5GHz sufre menos interferencia que las de 900MHz y 2.4GHz y se utiliza para las redes 802.11a.

El hecho de que sean bandas libres de licencia, no significa que no tengan restricciones. Los usuarios deben seguir algunas regulaciones, por ejemplo: los equipos deben utilizar muy poca potencia para transmitir y deben ser resistentes a las interferencias. Los equipos pueden sufrir interferencia debido a que no se puede garantizar el uso exclusivo de cualquiera de las frecuencias libres de licencia [Engst, 2003].

■ II.2 [Componentes de una red inalámbrica]

Existen dos tipos de componentes que integran una red inalámbrica, los componentes lógicos y los componentes físicos. Los componentes lógicos son las funciones y subsistemas requeridos para realizar funciones de red en un sistema inalámbrico, El componente lógico principal en una WLAN es el sistema de distribución DS (Distribution System).

DS se refiere a la topología de la red cableada que se conectará a la WLAN para poder acceder a diferentes servicios y aplicaciones, es absolutamente necesario cuando se utilizan bases de datos, sistemas de impresión alámbricos, etc. Otros componentes lógicos son las técnicas de acceso al medio, la sincronización y el control de errores.

Los componentes físicos son los equipos que se utilizan para poder implementar una red inalámbrica. Los principales componentes físicos son los siguientes:

- AP
- Tarjetas de cliente o (adaptadores de red inalámbrica)
- Antenas

■ II.2.1 [AP]

El punto de acceso (Access Point) AP es el centro de una red inalámbrica, podría decirse que realiza funciones similares a las de un hub, pues brinda comunicación a todos los que se conecten a él, pero puede efectuar tareas un poco más complejas, ya que puede actuar como un gateway pues conecta a redes cableadas con redes inalámbricas, o conecta a una red inalámbrica a Internet. Se encarga también de gestionar la seguridad en la red.

Se caracteriza por que puede tener uno o más radios inalámbricos. Los parámetros que siempre se configuran en un AP son: el SSID (Service Set Identifier) nombre de la red, el canal en el que se va a transmitir (dependiendo del estándar que se este utilizando), y la clave WEP (si es que se van a encriptar los datos)



Figura II.2 Access Point

■ II.2.2 [Tarjetas inalámbricas]

También llamadas adaptadores de red inalámbrica, estación del cliente o tarjeta del cliente. Consiste en un radio que se instala en una computadora con el fin de tomar la señal de radio proveniente de un AP. La mayoría de las computadoras portátiles actuales, ya tienen tarjetas de red inalámbrica instaladas.

Pero en caso de necesitar alguna, existen tres diferentes tipos de adaptadores de red inalámbrica:

- Adaptadores PCMCIA

PCMCIA (Personal Computer Memory Card International Association), se creó en 1989, con el fin de desarrollar una norma para tarjetas de memoria intercambiables. Casi todas las laptops cuentan con slots PCMCIA. Los puertos PCMCIA son unas ranuras en las que se puede insertar tarjetas (PC Cards) externas de tamaño pequeño que son fáciles de instalar.

Existen tres tipos de acuerdo al grosor de las ranuras:

- o Tipo I = grosor de 3.3mm
- o Tipo II = grosor de 5mm
- o Tipo III = grosor de 10.5mm

Las principales características de estas tarjetas son: su bajo peso, el tamaño reducido además de que consumen poca energía y son resistentes a los golpes típicos de los dispositivos móviles. Los adaptadores para Wi-Fi son PCMCIA Tipo II con un bus de 32bits tipo cardbus.

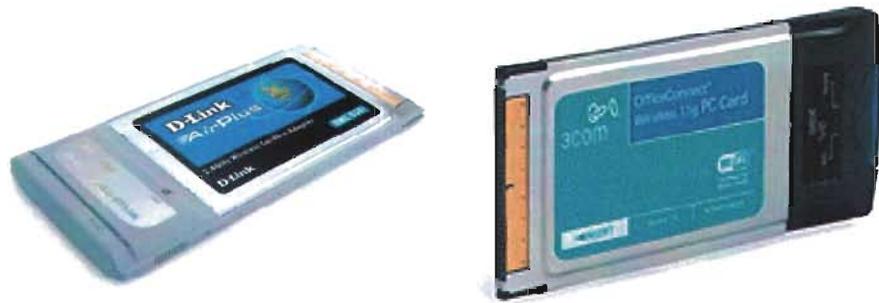


Figura II.3 Adaptadores PCMCIA tipo PC card

- Adaptadores PCI e ISA

Debido a que las computadoras de escritorio no cuentan con puertos PCMCIA, se les puede instalar un adaptador que se inserta en las ranuras PCI (Peripheral Components Interconnect) interconexión de componentes periféricos o ISA (Industry Standard Architecture) Arquitectura normalizada de la industria, que están dentro de la tarjeta madre de la computadora. Para instalar este tipo de adaptadores es necesario abrir la computadora. Algunas de estas tarjetas cuentan con pequeñas antenas externas con el fin de captar mejor la señal de radio. Existen adaptadores PCI o ISA a PCMCIA, lo que implicaría comprar el adaptador, y aparte comprar una PCcard.



Figura II.4 Adaptadores de red inalámbrica para PCI

- Adaptadores USB

USB (Universal Serial Bus), es el adaptador de red inalámbrico más flexible que existe, ya que no se requiere apagar la computadora para conectarlo o desconectarlo, además de que lo reconoce automáticamente. Son muy cómodos y fáciles de utilizar, el único inconveniente es que no quedan integrados dentro de la computadora como PCMCIA o PCI



Figura II.5 Adaptadores de red inalámbrica para USB

- Adaptadores para PDA o Pocket PC

Debido a que los PDAs cuentan con pequeños adaptadores, se les pueden colocar tarjetas inalámbricas tipo Compact Flash en la ranura dedicada para las memorias de almacenamiento, con el fin de que puedan acceder a Internet. Algunos PDAs requieren de un accesorio especial (varia de acuerdo al modelo de PDA)



Figura II.6 Adaptador de red inalámbrico tipo Compact Flash



■ II.2.3 [Antenas]

Una antena puede describirse como un sistema conductor metálico capaz de radiar y recibir la señal modulada (u ondas electromagnéticas) a través del aire para que el receptor pueda captarlas. Las antenas se agregan a los equipos con el fin de extender el rango de la red, pues mejoran el desempeño del radio inalámbrico.

“Las antenas tienen ciertas características que contribuyen a la calidad y fuerza de la señal que proveen”¹⁵ Algunas de estas características son:

- **Ancho de banda** – rango de frecuencias en las que trabaja (disponible para datos)
- **Ganancia** – describe el grado de amplificación de la señal, o el grado en que la energía es transmitida en una determinada dirección. Se mide en dB, pero también se puede expresar en dBi.
- **Polarización** – La polarización (P) de la antena describe la orientación de los campos magnéticos (H) que irradia o recibe. Cuando el campo E (eléctrico) está orientado en forma perpendicular con respecto al horizonte terrestre se dice que tiene una polarización vertical. Si el campo E está orientado paralelo al horizonte terrestre se dice que tiene una polarización horizontal. Cuando el campo eléctrico rota mientras la señal se propaga se dice que se tiene una polarización circular. Tanto la antena transmisora como la receptora deben tener la misma polarización con el fin de minimizar las pérdidas y evitar generar señales de ruido

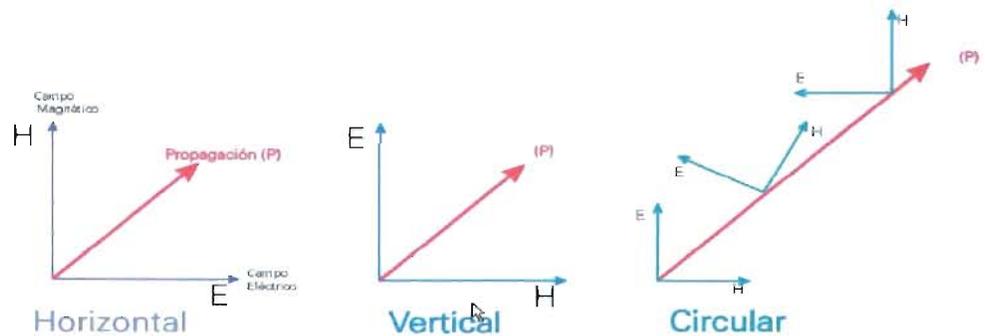


Figura II.7 Tipos de Polarización

- **Patrón de radiación** – es un diagrama polar que representa la fuerza de los campos electromagnéticos radiados (patrones de cobertura) de una antena. Existen dos patrones de radiación.
 - o En el primero se muestran todos los ángulos del plano E con un ángulo en el plano H igual a cero.
 - o En el segundo se muestran todos los ángulos del plano H y los ángulos del plano E están en cero.
 El radio del diagrama puede ser calibrado con respecto a dos variantes:
 - o La potencia lineal en escala de 1 con incrementos de 0.25 o 0.2 por división
 - o La potencia logarítmica relativa, típicamente de -5dB o -10dB por división, como

¹⁵ Ibid. 52

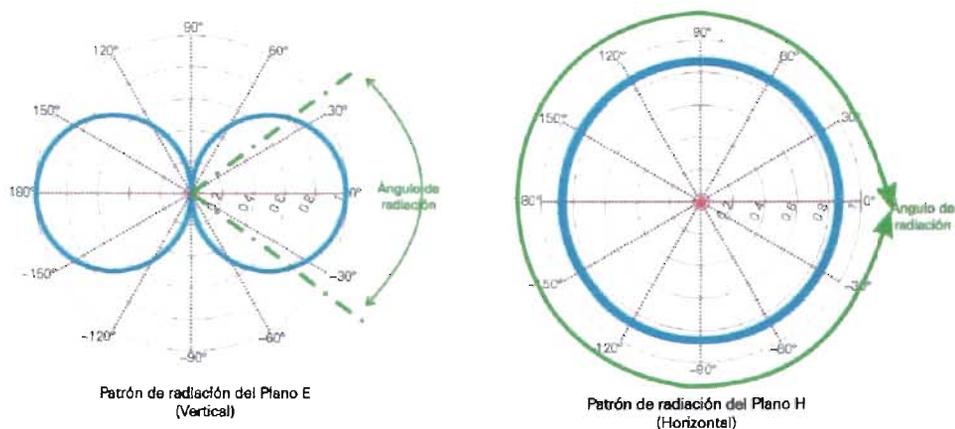


Figura II.8 Patrones de radiación

- **Antena isotrópica** – es una antena que irradia la misma cantidad de energía (en igual intensidad) en todas direcciones desde el punto de origen. Este tipo de antena es teórica.
- **Relación señal a ruido (S/N)** – es la relación de la fuerza de la señal de datos, comparada con la fuerza de la señal de ruido en el ambiente. Tanto al transmitir como al recibir es inevitable enviar o recibir ruido. Se mide en dB.

47

a) Tipos de antenas

Las antenas se pueden clasificar principalmente en omnidireccionales y direccionales.

• Antenas omnidireccionales

La señal se irradia en todas direcciones al mismo tiempo (en forma de círculos). La característica principal de estas antenas es que si un dispositivo inalámbrico se coloca justo abajo o arriba de la antena la señal será muy débil, es necesario alejarse un poco de la antena para obtener una mejor recepción. Estas antenas distribuyen la señal en un área amplia, y son útiles cuando los clientes están dispersos por toda el área.

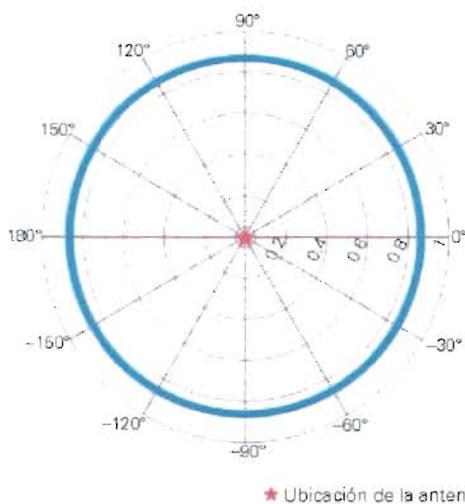


Figura II.9 Patrón de radiación de una antena omnidireccional

También son apropiadas para usarse en un punto multipunto (en el punto central) pues pueden captar todas las señales provenientes de varios lugares. La máxima ganancia que tienen las antenas omnidireccionales, es aproximadamente de 15dBi.



Figura II.10 Antena omnidireccional

- Antenas direccionales

Las antenas direccionales concentran su radiación en una dirección, son utilizadas para alcanzar mayores distancias que las antenas omnidireccionales. Además de que es menos probable que causen interferencia a otros sistemas de radiofrecuencias. Cuanto más direccional es una antena, mayor es su alcance.

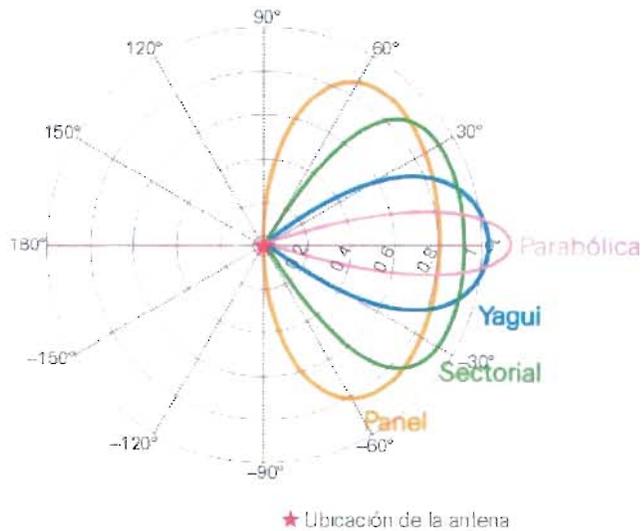


Figura II.11 Patrón de radiación de los distintos tipos de antenas direccionales

Existen varios modelos de antenas direccionales, los más utilizados en sistemas inalámbricos son los siguientes:

* Antena sectorial

Este tipo de antena es plana con un reflector detrás de la superficie de la antena para dirigir la señal. Puede tener tanto polarización horizontal como vertical. Provee un radio de señal que normalmente va de los 60 a los 180°, no más debido a que el reflector previene que se irradie detrás de la antena. Se utilizan para enfocar la señal en áreas pequeñas, en ambientes donde hay múltiples redes que operan cerca con proximidad entre una y otra.



Figura II.12 Antenas sectoriales

* Antena tipo panel

Es una antena sólida plana, que se utiliza principalmente para conexiones punto a punto. Tiene una buena ganancia entre 15 y 20dBi aproximadamente. Su principal desventaja es que por su forma son susceptibles a interferencias por el viento, pues este puede moverlas si no están bien fijas, por lo que es recomendable instalarlas planas sobre una pared.

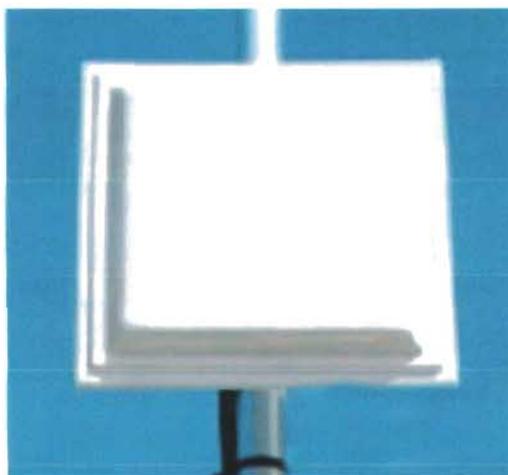


Figura II.13 Antena tipo panel

• Antena Yagui

Esta antena es de forma cilíndrica, compuesta por un tubo grueso de plástico que recubre una serie de círculos o barras de metal de diferentes tamaños. Proporciona un haz bastante enfocado, que puede medir entre 15 y 60°. Provee mejor ganancia que las antenas sectoriales, entre 6 y 21 dBi aproximadamente.

Se utilizan para conexiones punto a punto principalmente y se ve menos afectada por el viento debido a su forma. Para direccionar bien la antena se recomienda no apuntar directamente a la antena del otro extremo, sino ponerla ligeramente elevada a la izquierda o a la derecha del punto a alcanzar.



Figura II.14 Antena Yagui

• Antena Patch

Es una antena con forma plana o puede ser también un poco redondeada, que emite su energía semiesféricamente. Esta diseñada para ser montada en la pared y puede proporcionar ganancias de 12 a 22dBi aproximadamente, generalmente se ocupan para interiores.



Figura II.15 Antenas patch



* Antena Parabólica

Son las más potentes, tienen la apariencia de un pequeño plato satélite, pero esta hecho de una rejilla de metal en vez de ser un plato sólido. Estas antenas están diseñadas para operar en largas distancias (alcanzan varios kilómetros), pues su patrón de radiación es muy estrecho, va de los 8 a los 15°. Las hay tanto con polarización vertical como horizontal y pueden dar ganancias de 15 a 24dBi.



Figura II.16 Antenas parabólicas de rejilla

■ II.3 [Estándares para redes inalámbricas]

Existen varios estándares inalámbricos en el mercado, pero no todos ellos han tenido gran éxito. Un estándar es importante ya que asegura que los equipos que se elaboran bajo ese estándar tengan interoperabilidad entre ellos, además de que dan mayor seguridad a las compañías, ya que si compran un equipo que no pertenezca a un estándar no saben que tan confiable es o cuales son las características mínimas que deben soportar para operar con otros equipos.

La demanda de redes inalámbricas se ha incrementado en los últimos años, lo cual ha llevado a varias compañías a crear estándares que proporcionen las soluciones necesarias para la demanda del mercado.

Muchos de los estándares disponibles tienen varias características en común como son: el uso de las bandas ISM (2.4GHz y 5GHz), el espectro extendido e incluso algunas de las estructuras de red son similares.

Los estándares más comunes en todo el mundo debido a su rápida aceptación y desempeño son Wi-Fi y Bluetooth, aunque también HomeRF e HiperLAN han destacado. Se puede decir que los únicos estándares diseñados para soportar Banda Ancha son Wi-Fi e HiperLAN. En cambio Bluetooth y HomeRF se utilizan más para el mercado residencial.

A continuación se describe brevemente a Wi-Fi (802.11a, b y g) solo para dar una idea general de sus características y analizar su desempeño en relación con los otros estándares. En los subcapítulos WLAN y Seguridad se retomará Wi-Fi y estudiará más detalladamente.

■ II.3.1 [Wi-Fi]

El término "Wi-Fi" de Wireless Fidelity o Fidelidad Inalámbrica, es un nombre comercial (marca registrada) desarrollado por un grupo llamado Alianza Wi-Fi (formalmente WECA o Wireless Ethernet Compatibility Alliance), cuya finalidad es certificar y garantizar la interoperabilidad entre múltiples fabricantes de equipos inalámbricos.

La WECA o Wi-Fi Alliance se creó en 1999, sin fines de lucro para promover IEEE 802 y desarrollar un programa de certificación que asegure que los productos inalámbricos se acoplan completamente al estándar 802.11.

El 26 de junio de 1997 El IEEE anunció la ratificación del estándar para redes de área local inalámbricas 802.11. Este estándar describe la capa física y de enlace de datos (MAC), las frecuencias para enviar y recibir información, la velocidad de transmisión, pero no garantizaba que los productos entre diversos fabricantes fueran compatibles, por eso se realizaron revisiones a este estándar, dando origen a los estándares 802.11 a, 802.11b, y 802.11g.

En un principio Wi-Fi solo se utilizaba para describir los dispositivos con velocidades máximas de 11Mbps que operaban en la porción de 2.4GHz del espectro de frecuencia y que cumplieran con las especificaciones 802.11b. Más tarde se decidió ampliar el concepto Wi-Fi e incluir los productos que trabajan a velocidades de 54Mbps, que operan en las porciones de 2.4GHz y 5GHz del espectro de frecuencias y que están basados en las especificaciones 802.11g y 802.11a.

Cuando un fabricante desea que sus equipos estén certificados con Wi-Fi, la WECA realiza una serie de pruebas para verificar que estos equipos cumplen con los requerimientos necesarios, y se aseguran de su interoperabilidad con productos de otros fabricantes. Después que el producto ha pasado estas pruebas puede entonces exhibir el logo de certificación Wi-Fi en su empaque, el cual asegura al comprador la completa adaptación con el estándar y con otros productos que también exhiban el logo Wi-Fi

Debido a que los estándares IEEE 802 operan tanto en la capa física como de enlace de datos del modelo OSI, 802.11 define su modelo de referencia de la siguiente manera:

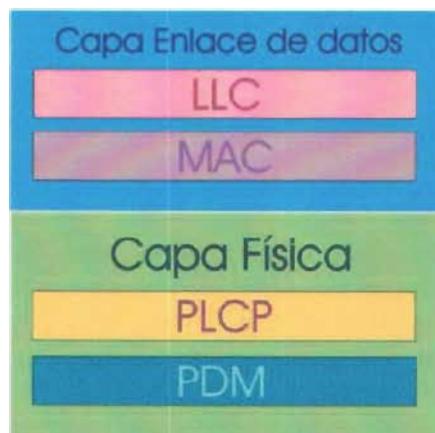


Figura II.17 Modelo de referencia 802.11

Capa Física (PHY)

La capa física se encarga de definir los parámetros para llevar a cabo la modulación y la transmisión de información en un medio determinado.

Se divide en dos subcapas que son: PLCP (Physical Layer Convergence Procedure) Subcapa de Procedimiento de Convergencia de la capa Física y PDM (Physical Medium Dependent) Subcapa Dependiente del Medio Físico.

La subcapa PLCP se encarga de convertir los datos a un formato compatible con el medio físico, la codificación, técnica de propagación y modulación; además sirve de enlace entre la capa PHY y la de enlace de datos. PDM se encarga de transmitir los datos que recibe de PLCP al aire (difusión de la señal), y comprobar que el canal esté libre.

Las técnicas de espectro extendido que se pueden utilizar en la capa física son las siguientes [Brisbin, 2002]

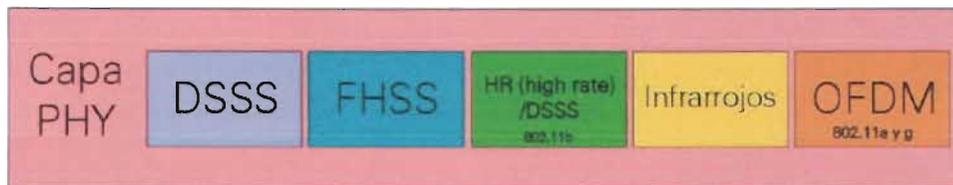


Figura II.18 Técnicas de espectro extendido para 802.11

Capa de enlace de datos.

Esta capa se divide en dos subcapas: LLC (Logical Link Control) Control lógico del enlace y MAC (Medium Access Control) Control de acceso al medio.

La subcapa LLC se encarga de encapsular los paquetes de datos que recibe de los niveles más bajos de la red para transferirlos a capas más altas. Debajo de LLC se encuentra la subcapa MAC cuyo trabajo es manejar el acceso al medio de la red.

Subcapa MAC

La subcapa MAC usa CSMA (Carrier Sense Multiple Access) Acceso múltiple por sensor de portadora para acceder al medio al igual que Ethernet. Pero Ethernet utiliza la tecnología CSMA/CD (Collision Detect) Detección de colisiones y Wi-Fi emplea la tecnología CSMA/CA (Collision Avoidance) (Acceso Múltiple por sensor de portadora con evasión de colisiones).

Ethernet puede utilizar la detección de colisiones debido a que las colisiones en un medio cableado pueden manejarse, un equipo puede transmitir y recibir al mismo tiempo y detectar las colisiones. Pero en el medio inalámbrico es imposible, ya que un equipo no puede transmitir y recibir al mismo tiempo por el mismo canal (pues la señal se perdería al chocar).

El mecanismo CSMA/CA se asegura de no transmitir a menos que tenga la atención del receptor y que ninguna otra estación este transmitiendo, comprueba primero si el medio esta libre antes de transmitir, (el transmisor "escucha" lo que ocurre en el entorno) si esta en uso espera un tiempo y

vuelve a escuchar y sin nadie más esta usando el medio puede empezar a transmitir. El tiempo que espera una estación antes de volver a comprobar el medio es aleatorio [Carballar, 2004]

La subcapa MAC también se encarga de proporcionar servicios de estación y distribución (para los AP). En total son nueve diferentes servicios, de los cuales 4 son los servicios de estación y 5 los servicios de distribución. Los servicios de estación son los siguientes: Autenticación, Desautenticación, Privacidad y Entrega de datos MSDU y proveen funcionalidad igual a la de las redes cableadas basadas en 802.3. Los servicios de distribución son: Asociación, Disasociación, Reasociación y Distribución. Además proporciona otras funciones como RTS/CTS y el modo de ahorro de energía, estos se llevan a cabo entre la subcapa MAC y LLC con el fin de tomar decisiones tales como el lugar al que deben ser enviadas las tramas 802.11 o como llevar a cabo el roaming cuando un dispositivo está en movimiento

Servicios de estación:

- **Autenticación:** Un dispositivo que quiere asociarse con otra estación o AP, se autentica (comprueba su identidad) para así autorizar su acceso en la red. Un equipo puede autenticarse al mismo tiempo con más de un punto de acceso en la misma red. Existen dos tipos de Autenticación: sistema abierto (SSID) y clave compartida (WEP). Si la autenticación no se puede establecer entre los equipos la asociación no se establecerá y el dispositivo no tendrá acceso a la WLAN.
- **Desautenticación.** Se cancela la autenticación existente, lo que da por concluida la conexión. La desautenticación causará que la asociación de la estación se termine. Este servicio se invoca cuando un dispositivo inalámbrico se apaga o sale fuera del área de cobertura.
- **Privacidad:** Utilizado para proteger los datos mientras viajan inalámbricamente, evita el acceso de estaciones no autorizadas a la red mediante el algoritmo WEP. La estación cifra una trama con cierta clave WEP establecida, el AP descifra la trama usando la misma clave WEP y puede entonces intercambiar información.
- **Envío de datos MSDU:** La Unidad de datos de servicio MAC (MSDU, MAC Service Data Unit) se encarga de que los datos transmitidos lleguen a su destinatario de una MAC a otra.

Servicios de Distribución:

- **Asociación:** para que los equipos puedan comunicarse entre sí (por medio de un AP) es necesario estar asociado a un punto de acceso. Un dispositivo envía una trama de asociación al AP, si el AP responde a esta solicitud se intercambia información como las velocidades de datos soportadas. En una red donde existen múltiples AP un dispositivo inalámbrico solo puede estar asociado con un punto de acceso, aunque se haya autenticado con varios APs- La asociación siempre comienza por la estación móvil, no por el AP.
- **Desasociación:** cuando un dispositivo deja la red (sale del área de cobertura) o el AP termina la conexión se cancela la asociación existente entre el AP y el dispositivo.
- **Reasociación:** se da cuando un dispositivo cambia su asociación, (si el dispositivo se mueve del área de cobertura de un AP al área de cobertura de otro AP) se transfiere la información de asociación entre dos APs. Es similar a la asociación, pero incluye información acerca del dispositivo móvil; la información que se intercambia es sobre a que AP estaba asociado anteriormente el equipo, lo que permite recoger las tramas de datos que estén en espera en el AP anterior y reenviarlos a su destino correspondiente. La reasociación siempre comienza por parte del dispositivo móvil.
- **Distribución:** cuando se envía información de una estación a otra, este servicio se asegura de que los datos alcancen su destino final. y también para determinar si enviará la trama de datos a otro

dispositivo móvil, o si la trama tiene como destino la LAN cableada.

- **Integración:** facilita la comunicación entre una red Wi-Fi y cualquier otra red (Ethernet, Internet, etc.) mediante el uso de portales. Sirve de traductor del formato de trama 802.11 al formato de trama de la red cableada y viceversa.

Otros servicios:

- **RTC/CTS:** este servicio consiste en intercambiar la información del uso del medio a través de tramas de control llamadas RTC (Request To Send) solicitud de envío y CTS (Clear To Send) listo para enviar. Cuando un equipo necesita enviar información, envía primero una trama RTC en donde especifica a donde va la información, quien la envía y el tiempo que tardara en enviarla. El AP (si esta desocupado) responde con una trama CTS que envía a todas las estaciones de su área de cobertura, con la información del tiempo que va a estar ocupado el medio; así las estaciones no intentarán transmitir durante ese tiempo y de esta manera los datos se intercambian entre nodos con la mínima posibilidad de que ocurra una colisión.

- **Modo ahorro de energía:** ayuda a mantener la vida de la batería en equipos como PDA's y Tarjetas en computadoras portátiles, pues los equipos pueden entrar en un estado de inactividad y consumir menos energía.

Existen otras funciones importantes que desempeña la subcapa MAC como son el reconocimiento de datos ACK (Data acknowledgement) y la fragmentación de tramas.

- **ACK (Data Acknowledgment):** Para asegurarse que los datos no se pierdan y que la transmisión se llevó a cabo correctamente se introdujo un patrón de reconocimiento ACK. Cuando se envían los datos, se envía una notificación al destinatario, si este responde con un ACK los datos fueron recibidos correctamente, si no responde con un ACK se sabrá que el paquete no fue recibido y se retransmitirá el paquete.

- **FRAGMENTACIÓN:** El estándar 802.11 hace posible la fragmentación de los paquetes envidados en unos de menor tamaño con el fin de permitir una rápida retransmisión, y menor pérdida en la información en ambientes donde hay interferencia. La desventaja de hacer esto es que en el caso de que los paquetes no tengan errores, el costo de enviar paquetes muy cortos es mayor que el costo de enviar la misma información en un par de paquetes largos. Como el estándar 802.11 tiene como configurable esta función, el administrador de la red puede especificar que tipo de paquetes desea fragmentar en ciertas zonas. Paquetes cortos para áreas con mayor presencia de interferencia y paquetes normales para áreas sin interferencia.

- **ROAMING:** el roaming es la capacidad que tiene un dispositivo inalámbrico de saltar de un área de cobertura a otra con el fin de no perder conexión, cuando el dispositivo se encuentra en movimiento. Debido a que los dispositivos inalámbricos tienen la capacidad de determinar la calidad de la señal inalámbrica cuando encuentran un AP, pueden decidir y switchear comunicaciones con un AP diferente si este tiene una señal mucho más clara y fuerte.

El roaming funciona de la siguiente manera: el AP envía una señal con información llamada beacon con la calidad del enlace. El dispositivo inalámbrico escucha a estos beacons y determina con cual AP tiene una mejor señal. El dispositivo se autentificará con el nuevo AP y se realizará una reasociación. El nuevo AP recogerá las tramas de datos pendientes en el AP anterior y le notificará (al AP anterior) que ya no acepte mensajes para ese dispositivo inalámbrico. Este proceso se hace tan rápido que es prácticamente transparente para el usuario, pues no se pierde la conexión.

a) 802.11a

802.11a es una extensión o suplemento del estándar 802.11, que se ratificó en septiembre de 1999.

Su nombre completo es. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5GHz Band" (Especificaciones de nivel de control de acceso al medio (MAC) y del nivel físico (PHY) de las LAN inalámbricas: Nivel físico de alta velocidad en la Banda de 5GHz).

Fue hasta finales del 2001 que empezó a popularizarse, fue Proxim uno de los primeros fabricantes en liberar productos 802.11a.

Este estándar opera en las distintas bandas ISM en la porción del espectro de frecuencia de 5GHz; esto es bastante benéfico, pues estas bandas no se encuentran tan saturadas por otros aparatos inalámbricos, como la banda de 2.4GHz.

Las bandas que utiliza son conocidas como U-NII Unlicensed Nacional Information Infrastructure (Infraestructura Nacional de información libre de licencia). Son tres bandas:

- U-NII 1: Banda inferior, diseñada para el uso en interiores
- U-NII 2: Banda media, para el uso en interiores y exteriores
- U-NII 3: Banda superior, diseñada para el uso externo exclusivamente.

Cada país tiene un reglamento especial para el uso de estas bandas, en el caso particular de Estados Unidos y los países que se rigen por la FCC, la distribución de los canales queda de la siguiente manera:

BANDA (GHz)	Número de canal	Frecuencias centrales por canal (MHz)
U-NII 1 (banda inferior) (5.15 – 5.25)	36	5180
	40	5200
	44	5220
	48	5240
U-NII 2 (banda media) (5.25 – 5.35)	52	5260
	56	5280
	60	5300
	64	5320
U-NII 3 (banda superior) (5.275 – 5.825)	149	5745
	153	5765
	157	5785
	161	5805

Tabla II.1. Distribución de canales para las bandas U-NII 1, U-NII 2 y U-NII 3.

La banda baja y media proporcionan entre ambas un ancho de banda total de 200MHz repartido en 8 canales (son los que se utilizan en México). Y la banda superior acomoda cuatro canales en un ancho de banda de 100MHz.

Para Europa se ocupan 19 canales, para Japón 4 canales, para Estados Unidos y Canadá 12 canales y para México solo se utilizan 8 canales.

La potencia máxima de transmisión de acuerdo con el estándar es la siguiente:

BANDA (GHz)	Máxima potencia de salida con una antena de 6dBi (mW)
U-NII 1 (banda inferior) (5.15 – 5.25)	40mW (2.5mW/MHz)
U-NII 2 (banda media) (5.25 – 5.35)	200 (12.5mW/MHz)
U-NII 3 (banda superior) (5.275 – 5.825)	800 (50mW/MHz)

Tabla II.2 Potencia máxima de transmisión para 802.11a

La banda inferior de U-NII 1 prohíbe el uso de cualquier antena externa, todo debe de estar integrado dentro del equipo inalámbrico de fábrica. De tener alguna pequeña antena externa debe de estar soldada al equipo y no podrá ser desmontable.

La sensibilidad es el valor de potencia mínimo que un receptor puede escuchar. 802.11a requiere una señal con mayor potencia que otros estándares, esto tiene como resultado una disminución en la velocidad y la distancia a la que se puede encontrar el dispositivo inalámbrico del AP. De acuerdo con el estándar¹⁶

Velocidad (Mbps)	Sensibilidad mínima (dBm)
6 Mbps	-82
9 Mbps	-81
12 Mbps	-79
18 Mbps	-77
24 Mbps	-74
36 Mbps	-70
48 Mbps	-66
54 Mbps	-65

Tabla II.3 Sensibilidad mínima de recepción para las distintas velocidades de 802.11a

802.11a utiliza el método de espectro extendido OFDM (Orthogonal Frequency-Division Multiplexing) Multiplexión por división ortogonal de Frecuencia, para transmitir la información y así poder proporcionar velocidades de datos altas.

Las velocidades de datos que se pueden alcanzar son 6, 9, 12, 18, 24, 36, 48 y 54Mbps. De acuerdo con el estándar existen algunas velocidades que son obligatorias y otras opcionales que el fabricante de un equipo puede o no proporcionar. Las velocidades obligatorias son 6, 12 y 24Mbps.

¹⁶ IEEE, Std 802.11 a-1999, 31

Para poder alcanzar estas velocidades es necesario aprovechar las características de OFDM y juntarlo con órdenes de modulación más altos (que los que se usan en 802.11b)

La siguiente tabla muestra los diferentes tipos de modulación empleados para alcanzar dichas velocidades.¹⁷

Velocidad de la capa física	Modulación	Velocidad de codificación	Número de bits codificados
6Mbps	BPSK	1/2	1
9Mbps	BPSK	3/4	1
12Mbps	QPSK	1/2	2
18Mbps	QPSK	3/4	2
24Mbps	16QAM	1/2	4
36Mbps	16QAM	3/4	4
48Mbps	64QAM	2/3	6
54Mbps	64QAM	3/4	6

Tabla II.4 Tipos de modulación para 802.11a

802.11a emplea la Modulación de fase por desplazamiento binario BPSK (Binary Phase Shift Keying) para alcanzar las velocidades de 6 o 9Mbps, y la Modulación de Fase por desplazamiento de cuadratura QPSK (Quadrature Phase Shift Keying) para las velocidades de 12 o 18Mbps.

Para las velocidades de datos más altas usa la Modulación de amplitud de cuadratura QAM (Quadrature Amplitud Modulation).

QAM al igual que PSK expresan su codificación en términos de bits de datos por símbolo, 16QAM, usado en velocidades de 24 y 36Mbps codifica 4 bits de datos usando 16 símbolos por subcanal 64QAM, usado en las velocidades de 48 y 54Mbps utiliza 64 símbolos para codificar 16 bits por subcanal.

“Algunos fabricantes de dispositivos ofrecen una opción TURBO que proporciona velocidades de datos de 72Mbps o incluso 108Mbps. Estas velocidades se alcanzan mediante un proceso de vinculación de canales, esto es que dos canales son multiplexados, cada uno proporcionará una velocidad de datos de 36Mbps, lo que da como resultado 72Mbps”¹⁸. Para obtener los 108Mbps se vinculan 2 canales que ofrecen la velocidad máxima de 54Mbps.

Aunque esto suene muy prometedor, se tienen varias desventajas, ya que al usar el modo TURBO se sacrifican canales y se tendrían que comprar todos los productos de un mismo fabricante (AP y tarjetas de cliente), pues estas velocidades no están ratificadas por el estándar, y aunque las velocidades ofrecidas son altas, la capacidad real de salida de 108Mbps no es más alta que la capacidad de salida de 54Mbps.

¹⁷ IEEE. *op. cit.* 9

¹⁸ REID. *Manual de redes inalámbricas. 802.11 (WiFi)*. 128

Algunas de las principales características de los equipos 802.11 a son:

- Entre más cercanos se encuentren los equipos de comunicación, mas fuerte será la señal y más alta será la velocidad de transmisión.
- Los equipos tienden siempre a comunicarse a la velocidad más alta, pero si durante la transmisión se llevan a cabo muchos errores y retransmisiones los equipos descenderán a la siguiente velocidad de datos más alta, repitiendo este proceso hasta que la señal sea lo más clara y fuerte posible.
- Aunque 802.11 a tiene un rango mucho menor que 802.11b y 802.11g (es decir cubre áreas de menor tamaño) "es sólido en términos de interferencias y distorsión de trayectorias múltiples"¹⁹ por lo que es muy bueno para su uso en interiores.

b) 802.11b

802.11b es también un suplemento del estándar 802.11; fué ratificado el mismo día que el estándar 802.11a en septiembre de 1999, con el fin de presentar mejoras y cambios al estándar 802.11. Su nombre completo es. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 2.4GHz Band" (Especificaciones de nivel de control de acceso al medio (MAC) y del nivel fisico (PHY) de las LAN inalámbricas: Nivel fisico de alta velocidad en la Banda de 2.4GHz).

El ancho de banda total de la porción del espectro de frecuencias que utiliza 802.11b va de 2.401GHz a 2.4835GHz y es de 83.5MHz.

La distribución de los canales que se puede utilizar en esta banda varía de acuerdo a las regulaciones de cada país. Para la FCC (Estados unidos y los países regulados por ese domino) son 11 los canales que están disponibles; para Europa son 13 canales y para Japón son 14 canales.

1	2.412	✓
2	2.417	✓
3	2.422	✓
4	2.427	✓
5	2.432	✓
6	2.437	✓
7	2.442	✓
8	2.447	✓
9	2.452	✓
10	2.457	✓
11	2.462	✓
12	2.467	x
13	2.472	x
14	2.477	x

Tabla II.5 Distribución de frecuencias para los canales en la banda de 2.4GHz

Debido a que cada canal tiene un ancho de banda de 22MHz, solo hay 3 canales que no se traslapan, estos canales son 1, 6 y 11, con 3 MHz de separación entre canal y canal.

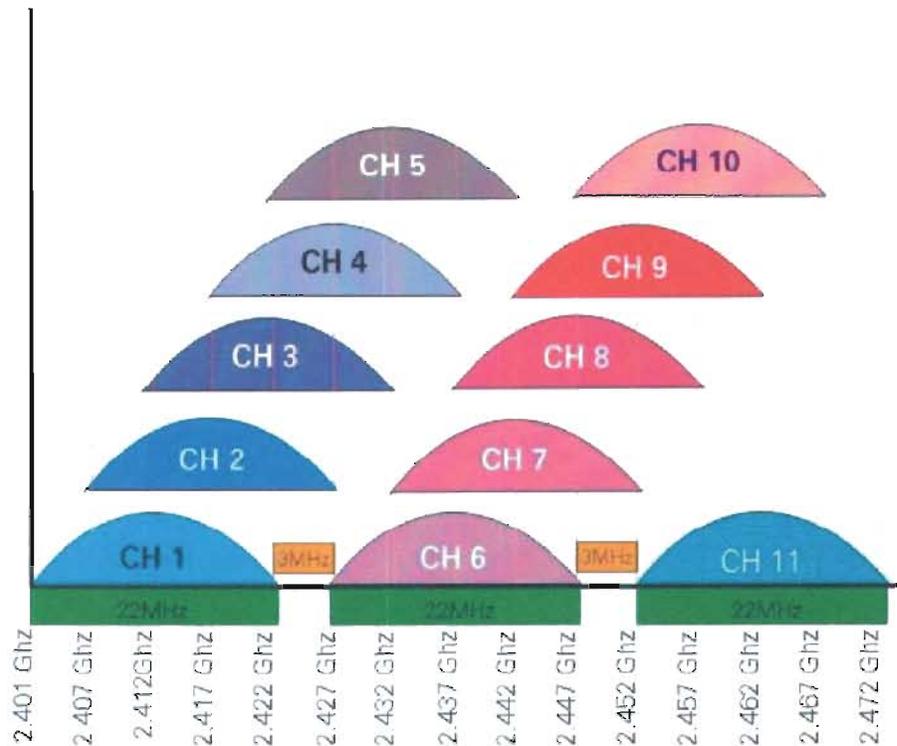


Figura II.19 Canales sin traslape para la banda de 2.4GHz

Para una red que contiene un buen número de APs en una misma zona es importante arreglar los canales de manera que no se traslapen, pues si quedan 2 canales empalmados con la misma frecuencia los datos se perderán a causa de la interferencia.

La principal contribución del estándar 802.11b fue la implementación de 2 nuevas velocidades de datos 5.5 y 11Mbps, además de la estandarización de la capa física para utilizar solamente DSSS, ya que FHSS no soporta altas velocidades de datos sin violar las regulaciones de la FCC

El estándar también presenta la implementación de DSSS de alta velocidad HR/DSSS (High Rate / Direct Sequence Spread Spectrum), La principal diferencia entre DSSS y HR/DSSS es la técnica de modulación de la frecuencia, pues en HR hay una doble modulación de los datos para poder alcanzar una transmisión a 5.5 y 11Mbps.

Las técnicas de modulación que emplea 802.11b son BPSK (Binary Phase Shift Keying), QPSK (Quadrature Phase Shift Keying), CCK (Complementary Code Keying), y como una técnica de modulación opcional PBCC (Packet Binary Convolutional Code).

Velocidades de datos	Modulación	Numero de bits codificados
1	BPSK	2
2	QPSK	4
5.5	CCK / QPSK	4
11	CCK	8

Tabla II.6 Técnicas de modulación para 802.11b

Soporta las velocidades ofrecidas por 802.11, 1 y 2Mbps (para ser compatible) y agrega dos tipos nuevos de modulación CCK (Manipulador de código complementario) y PBCC (Codificación compleja de paquetes binarios). Para las velocidades de 1 y 2Mbps utiliza la modulación BPSK y QPSK respectivamente, para alcanzar la velocidad de 5.5Mbps puede utilizar tanto CCK como QPSK. CCK utiliza un esquema de modulación de portadora única.

La potencia máxima de transmisión de los dispositivos 802.11b es de 100mW.

Este estándar fue el que obtuvo un mayor apoyo por parte de los fabricantes. Es el más popular de los estándares 802.11 debido a que el costo de sus equipos es mucho más bajo que 802.11a esto sumado a los beneficios que se tienen al implementarlo, pues se puede tener una mayor área de cobertura por cada equipo ya que se permiten utilizar, conectores y antenas externas para extender el alcance de la señal.

Los dispositivos 802.11b tienen la capacidad de seleccionar dinámicamente la velocidad, esto permite ajustar automáticamente las velocidades de datos para compensar interferencias o problemas de rango en un determinado canal.

61

TRAMA 802.11b

Existen tres tipos básicos de tramas: control, datos y administración. Las tramas de Control son utilizadas para regular el acceso al medio de la red y reconocer las tramas de datos transmitidas. Las tramas de administración se utilizan para intercambiar información de administración de la red, tales como la asociación y la autenticación. Las tramas de datos son utilizadas para transmitir datos de los niveles superiores entre estaciones. [Craig, 2002]

El formato de trama para 802.11b queda compuesto de la siguiente manera:

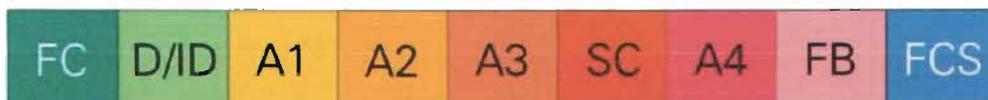


Figura II.20 Formato de trama para 802.11b

FC= (Frame control) Control de trama

D/ID= Duración / ID

A1 = (Address 1) Dirección 1

A2 = (Address 2) Dirección 2

A3 = (Address 3) Dirección 3

SC = (Secuence Control) Secuencia de control

A4 = (Address 4) Dirección 4

FB = (Frame Body) Cuerpo de la trama

FCS (Frame Check Sequence) Secuencia de verificación de trama.

- **FC (2 bytes)** – Es el primer campo en la trama, y contiene 10 subcampos que son:
 - Versión del protocolo (2bits) – el valor estándar es cero
 - Tipo (2 bits) – especifica el tipo de trama del que se trata sus valores son:
 - 00 si la trama es de administración
 - 01 si la trama es de control

10 si la trama es de datos

Además de que utiliza 4 bits más para identificar la función de la trama.

- A el Sistema de Distribución DS (1 bit) – se establece en 1 cuando una estación asociada con un AP envía una trama destinada para la red detrás del AP
- De el Sistema de Distribución DS (1 bit) el valor del bit se establece en 1 cuando la trama se recibió en el DS
- Más fragmentos (1bit) – se pone en 1 cuando el paquete contiene un fragmento de una trama y hay mas tramas por transmitir.
- Reintento (1 bit) – se pone en 1 en todas las tramas de datos o de administración que son retransmisiones de tramas anteriores. Cuando es la primera vez que se envía la trama se pone en 0.
- Administración de energía (1bit) – se utiliza para indicar el modo de administración de energía de la estación. Un valor de 1 indica que la estación esta en modo ahorro de energía y 0 en modo activo.
- Mas datos (1 bit) – usado para decirle a una estación asociada en modo ahorro de energía que una o más tramas están almacenadas para el en el AP (valor 1).
- WEP (1bit) – Si el valor es de 1 el cuerpo de la trama contiene datos encriptados en WEP.
- Orden (1 bit) – Si la trama contiene datos usando la clase de servicio "en estricto orden" el valor del bit será 1.

• **D/ID (16 bits)** – Es el siguiente campo de la trama, que se utiliza para contener la identidad de asociación de una estación con un AP.

- **Campos de dirección** – A1, A2, A3 y A4 (cada una mide 6 bytes).

Existen varios tipos de direcciones:

BSSI (Basic Service Set Identifier) contiene la dirección MAC del AP.

DA (Destination Address) contiene la dirección MAC del destino final.

SA (Source Address) contiene la dirección MAC de la estación que generó la información.

RA (Receiver Address) contiene la dirección MAC del receptor inmediato de la información.

TA (Transmitter Address) contiene la dirección MAC de la estación que transmitió la trama.

• **SC (2 bytes)** – Campos utilizados para asociar los fragmentos de una secuencia en particular y reensamblarlos en orden correcto en el destino.

- **FB** – puede medir de 0 a 2312 bytes y contiene los datos encapsulados (información a transmitir).
- **FCS (4 bytes)** – Se utiliza para el control de errores.

c) 802.11g

Este estándar se realizó con la finalidad de mejorar las velocidades de datos alcanzadas en la banda de 2.4GHz. En noviembre del 2001, el IEEE aprobó el primer borrador del estándar, pero fue hasta 2003 cuando el estándar fue ratificado con el nombre de "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 4: Further Higher Data Rate extensión in the 2.4GHz Band" (Especificaciones de nivel de control de acceso al medio (MAC) y del nivel físico (PHY) de las LAN inalámbricas: Enmienda 4: Extensión Posterior de alta velocidad en la banda de 2.4GHz).

Combina lo mejor de las tecnologías de los estándares 802.11a y b; de 802.11a utiliza la técnica de propagación OFDM (Orthogonal Frequency Division Multiplexing) y de 802.11b los índices de modulación CCK y PBCC; esto lo hace compatible con el estándar 802.11b, lo que le dará mayor popularidad, pues los usuarios de 802.11b y g podrán convivir en una misma red.

El estándar 802.11g puede alcanzar la velocidad de 54Mbps, superando la velocidad obtenida por 802.11b e igualando la velocidad del estándar a, pero en una banda diferente.

Ya que 802.11g opera en la banda de 2.4GHz tiene permitido el uso de aditamentos externos (antenas y conectores) por lo que la señal se puede propagar a una mayor distancia que 802.11a. La desventaja sigue siendo el limitado número de canales sin traslape con los que cuenta esta banda.

El estándar estableció ciertos parámetros obligatorios que todos los fabricantes deben cubrir, estos parámetros son:

- Soportar OFDM
- Mantener compatibilidad con 802.11b
- Manejar las siguientes velocidades de datos: 1, 2, 5.5, 11, 6, 12 y 24Mbps.

Entre los parámetros opcionales que maneja el estándar están:

- Las velocidades de datos de: 9, 18, 22, 33, 36, 48 y 54Mbps
- El uso de la modulación PBCC (Packet Binary Convolutional Code)

Se agregaron nuevos tipos de modulación para poder alcanzar las altas velocidades de transmisión: ERPHY (Extended Rate PHY) Velocidad extendida PHY y DSS-OFDM

Este nuevo tipo de modulación ha sido diseñado para coexistir con los ya existentes en 802.11b, con el fin de que las estaciones no tengan problema al conectarse. Cuando una estación 802.11b se conecte a un AP 802.11g, la máxima velocidad de transmisión será de 11Mbps; y si alguna estación 802.11g se conecta con un AP 802.11b, la velocidad máxima será 11Mbps.

A continuación se enlistan los diferentes tipos de modulación que hay y las velocidades de datos que originan:

MODULACIÓN	VELOCIDADES DE DATOS
ERP-DSS	1, 2Mbps
ERP-CCK	5.5 y 11Mbps
ERP-OFDM	6, 9, 12, 18, 24, 36, 48 y 54Mbps
ERP-PBCC	5.5, 11, 22 y 33Mbps
DSS-OFDM	6, 9, 12, 18, 24, 36, 48 y 54 Mbps

El hecho de que 802.11g sea compatible con 802.11b hará este estándar tenga mayor popularidad y despliegue en el mercado, pues los usuarios actuales de 802.11b podrán migrar sus redes de 11Mbps a 54Mbps paulatinamente sin tener que cambiar todos los equipos de una sola vez, pues podrán atender tanto a clientes que ya tengan tarjetas g como a clientes con tarjetas b.

■ II.3.2 [Bluetooth]

Bluetooth es un estándar de comunicaciones inalámbricas, cuyo objetivo original es reemplazar los cables conectados de un dispositivo a otro mediante el uso de un radio de bajo consumo de energía colocado en un chip.

En la práctica Bluetooth no solo se ocupa como reemplazo del cable sino para realizar comunicaciones inalámbricas de corto alcance entre equipos tales como computadoras portátiles, PDA's, teléfonos celulares y sus periféricos.

Fue creado en 1994 por L.M. Ericsson Company en Suiza, y poco a poco fue despertando interés en otros fabricantes, así que para el año de 1998 se fundó el "Bluetooth Special Interest Group (SIG) Inc." conformado por Ericsson, IBM, Intel, Nokia y Toshiba. Este grupo se encargó de "desarrollar una especificación para tener conectividad inalámbrica, de corto alcance y siempre activa basada en la tecnología Bluetooth de Ericsson. Esta especificación fue liberada públicamente en 1999."²⁰

Actualmente hay más de 2000 compañías registradas en Bluetooth SIG, entre las cuales se encuentran: 3COM, Microsoft, Motorola y Lucent.

Bluetooth fue llamada así por el Rey Danés del siglo X Harald Blaataand "Bluetooth II". Este rey consiguió unificar Dinamarca y llevar la cristiandad a Escandinavia.

Bluetooth es una tecnología diseñada para ser de bajo costo, tamaño compacto, consumir poca potencia para conservar la vida de la batería de PDA's, teléfonos celulares etc. Y se adapta a trabajar en ambientes ruidosos en la frecuencia. Puede conectar dispositivos desde 10cm hasta 10mts, si se incrementa la potencia puede alcanzar hasta los 100mts (pero en algunos países no esta permitido incrementar demasiado la potencia de un dispositivo Bluetooth). Permite tres tipos de potencia:

Clase 1 = 100mW (20dBm) puede alcanzar un área de cobertura hasta 100m.

Clase 2 = 2.5mW (4dBm)

Clase 3 = 1mW (0dbm) alcanza un área de cobertura máxima de 10m

Para que los dispositivos puedan conectarse es necesario que estén por mínimo a 10cm de distancia entre un radio y otro.

No compite directamente con Wi-Fi (802.11b) ya que Bluetooth permite interconectar dispositivos próximos dentro de un rango de pocos metros, forma una PAN (Personal Area Network). La principal función de una PAN es comunicar y sincronizar información, pero no esta diseñada para soportar grandes cargas de tráfico.

Los dispositivos Bluetooth se comunican por medio de piconets (picored), que es un grupo de dispositivos conectados entre sí. Cada piconet esta formada por un "maestro" (el primero que inicia la conexión) y por varios "esclavos"

El maestro pone la secuencia de salto de frecuencia, controla el medio determinando cuando los equipos pueden transmitir y el ancho de banda del que dispondrá cada esclavo. El esclavo se sincroniza al maestro, es decir, adopta la misma secuencia de saltos.

²⁰ Walter. *Wireless LAN end to end*. 44

Las conexiones entre los dispositivos pueden ser de solo datos, solo voz o voz y datos.

- **Solo datos:** un maestro solo puede manejar comunicaciones de datos hasta con siete esclavos. Los equipos esclavos (adicionales) que deseen agregarse a la piconet, pueden dejarse en espera. Este tipo de conexión es asíncrona
- **Solo voz:** un maestro para soportar las conversaciones de voz solo puede manejar un número máximo de 3 esclavos. Estas piconets usan conexiones síncronas.
- **Voz y datos:** este tipo de conexión solo puede existir entre dos dispositivos a la vez. Se llama conexión isócrona, debido a que la porción de voz debe entregarse siempre en modo síncrono y los datos pueden tardar un poco en entregarse en conexión asíncrona.

Un dispositivo puede pertenecer a varias piconets en cualquier momento y funcionar tanto como esclavo o como maestro. Cuando varias piconets tienen uno o más dispositivos en común, esta estructura recibe el nombre de scatternet (red dispersa)

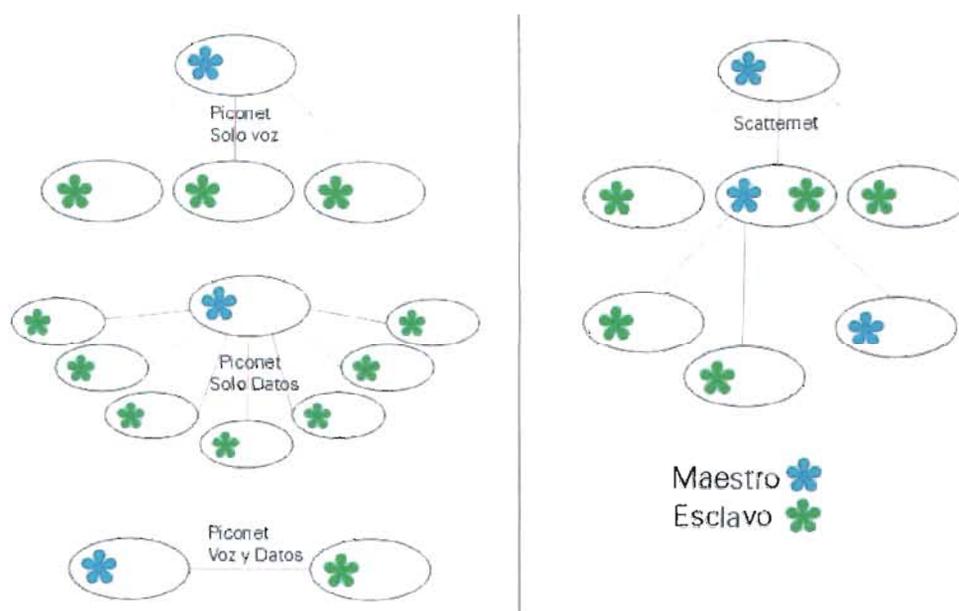


Figura II.21 Tipos de conexiones para Bluetooth

Tipos de Enlaces.

En Bluetooth existen dos tipos de enlace:

- SCO (Synchronous Connection Oriented)
- ACL (Asynchronous Connectionless)

El enlace SCO se usa para transmitir voz, un maestro establece un enlace punto a punto con un solo esclavo, esta conexión reserva ranuras de tiempo para garantizar la transmisión sin demoras (pues los paquetes SCO nunca se retransmiten). Este enlace provee 64Kbps en la transmisión de voz en cada dirección.

El enlace ACL se emplea para transmitir datos. Soporta transmisiones punto a multipunto. La máxima velocidad para el servicio asimétrico es de 723.2Kbps en una dirección y 57.6Kbps en otra dirección. También puede soportar un enlace simétrico que funciona a 433.9Kbps en ambas direcciones.

Modelo de Referencia Bluetooth.



Bluetooth tiene un modelo de referencia diferente al de 802.11b [Walter, 2002]

Figura II.22 Modelo de referencia de Bluetooth

Capa de Radiofrecuencia (RF)

Esta capa es la que se encarga de definir las características necesarias para poder realizar un enlace de radio (interfaz), como serían la modulación, la técnica de propagación, etc.

“Usa un esquema de modulación llamado GPBFSK (Gaussian Prefiltered Binary Frequency Shift Keying)”²¹ el cual genera una derivación (desviación) positiva en la frecuencia de la frecuencia portadora cuando se transmite un 1 y una derivación negativa cuando se transmite un 0. Este tipo de modulación emplea un filtro Gaussiano para aislar las transiciones de frecuencia, esto reduce los lóbulos laterales espectrales emitidos, permitiendo mayor eficiencia espectral y menor interferencia intersímbolo.

Bluetooth opera en la banda de 2.4GHz, y utiliza espectro extendido de salto de frecuencia FHSS (Frequency Hopping Spread Spectrum) para transmitir los datos. Salta 1600 veces por segundo entre 79 canales para EU y Europa; y 23 canales para Japón todos de 1MHz. Cada señalización de datos se da en 1Msímbolo por segundo; para obtener el máximo de ancho de banda de canal disponible.

²¹ Ibid. 50

Debido a que la banda ISM (2.4GHz) está saturada por otros dispositivos Bluetooth emplea varias técnicas para ser menos susceptible a interferencias, estas son:

- Salto de frecuencia
- Control de potencia adaptiva
- Paquetes de datos cortos.

La cantidad tan alta de saltos lo hace menos susceptible a interferencias. Se transmiten solo 625µs en cada canal antes de saltar al siguiente.

En caso de que existieran muchas picoredes juntas en un área pequeña, cada piconet establece su propio patrón de saltos para así evitar interferencias entre ellos. Si 2 picoredes se encuentran en la misma frecuencia después del siguiente salto de frecuencia, los datos que pudieron haberse perdido, se retransmitirán en otra frecuencia diferente a la que se transmitieron.

Al saltar de un canal a otro, "los equipos Bluetooth usan la totalidad de la banda ISM disponible."²²

Capa Banda base (Baseband)

Esta capa es la responsable de la codificación y decodificación de canales, de brindar corrección de errores y seleccionar el patrón de salto. También maneja los enlaces SCO y ACL, los paquetes, la autenticación de los dispositivos.

Bluetooth utiliza 5 canales lógicos para mandar diferentes tipos de datos, los cuales son:

- LC (Link Control Channel)
- LM (Link Manager Channel) Usado en la capa de enlace
- UA } Canales que llevan la información para enlaces Asíncronos, Isócronos y Síncronos
- UI }
- US }

Capa Link Manager Protocol (LMP) Protocolo administrador del enlace.

LMP maneja el proceso de establecimiento de la conexión. Se encarga de funciones de seguridad (encriptación), intercambio de información (como son: control de reloj, versión, características que soporta el dispositivo, etc.)

Capa Host Controller Interface (HCI) Controlador de interfaz del host

Esta subcapa es adicional, ya que aquellos dispositivos que implementan todas las capas tanto en hardware como en software no ocupan esta subcapa. Su función es servir de traductor entre el hardware y el software, maneja comunicaciones entre un host separado y un módulo Bluetooth.

El HCI conduce los datos en el host (PC) toma los datos de L2CAP (desarrollados en el software) les da formato y los envía sobre el bus físico de la PC (tarjeta PCI o USB) al HCI en el hardware (dispositivo) Bluetooth. Entonces HCI pasa los datos a la capa Baseband.

²² VARGAS, *Tendencias inalámbricas en México WPAN WLAN WWAN WMAN*. 42

Capa L2CAP (Logical Link Control and Adaptation Protocol)

Esta capa desempeña las siguientes funciones:

- Interactúa con las aplicaciones del software
- Reduce el tamaño de los paquetes enviados por las aplicaciones al tamaño de los paquetes aceptados por la capa Baseband. Los datos de un paquete pueden ser de hasta 2745 bits de longitud.
- Proporciona el uso simultáneo de aplicaciones, de un enlace entre 2 dispositivos.
- Habilita aplicaciones que demanden QoS

Capa de Aplicación

Es la capa más alta del modelo de referencia, usada por el software de aplicación para operar a través de la conexión de una piconet y tal vez a través de una red, como TCP/IP, PPP, FTP, o correo electrónico.

Está conformada por las siguientes subcapas:

- RFCOMM (Wireless Emulation of RS-232) proporciona una interfaz serial RS232
- SDP (Service Discovery Protocol) permite a los equipos Bluetooth descubrir que servicios soporta otro equipo Bluetooth.

■ II.3.3 [Otros estándares]

a) HomeRF

En marzo de 1998 el Home Radio Frequency Working Group (HomeRF WG) lanzó el estándar HomeRF. Este estándar está basado en el teléfono inalámbrico digital mejorado (Digital Enhanced Cordless Telephone, DECT), establecido por Siemens.

HomeRF WG tiene 6 compañías promotoras principales que son: Proxim, Motorola, Siemens, Compaq, Intel y Nacional Semiconductor, y al menos 100 compañías miembro.

Debido a que la primera versión de HomeRF ofrecía velocidades entre 800Kbps y 1.6Mbps se hizo una revisión al estándar que dió origen a HomeRF 2.0 basado en la especificación de un protocolo denominado SWAP (Shared Wireless Access Protocol).

El objetivo de HomeRF son las redes caseras para permitir que aparatos electrónicos, teléfonos inalámbricos, computadoras, impresoras se comuniquen entre sí, por lo cual no es una solución para redes empresariales.

HomeRF 2.0 puede brindar aplicaciones y servicios de banda ancha como serían:

- Acceso a Internet por todo el hogar con dispositivos portátiles
- Distribuir audio con calidad CD a bocinas inalámbricas
- Compartir una sola conexión ISP entre varias PCs u otros dispositivos.

Debido a que HomeRF soporta DECT puede transportar tráfico de voz con calidad de una llamada telefónica normal. Este estándar se ha desarrollado principalmente en Europa pues DECT está bien establecido y HomeRF al ser compatible con DECT no sufre interferencias, es difícil que tenga futuro en EU pues no es compatible con 802.11b. De acuerdo con la especificación 2.01, la red HomeRF puede operar como una red ad-hoc de solo nodos de datos o como una red controlada por un punto de conexión para comunicaciones de voz, audio o video. [HomeRF WG, 2001]

Los dispositivos que puede soportar una red HomeRF son los siguientes:

- Un punto de conexión CP (Connection Point), cuya función es interconectar una PC con la red pública y otros dispositivos compatibles con HomeRF (tiene la función de un gateway y es parecido a un AP)
- Dispositivos de datos síncronos (A-nodes), proporciona servicios de datos como las tarjetas de interfaz de red inalámbricas (NIC)
- Dispositivos de datos isócronos (I-nodes), proporciona servicios de voz interactiva como los microteléfonos inalámbricos.
- Dispositivos combinados asíncronos (AI-nodes), proveen servicios tanto asíncronos como isócronos
- Dispositivos de flujo "streaming" (S-nodes), estos dispositivos soportan flujos de información en tiempo real como audio y video.
- Dispositivos combinados streaming/isócronos (SI-nodes), proveen servicios de datos de prioridad asíncrona, es decir isócrona y asíncrona.

Los dispositivos HomeRF "incluyen un conjunto impresionante de capacidades de voz, como el identificador de llamadas, llamada en espera e intercomunicación dentro del hogar"²³ Para la seguridad, utiliza el algoritmo llamado "Blowfish", que consiste en claves de hasta 448bits (similar al GSM A5). Este algoritmo fue creado por Bruce Schneier, y es un algoritmo rápido ya que ocupa una menor capacidad de memoria, es simple y seguro. Puesto que las claves son dinámicas. Utiliza el algoritmo LZRW3-A para la compresión de datos.

Modelo de referencia de HomeRF

HomeRF utiliza referencias existentes en la capa de red, pero ha modificado las tecnologías para la capa física y de enlace de datos (MAC). De acuerdo con Eamon Myers, el modelo es el siguiente:



Figura II.23 Modelo de referencia de Home RF.

²³REID. op. cit. 35

Capa Física de HomeRF

Trabaja en la frecuencia de 2.4GHz, y utiliza una variación del espectro extendido con salto de frecuencia (FHSS), dando 50 saltos por segundo.

Tiene un alcance de 50m aproximadamente. Y para la modulación utiliza la manipulación por frecuencia (Frequency Shift Keying) 2FSK y 4FSK que pueden ser tanto LR (low-rate) de baja velocidad, como de alta velocidad HR (high-rate), quedando en total cuatro tipos diferentes de modulación: LR-2FSK, LR-4FSK, HR-2FSK y HR-4FSK.

Capa MAC

La capa MAC se encarga de las siguientes funciones:

- Manejo de nodos isócronos, y asíncronos
- Puede sostener cuatro conversaciones de voz de alta calidad (soporta DECT)
- Soporta QoS para asegurar un ancho de banda adecuado para cada aplicación
- Se encarga de la seguridad de los datos
- Utiliza tanto TDMA (Time Division Multiple Access) para proveer soporte a servicios isócronos de datos y flujo de video en tiempo real, como CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) para servicios asíncronos de datos de alta velocidad.

Las cuatro clases de servicios de datos que proporciona la capa MAC son las siguientes:

- **Servicio Asíncrono (sin conexión):** usado para transmitir paquetes de datos. Su prioridad es la más baja.
- **Servicio con Prioridad Asíncrona (orientado a sesión):** usado para transportar flujos como el audio y el video. Para poder prestar este servicio se requiere tener un punto de conexión (CP). Tiene el tercer lugar en prioridad.
- **Servicio Isócrono (orientado a la conexión):** usado principalmente para transportar voz interactiva, este servicio también necesita un CP. Tiene la prioridad más alta entre los servicios de datos.
- **Servicio Isócrono Broadcast (difusión sin conexión) ICBS (Isochronous Connectionless Broadcast Service),** usado para transportar mensajes tal como "paging" de I-nodes, identificador de llamadas (Caller-ID). Es el segundo en importancia de los servicios de datos.

b) HiperLAN

HiperLAN/1 e HiperLAN/2 se desarrollaron en Europa por el grupo Broadband Radio Access Network (BRAN) junto con el Instituto Europeo de estándares de Telecomunicaciones ETSI (European Telecommunications Standards Institute). HiperLAN/1 alcanza velocidades de hasta 24Mbps, debido a que HiperLAN/1 no ofrecía tantos servicios no tuvo gran éxito, así que ETSI desarrollo la segunda versión de este estándar HiperLAN/2 provee una velocidad máxima de 54Mbps.

Los principales promotores de este estándar son: Nokia, Ericsson, Motorola, Panasonic y Sony. HiperLAN/2 es una red de radio de área local de altas prestaciones, cuya intención es facilitar la comunicación inalámbrica multimedia (datos, voz y video) entre terminales móviles y redes de banda

ancha usando el espectro de 5GHz de frecuencia. La principal ventaja de HiperLAN/2 es que tiene una alta capacidad de salida, otras de sus características son el soporte de QoS (Quality of Service), provee movilidad, seguridad y es un servicio orientado a la conexión.

La capa de convergencia de HiperLAN está diseñada para interactuar con ATM, PPP, Ethernet y UMTS entre otros. Una red HiperLAN/2 esta conformada principalmente por: terminales móviles MT (Mobile Terminals) y por puntos de acceso AP (Access Points). Las terminales móviles pueden desplazarse a una velocidad de hasta 10m/s sin perder la conexión. HiperLAN/2 está basado en la topología de una red celular combinada con la capacidad de una red ad-hoc. Soporta dos modos básicos de operación:

- **Modo centralizado CM (Centralized Mode)** se usa en la topología de red celular, donde cada célula de radio es controlada por un AP para cubrir cierta área geográfica, normalmente se requiere de varias células de radio para cubrir un área determinada. Su principal aplicación es para ambientes empresariales, tanto para interiores como
- **Modo directo DM (Direct Mode)** este modo usa la topología de red ad-hoc, típicamente se usa en ambientes del hogar donde una célula de radio cubre el área total de servicio.

En ambos casos, el AP controla el acceso al medio así como la asignación de los recursos de radio.

Debido a que la calidad del enlace de radio depende de las interferencias que existan en el ambiente, HiperLAN/2 tiene la capacidad de compartir el espectro disponible evitando el uso de frecuencias interferidas. El sistema automáticamente selecciona frecuencias para cada AP, mediante el método de selección dinámica de frecuencia DFS (Dynamic Frequency Selection); esta selección de frecuencias se sustenta en la medición de las interferencias, que realizan tanto el AP como las MT (estaciones móviles).

Modelo de referencia de HiperLAN/2

El modelo de HiperLAN/2 esta dividido en dos partes, la parte del "Plano de Control", que incluye funciones para el control del establecimiento, liberación y supervisión de la conexión; y la parte del "Plano del Usuario", que realiza funciones para la transmisión del tráfico sobre conexiones ya establecidas. De acuerdo con el estándar, el modelo esta conformado por tres capas básicas:



Figura II.24 Modelo de referencia de HiperLAN/2

Capa de Convergencia

Tiene dos funciones principales, adaptar el servicio solicitado por las capas superiores al servicio ofrecido por el DLC y convertir los paquetes de las capas superiores en paquetes con longitud fija para ser usados dentro del DLC.

Existen dos tipos de capa de convergencia:

- Capa de convergencia basada en paquetes: está definida para manejar capas superiores con paquetes de longitud variable, por ejemplo Ethernet.
- Capa de convergencia basada en celdas: se usa para manejar paquetes de longitud fija provenientes de las capas superiores, como serían los paquetes de las redes ATM.

Capa de Control de Enlace de Datos (DLC)

“La capa DLC (Data Link Control) constituye un enlace lógico entre el AP y la MT, e incluye funciones tanto para acceder al medio y transmitir (Plano del usuario) como para manejar la conexión (Plano de control).”²⁴

Esta capa esta formada por: la subcapa de control del enlace de radio RLC (Radio Link Control), un protocolo de control de errores EC (Error Control) y un protocolo de control de acceso al medio MAC (Medium Access Control).

- Control de enlace de radio (RLC)

Esta subcapa tiene tres funciones principales:

1. **Control de asociación:** usado para el manejo de claves, la autenticación, asociación/desasociación, y encriptación.
2. **Control de recursos de radio (RRC, Radio Resource Control):** se encarga de la selección dinámica de frecuencia, economización y control de la potencia y manejo de las terminales móviles (encendidas/ausentes).
3. **Control de conexión de usuarios:** establece y libera las conexiones de usuario multicast y broadcast.

RLC se ocupa para intercambiar datos en el “plano de control” entre un AP y una estación móvil.

- Control de errores (EC)

El control de errores define diferentes modos de operación para soportar distintos tipos de servicios:

1. **Modo de reconocimiento (acknowledgment).** “Provee transmisiones confiables y utiliza la retransmisión para mejorar la calidad del enlace. El mecanismo utilizado para incrementar la credibilidad sobre el enlace de radio es la repetición selectiva (SR, Selective Repeat) con solicitud automática de repetición (AQR, Automatic Repeat Request).

²⁴ JOHNSSON. *HiperLAN/2 - The Broadband Radio Transmission Technology Operating in the 5GHz Frequency*. 7

2. **Modo de repetición (repetition mode)**. Provee una transmisión bastante confiable repitiendo las unidades de datos de paquetes (PDU) de los DLC portadores de datos. El transmisor puede retransmitir las PDUs arbitrariamente.

3. **Modo sin reconocimiento**. Provee una transmisión poco confiable de baja latencia. El transmisor enviara las PDUs incrementando una secuencia numérica, y el receptor deberá entregar todos los paquetes que hayan sido recibidos correctamente a la capa de convergencia”²⁵

Los datos unicast se pueden mandar usando tanto el modo de “reconocimiento” como el modo “sin reconocimiento”. Los servicios Broadcast son soportados tanto por el modo de “repetición” como por el modo “sin reconocimiento”, y los servicios multicast pueden ser enviados en el modo de “repetición” o pueden multiplexarse hacia transmisiones unicast ya existentes.

• **Control de acceso al medio (MAC)**

Se utiliza para acceder al medio, el control se centra en el AP, el cual informa a las terminales móviles cuando pueden transmitir sus datos y se adapta de acuerdo con las solicitudes de los recursos que cada estación móvil hace al AP.

La interfaz del aire esta basada de acuerdo con el estándar en una comunicación Duplex con División de Tiempo (TDD, Time Division Duplex) y el Acceso Múltiple por División de Tiempo (TDMA, Time Division Multiple Access). [HiperLAN/2 Global Forum, 1999]

Capa Fisica

Se utiliza OFDM (Orthogonal Frequency Division Multiplexing) multiplexión por división ortogonal de frecuencia para poder propagar la información. Existen diferentes modalidades de la capa fisica que varían de acuerdo a la velocidad de codificación y al esquema de modulación.

Los esquemas de modulación de subportadora soportados son BPSK, QPSK, y 16QAM; 64QAM puede ser usado como un modo opcional. El control de errores se lleva a cabo por un código que trabaja a velocidades de 1/2, 3/4 y 9/16.

Los 7 modos de la capa fisica son:

1	BPSK	1/2	6Mbps
2	BPSK	3/4	9Mbps
3	QPSK	1/2	12Mbps
4	QPSK	3/4	18Mbps
5	16QAM	9/16	27Mbps
6	16QAM	3/4	36Mbps
7	64QAM	3/4	54Mbps

Tabla II.7 Modos de la capa fisica para HiperLAN/2

²⁵ MALMGREN. *HiperLAN type 2. An emerging world wide WLAN standard*. 3

II. TECNOLOGÍAS INALÁMBRICAS

	802.11a	802.11b	802.11g	Bluetooth	Home RF	Hiper LAN / 2
Banda del espectro de Frecuencia en la que trabaja	5GHz	2.4GHz	2.4GHz	2.4GHz	2.4GHz	5GHz
Velocidad máxima de transmisión	54Mbps	11Mbps	54Mbps	1Mbps	10Mbps	54Mbps
Técnica de propagación	OFDM	FHSS / Normalmente DSSS	OFDM	FHSS	FHSS	Portadora simple con selección Dinámica de Frecuencia
Número de Saltos de Frecuencia	-	2.5 Saltos por segundo si utiliza FHSS	-	1600 saltos por segundo	50 saltos por segundo	-
Potencia máxima de transmisión permitida	40mW - Banda baja 200mW -Banda media 800mW - Banda alta	800 mW	800mW	Clase 1 = 100mW Clase 2 = 2.5mW Clase 3 = 1mW	100mW	200mW
Número máximo de dispositivos que puede soportar	512	de 192 hasta 250	128	Hasta 26 (8 piconets y hasta 10 piconets en un radio de 10m)	127	152
Seguridad	WEP 40,128 bits RCA, TKIP, 802.1x	WEP 40,128 bits RCA, TKIP, 802.1x	WEP 40,128 bits RCA, TKIP, 802.1x	Autenticación, Cifrado de 40 y 64 bits	Algoritmo Blowfish NWD/Cifrado	DES, 3DES
Rango	300m sin obstáculos	460m sin muros	460m sin muros	10m y si se incrementa la potencia hasta 100m	46.7m	30-150m
Alcance exterior al hogar	Si	Si	Si	No	No	Si
Método para acceder al medio	CSMA/CA	CSMA/CA	CSMA/CA CCA (Clear Channel Assessment)	DS-SSMA (Direct Sequence Spread Spectrum) FS-SSMA (Frequency Spread Spectrum) FDMA, TDMA	CSMA/CA, TDMA, SWAP	Central Resource Control TDMA/TDD
Velocidades a las que puede trabajar	6, 9, 12, 18, 24, 36, 48 y 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 y 54 Mbps	1Mbps	803Kbps 1.6, 5 y 10Mbps	6, 9, 12, 18, 27, 36, 48 y 54 Mbps
Número de canales	8 o 12 sin traslape (varía de acuerdo a las regulaciones de cada país)	3 sin traslape (11 canales en total)	3 sin traslape (11 canales en total)	79 canales para EU y Europa y 23 Canales para Japón	75 canales de 1 MHz, 15 canales de 5MHz. Para México son 27 canales de 1MHz	19 Canales en Europa, 8 canales sin traslape
Tipo de Modulación	BPSK QPSK 16QAM 64QAM	QPSK/COF (11 y 5 Mbps) QPSK (2Mbps) BPSK (1Mbps)	OFDM/COF OFDM QPSK/COF QPSK BPSK	GFSK CVSD (Continuously Variable Slope Delta Modulator)Para transmitir voz	LR 2 PSK LR 4 PSK HR 2 PSK HR 4 PSK	16QAM (OPCIONAL) BPSK QPSK

■ 11.3.4 [Tabla comparativa de los estándares inalámbricos]

■ II.4 [WLAN]

■ II.4.1 [Topologías]

Una topología nos determina la composición y estructura de la red. Existen diferentes propuestas para dividir o nombrar a las topologías existentes en las redes inalámbricas, algunos autores solo mencionan 2: ad-hoc e infraestructura [Walter, 2002] Otros mencionan solo BSS y ESS. La división que considero más adecuada es la siguiente [Brisbin, 2002].

Existen tres tipos de topologías:

- BSS (Basic Service Set) Conjunto de servicio Básico
- IBSS (Independent Basic Service Set) Conjunto Independiente de servicio básico
- ESS (Extended Service Set) Conjunto de servicio extendido

75

a) BSS (Ad-hoc)

También recibe el nombre de infraestructura. Esta topología consiste en un AP y varias estaciones de trabajo. Todas las estaciones de trabajo se encuentran dentro del área de cobertura del AP, lo que les permite reconocerse entre sí y trabajar en conjunto unos con otros. El AP actúa como controlador central y maneja la transmisión y recepción de información entre los dispositivos que están en su área de cobertura así como la seguridad.

Si una estación requiere comunicarse con otra, tendrá primero que comunicarse a través del AP y del AP se llevará a cabo la comunicación con la otra estación. Las estaciones nunca se comunicarán directamente una entre otra. El AP puede o no estar conectado a una red cableada, pero servirá como servidor lógico de una sola célula (área de cobertura) o canal, este tipo de red proporciona un área de mayor cobertura que un IBSS y maneja un número mayor de dispositivos.

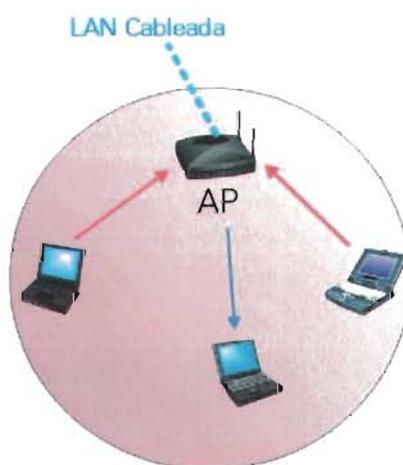


Figura II.25 Basic Service Set

b) IBSS (Infraestructura)

Se conoce también con el nombre de ad-hoc o peer-to-peer. En este tipo de topología no existe ningún controlador central (AP) que interconecte a los dispositivos, estos se comunican directamente uno con otro.

Son redes completamente autónomas, con ningún acceso a recursos fuera de la red. Son útiles cuando es necesario crear una red de manera fácil y rápida en cualquier lugar donde no exista un AP. Por lo general son redes temporales y sus usos principales son para comunicar PDAs con Laptops, Laptops con Laptops en un área reducida.

Debido a las características de esta red, se cubren áreas muy pequeñas y los dispositivos que la conforman deben de estar juntos. Para configurar una red ad-hoc lo único que se requiere es configurar a los adaptadores inalámbricos de las estaciones para que trabajen en modo ad-hoc, seleccionar el mismo canal y darles a todos el mismo nombre de red (SSID Service Set Identifier), Un dispositivo no puede estar configurado en modo ad-hoc e infraestructura al mismo tiempo.

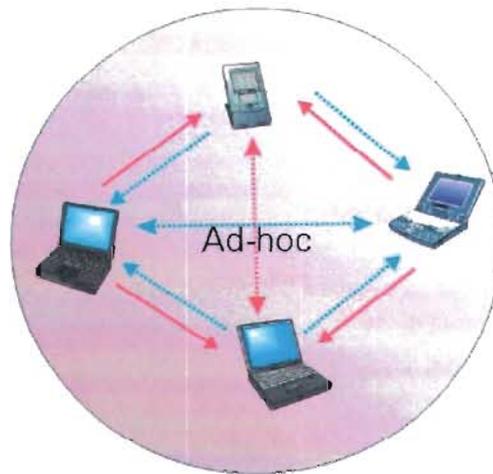


Figura II.26 Independent Basic Service Set o Ad-hoc

c) ESS (Extended Basic Service Set)

Esta topología está formada por un conjunto de BSS, es decir, está compuesto por varios APs dispersos en un área grande con el fin de cubrirla completamente, es decir, consiste en una serie de células superpuestas en donde los dispositivos pueden desplazarse de un lado a otro sin perder la conexión. Normalmente los APs se encuentran conectados a través de un sistema de distribución (DS) o red cableada, que proveerá servicios al ESS, tales como Internet, DHCP, etc.

Los APs que conforman el ESS deben de soportar roaming, con el fin de que cuando el usuario se mueva de su lugar no pierda su conexión, y el cambio de asociación entre un AP y otro sea transparente. Para configurar a los equipos en este tipo de topología es necesario dar a todos los APs el mismo nombre de red (SSID), pero deben estar en diferentes frecuencias con el fin de limitar la interferencia entre los radios de los APs.

Los dispositivos que se van a comunicar no necesitan estar cerca el uno del otro, sino pueden encontrarse en una célula diferente. Para que los APs sepan si hay estaciones conectadas a la red de otro AP, es necesario que intercambien información entre ellos, con el fin de entregar correctamente los datos.

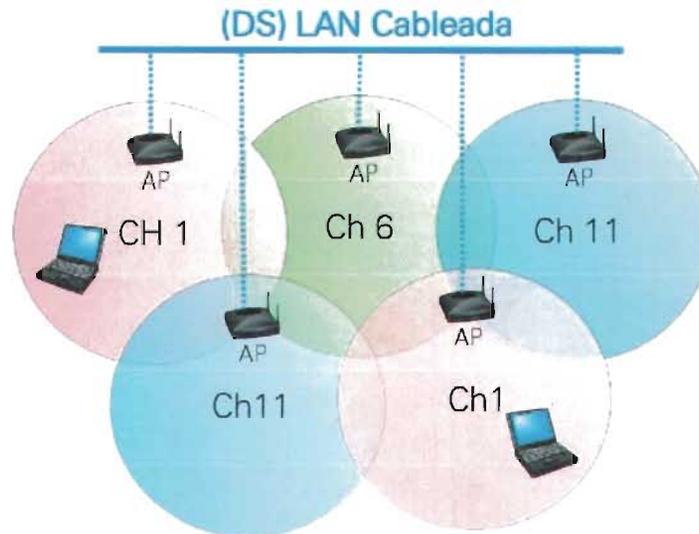


Figura II.27 Extended Service Set

■ II.4.2 [Técnicas de propagación]

“La diferencia entre una técnica de modulación y una de propagación es que una técnica de propagación distribuye la información a través de una variedad de canales, en tanto que una técnica de modulación modula la información a través de cada uno de los canales. El espectro extendido de secuencia directa (DSSS), el espectro extendido de saltos de frecuencia (FHSS), el acceso multiplexado de división de código (CDMA), y la multiplexión por división ortogonal de frecuencia (OFDM), son ejemplos de técnicas de propagación.”²⁶ OFDM es la técnica de propagación que se utiliza en 802.11a y 802.11g.

TECNOLOGIA DE ESPECTRO EXTENDIDO

Esta tecnología dispersa la señal a lo largo de un espectro de frecuencias de radio disponible. El espectro extendido es una técnica de codificación para transmisión digital. Fue desarrollada para el uso militar en 1950. Inventada por Hedy Lamarr y George Antheil durante la segunda guerra mundial por su deseo de contribuir para derrotar a Hitler, y patentada en 1940. Lamarr era una famosa actriz australiana en los años de 1930 y 1940, y Antheil era un músico compositor.

La patente original se llamó Sistema de Comunicación Secreto (Secret Communication System), y brindaría un sistema de comunicación rápido y seguro, pero no pudieron convencer al gobierno de los Estados Unidos para utilizarlo, puesto que en ese entonces no había equipo alguno que pudiera realizarlo. La patente expiró mucho antes de que el gobierno lo implementara para su uso comercial.

²⁶ REID. *Op. cit.* 50

El propósito militar del código de espectro extendido era transformar la señal de información de manera que pareciera ruido, lo que hacía muy difícil interceptar las señales.

Esta técnica consiste en modificar el espectro de la señal para extenderlo sobre un rango de frecuencias, y así incrementar el ancho de banda. En vez de transmitir una señal continuamente, se transmiten varias partes separadas, sobre un amplio espectro de frecuencias de radio. Esta señal tiene una baja densidad de potencia y es resistente a la interferencia.

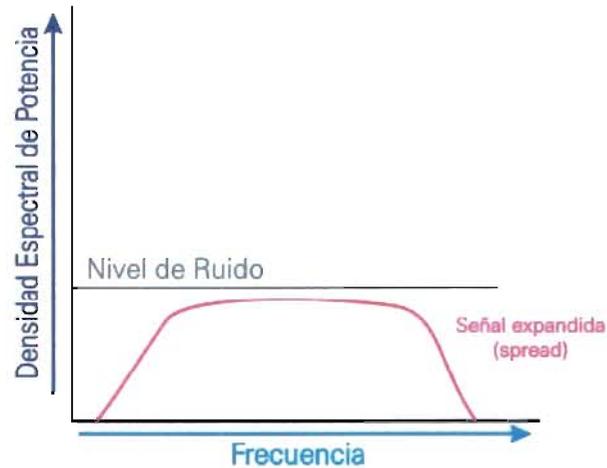


Figura II.28 Señal de espectro extendido.²⁷

Existen dos técnicas diferentes de espectro extendido:

- FHSS (Frequency Hopping Spread Spectrum) Espectro extendido por salto de frecuencia.
- DSSS (Direct Sequence Spread Spectrum) Espectro extendido por secuencia Directa.

a) Espectro extendido por salto de frecuencia (FHSS)

El ancho de banda disponible se divide en diferentes canales (por lo menos 75 para la banda de 2.4GHz, de acuerdo con la FCC), para Norteamérica son 79 canales.

La señal brincará (saltará) rápidamente de una frecuencia a otra, transmitiendo ráfagas de información en cada canal, en un tiempo determinado. El tiempo que puede permanecer un equipo en una frecuencia determinada es de 400ms y recibe el nombre de dwell time, después de transcurrido este tiempo brincará a otra frecuencia.

Para que el receptor pueda reconstruir la información es necesario que conozca el patrón de saltos que tiene el receptor. Este tipo de tecnología presenta dos principales beneficios: No se ve tan afectado por las interferencias, pues si hay ruido solo se verá afectada una pequeña parte de la señal, la segunda es que puede evitar brincar por una frecuencia determinada si esta se encuentra ocupada por otro equipo. Este tipo de técnica utiliza una menor cantidad de potencia que los radios de DSSS.

²⁷ AGUILAR. Sistema de enlace de la Dirección General de Obras. 126

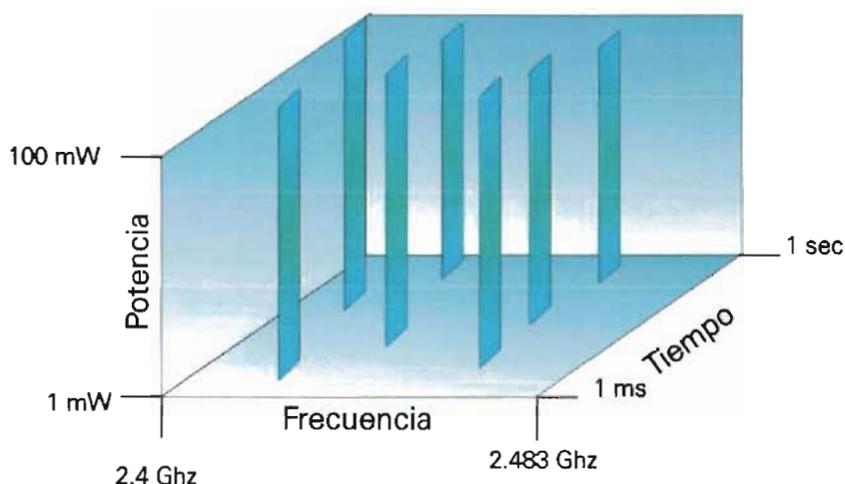


Figura II.29 Espectro Extendido por salto de frecuencia, FHSS ²⁸

b) Espectro extendido por secuencia directa (DSSS)

DSSS dispersa la información sobre múltiples canales, en un rango de frecuencias dado, lo que permite que varios sistemas puedan funcionar en paralelo sin interferencias, utilizando un esquema de codificación específico, y baja potencia.

A la información a transmitir se le agrega un código redundante llamado "chip" (también llamado código de dispersión, Pseudo ruido o Código Barrer), con el fin de proteger cada bit de información de posibles pérdidas, pues el receptor podrá reconstruir la información aunque se vea afectada por interferencias. La señal no se divide en partes, en lugar de esto, se codifica con cada uno de estos chips y el transmisor mandará la misma parte de información pegada de varios chips.

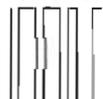
Una mayor cantidad de chips pegados a la señal indica una mayor resistencia a la interferencia. Para que el receptor pueda recuperar la señal correctamente es necesario que conozca la secuencia de chips del transmisor. Una vez que el receptor capta la transmisión remueve todos los chips de relleno para obtener la señal original. Usualmente se ocupan chips de 11 o 20 bits.

Código de dispersión

0 = 10010010110



1 = 01101101001



Bit 1 de datos



Bit 0 de datos

Figura II.30 Codificación de la señal para DSSS

²⁸ OVELLET. Op. cit. 53

Debido a la cantidad de espectro que necesita DSSS para poder transmitir la información solo se pueden utilizar tres canales en la banda de 2.4GHz. Esta técnica de propagación alcanza a cubrir una mayor distancia que FHSS.

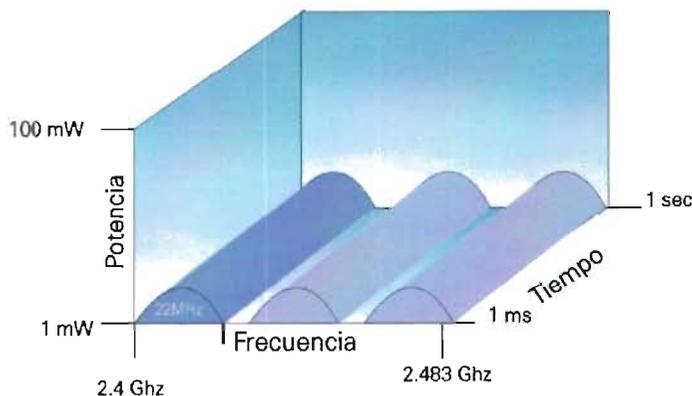


Figura II.31 Espectro extendido por secuencia directa, DSSS²⁹

c) Multiplexión Ortogonal por División de Frecuencia (OFDM)

Esta tecnología en vez de crear una larga fila de datos, transmite bits usando un número de subcanales (el ancho de banda se divide en subcanales más pequeños) que operan en paralelo en diferentes frecuencias, es decir, es un esquema de modulación de portadoras múltiples. Esta basado en un proceso matemático llamado FFT (Fast Fourier Transform) transformada rápida de Fourier, que fue patentada en 1970 por los laboratorios Bell. "OFDM divide la frecuencia portadora en 52 subportadoras solapadas, 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor"³⁰ Cada tono (fragmento de la frecuencia portadora) es ortogonal (independiente) a los tonos adyacentes.

OFDM permite en cada subcanal concentrar una pequeña cantidad de información. Al final de la transmisión de datos, todos los subcanales se multiplexan; el resultado es que la energía se envía a lo largo de todos los canales al mismo tiempo, lo que proporciona una alta eficiencia por canal. Entre las ventajas que presenta OFDM están su uso eficiente del espectro radioeléctrico, la alta resistencia a interferencias y a la distorsión por trayectorias múltiples (producidos por ondas reflejadas).



Figura II.32 Multiplexión por división ortogonal de frecuencia, OFDM³¹

²⁹ OVELLET, Idem.

³⁰ CARBALLAR, *Wi-Fi: cómo construir una red inalámbrica*, 39

³¹ REID, *Op.cit.* 52

■ II.4.3 [Tipos de modulación]

Las ondas de radio pueden variar en amplitud (tamaño), frecuencia (ondas por segundo) y fase (tiempo en el que empieza la onda). La interferencia tiende a afectar la amplitud de la señal, pero no su frecuencia ni su fase, por lo cual es conveniente empaquetar las señales de datos en señales analógicas que varíen principalmente en su frecuencia y fase. "Debido a que la FCC regula la frecuencia a la que un radio puede transmitir, existe un límite para la velocidad a la que se puede codificar la información. Entre más alta sea la frecuencia mayor será el potencial de velocidad de datos, debido a que la frecuencia de la señal no puede incrementarse, es necesario incrementar la complejidad de las técnicas de modulación para enviar los datos más rápido a velocidades mayores"³²

MODULACIÓN POR FASE.

La modulación por fase es muy eficiente para convertir señales digitales, ya que toma la ventaja de la forma de onda. Una señal digital esta compuesta por bits de datos (0 y 1), puesto que la onda de radio es una onda analógica, la señal de datos digital debe modularse para poder transmitirse en una señal portadora. Una señal digital, sin portadora ocupa un gran ancho de banda y es extremadamente ineficiente. "Los muchos ángulos o fases de la onda senoidal dan origen a diferentes caminos de enviar la información."³³ Las técnicas de modulación por fase se han vuelto cada vez más complejas con el fin de llevar una mayor cantidad de información en cada onda.

a) BPSK (Binary Phase Shift Keying)

Modulación de fase por desplazamiento binario. Este tipo de modulación consiste en representar la señal binaria por medio de varias fases de la onda senoidal, es decir hay desplazamientos en el inicio de la onda para indicar que estado binario es el que se esta codificando (una determinada fase para representar el 1 binario y otra para representar el 0 binario). Solo se codifica un bit a la vez, lo que da como resultado una velocidad de 1Mbps. La señal de entrada de la portadora se multiplica por los datos binarios. Son posibles dos fases de salida para una sola frecuencia de portadora. "BPSK es un tipo de modulación muy sólido, por lo que se emplea para todos los encabezados de las tramas de datos, sin importar cual tipo de modulación se use para la carga de información"³⁴

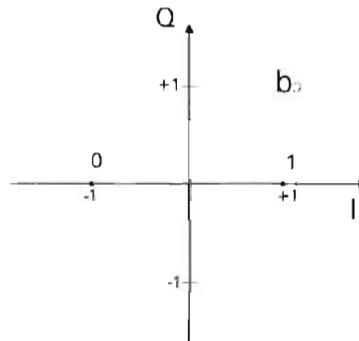


Figura II.33 Constelación BPSK

³² WALTER. *Wireless LAN end to end*. 19

³³ OVELLET. *Op. cit.*, 44

³⁴ REID. *Op. cit.*, 95

Ejemplo de una señal en BPSK

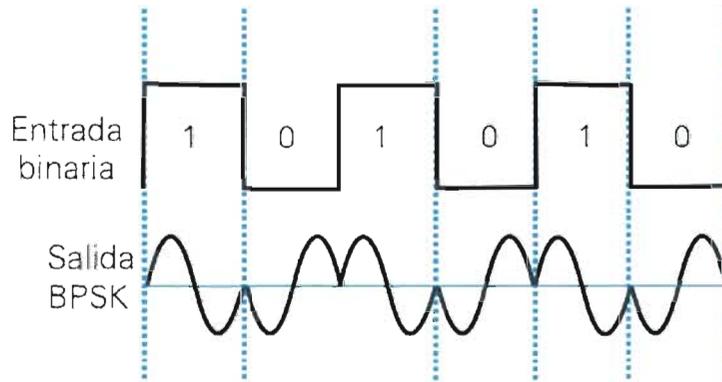


Figura II.34 Señal modulada en BPSK

b) QPSK (Quadrature Phase Shift Keying)

Modulación de fase por desplazamiento en cuadratura. Se necesita más de un bit de entrada, por lo que los bits de entrada se combinan en grupos de 2 bits, lo que incrementa la velocidad y la cantidad de datos transferidos. La portadora experimenta cuatro cambios en fase para representar los siguientes conjuntos de bits: 00, 01, 10, 11.

“QPSK manipula y cambia el patrón normal de una onda senoidal moviendo su alternancia y forzando a la onda a caer a su línea base o punto de inicio antes de que la onda caiga naturalmente a este punto, cada vez que se transmite un par de bits.”³⁵

Para entender mejor como funciona QPSK diremos que una porción de la fase (0 a 90°) se utilizara para representar el 00, de 90 a 180° para representar 11 y así sucesivamente. Debido a que se duplica la cantidad de bits también se duplica la velocidad de transmisión a 2Mbps.

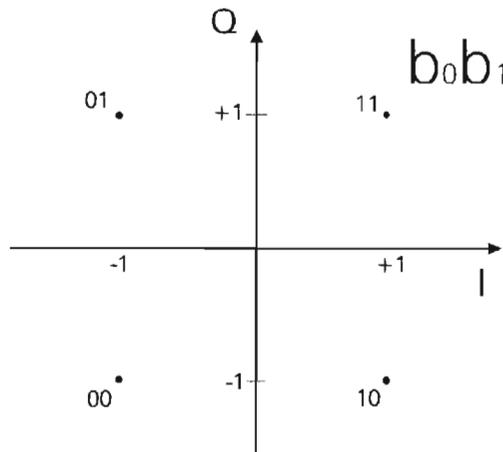


Figura II.35 Constelación QPSK

³⁵OVELLET. Op. cit. 46

Ejemplo de una señal QPSK

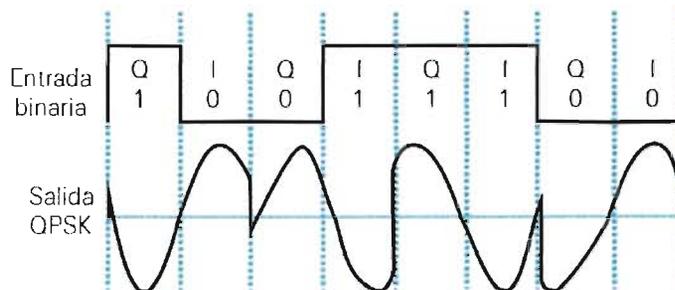


Figura II.36 Señal modulada en QPSK

c) CCK (Complementary Code Keying)

Modulación de código complementario. Se basa en otra técnica de modulación llamada MOK (Mary Orthogonal Keying), y fue diseñado con el fin de superar los límites de las bajas velocidades que se obtienen modulando en BPSK o QPSK.

Consiste en una modulación QPSK codificada, es decir, la señal a transmitir será modulada dos veces en vez de una, por lo que requiere un canal de transmisión mucho más claro que para las otras modulaciones. Una de las principales ventajas de CCK es que sufre menos de interferencias por trayectorias múltiples en comparación con QPSK y BPSK.

“Los bits originales de datos son mapeados a un símbolo modificado correspondiente de los datos, 8 bits por 8 bits símbolo. A estos símbolos de datos se les aplicará una modulación para variar las fases de la onda analógica. El resultado de la forma de onda es la misma que QPSK, pero la velocidad será mucho más alta. CCK utiliza un complejo juego de funciones conocido como código complementario para enviar datos adicionales a la onda.

CCK provee un bit adicional de datos en cada canal ya sea I (In-phase, en fase) o Q (Quadrature, en cuadratura) al invertir o rotar la forma de onda 90°. Este nuevo tipo de símbolo para 6 bits puede ser modulado en QPSK para llevar dos bits más. El resultado es que 8 bits son transmitidos con cada símbolo por lo que la forma de onda resultante tendrá 16 bits de complejidad.”³⁶

d) QAM (Quadrature Amplitude Modulation)

Modulación de amplitud en cuadratura. La información digital está codificada a través de cambios tanto en la amplitud como en la fase de la portadora transmitida.

- Quando se codifica 1 bit es posible obtener 2 símbolos
- Quando se codifican 2 bits es posible obtener 4 símbolos
- Quando se codifican 3 bits es posible obtener 8 símbolos.
- Quando se codifican 4 bits es posible obtener 16 símbolos
- Quando se codifican 6 bits es posible obtener 64 símbolos.

³⁶ Ibid. 47

16-QAM

Los datos de entrada se separan en grupos de 4 bits, dos de ellos se encargan de producir 2 magnitudes diferentes y los otros dos de producir 2 fases distintas. Las diferentes combinaciones de estos bits producen 16 salidas diferentes con cambios tanto en cuadratura como en fase.

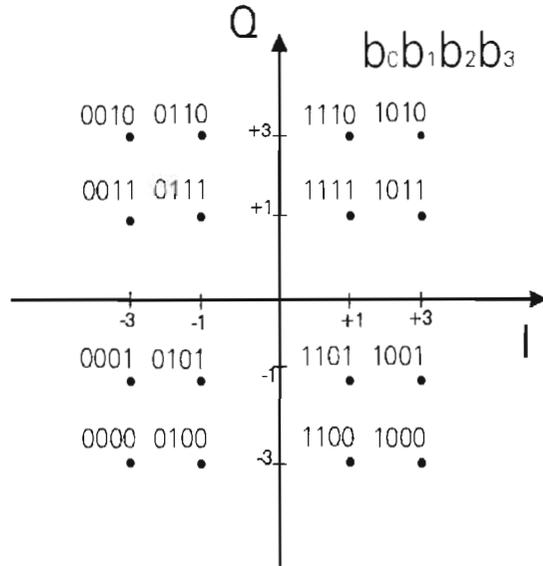


Figura II.37 Constelación para 16-QAM

Ejemplo de onda de 16-QAM

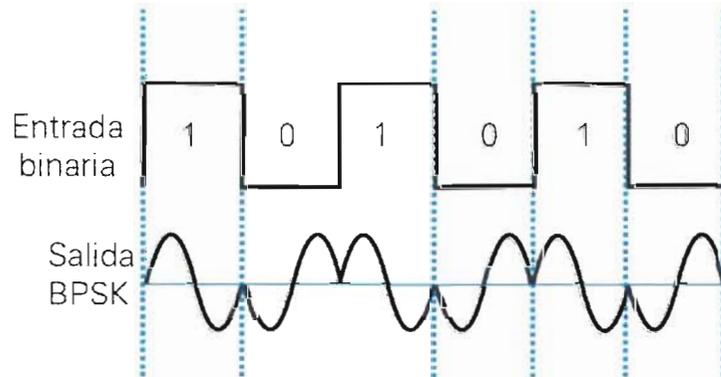


Figura II.38 Señal modulada en 16-QAM

■ II.5 [Seguridad]

Aunque las redes inalámbricas presentan muchas ventajas, tales como la movilidad y la comodidad, tienen una debilidad muy importante en comparación a las redes cableadas, esa debilidad es la seguridad.

Una red alámbrica está limitada por el cableado y los edificios, esta contenida en un cierto espacio, y la única forma de irrumpir en la red es conectándose directamente a ella. En una red inalámbrica la información esta en el aire, no esta contenida en un espacio delimitado y esta al alcance de todos, por lo que cualquiera puede tomarla. Para evitar que esto suceda, es importante implementar ciertas medidas, como son la autenticación, el cifrado, etc.

Existen tres elementos básicos que deben cubrirse para brindar seguridad a una WLAN que son confidencialidad o privacidad, integridad y autenticación.

- **CONFIDENCIALIDAD**

Confidencialidad es asegurarse que la información que provee un cliente será protegida y se mandará en calidad de privada. Proteger a la información del acceso no autorizado mientras se lleva a cabo la comunicación entre el emisor y el receptor.

- **INTEGRIDAD**

Consiste en identificar y rechazar cualquier mensaje que pudiera haber sido "manoseado" en el trayecto. La integridad asegura la exactitud y completariedad de la información en su viaje.

- **AUTENTICACIÓN**

Consiste en validar que las entidades son en realidad quienes dicen ser, y que ambas reconozcan su identidad para así poder intercambiar información.

Aunque la seguridad en las redes inalámbricas sea una debilidad no significa que no puedan utilizarse ciertos métodos o implementar ciertas medidas preventivas con el fin de proporcionar un nivel general de seguridad, tales medidas pueden ser:

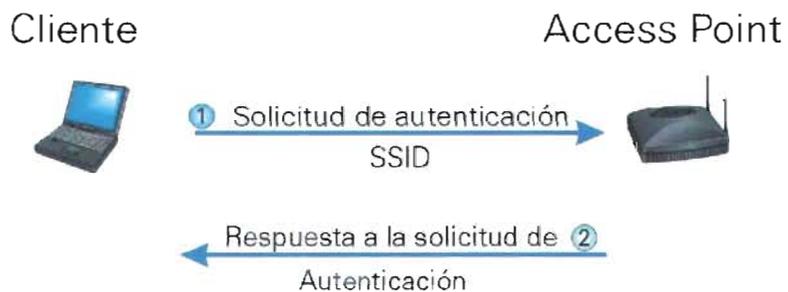
- a) Cambiar el SSID y el password que vienen configurados de fábrica por default, cuando se instala un equipo es importante personalizar estos valores, pues muchos pueden conocer los valores que da por default el fabricante.
- b) Habilitar WEP, y cambiar la clave de encriptación regularmente.
- c) Si el área que se va a cubrir no es muy grande, se recomienda el uso de antenas direccionales con el fin de que la señal no se disperse por todos lados
- d) Aplicar filtrado de direcciones MAC
- e) Si es posible deshabilitar la administración remota del AP
- f) Cambiar frecuentemente el password de administración del equipo.

A continuación se describen otras medidas importantes de seguridad.

■ II.5.1 [Autenticación]

El objetivo principal de la autenticación es restringir el acceso a la red o al sistema y solo permitir a ciertas entidades. Un cliente inalámbrico debe autenticarse con el AP para poder tener conexión. Existen 2 tipos básicos de autenticación:

- **Open system (Sistema abierto o autenticación abierta o NULL authentication).** Permite a cualquier dispositivo autenticarse. Cualquier equipo que quiera comunicarse con el AP puede comunicarse sin mayor problema. El cliente solo necesita conocer el SSID de la red. Si el AP tiene una clave WEP activada, el cliente debe saberla también, si ambas claves coinciden podrán comunicarse entre ellos, de no ser así la autenticación si se llevara a cabo pero no habrá intercambio de datos. Este tipo de autenticación no requiere de algún servidor de autenticación externo.



Una vez autenticado el cliente puede intercambiar información con el AP

Figura II.39 Autenticación Abierta

- **Shared-Key Authentication (Autenticación de clave compartida).** El AP envía un "texto de desafío" descriptado a cualquier dispositivo que desee comunicarse con el. El dispositivo responde a la autenticación encriptando el "texto desafío" y lo envía regreso al AP. Si el texto de desafío es encriptado correctamente, el AP permite al dispositivo autenticarse. Debido a que tanto el "desafío" encriptado, como el desafío descriptado pueden ser monitoreados por algún intruso, este tipo de autenticación puede ser menos seguro que la autenticación abierta. Este tipo de autenticación tampoco reside en un servidor de autenticación que se encuentre en la red.



Figura II.40 Autenticación de clave compartida

■ II.5.2 [Control de acceso por filtrado de direcciones MAC]

Debido a que para facilitar la entrega del tráfico en la red, se le asigna a cada dispositivo una dirección única (MAC) programada de fábrica y esta dirección debe ser única en toda la red, se puede utilizar con el fin de limitar el acceso a la red. El filtrado de direcciones MAC consiste en declarar una lista al AP con todas las direcciones MAC de los equipos inalámbricos que tienen derecho o están autorizados para conectarse.

Cuando un dispositivo inalámbrico desea conectarse a la WLAN enviará una solicitud de autenticación, el AP responderá al equipo la autenticación y cuando el equipo desee iniciar el proceso de asociación con el AP, el AP buscará en su lista (previamente definida) la dirección MAC del equipo que lo solicita; si la dirección MAC se encuentra en la lista el equipo podrá asociarse.



Figura II.41 Control de acceso por direcciones MAC

Este tipo de control de acceso no es una solución completa de seguridad, pues algunos dispositivos tienen la modalidad de cambiar su dirección MAC, por lo que algún extraño puede obtener una dirección MAC válida y falsificarla en su equipo. Presenta otras desventajas, ya que cada vez que un equipo nuevo desee agregarse a la red deberá actualizarse (manualmente) la lista de direcciones MAC que se encuentra en el AP.

■ II.5.3 [WEP]

WEP (Wired Equivalent Protocol), forma parte de IEEE 802.11 en su versión original en 1997, recibió el nombre de Privacidad equivalente al cableado, y fue retomado en 802.11b. WEP fue creado con el la intención de proteger las comunicaciones inalámbricas de intromisiones, al encriptar los datos mientras viajan a lo largo de la red. Para lograr esto se utiliza una clave de cifrado (llamada WEP Key).

Esta clave de cifrado tiene que ser distribuida y configurada en cada estación y AP que necesiten comunicarse, para que puedan descifrar los datos una vez recibidos.

Existen principalmente dos tipos de claves WEP: de 40 bits (mejor conocida como de 64bits) y de 104bits (o 128 bits) la diferencia son 24 bits de un vector de inicialización IV (Initialization Vector) cuya finalidad es aumentar el número de claves posibles generadas y prevenir el re-uso de claves en un cierto tiempo.

El vector de inicialización es usado para crear tramas de cifrado, que se utilizan para realizar la encriptación.

Funcionamiento de WEP para encriptar la información [Walter, 2002]

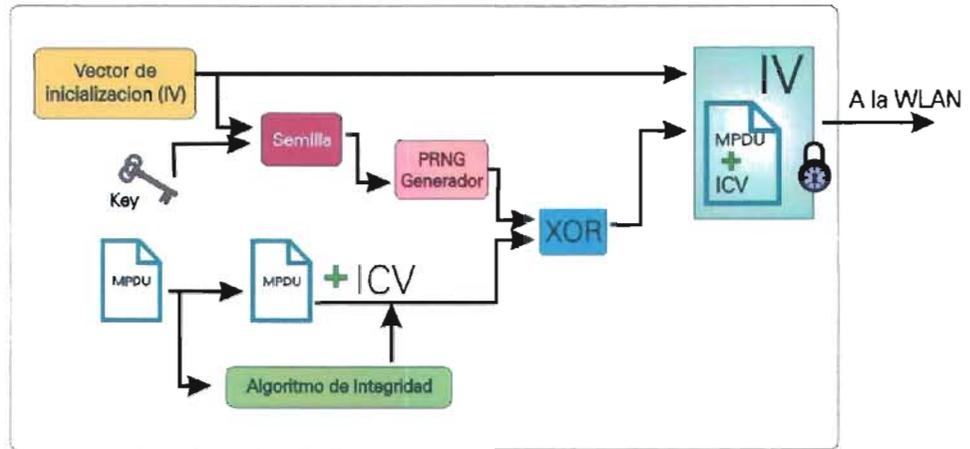


Figura II.42 Proceso de encriptación

1. La estación que va a enviar los datos utiliza un algoritmo de integridad para generar 32bits de redundancia cíclica (CRC Cyclic Redundancy Check) en base a la MPDU que recibe de las capas superiores. El valor generado recibe el nombre de valor de chequeo de integridad ICV, con el fin de que el destinatario pueda utilizarlo para asegurarse de que los datos no han sido alterados durante la transmisión. El valor de chequeo se enviará junto con la MPDU de datos .

2. Se genera un vector de inicialización IV con 24bits que se enlazarán con la clave WEP compartida para formar una "Semilla".

3. Estos 64 o 128 bits resultantes de la suma del IV + clave WEP, se envían a un generador de números pseudos-aleatorios PRNG (Pseudorandom Number Generator) que utiliza el algoritmo RC4 (algoritmo de cifrado diseñado por Ron Rivest para RSA Data Security) El resultado es una secuencia de bits que es igual en longitud a la suma del valor de integridad ICV + MPDU .

4. Se aplica una operación XOR para combinar esta secuencia generada con los datos MPDU + ICV sin cifrar (en limpio). El resultado es la trama MPDU+ICV cifrada.

5. Este mensaje es el que se enviará a través de la LAN junto con el vector de inicialización IV sin cifrar para que el destinatario pueda descifrar la información.

El proceso para descryptar es el siguiente:

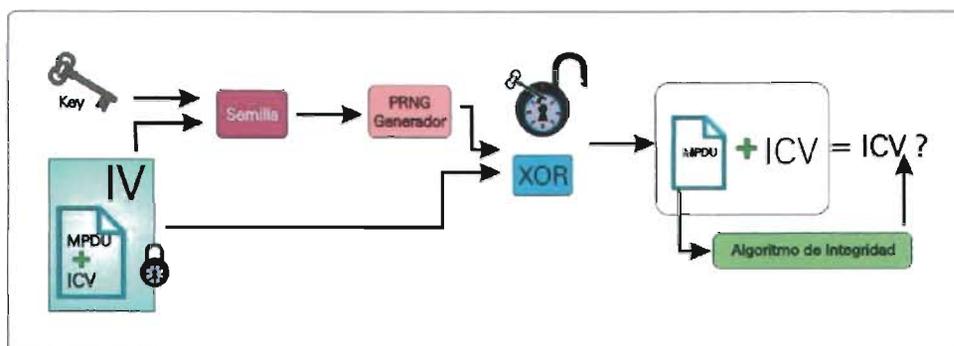


Figura II.43 Proceso de descifrado

1. Ya en el destino, la clave WEP se combina con el vector de inicialización que llegó en el paquete recibido.
2. La semilla se envía al generador PRNG para generar una secuencia de bits que descifre el mensaje.
3. Se combinan con una operación XOR el texto cifrado con la secuencia de bits obtenida en el generador y se obtienen así los datos MPDU + ICV .
4. A partir de la MPDU ya sin cifrar, se genera con el mismo algoritmo de integridad utilizado en el origen, un vector de 32 bits para verificar la integridad.
5. Se compara el ICV generado con el ICV recibido, si ambos valores coinciden se determina que los datos llegaron intactos.

WEP presenta ciertas desventajas:

- Una vez que se conoce la clave de cifrado, se puede tener acceso a la información
- El algoritmo de encriptación RC4, puede generar claves aleatorias diferentes, que con el tiempo pueden repetirse.
- La clave compartida es estática, una vez asignada se configura tanto en el AP como en la estación y permanece constante hasta que el administrador decida cambiarla.

WEP por sí solo, no brindará mayor seguridad a la red. Existen diversas herramientas y trucos para romperlo. 802.11i cubrirá las debilidades o huecos que tiene WEP.

■ II.5.4 [Autenticación 802.1x]

802.1x es un estándar que fue ratificado por el IEEE en junio del 2001, para el control de acceso a la red basado en puertos que se utilizan para proporcionar acceso autenticado a la red. Se diseñó para las redes cableadas como Ethernet, pero se puede utilizar también para las redes inalámbricas con el fin de proporcionar una autenticación segura para los usuarios de una WLAN.

Está basado en 2 estándares de seguridad:

- EAP (Extensible Authentication Protocol), Protocolo extensible de autenticación, es una extensión al protocolo Punto a Punto (PPP), pues provee una arquitectura abierta para incorporar virtualmente

cualquier esquema de autenticación para asegurar sesiones PPP por medio del encapsulado de datos.

- RADIUS (Remote Authentication Dial- In Service) Servidor de servicio de autenticación remota de usuario, que provee autenticación, autorización y confiabilidad.

La autenticación para redes LAN inalámbricas esta conformada por tres componentes principales, el solicitante, el autenticador y el servidor de autenticación. El solicitante es la estación que pide la conexión: un usuario con una laptop y una tarjeta de red inalámbrica instalada. El autenticador es un AP que soporta 802.1x. El servidor de autenticación es por lo general un servidor RADIUS.

La autenticación 802.1x funciona de la siguiente manera:

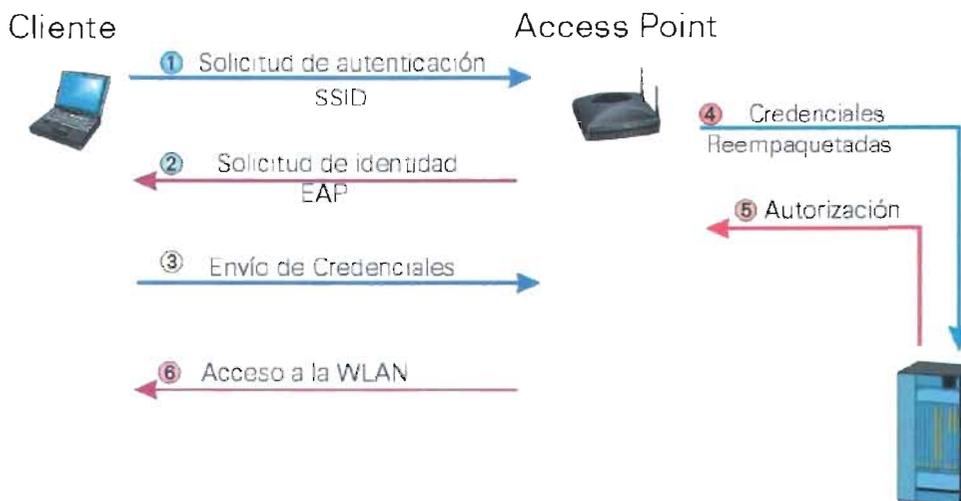


Figura II.44 Autenticación 802.1x

1. Una estación solicita autenticarse con el AP
2. El autenticador detecta a un solicitante que requiere ser autenticado. El AP habilita un puerto para el cliente y fuerza al puerto a un estado no autorizado, el único tráfico que puede circular es el tráfico 802.1x, otro tipo de tráfico tal como http, ftp, SMTP o POP3 será bloqueado. Una vez hecho esto, el AP le envía a la estación móvil un desafío encapsulado con EAP, en el que solicita al equipo sus credenciales para conocer su identidad
3. El cliente envía sus credenciales al autenticador, este reempaquetará estas para reenviarlas al servidor de autenticación.
4. El servidor de autenticación compara las credenciales enviadas por el AP con las que tiene almacenadas en su base de datos. El servidor realiza una serie de preguntas al cliente con el fin de determinar si es realmente quien dice ser y el cliente también hará una serie de preguntas al servidor RADIUS, con el fin de que ambos comprueben su identidad (Autenticación Mutua)
5. Una vez que el cliente ha sido autenticado, el servidor de autenticación informa al AP. El AP hará que el puerto en el que el cliente se encuentra pase a un estado autorizado y le permite entonces tener acceso a la red.

Aunque el intercambio de una clave de encriptamiento, no está especificado para las redes inalámbricas 802.1x, no significa que no pueda utilizarse, todo dependerá del fabricante si lo implementa o no.

■ II.5.5 [802.11i]

En mayo de 2001 la IEEE asignó un grupo de trabajo dedicado a desarrollar un estándar para seguridad en redes inalámbricas, que ofrezca interoperabilidad. El principal objetivo del grupo es resolver el problema de WEP. 802.11i provee mejoras en la seguridad para los estándares 802.11a, 802.11b y 802.11g, estas mejoras en la seguridad incluyen nuevos procedimientos de autenticación, robustos esquemas de encriptación y asignación de claves dinámicas.

El estándar incluirá soporte para 802.1x control de acceso basado en puertos, protocolo de integridad de clave temporal TKIP (Temporal Key Integrity Protocol) y el estándar de cifrado avanzado AES (Advanced Encryption Standard).

91

a) AES

Estándar de cifrado avanzado, es un algoritmo de encriptación que soporta diferentes longitudes de clave de 128, 192 y 256bits, lo que dará aproximadamente 10^{38} , 10^{57} , y 10^{77} claves posibles, por lo que es muy difícil de romper.

AES es implementado como bloque de cifrado pues encripta los datos en corto tiempo. La estructura matemática de AES es lo suficientemente simple para que sea factible implementarla en dispositivos pequeños, como PDAs y celulares que tienen un poder de procesamiento limitado.

b) TKIP

Es el reemplazo para WEP, y agrega las siguientes mejoras:

- MIC (Message Integrity Protocol), mensaje de comprobación de integridad; se usa para garantizar la integridad de los paquetes y determina si un intruso ha capturado o modificado los paquetes "las direcciones de envío y recepción a demás de otra información única se integra en la carga cifrada"³⁷
- La clave de cifrado se combina con la dirección MAC del emisor para complicar la clave básica
- Agrega un mecanismo para generar claves dinámicas y reemplazar a las claves estáticas usadas en WEP.

Debido a que el estándar no había sido liberado para noviembre del 2002, la Wi-Fi Alliance decidió liberar una actualización para WEP llamada Wi-Fi Protected Access (WPA Acceso Protegido a Wi-Fi), que corrige algunos de los defectos de WEP además de que será compatible con 802.11i cuando sea liberado.

³⁷ REID. Op. cit. 236

c) WPA

Para poder utilizar las ventajas de WPA es necesario actualizar las versiones de firmware y software en los equipos que se encuentran disponibles en Internet. WPA aumenta el tamaño del vector de inicialización de 24bits (usado en WEP) a 48bits garantizando que la elección de este número no es predecible lo que amplía la complejidad del sistema de cifrado.

Mejora a WEP en dos aspectos principalmente:

- Utiliza la encriptación de datos con TKIP para asegurar la confidencialidad en las comunicaciones
- Soporta autenticación por 802.1x y EAP junto con un servidor RADIUS.

■ II.5.6 [Ataques comunes]

Los ataques que sufren comúnmente las redes inalámbricas pueden clasificarse en 3 principalmente:

- Sniffing (husmear)

Es “escuchar detrás de las puertas”, significa que un equipo analiza el tráfico de otros equipos en la red. Cualquier comunicación que pasa por la red inalámbrica puede ser vista por cualquiera que este escuchando. Una estación ni siquiera necesita estar asociada a una red para poder husmear. Existen diferentes programas diseñados para realizar este tipo de actividades entre ellos se encuentran el Netstumbler y el AiroPeek. Estos softwares ponen a la tarjeta inalámbrica en un modo de solo escucha, cada paquete que pasa por la tarjeta es capturado y la información será desplegada en la ventana del software correspondiente. Este tipo de aplicaciones dan información tal como la MAC address del equipo, el fabricante, el SSID, si la clave WEP esta activa o no, algunos pueden determinar la intensidad de la señal, el tipo de tráfico pues se pueden capturar paquetes y cazar la clave WEP. Esto proporciona a los atacantes varios elementos importantes.

- Spoofing (burlar el acceso a la red)

El atacante puede engañar al equipo de red, haciéndole creer que la conexión que está solicitando proviene de un equipo que es válido y pertenece a su red. El modo más fácil de engañar a un equipo es sustituir una dirección MAC de una estación no autorizada, por la dirección MAC de una estación válida. No se requieren herramientas muy complejas para burlar la MAC address, lo único que se tiene que hacer es obtener una dirección MAC válida y clonarla en un adaptador al que se le pueda cambiar la dirección MAC.

- Hijacking (asaltar o robar alguna sesión o identidad)

El atacante puede robar la identidad de algún AP y puede entonces tener acceso a los paquetes de datos, pues los dispositivos conectados a él creerán que es el AP legítimo. Normalmente esto lo hacen con el fin de obtener la información necesaria como passwords y nombres de usuario. Este método tiene una variante conocida como “El hombre de en medio” En este caso el atacante intercepta los paquetes antes de que lleguen a su destino, tiene dos opciones, alterarlos para tratar de descifrar las claves de encriptación en la red, o puede registrar todos los paquetes de información que se intercambien, para después descubrir cual es la clave WEP.



[APLICACIONES]



III. APLICACIONES

Las redes inalámbricas han ido adentrándose en nuestra vida cotidiana cada vez más, debido a las múltiples aplicaciones que de ellas derivan, ya que nos son de gran utilidad tanto en el interior de una empresa, una casa, un restaurant, como en la explanada de un campus universitario; pues nos brindan movilidad y comodidad para realizar diversas actividades.

Podríamos decir que las principales aplicaciones de las redes inalámbricas son: como una extensión de las redes alámbricas y para crear redes locales. Los dispositivos Wi-Fi se utilizan también para "crear un enlace de comunicación entre dos puntos,"³⁸ es decir, unir dos redes ya sean alámbricas o inalámbricas. Los equipos especializados para realizar este tipo de trabajo reciben el nombre de Wireless Bridges (Puentes inalámbricos), pues interconectan dos redes mediante una conexión inalámbrica.

Este tipo de enlaces son mucho mas barato que los enlaces de microondas, ya que para hacerlo, lo único que se compra es el equipo Wi-Fi y no es necesario obtener una licencia pues la banda en la que operan es libre. Si se contrata un enlace de microondas con alguna compañía la tarifa que se paga es mensual y los costos pueden llegar a ser muy elevados. Se pueden llevar a cabo dos tipos de enlaces: Punto a punto y Punto multipunto.

95

ENLACE PUNTO A PUNTO

Se lleva a cabo solamente entre dos equipos inalámbricos.

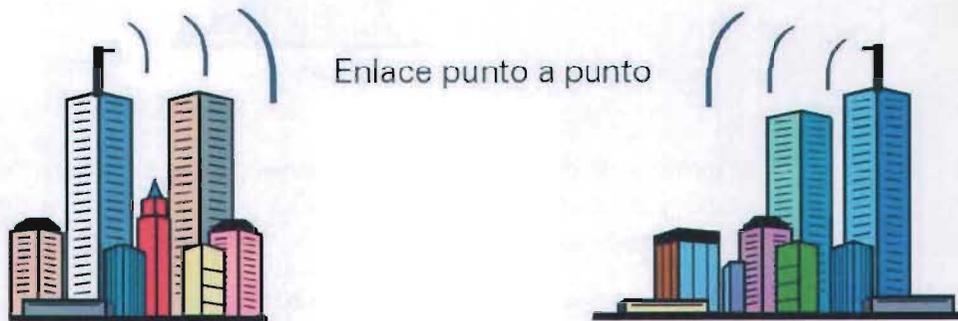


Figura III.1 Enlace punto a punto

Debido a que la función de "bridge" entre dos APs (inalámbrico e interfaces cableadas) se lleva a cabo en la capa MAC del modelo de referencia OSI y está basado en tramas de direcciones, los APs utilizados como puentes inalámbricos punto a punto, típicamente se comunican solo con el otro AP y no proveen alguna interfaz para conectarse con estaciones inalámbricas. A cada equipo se le declara la dirección MAC del equipo del otro extremo, con el fin de que solo se "vean" entre ellos y el mismo nombre de red (SSID).

Para hacer un enlace punto a punto se requieren dos APs (wireless bridges) dos antenas en cada extremo, las antenas que comúnmente se utilizan son direccionales, ya que se reduce el riesgo de interferir con otro equipo además de incrementar el rango de transmisión efectiva.

³⁸ CARBALLAR. *Op. cit.* 212

ENLACE PUNTO MULTIPUNTO.

En este tipo de enlace existe un AP (wireless bridge) maestro o punto central que interconecta a varios APs esclavos o remotos. El AP esclavo se comunica únicamente con el AP maestro y no con alguno de los otros APs esclavos. Los AP esclavos pueden verse entre sí solo a través del maestro pues no existe una conexión directa entre ellos.

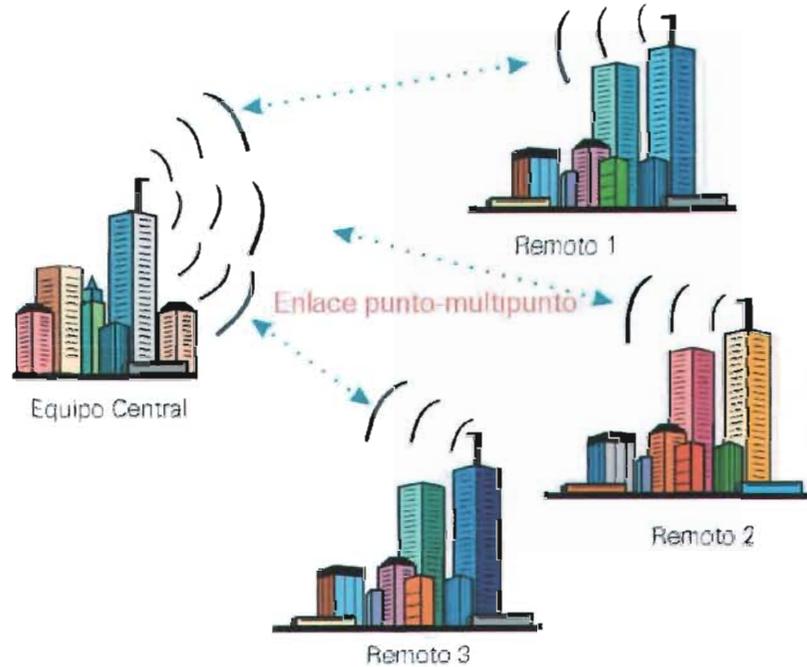


Figura III.2 Enlace punto multipunto

Al AP central se le declaran todas las direcciones MAC de los equipos remotos o esclavos (configuración punto multipunto). Y a cada uno de los remotos se le dará la dirección MAC del AP central en una configuración punto a punto.

La cantidad de dispositivos que se pueden conectar en un punto multipunto dependen de las características que cada vendedor ofrezca, para los equipos de Enterasys RoamAbout RBTR2 (específicamente), el número máximo de equipos remotos que se pueden conectar con el AP central es seis.

Configurar un enlace, ya sea punto a punto, o punto multipunto requiere tener en cuenta las siguientes consideraciones, ya que no es tan sencillo realizarlo pues ciertos factores pueden impedir que el enlace se lleve a cabo de manera adecuada.

- **Zona de Fresnel.** Es la principal consideración que se debe tener en cuenta en un enlace punto a punto, debido a que una señal electromagnética que viaja entre dos antenas no viaja en una línea recta, sino que se dispersa conforme se propaga y las ondas que componen esta señal no viajan a una velocidad constante. Se dice que la trayectoria que existe entre un par de antenas es elíptica y tridimensional; esta trayectoria elíptica está dividida en varias zonas, basándonos en la fase y la velocidad de las ondas que se propagan. Estas zonas reciben el nombre de zonas "Fresnel" y cada

zona difiere en fase por más de media longitud de onda o 180° . Para que un enlace se pueda llevar a cabo se debe calcular la zona de Fresnel para proveer espacio libre de radio en el centro de dicha zona.

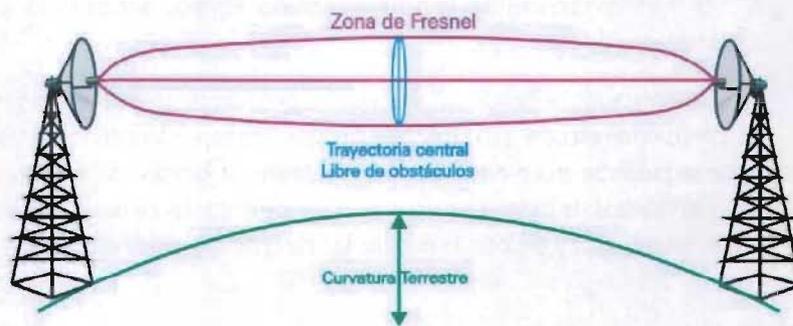


Figura III.3 Zona de Fresnel

• **Línea de Vista.** Es otro factor importante que puede determinar si el enlace es viable o no. Los dos equipos de radio (o antenas) deben de "verse" entre sí; esto quiere decir que si alguna estructura (árboles, edificios, montañas, etc.) bloquean la vista física entre ambos, es muy probable que no se pueda llevar a cabo el enlace pues la señal se perdería en los obstáculos.

97

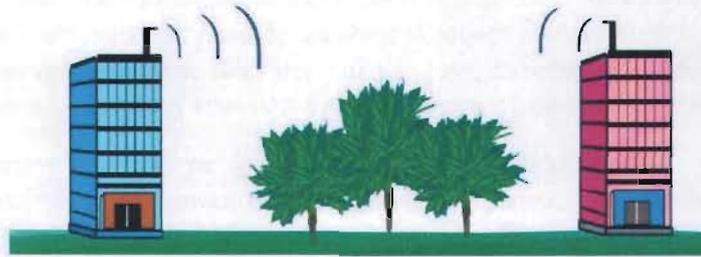


Figura III.4 Línea de Vista.

• **Curvatura terrestre (Earth Bugle).** Cuando se montan antenas sobre edificios altos o torres muy altas con el fin de tener una línea de vista clara, es necesario tener en cuenta que aunque el terreno sea totalmente plano, con la distancia se puede incrementar la elevación del lugar debido a la curvatura de la tierra.

"Para determinar que tan alta necesita estar una antena para librar la curvatura de la tierra en un terreno plano, se puede utilizar la siguiente fórmula:

$$\text{Altura de la antena} = (D/2.448)^2 \text{ ft}$$

D = distancia entre las dos antenas en millas"³⁹

Cuando no se está en un terreno plano se necesita consultar un mapa topográfico para determinar si hay línea de vista ente ambos sitios.

³⁹ WALTER. Op. cit. 315

- **Distancia.** La distancia es otro elemento importante, pues la señal va decreciendo conforme la distancia entre los extremos se incrementa. Si la señal que se recibe es muy baja no se puede llevar a cabo el enlace, o en su defecto la señal es intermitente.

En muchos lugares se han implementado equipos inalámbricos para cubrir las diferentes necesidades de cada lugar.

A continuación se mencionan algunos casos con diferentes marcas y modelos de equipos empleados. La decisión de escoger a un fabricante en específico dependerá del costo, las características adicionales que se pudieran incluir en los equipos, el tamaño, la facilidad de instalación, en comparación con los requerimientos de cada lugar. La mayoría prefiere inclinarse por un solo fabricante para asegurar la interoperabilidad y explotar la máximo las características de cada equipo.

■ III.1 [Hidden Villa Ranch]

Hidden Villa Ranch, con su corporativo ubicado en Fullerton, California provee huevos a millones de personas alrededor del mundo. En el 2001, Hidden Villa remodeló una de sus instalaciones en Ramona, California. Este nuevo edificio se encuentra a 500mts de las oficinas centrales en donde se encuentran los equipos de telefonía. Se tendió un tubo subterráneo entre los dos edificios y por ellos se corrieron 25 pares de cobre, este cable permitía conectarse a módems analógicos pero no era suficiente para transmitir un enlace WAN entre Ramona y el corporativo.

Hidden Villa Ranch empezó a buscar una solución para poder conectarse con el resto del corporativo, algunas de las soluciones que tuvieron en mente fue pasar cable nuevo de mejor categoría o fibra óptica, pero se dieron cuenta de que la tubería ya estaba llena y que además el costo era demasiado.

Fue entonces cuando pensaron en una solución inalámbrica, y después de evaluar a varios proveedores escogieron a CISCO para montar un enlace punto a punto a lo largo de los 500mts.

El costo del equipo y la instalación era mucho más accesible que tender fibra óptica a lo largo de la tubería.

Se instalaron dos equipos Cisco Aironet 340 Series Wireless Bridges, uno en cada edificio. Con esto no solo lograron interconectar los dos edificios sino mantener una rápida conectividad entre Ramona y la WAN a una velocidad de 11Mbps.

Además de que implementaron nuevas aplicaciones como el uso de dispositivos de mano inalámbricos útiles para recolectar datos sobre la producción de huevos, los cuales se usan manualmente y los datos se transmiten inmediatamente al corporativo.



■ III.2 [Alvear Palace Hotel]

El Alvear Palace Hotel ubicado en Buenos Aires, Argentina cuenta con una estructura arquitectónica que data del año de 1932. Este Hotel implementó en 1999 por primera vez en sus instalaciones una red inalámbrica para dar conectividad a sus clientes de forma limitada.

Para el año 2003, el hotel se dio cuenta de que los 4 Access Points que había instalado eran insuficientes, por lo que era necesario expandir el alcance de la red y permitir el acceso móvil a Internet desde todas las habitaciones. Necesitaban ofrecer servicios de última generación sin alterar la integridad del edificio histórico.

Con el fin de lograr su objetivo, el hotel realizó una investigación entre distintos vendedores, comparando funcionalidad y costos, el resultado de esta investigación fue satisfactorio para 3com, pues instaló 24 Access Point Wireless LAN AP 6000, un Wireless LAN Workgroup Bridge, un Ethernet Client Bridge y 6 tarjetas inalámbricas. Estos Access Points fueron distribuidos en los 8 pisos de habitaciones que se encuentran en el hotel.

Cada AP provee conectividad de hasta 100m, dando oportunidad hasta 65 usuarios de estar conectados a la red al mismo tiempo.

Lo único que tienen que hacer los huéspedes para poder disponer de este servicio, es solicitar en la recepción una tarjeta inalámbrica y un código de acceso.

La instalación se llevó a cabo en dos semanas, incluyendo el cableado; se llevaron a cabo pruebas de radiación y además se capacitó al personal del hotel para poder brindar el servicio.

El hotel tiene pensado instalar otros equipos inalámbricos en el bar y el área de restaurantes, para hacer que sus huéspedes aprovechen al máximo su estadía y facilitar su trabajo.

■ III.3 [Florida Hospital]

El hospital de Florida, comprende una red de 17 hospitales y 12 centros de cuidado intensivo que atienden a más de 1 millón de pacientes cada año. Este hospital ofrece una amplia gama de especialidades como son, cardiología, oncología, neurología, trata la diabetes y da rehabilitación física.

El hospital quería aprovechar los avances de la tecnología inalámbrica para mejorar y facilitar el servicio a los pacientes, mejorando el control de los registros en el hospital.

Debido a que la red del hospital de Florida, está basada en productos de Cisco (routers y switches), decidieron adquirir los equipos inalámbricos del mismo fabricante, para aprovechar al

máximo sus equitos. Los elementos principales que conforman su red inalámbrica son Cisco Aironet 1200 Access Points, Cisco Aironet 350 Series y 1400 Series Wireless bridges.

Los equipos Cisco Aironet 1200 series, se utilizaron para cubrir los 7 edificios del hospital, Los Aironet 350 Series se utilizan para conectar 90 sitios del centro de datos del hospital. Y el Aironet 1400 Series permite comunicar un sitio remoto al hospital por medio de un enlace a 54Mbps.

Los Aironet 1200 series soportan autenticación 802.1x, además de incluir LEAP (Extensive Authentication Protocol),

Debido a que la seguridad es muy importante por el tipo de datos que se manejan en el hospital se utiliza Cisco LEAP, IEEE 802.1x para autenticarse en un servidor y solo permitir la entrada a la red al personal necesario.

Además de eso utilizan una solución que ofrece Cisco WSLE (Cisco works Wireless LAN Solution Engine) para controlar a todos los equipos inalámbricos. Esta herramienta provee un control centralizado de los equipos, brinda capacidades de configuración además de que permite manejar a un número muy grande de APs y bridges. Entre sus funciones principales están: monitorear al servidor LEAP, aplicar políticas de seguridad a cada AP, detectar desconfiguraciones en los equipos (APs y bridges), monitorear problemas en la red y las pérdidas en la eficiencia que pudieran presentarse por interferencia.

Los equipos tienen la característica de soportar power-in-line, lo que significa que por el mismo cable UTP por el que se transmiten los datos, se suministra la corriente eléctrica. Esta es una ventaja pues no es necesario poner tomas de corriente eléctrica a lo largo del edificio en cada lugar en el que se coloque un equipo.

Más de 14000 usuarios tienen acceso a la red inalámbrica del hospital, teniendo a lo largo del hospital 7000 laptops utilizadas para proveer servicios clínicos, y monitorear los datos de cada paciente en tiempo real, mientras recorren cuarto por cuarto.

■ III.4 [Aeropuerto de Sydney]

El aeropuerto de Sydney opera desde el año de 1920, y cubre un terreno de 907 hectáreas, Es el aeropuerto comercial más usado en Australia, tanto en vuelos nacionales como internacionales. En el año 2000 el AIC (Airport International Council) recomendó que los operadores de los aeropuertos deberían de tener el control del uso de los sistemas inalámbricos, tanto dentro como fuera de sus terminales aéreas. El objetivo es tener una sola infraestructura para todos los servicios inalámbricos.

Se desea una WLAN que pueda servir tanto a las aplicaciones operacionales, como para brindar accesos públicos a los clientes. Este tipo de organización es mucho más controlada, pues previene de tener múltiples redes inalámbricas instaladas, lo que podría ocasionar problemas en la seguridad, puntos sin coberturas y posibles ataques de hackers por sitios inseguros.



El aeropuerto de Sydney implementó equipos CISCO para este proyecto. La red cubre pistas de aterrizaje, edificios auxiliares y las terminales.

La red inalámbrica es una extensión de la red ATM del aeropuerto y toda la infraestructura y su control están a cargo de los administradores del aeropuerto. Esta estructurada de tal manera que ofrezca una disponibilidad de 99.6%, ya que tiene altos niveles de redundancia.

Más de 150 equipos Cisco Aironet 350 Series están distribuidos a lo largo del aeropuerto para lograr cobertura en todas las terminales y en un número de edificios cercanos a las pistas de aterrizaje y arrastre.

Los equipos Cisco 1100 se utilizan en el interior dentro de la Terminal nacional y los Cisco 1200 se utilizan para áreas exteriores, pues se les adaptaron antenas con mayor ganancia para cubrir los hangares y otras estructuras del campo de aviación.

Los APs 1200 pueden tener antenas externas instaladas lo que ayuda a ampliar la cobertura de la señal radiada.

Desde que se implementó la red, prácticamente no han tenido problemas con los equipos. La red se utiliza para dirigir y organizar el mantenimiento, además de ayudar en el manejo del tráfico aéreo en las pistas.

Debido a que la red también puede ser arrendada, el aeropuerto está negociando con diversas aerolíneas con el fin de utilizar la WLAN para el reconocimiento y control del equipaje, y con proveedores de servicios de Internet con el fin de brindar acceso en las áreas de Ascenso y Descenso de pasajeros así como en los principales restaurantes y tiendas ubicadas dentro de sus instalaciones.

■ III.5 [Aeropuertos y Servicios Auxiliares]

Es una organización estatal que se encarga principalmente de la distribución de turbosina y gasavión en diversos aeropuertos del país. En sus instalaciones se han visto beneficiados en varias áreas gracias a la aplicación de sistemas inalámbricos.

Algunas de sus principales aplicaciones son las siguientes:

- Aula de capacitación

Se disponía de un aula sin servicios en la que se tenían que instalar diez equipos de cómputo y conectarlos en red. Se instalaron tomas de energía eléctrica para cada equipo, pero resultaba muy difícil instalar la red eléctrica y la red de datos, además la instalación de canaleta y tubería afectaba la estética del lugar. Se comparó el costo de instalación de la red cableada con el de la red inalámbrica y fue mucho más rentable y práctico adquirir el equipo inalámbrico que montar una red tradicional.

RED CABLEADA		RED INALÁMBRICA	
CANTIDAD	PRECIO POR NODO	CANTIDAD	PRECIO
10 nodos	200 USD	1 nodo	200 USD
		1 Access Point	200 USD
		10 tarjetas inalámbricas	800 USD
TOTAL	2000 USD	TOTAL	1200 USD

Ahora cuentan con un aula que presta los servicios necesarios, es flexible en cuanto a la organización física de los equipos, puede dividirse de acuerdo a las necesidades y además ahorraron puertos de switch y de patch panel.

• Servicio de telefonía IP inalámbrico

ASA tiene un campus bastante amplio y la mayoría de los funcionarios realizan su trabajo fuera de su oficina pero dentro del campus. Esto implica que si se necesita localizar a un funcionario alguien deberá marcarle a su teléfono celular, este hecho incrementa el número de llamadas que se hacen, además de que refleja un gasto mensual de llamadas a celular de hasta \$2000 por funcionario.

Puesto que el objetivo es optimizar los recursos se aprovechó la infraestructura inalámbrica existente (que cubre todo el campus) y se adquirieron teléfonos IP inalámbricos.

Estos teléfonos funcionan exactamente igual que un teléfono celular dentro de las instalaciones de ASA, pues se conectan a la red inalámbrica y así es posible localizar a la persona con solo marcar una extensión, ahorrándose las llamadas a celular.

• Proyecto AVR-2000 (Estaciones de Combustible)

Las estaciones de combustible se encuentran en cada uno de los aeropuertos, y su función es tener un control de la facturación de turbosina y gasavión.

En la mayoría de los casos existe una distancia de hasta 3Km entre el aeropuerto y las estaciones de combustible.

El principal problema, era comunicar ambos sitios para fines de recolección y envío de datos, facturación, recepción de correo electrónico; además de realizar consultas a PEMEX.

Se pensaron varias opciones para solucionar este problema, una fue tender fibra óptica, pero el costo era demasiado alto; otra fue instalar un MODEM, pero el servicio era muy lento, así que se optó por instalar tecnología inalámbrica.



III. APLICACIONES

El proyecto consiste en cubrir con antenas inalámbricas las plataformas donde cargan combustible los aviones, y proveer al vehículo que despacha el combustible con de una computadora y un equipo inalámbrico con el fin de conectarse a la estación de combustibles.



103

Foto. 1. Vehículo despachador de combustible

Para instalar el proyecto tuvieron que tomarse en cuenta las siguientes consideraciones:

- Deberían de instalarse equipos a lo largo del Aeropuerto, y debido a que las terminales aeroportuarias no pertenecen a ASA, sino a una empresa diferente, el servicio de energía eléctrica no fue proporcionado
- Debería manejarse una frecuencia que no provocara interferencia de comunicación entre el avión y la torre de control.

La solución que se instaló fue la siguiente:

Se diseñó un sistema con celdas solares, para proveer a los equipos inalámbricos la energía suficiente para trabajar sin necesidad de estar conectados a la red eléctrica.



Foto 2. Celda Solar



Foto 3. Celda Solar

Se instalaron equipos de la marca Enterasys RBTR2-AZ que soportan dos radios inalámbricos.



Foto 4. Equipo inalámbrico.

Un radio se ocupó para conectar a todos los puntos instalados a lo largo del aeropuerto (enlace punto multipunto). Para realizar estos enlaces se ocuparon antenas direccionales en los puntos remotos y una antena omnidireccional en el punto central



Foto 5. Antenas direccionales tipo yagui

El otro radio se utilizó para radiar la plataforma, con una antena sectorial.



Foto 6. Antena Sectorial



Foto 7. Antena Sectorial y Antena Yagui





Foto 8. Antena omnidireccional.

El número de equipos instalados varió de acuerdo al tamaño del aeropuerto y el número de posiciones que se necesitaban cubrir. El estándar que se utilizó fue 802.11b, que trabaja en la frecuencia de 2.4GHz y no provoca interferencia entre las comunicaciones del avión y la torre de control. La instalación tardó aproximadamente un mes.

El sistema funciona de la siguiente manera: la unidad móvil que suministra el combustible acude a alguna de las posiciones en la plataforma, carga al avión y transmite inalámbricamente los datos al equipo remoto que cubre esa zona específica de la plataforma. El equipo remoto está conectado a la red LAN y entrega los datos a la estación de combustibles para imprimir las facturas y realizar consultas sobre los próximos servicios.

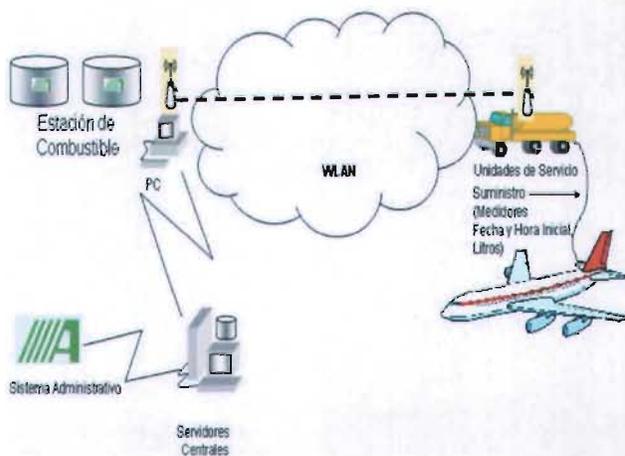


Figura III.5. Diagrama general del sistema.



IV [PROYECTO PARA LA IMPLEMENTACIÓN DE UNA red inalámbrica]



■ IV.1 [Objetivo del proyecto]

Definir el objetivo del proyecto en base a las necesidades del cliente: “La FES Cuautitlán desea ofrecer servicio de Internet a sus estudiantes en las áreas más concurridas, para lo cual pretende establecer un servicio de red inalámbrica”

OBJETIVO:

Implementar un servicio de acceso público a Internet (Hot spot) en la sala de consulta de la planta alta de la Biblioteca, y en la explanada ubicada entre los edificios de Gobierno, Servicios Escolares y Biblioteca de la Facultad de Estudios Superiores Cuautitlán Campus 4, con el fin de brindar al alumnado y a sus académicos una herramienta más que les ayude en el desempeño de sus actividades diarias.

Se eligieron esta zonas porque es en donde se reúne una mayor cantidad de usuarios.

Debido a que la mayoría de los equipos (PDAs y laptops) utilizan el estándar 802.11b se optó por implementarlo en esta red, pues es el más popular y conocido por el momento.

Considerando que la velocidad ofrecida por el mismo (11Mbps) es suficiente para cubrir las necesidades de los usuarios.

■ IV.2 [Diseño del proyecto]

Una vez definidos los objetivos, debemos de recolectar información básica para empezar a diseñar el proyecto. Se hace una lista de las actividades principales, con el fin de definir una serie de pasos a seguir.

El siguiente cronograma de actividades, muestra las principales actividades realizadas a lo largo del proyecto, así como su fecha de inicio y de término.

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Id	Nombre de tarea	Duración	Comienzo	Fin	10 abr '05							17 abr '05							24 abr '05						
					L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D
1	PROYECTO DE IMPLEMENTACION DE RED INALAMBRICA	17 días	mié 13/04/05	jue 28/04/05																					
2	Iniciación	8.5 días	mié 13/04/05	mié 20/04/05																					
3	Planteamiento del Problema	1 día	mié 13/04/05	mié 13/04/05																					
4	Propuesta de solución	1.25 días	mié 13/04/05	jue 14/04/05																					
5	Recorrido por el sitio	2 horas	mié 13/04/05	mié 13/04/05																					
6	Site Survey	1 día	jue 14/04/05	jue 14/04/05																					
7	Presentación y Aceptación de la propuesta	1 día	mié 20/04/05	mié 20/04/05																					
8	Planeación	6.5 días	mié 20/04/05	mar 26/04/05																					
9	Selección del Hardware	1 día	jue 21/04/05	jue 21/04/05																					
10	Compra de equipos	5 días	vie 22/04/05	mar 26/04/05																					
11	Compra de Materiales	2 días	vie 22/04/05	sáb 23/04/05																					
12	Solicitud de Permisos	1 día	mié 20/04/05	jue 21/04/05																					
13	Contactar a los instaladores	2 horas	mié 20/04/05	mié 20/04/05																					
14	Ejecución	1 día	mié 27/04/05	mié 27/04/05																					
15	Instalación de equipos y antena	1 día	mié 27/04/05	mié 27/04/05																					
16	Toma de fotografías	1 hora	mié 27/04/05	mié 27/04/05																					
17	Configuración de equipos	1 hora	mié 27/04/05	mié 27/04/05																					
18	Pruebas	2 horas	mié 27/04/05	mié 27/04/05																					
19	Cierre	1 día	mié 27/04/05	jue 28/04/05																					
20	Entrega de memoria técnica	1 día	mié 27/04/05	jue 28/04/05																					

IV.2.1 [Cronograma de actividades]

Proyecto: Implementación de una red inalámbrica Fecha: Abril 2005	Tarea		Hito		Tareas externas	
	Ornación		Resumen		Hito externo	
	Progreso		Resumen del proyecto		Fecha límite	

■ IV.2.2 [Propuesta de solución]

a) Evaluación del sitio

Empezaremos por analizar el área que es necesario cubrir, tomar en cuenta cuantos edificios requieren de cobertura inalámbrica, si todos los pisos de los edificios o solo ciertas oficinas o aulas se van cubrir, si las áreas externas a estos edificios van a tener cobertura también, etc.

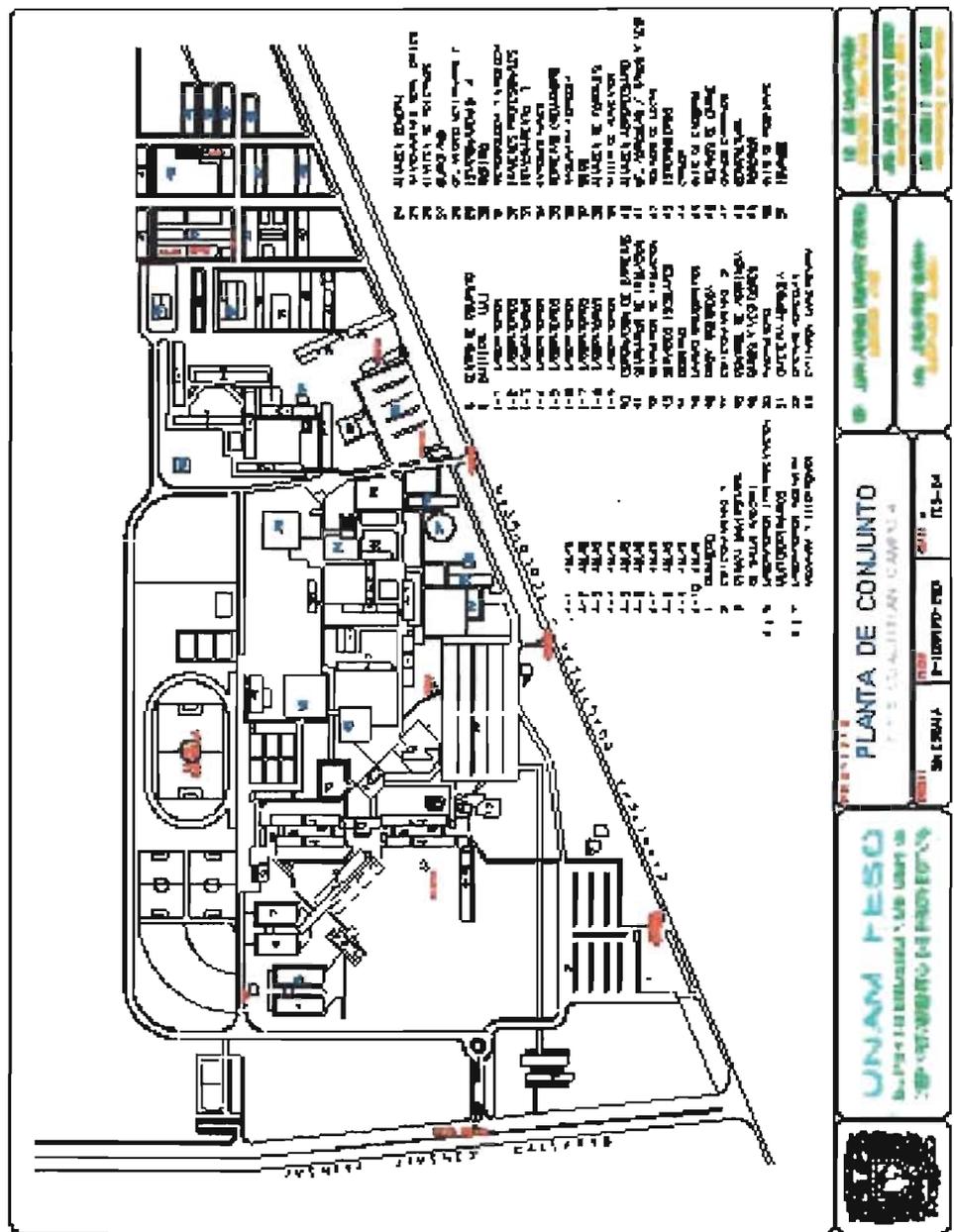
Es necesario tomar fotografías del sitio y obtener los planos arquitectónicos de los edificios y áreas externas, para poder marcar o determinar junto con el cliente cuales son las áreas más importantes que requieren ser cubiertas.

La mayoría de los clientes solicitan cubrir totalmente el área determinada, lo que requerirá de un considerable número de equipos, y antenas; pero en algunos casos solo es necesario cubrir ciertas zonas como oficinas o áreas comunes.

Estas son las fotografías y el plano del sitio de la Biblioteca y la explanada que se desean cubrir en la FES Cuautitlán.

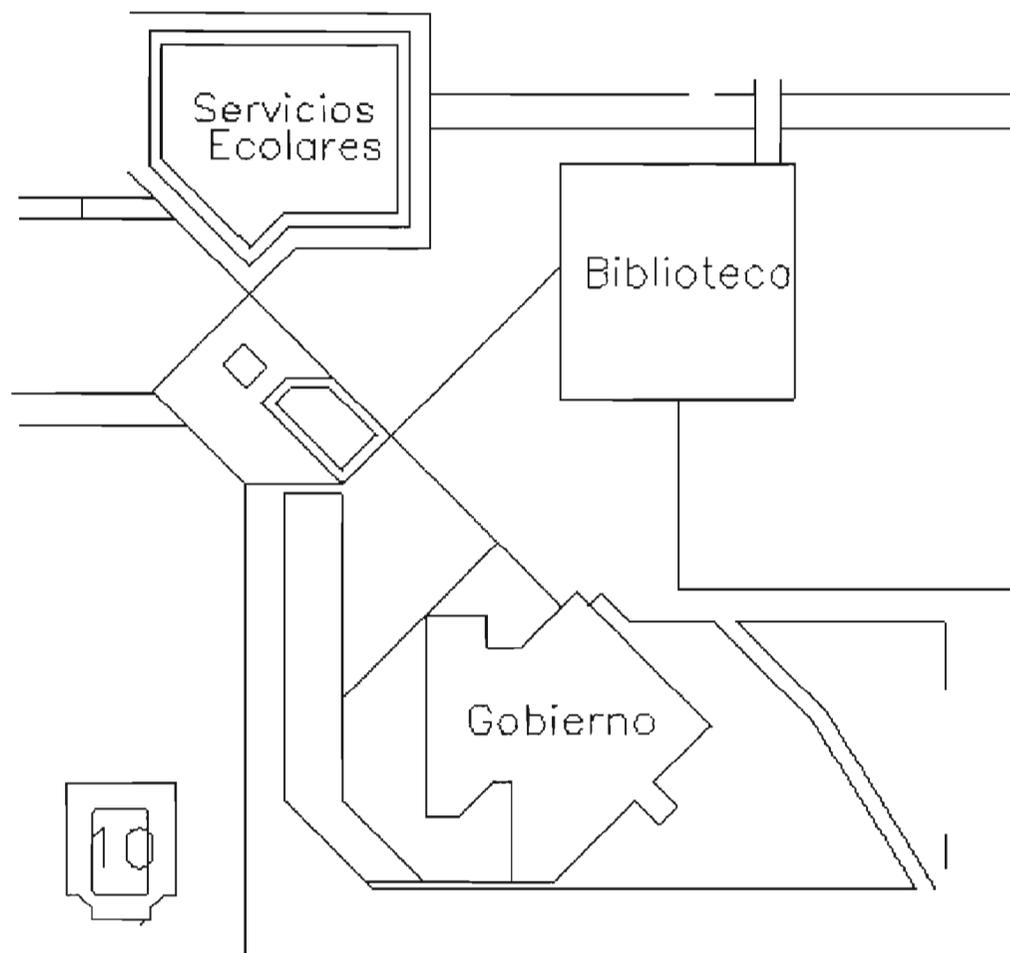
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALAMBRICA

• Planos del sitio
 PLANO DE LA FES CUAUTILTLAN



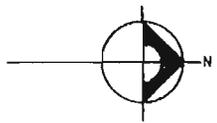
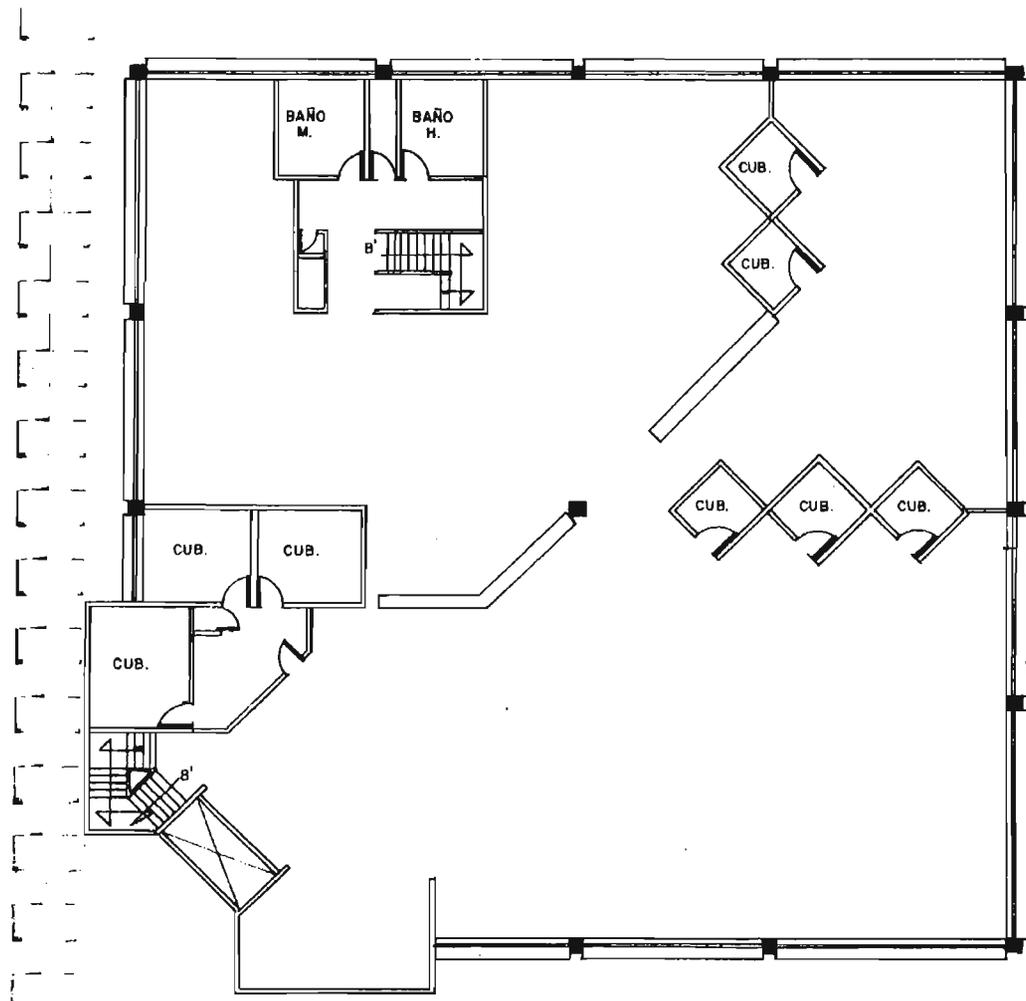
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

PLANO DE LA EXPLANADA





IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA



PLANO DE LA BIBLIOTECA PLANTA ALTA

BIBLIOTECA
PLANTA ALTA

FES CIAUTITLAN
CAMPO 4
ESC. 1-200
FECHA 98'

SUPERINTENDENCIA
DE OBRAS



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

- Fotografías del sitio

Una vez obtenidos estos datos, es necesario analizar que elementos podrían obstruir el paso de la señal, árboles, puertas de metal, las paredes del edificio, los elevadores, etc.

En el caso de la biblioteca, los estantes de metal repletos de libros podrían absorber una gran parte de la señal. En el caso de la explanada, los árboles podrían absorber también la señal.

FOTOGRAFÍAS DE LA EXPLANADA (DIFERENTES VISTAS)



Vista 1. Explanada



Vista 2. Explanada frente a la biblioteca



Vista 3. Centro de la explanada

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

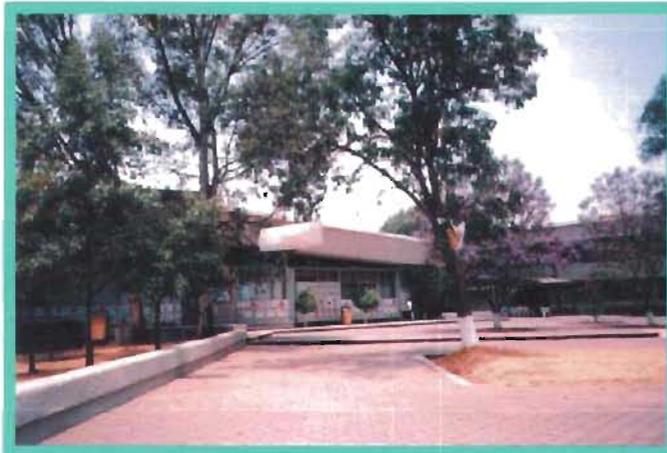
116



Vista 4. Edificio de Servicios escolares

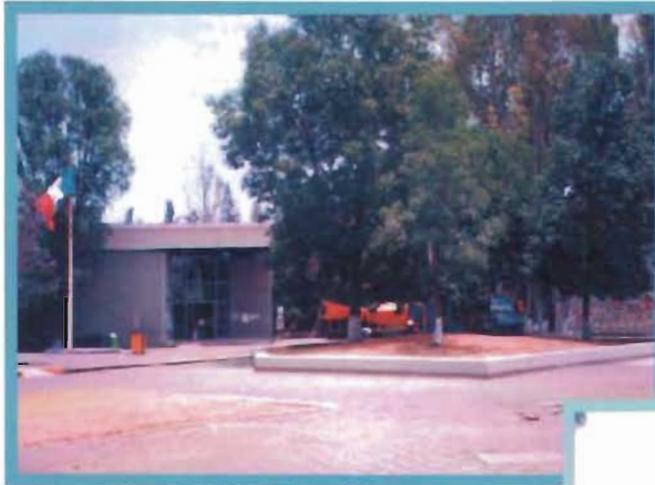


Vista 5. Edificio de Servicios escolares



Vista 6. Vista Edificio de Servicios escolares, y Biblioteca al fondo

FOTOGRAFIAS DEL EXTERIOR DE LA BIBLIOTECA



Vista 7. Edificio de la Biblioteca



Vista 8. Fachada principal de la Biblioteca

FOTOGRAFIAS DE LA SALA DE CONSULTA DE LA BIBLIOTECA INTERIOR



Vista 9. Sala de consulta planta alta de la biblioteca

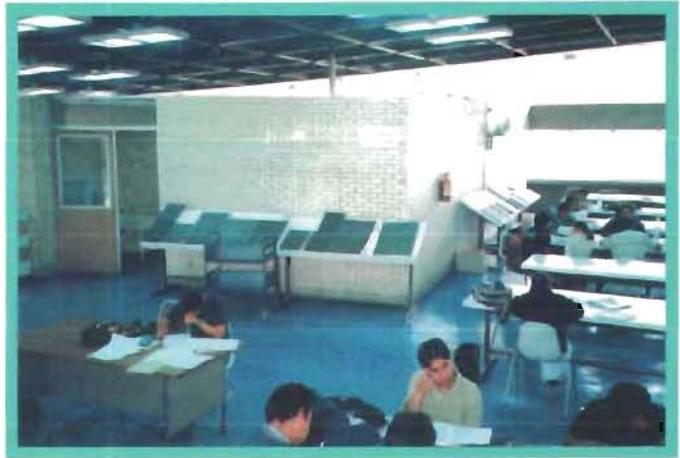


IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

118



Vista 10. Sala de consulta



Vista 11 Sala de consulta



Vista 12. Sala de consulta

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA



Vista 13. Sala de consulta



Vista 14. Sala de consulta



Vista 15. Sala de Consulta.



■ IV.2.1 [Pruebas de propagación]

Una vez evaluado el sitio, se hacen pruebas de propagación para analizar el comportamiento de la señal de manera específica en la zona y determinar de manera real la cobertura de un AP, con el propósito de determinar la cantidad de equipos necesarios y la mejor ubicación del equipo en el área. También nos servirá para determinar si es necesario instalar antenas externas a los equipos para proporcionarle a la señal una mayor ganancia.

Lo que se necesita para realizar estas pruebas es: una laptop con tarjeta de red inalámbrica (puede ser externa o integrada en el equipo), un software que mida la intensidad de la señal, y un AP.

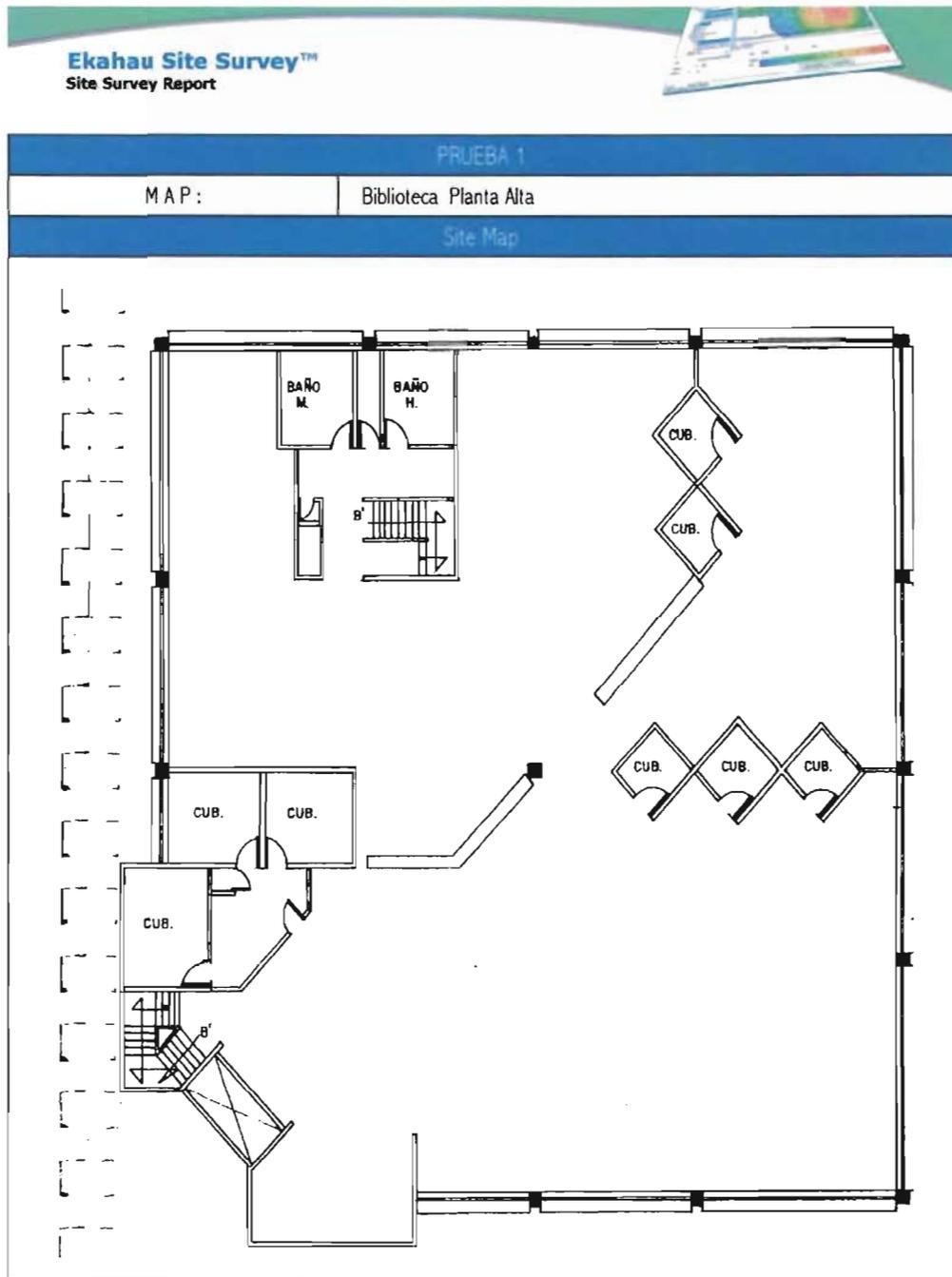
Para el caso específico de la FES Cuautitlán se realizaron pruebas de propagación con el software Ekahau Site Survey 2.1™. Este software permite agregar el plano de la zona con el fin de determinar gráficamente la intensidad de la señal conforme se va caminando por el área.

Se colocó el AP en diferentes posiciones, para determinar el comportamiento de la señal en cada uno de los puntos, y así seleccionar la mejor ubicación. Se realizaron 4 pruebas, 2 para el interior de la biblioteca y 2 para la explanada.

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

a) Prueba 1

El AP se colocó al centro de la biblioteca, al lado del pilar



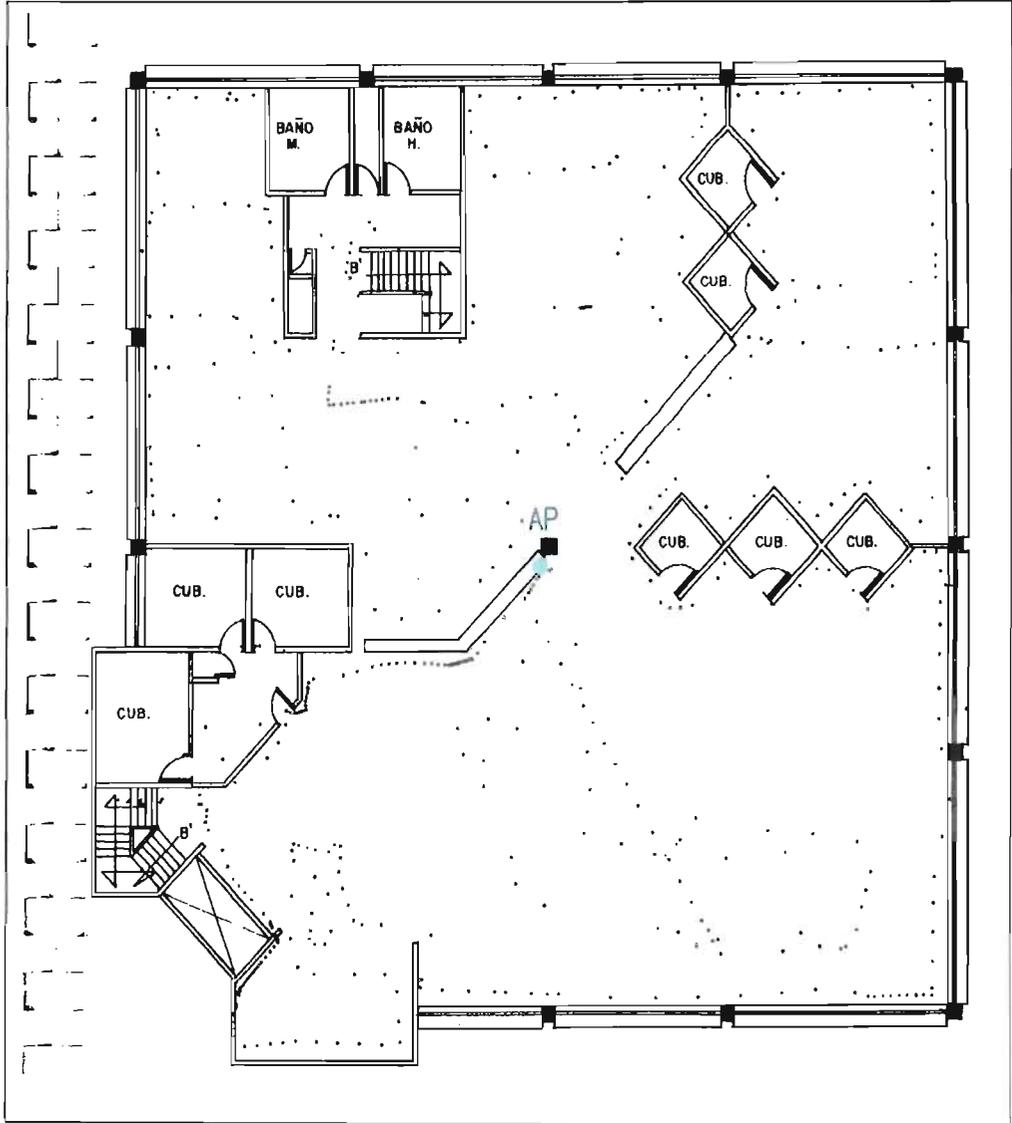
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

122

Access Point

ESSID	Name	Band / Channel	Privacy
cuautitlan	00:13:10:2A:CC:DB	802.11b/ 1	No

Puntos Muestreados y Ubicación del Access Point



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Fuerza de la Señal



Cobertura de la fuerza de la señal (RSSI) de los Access Points seleccionados. Se muestra la mayor intensidad por ubicación.

-100.0..-95.0	-95.0..-90.0	-90.0..-85.0	-85.0..-80.0	-80.0..-75.0	-75.0..-70.0	-70.0..-65.0



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Relación Señal a Ruido

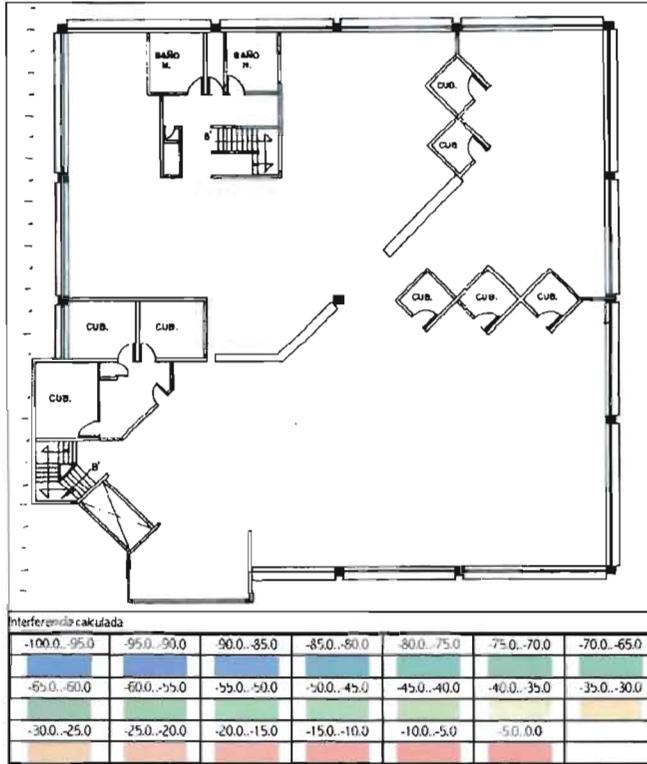


Relación señal a ruido calculada. Formula simplificada: $SNR = [Fuerza\ de\ la\ Señal] - [Interferencia]$

0.0..5.0	5.0..10.0	10.0..15.0	15.0..20.0	20.0..25.0	25.0..30.0
30.0..35.0	35.0..40.0	40.0..45.0	45.0..50.0	50.0..55.0	55.0..60.0
60.0..65.0	65.0..70.0	70.0..75.0	75.0..80.0		

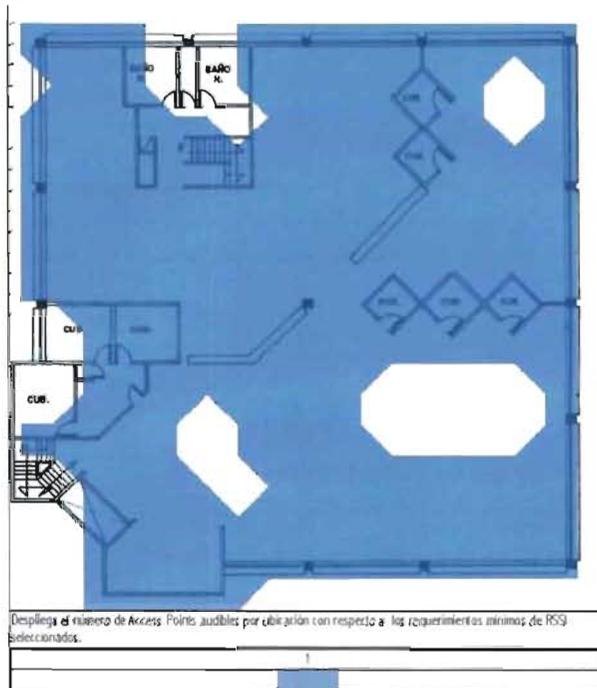
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Interferencia



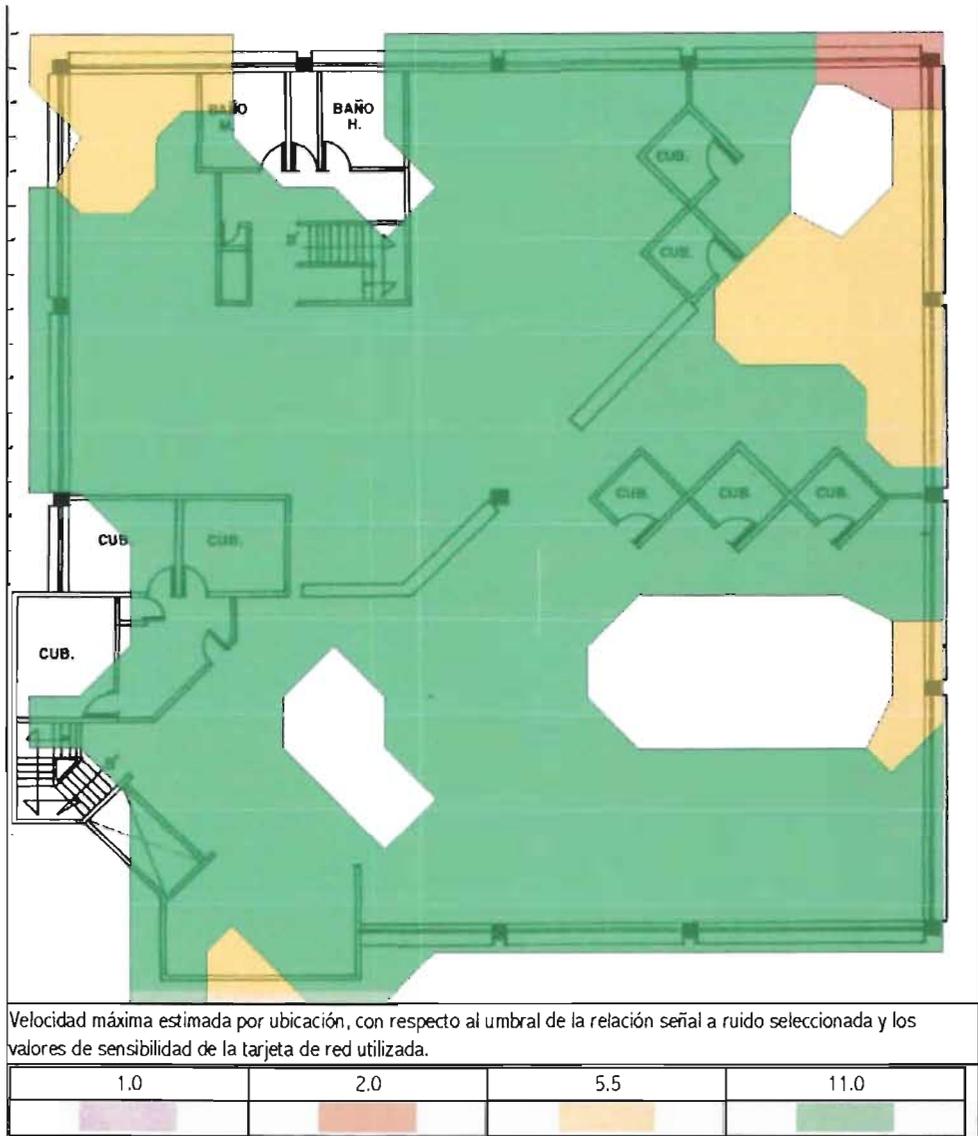
125

Cuenta de Access Point



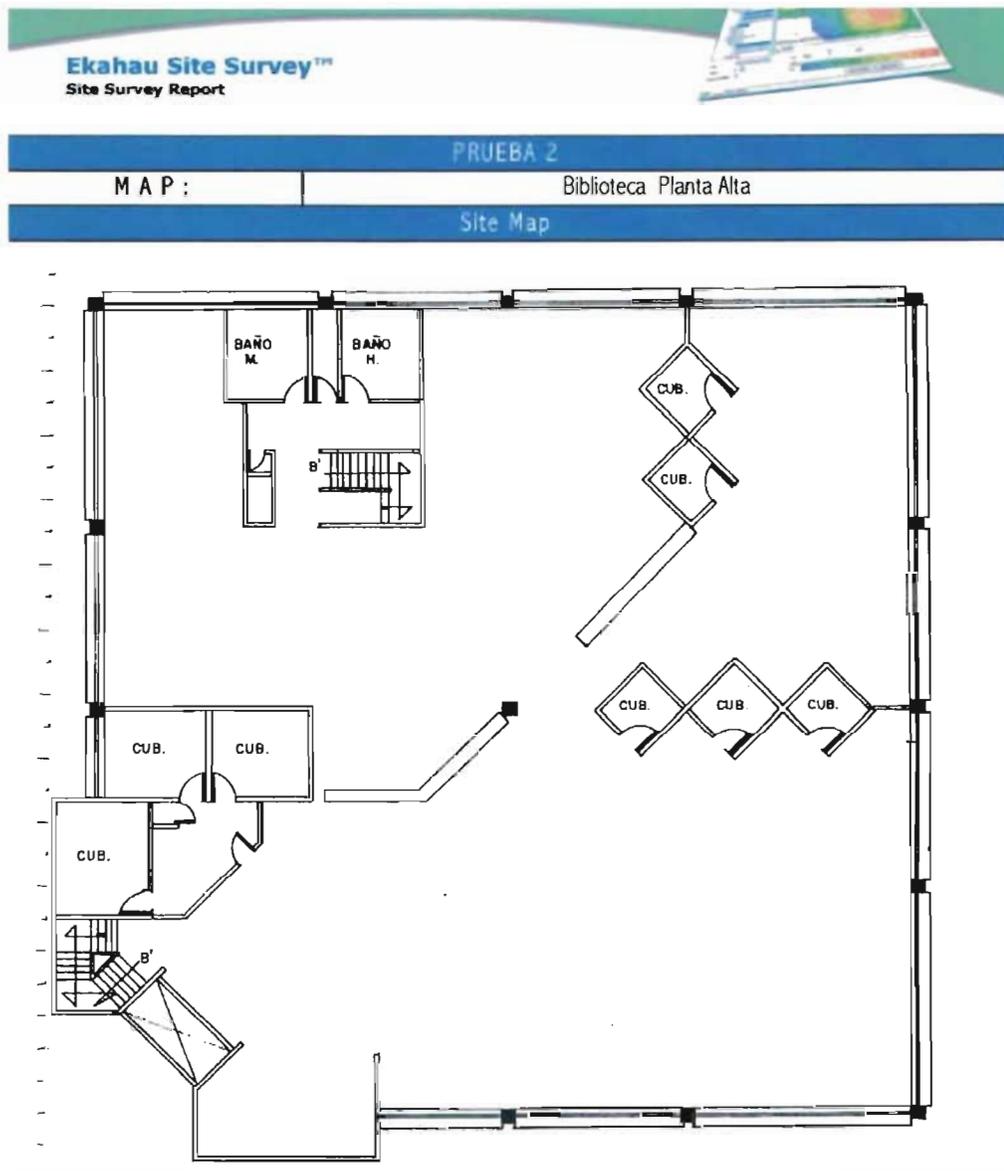
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Velocidades de Datos



b) Prueba 2

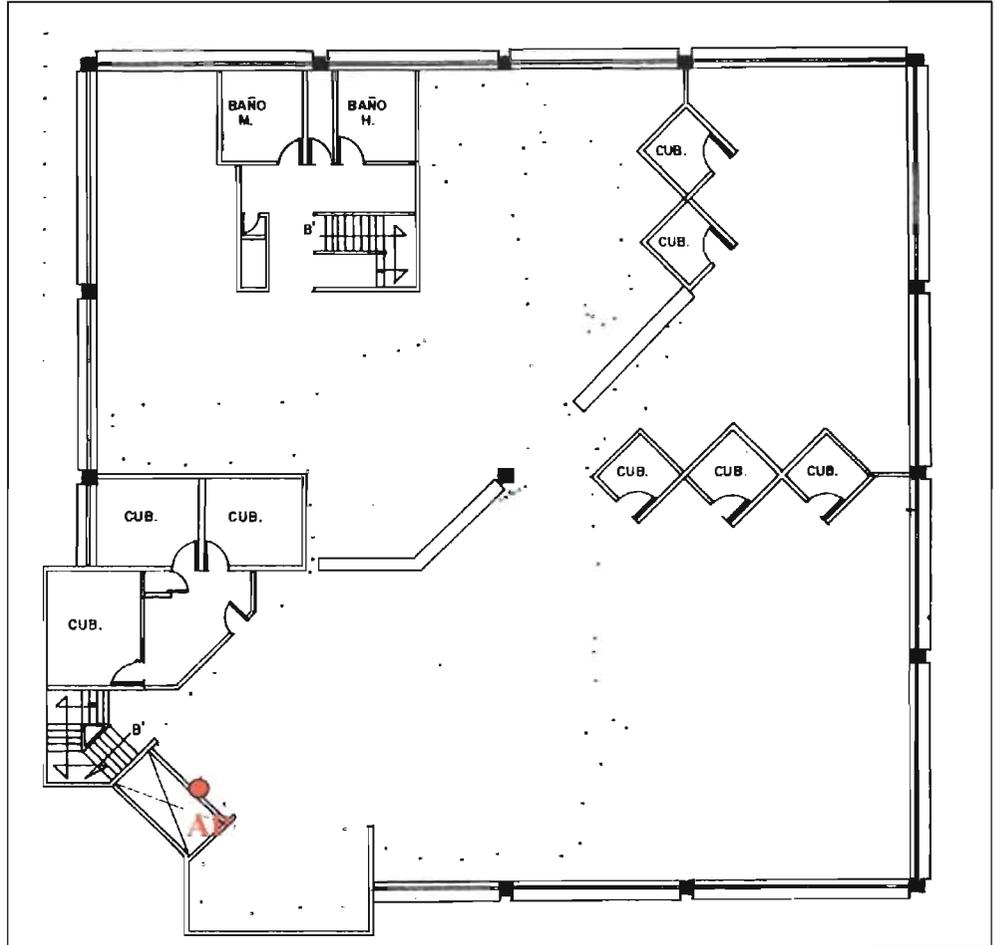
El AP se colocó al lado del ventanal que da hacia la entrada principal.



Access Point

ESSID	Name	Band / Channel	Privacy
cuautitlan	00:13:10:2A:CC:DB	802.11b/ 1	No

Puntos Muestreados y Ubicación del Access Point



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Fuerza de la Señal



Cobertura de la fuerza de la señal (RSSI) de los Access Points seleccionados. Se muestra la mayor intensidad por ubicación

-100.0..-95.0	-95.0..-90.0	-90.0..-85.0	-85.0..-80.0	-80.0..-75.0	-75.0..-70.0	-70.0..-65.0
65.0..-60.0	-60.0..-55.0	-55.0..-50.0	-50.0..-45.0	-45.0..-40.0	-40.0..-35.0	-35.0..-30.0
-30.0..-25.0	-25.0..-20.0	-20.0..-15.0	-15.0..-10.0	-10.0..-5.0	-5.0..0.0	



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Relación Señal a Ruido

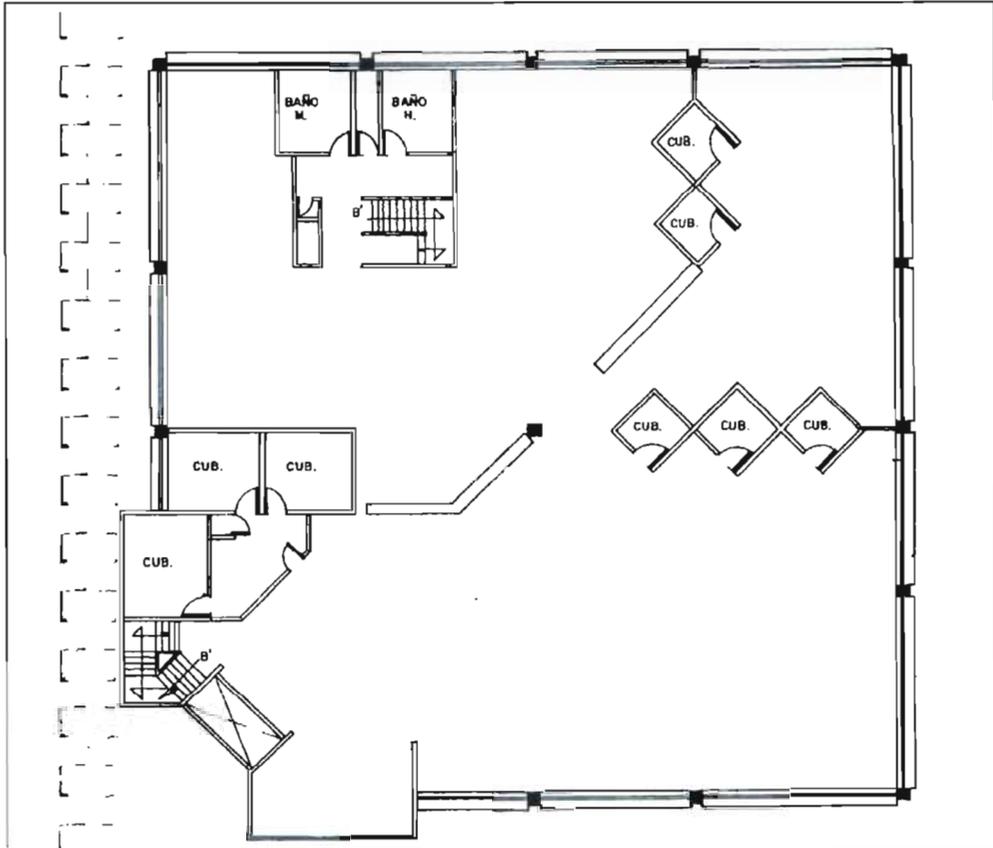


Relación señal a ruido calculada. Formula simplificada: $SNR = [Fuerza\ de\ la\ Señal] - [Interferencia]$

0.0..5.0	5.0..10.0	10.0..15.0	15.0..20.0	20.0..25.0	25.0..30.0
30.0..35.0	35.0..40.0	40.0..45.0	45.0..50.0	50.0..55.0	55.0..60.0
60.0..65.0	65.0..70.0	70.0..75.0	75.0..80.0		

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Interferencia

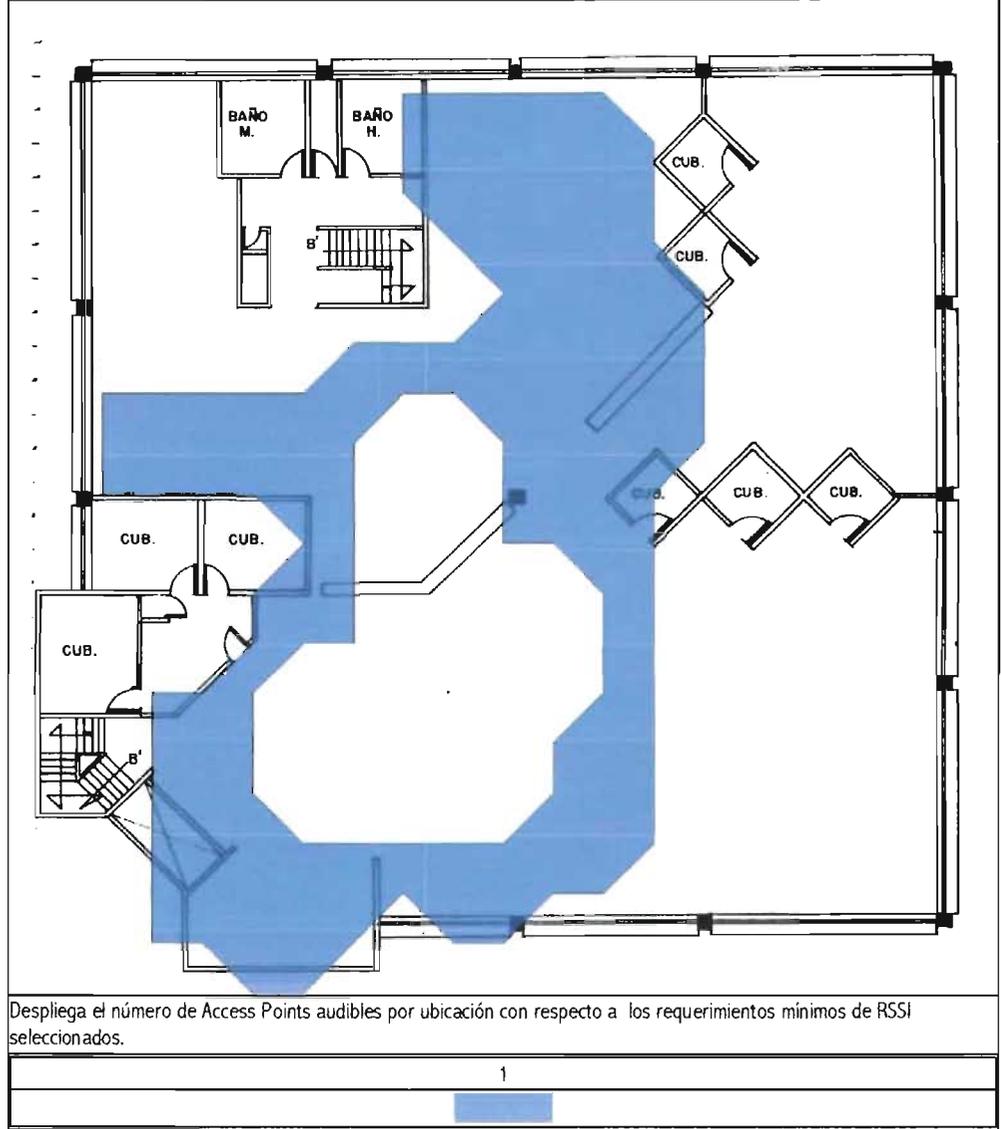


Interferencia calculada

-100.0..-94.1	-94.1..-88.2	-88.2..-82.4	-82.4..-76.5	-76.5..-70.6	-70.6..-64.7
-64.7..-58.8	-58.8..-52.9	-52.9..-47.1	-47.1..-41.2	-41.2..-35.3	-35.3..-29.4
-29.4..-23.5	-23.5..-17.6	-17.6..-11.8	-11.8..-5.9	-5.9..0.0	

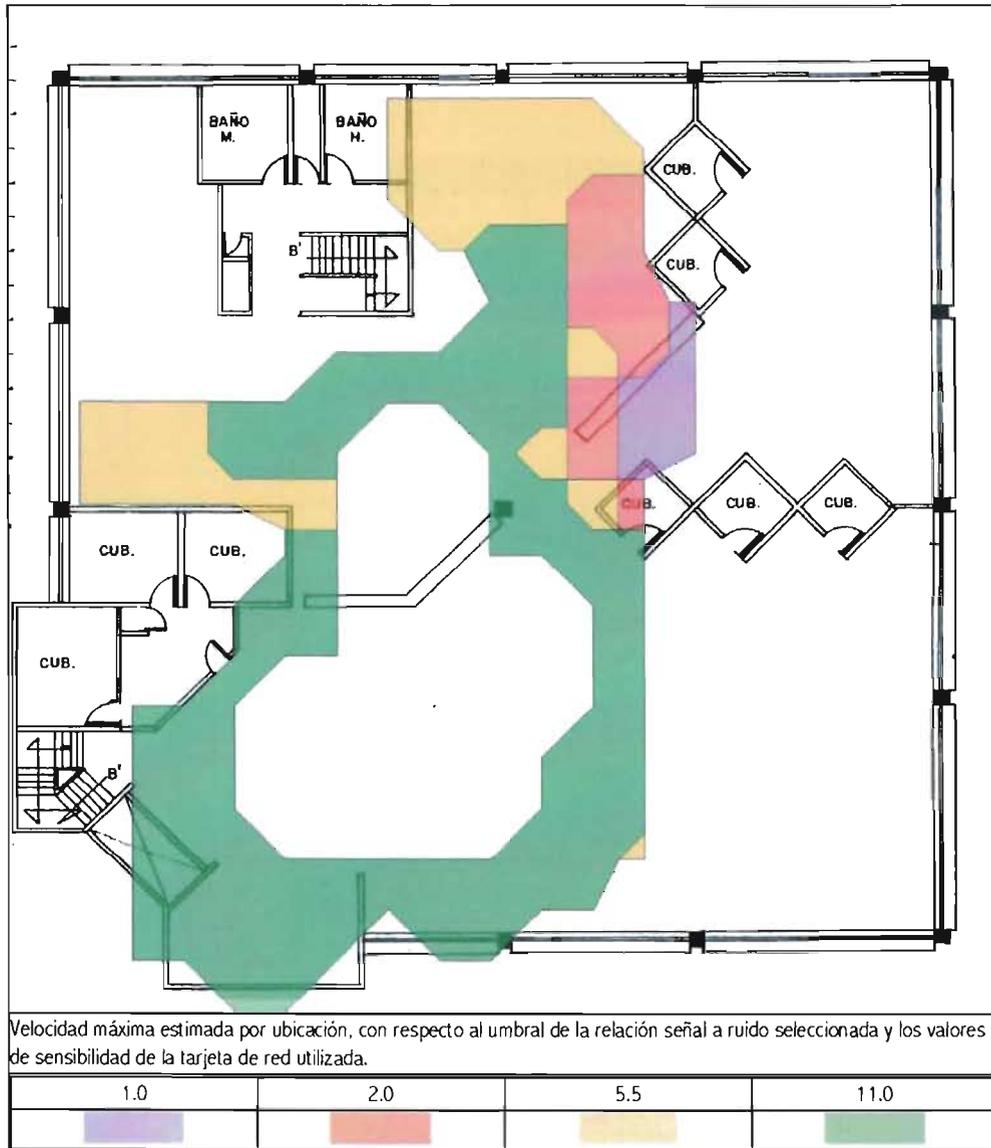
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Cuenta de Access Point



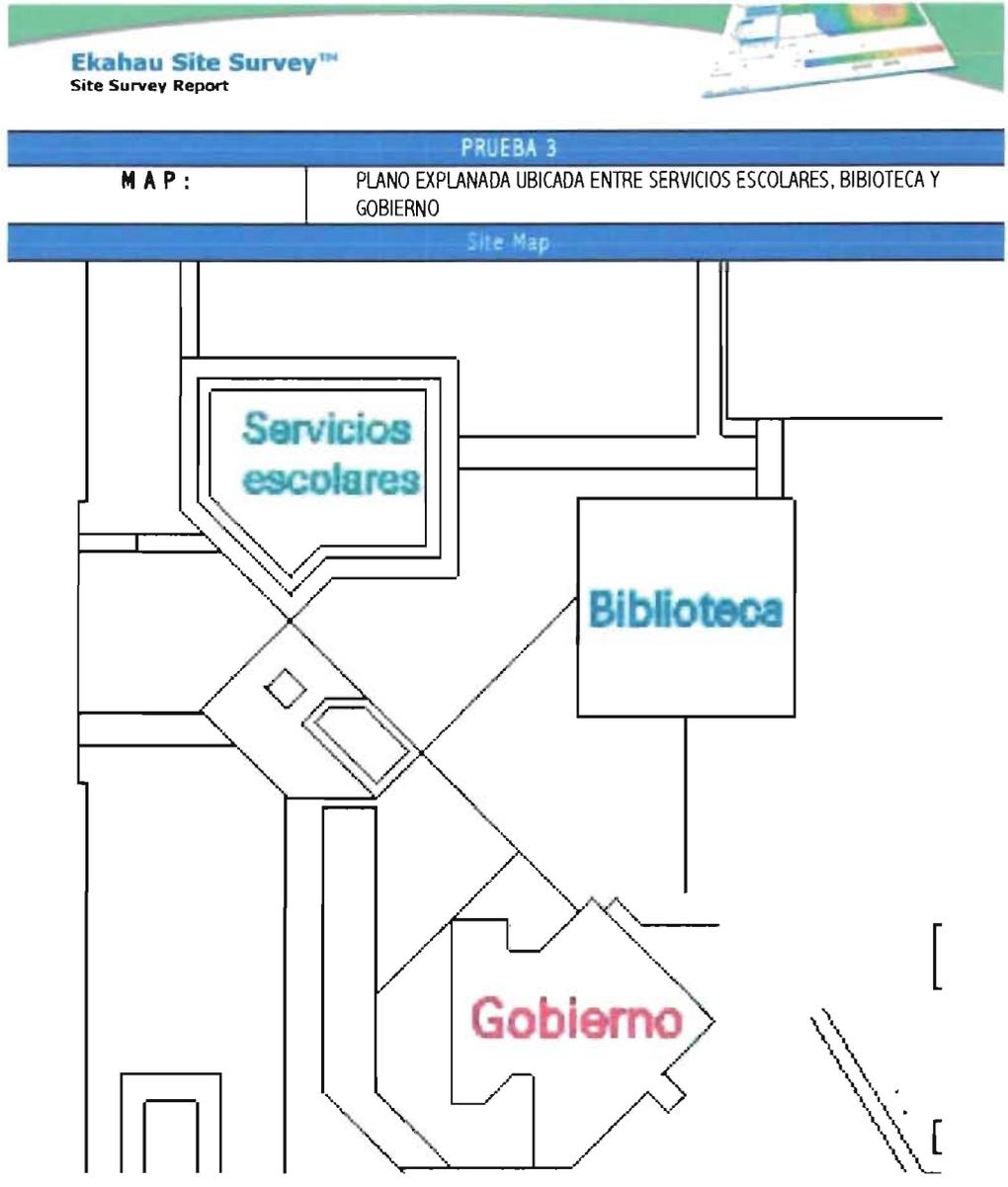
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Velocidades de Datos



c) Prueba 3

El AP se colocó al lado del ventanal que da hacia la entrada principal en la planta alta, para radiar en la explanada

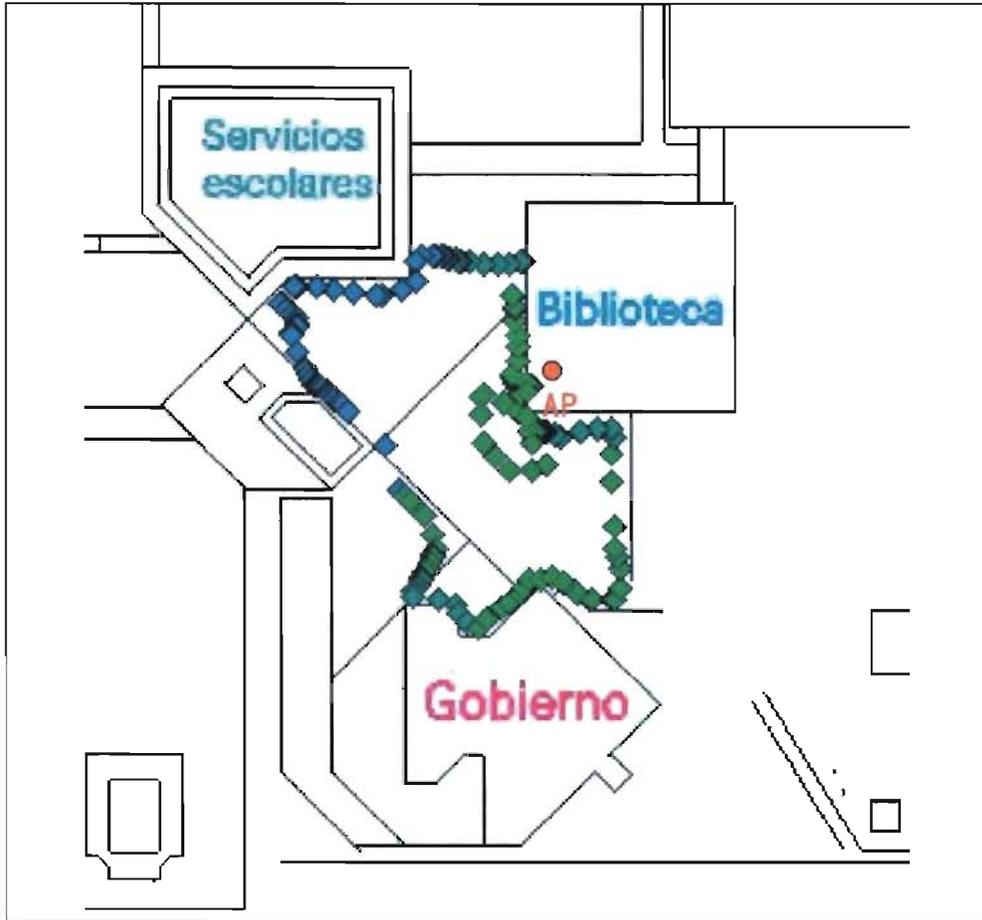


IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Access Point

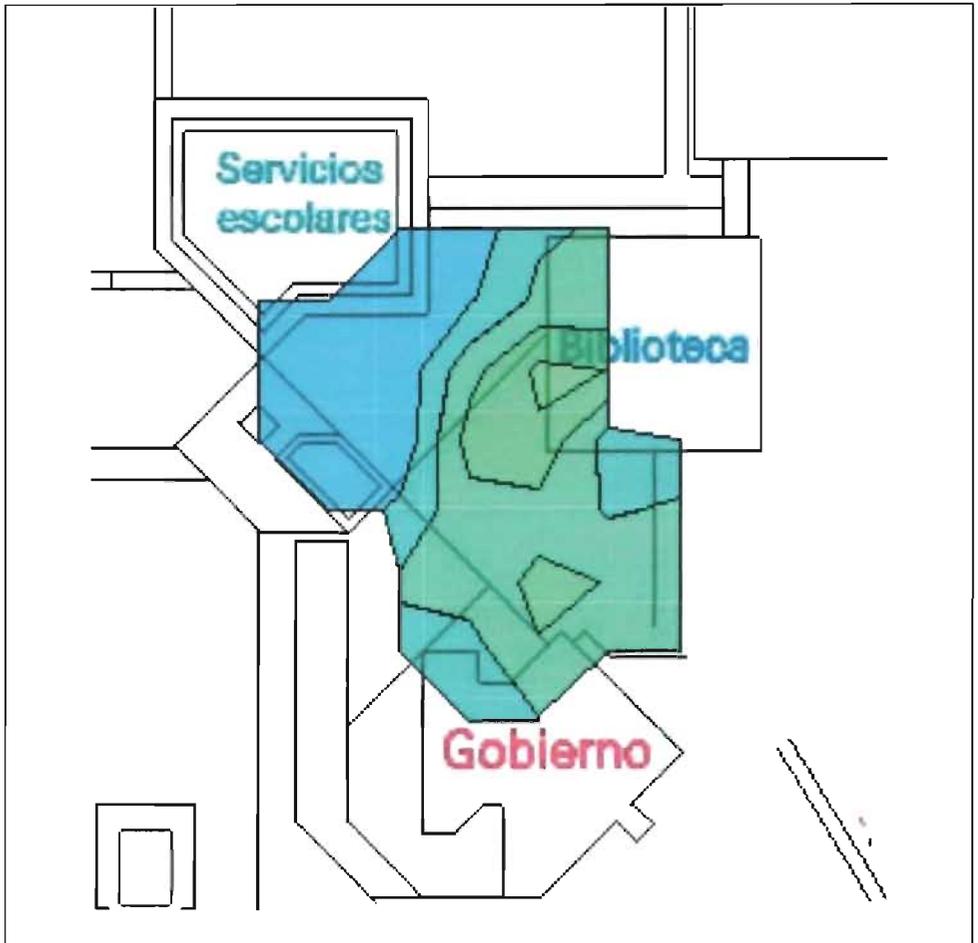
ESSID	Name	Band / Channel	Privacy
cuautitlan	00:13:10:2A:CC:DB	802.11b/ 1	No
suvimex	00:40:96:57:B2:33	802.11b/ 6	WEP

Puntos Muestreados y Ubicación del Access Point



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Fuerza de la Señal

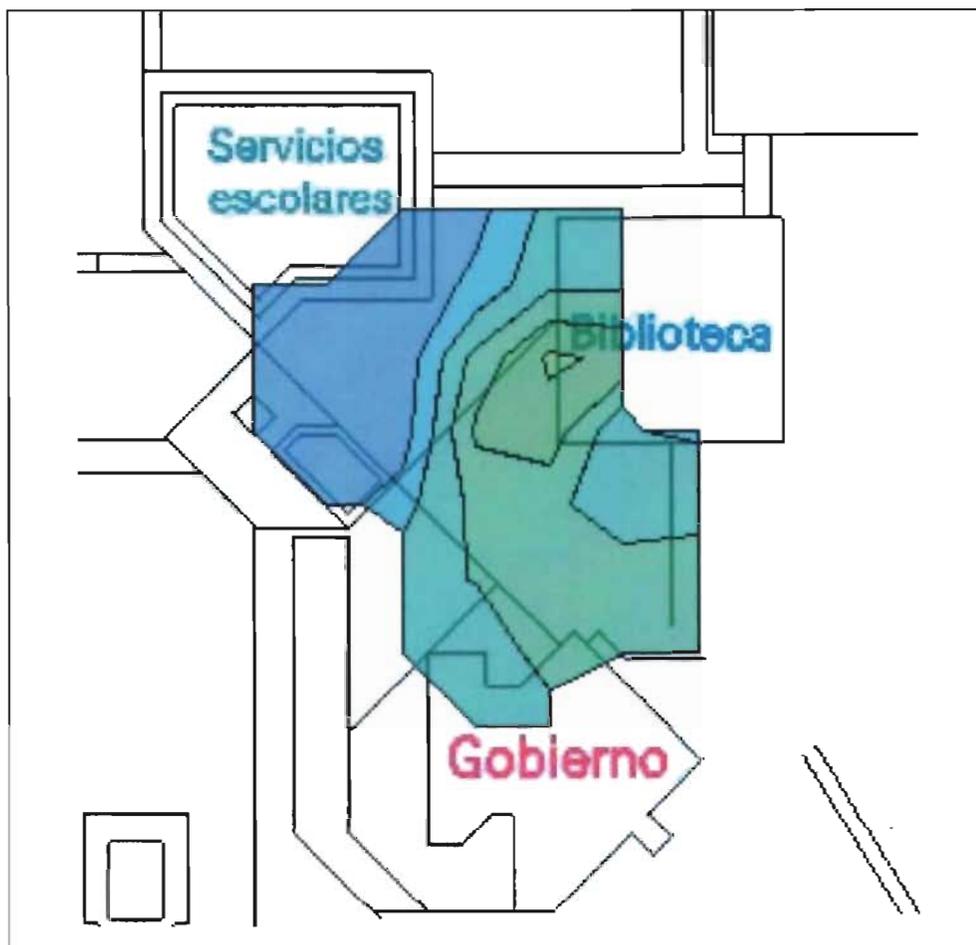


Cobertura de la fuerza de la señal (RSSI) de los Access Points seleccionados. Se muestra la mayor intensidad por ubicación.

-100.0..-95.0	-95.0..-90.0	-90.0..-85.0	-85.0..-80.0	-80.0..-75.0	-75.0..-70.0	-70.0..-65.0
65.0..-60.0	-60.0..-55.0	-55.0..-50.0	-50.0..-45.0	-45.0..-40.0	-40.0..-35.0	-35.0..-30.0
-30.0..-25.0	-25.0..-20.0	-20.0..-15.0	-15.0..-10.0	-10.0..-5.0	-5.0..0.0	

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Relación Señal a Ruido



137

Relación señal a ruido calculada. Formula simplificada: $SNR = [Fuerza\ de\ la\ Señal] - [Interferencia]$

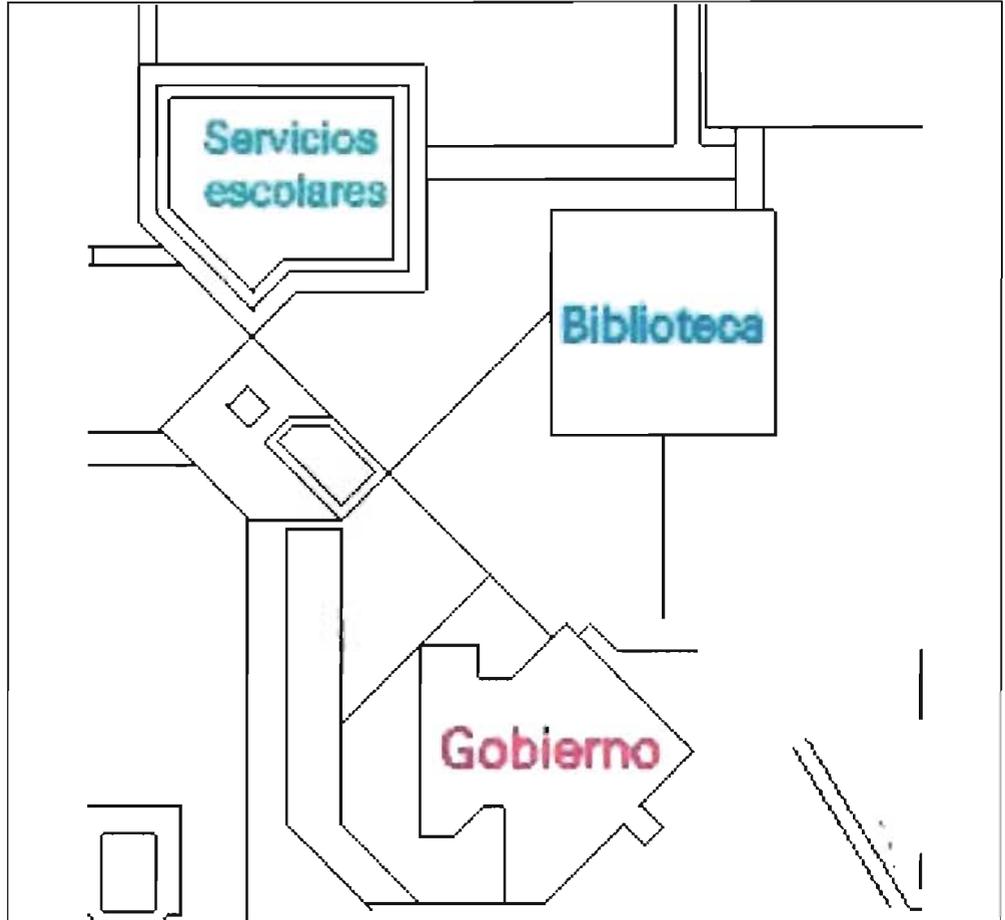
0.0..5.0	5.0..10.0	10.0..15.0	15.0..20.0	20.0..25.0	25.0..30.0
30.0..35.0	35.0..40.0	40.0..45.0	45.0..50.0	50.0..55.0	55.0..60.0
60.0..65.0	65.0..70.0	70.0..75.0	75.0..80.0		



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Interferencia

138

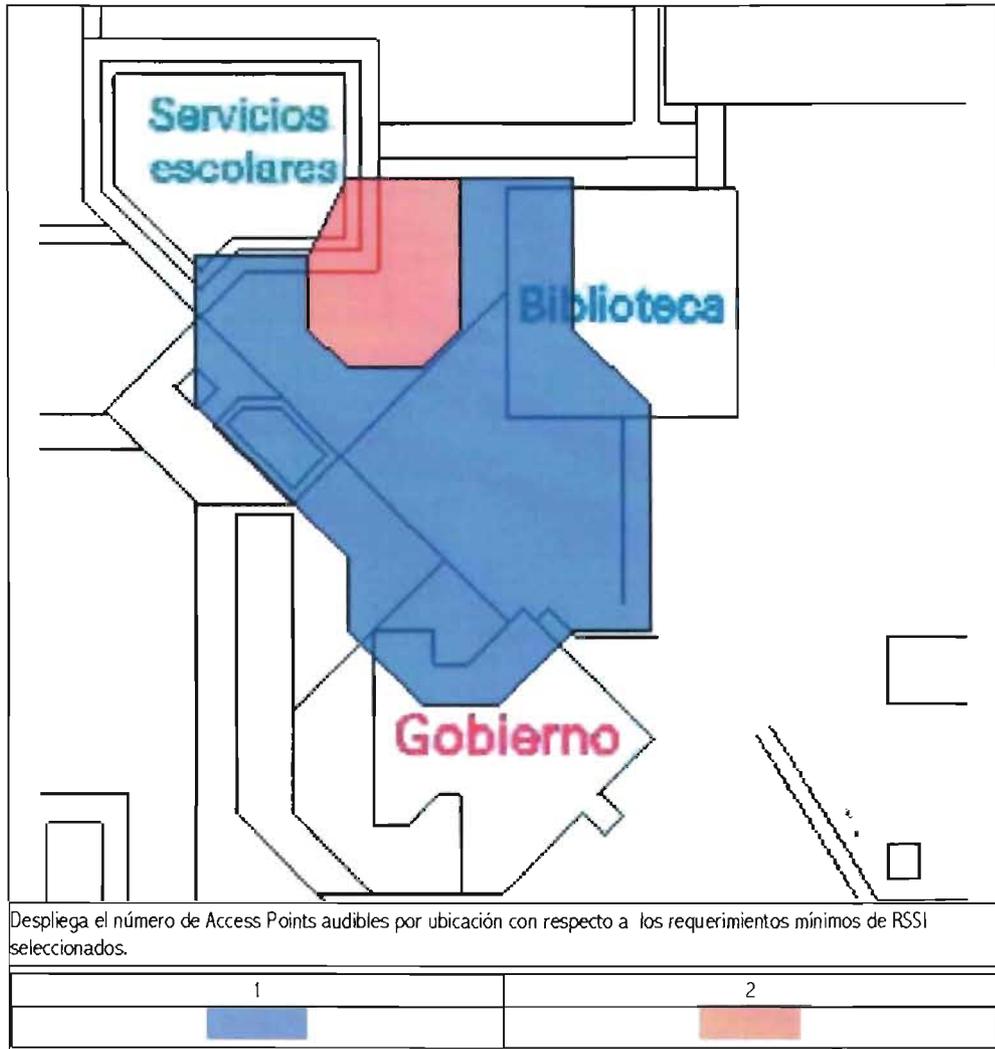


Interferencia calculada

-100.0...-95.5	-95.5...-90.9	-90.9...-86.4	-86.4...-81.8	-81.8...-77.3	-77.3...-72.7
-72.7...-68.2	-68.2...-63.6	-63.6...-59.1	-59.1...-54.5	-54.5...-50.0	-50.0...-45.5
-45.5...-40.9	-40.9...-36.4	-36.4...-31.8	-31.8...-27.3	-27.3...-22.7	-22.7...-18.2
-18.2...-13.6	-13.6...-9.1	-9.1...-4.5	-4.5...0.0		

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

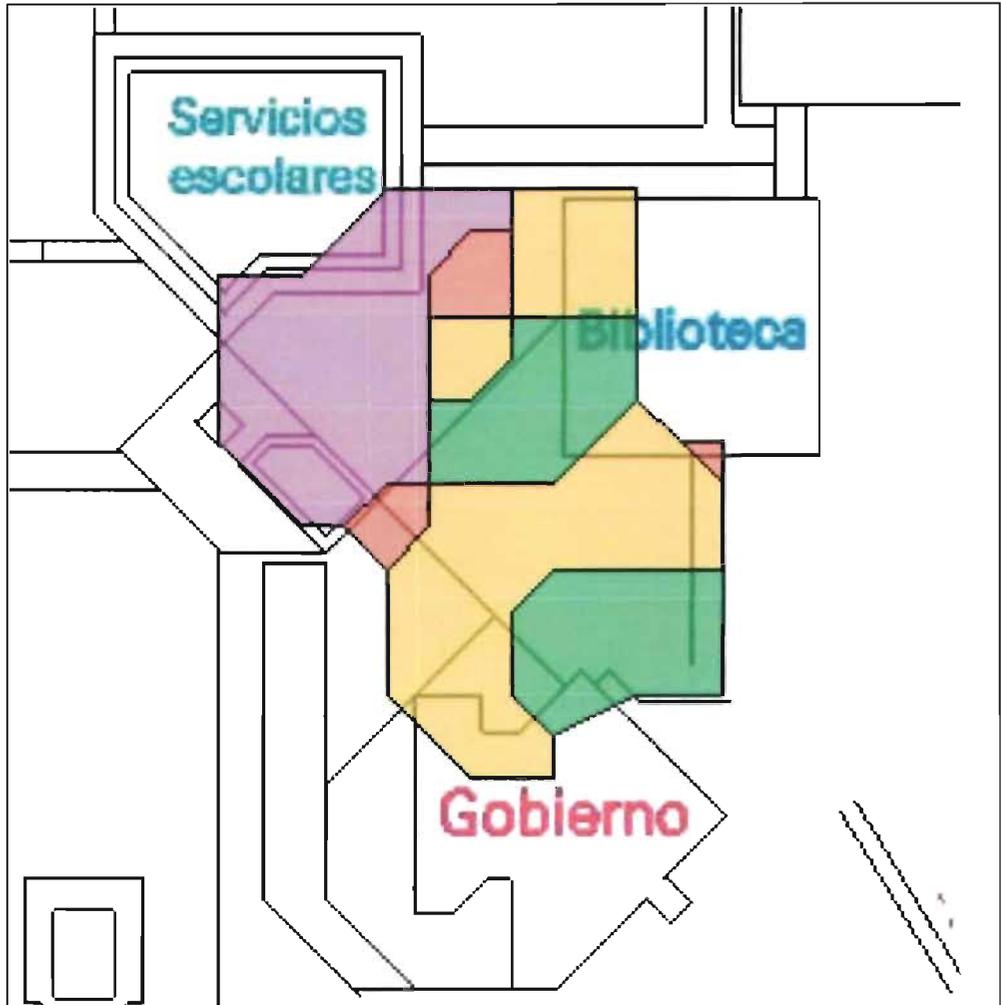
Cuenta de Access Point



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Velocidades de Datos

140



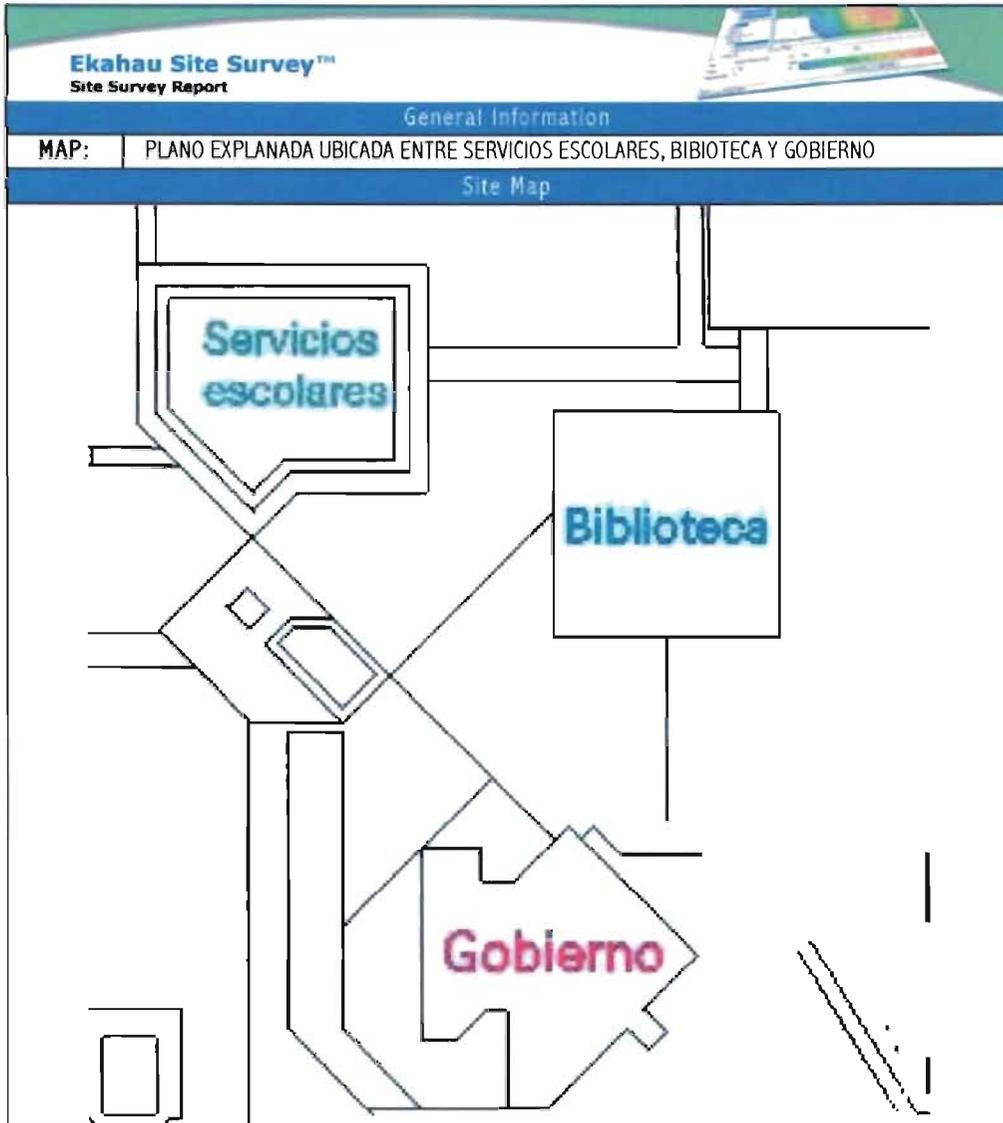
Velocidad máxima estimada por ubicación, con respecto al umbral de la relación señal a ruido seleccionada y los valores de sensibilidad de la tarjeta de red utilizada.

1.0	2.0	5.5	11.0

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

d) Prueba 4

El AP se en la planta baja de la biblioteca, para radiar la explanada



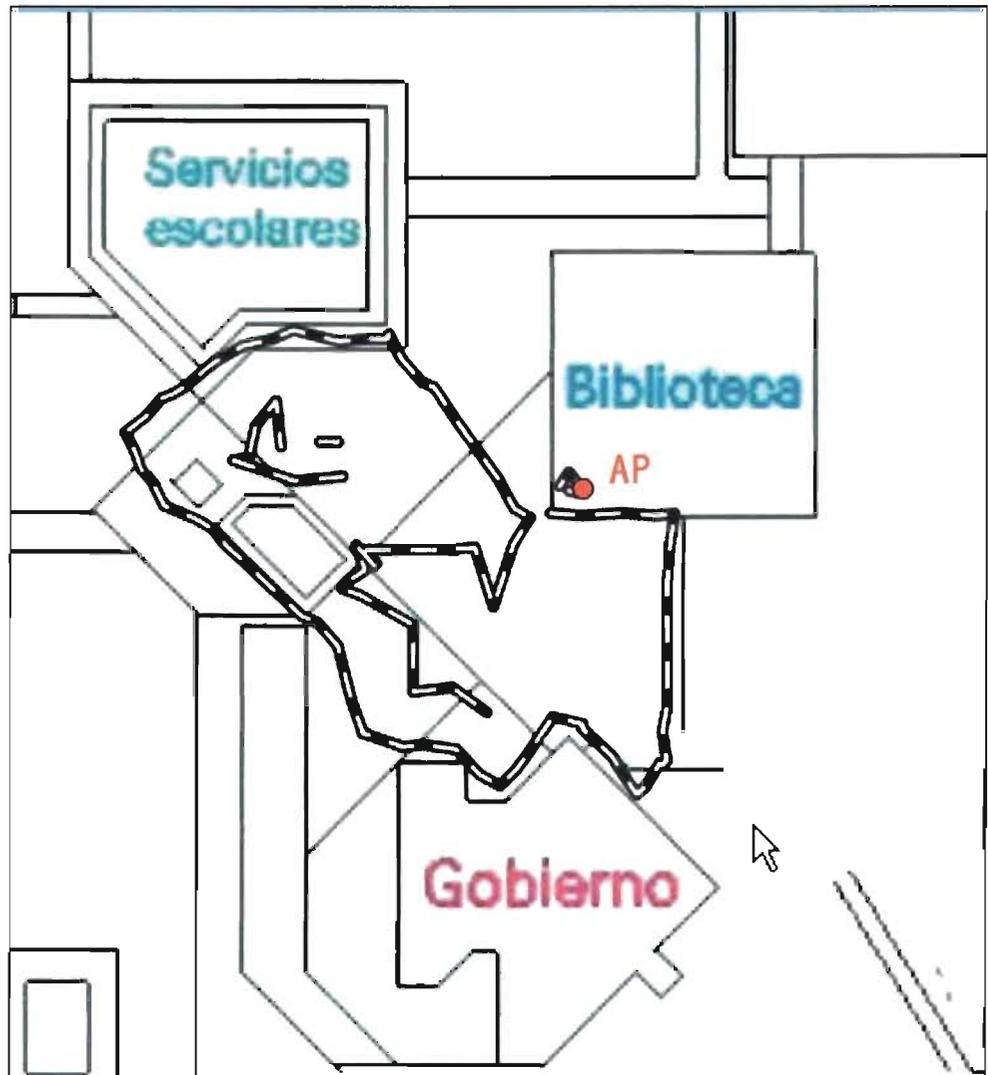
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

142

Access Points

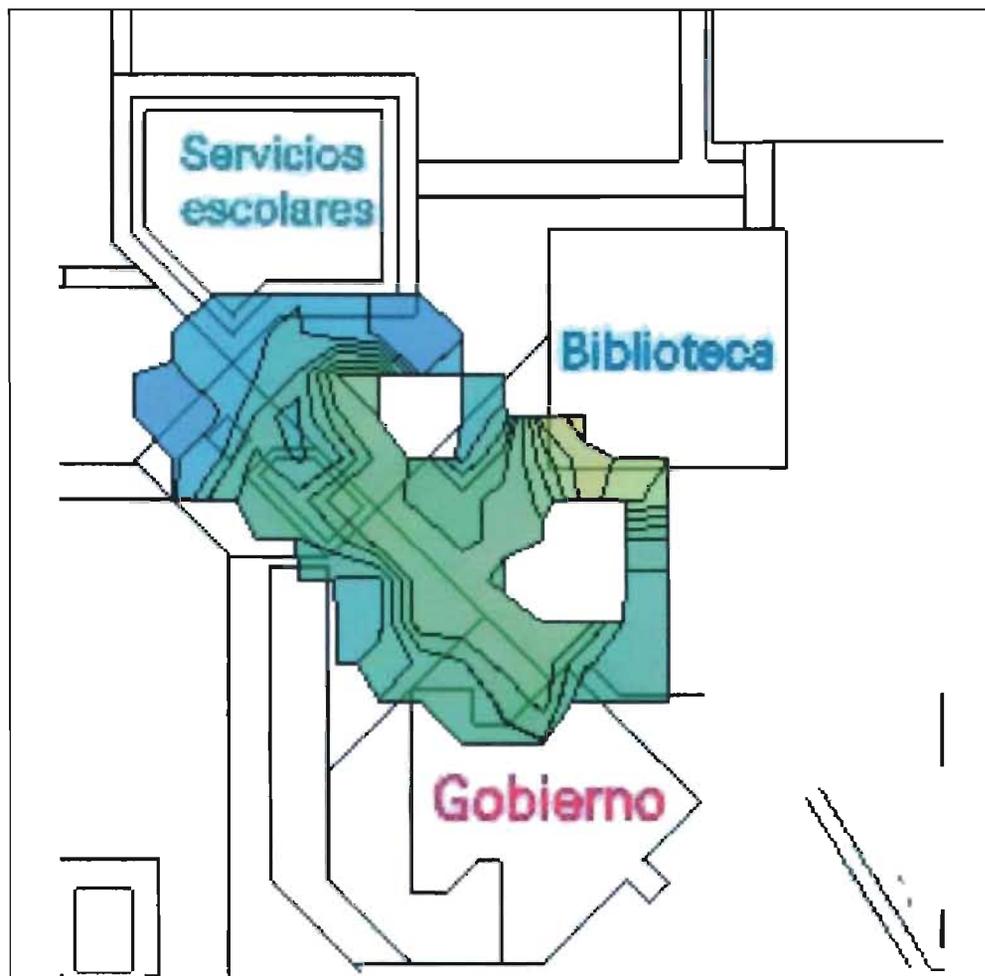
ESSID	Name	Band / Channel	Privacy
cautilan	00:13:10:2A:CC:DB	802.11b / 1	
suvimex	00:40:96:57:B2:33	802.11b / 6	WEP

Puntos Muestreados y Ubicación del Access Point



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Fuerza de la Señal



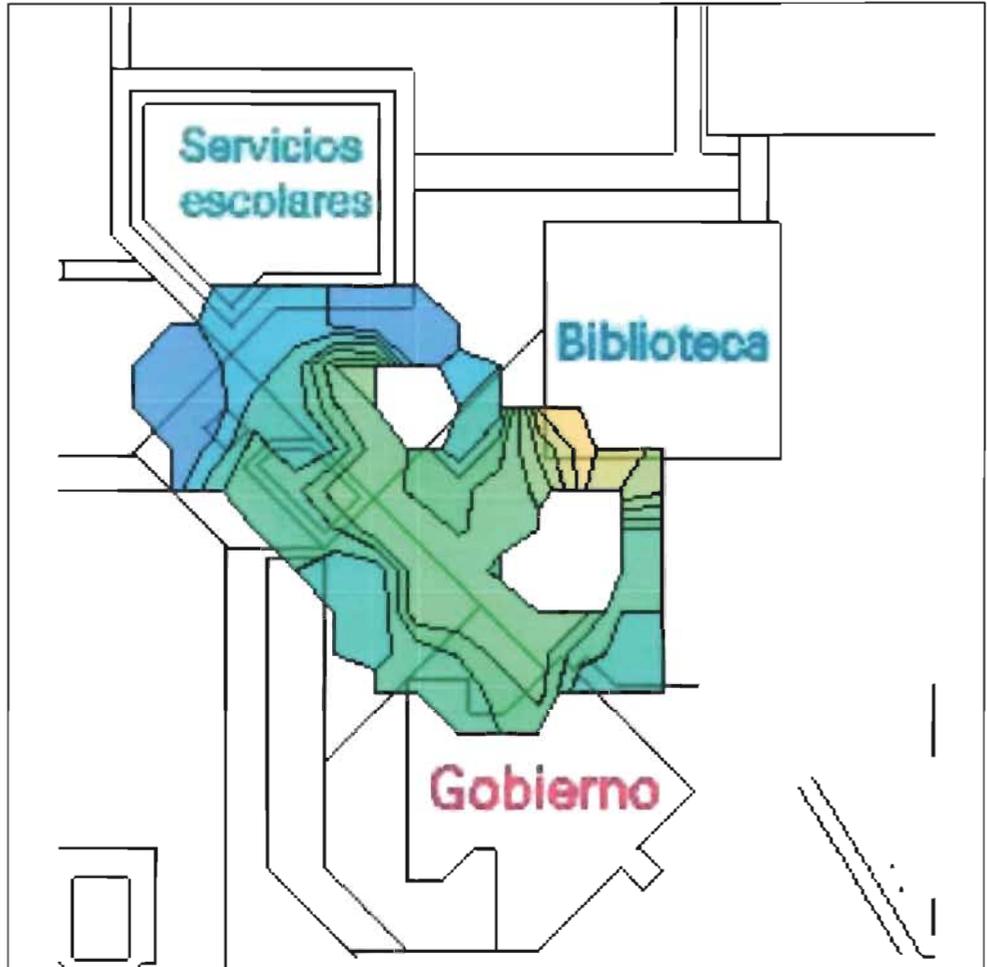
Cobertura de la fuerza de la señal (RSSI) de los Access Points seleccionados. Se muestra la mayor intensidad por ubicación.

-100.0..-95.5	-95.5..-90.9	-90.9..-86.4	-86.4..-81.8	-81.8..-77.3	-77.3..-72.7
-72.7..-68.2	-68.2..-63.6	-63.6..-59.1	-59.1..-54.5	-54.5..-50.0	-50.0..-45.5
-45.5..-40.9	-40.9..-36.4	-36.4..-31.8	-31.8..-27.3	-27.3..-22.7	-22.7..-18.2
-18.2..-13.6	-13.6..-9.1	-9.1..-4.5	-4.5..0.0		

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Relación Señal a Ruido

144

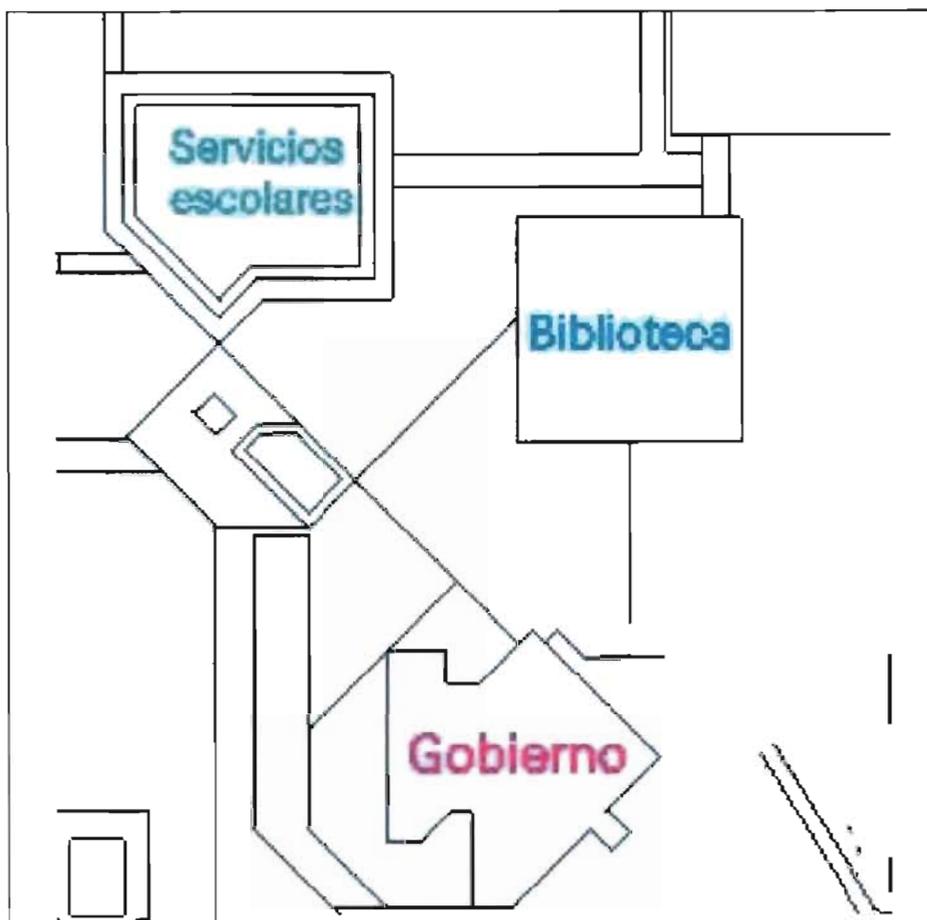


Relación señal a ruido calculada. Formula simplificada: $SNR = [Fuerza\ de\ la\ Señal] - [Interferencia]$

0.0..5.0	5.0..10.0	10.0..15.0	15.0..20.0	20.0..25.0	25.0..30.0
30.0..35.0	35.0..40.0	40.0..45.0	45.0..50.0	50.0..55.0	55.0..60.0
60.0..65.0	65.0..70.0	70.0..75.0	75.0..80.0		

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Interferencia



Interferencia calculada

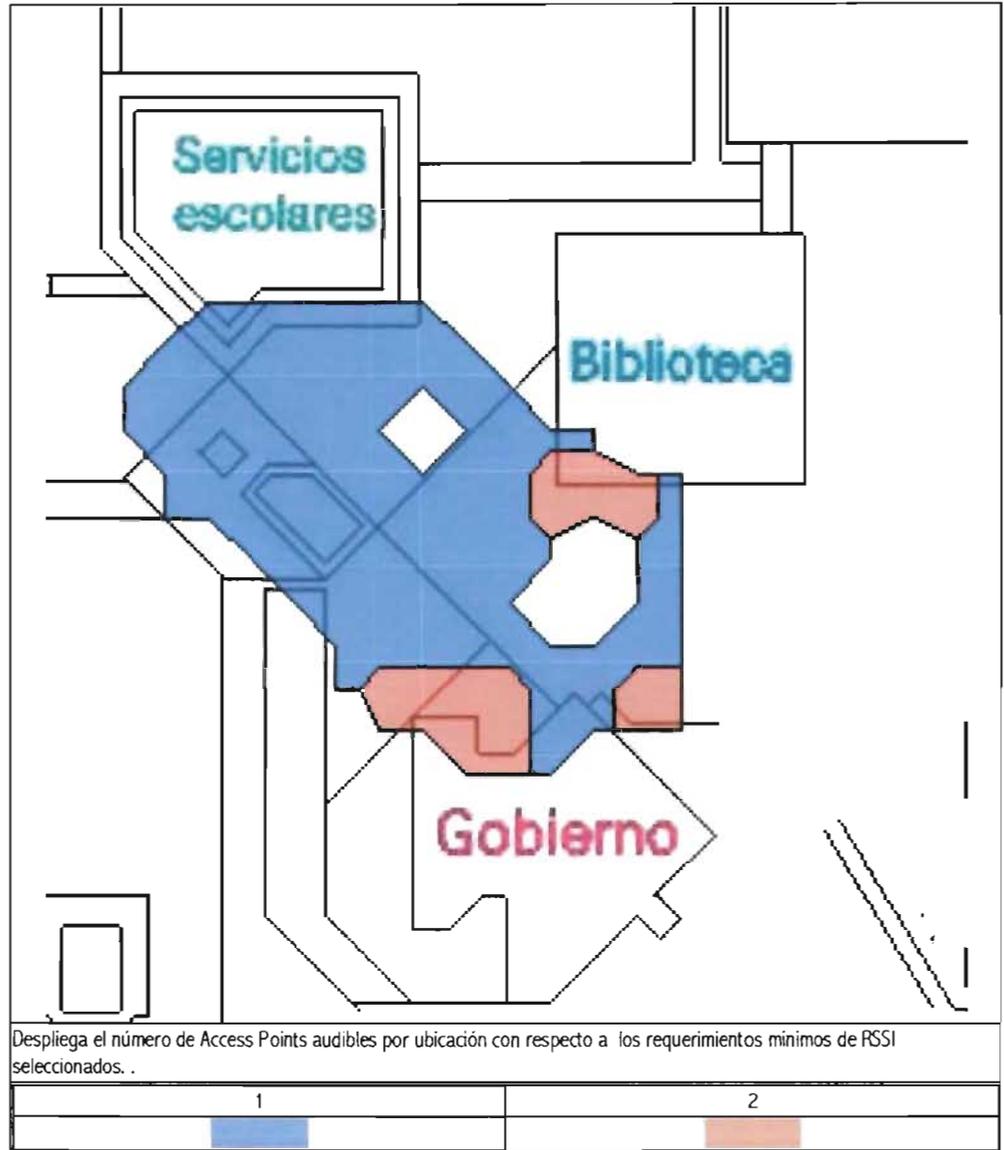
-100.0...-95.5	-95.5...-90.9	-90.9...-86.4	-86.4...-81.8	-81.8...-77.3	-77.3...-72.7
-72.7...-68.2	-68.2...-63.6	-63.6...-59.1	-59.1...-54.5	-54.5...-50.0	-50.0...-45.5
-45.5...-40.9	-40.9...-36.4	-36.4...-31.8	-31.8...-27.3	-27.3...-22.7	-22.7...-18.2
-18.2...-13.6	-13.6...-9.1	-9.1...-4.5	-4.5...0.0		



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

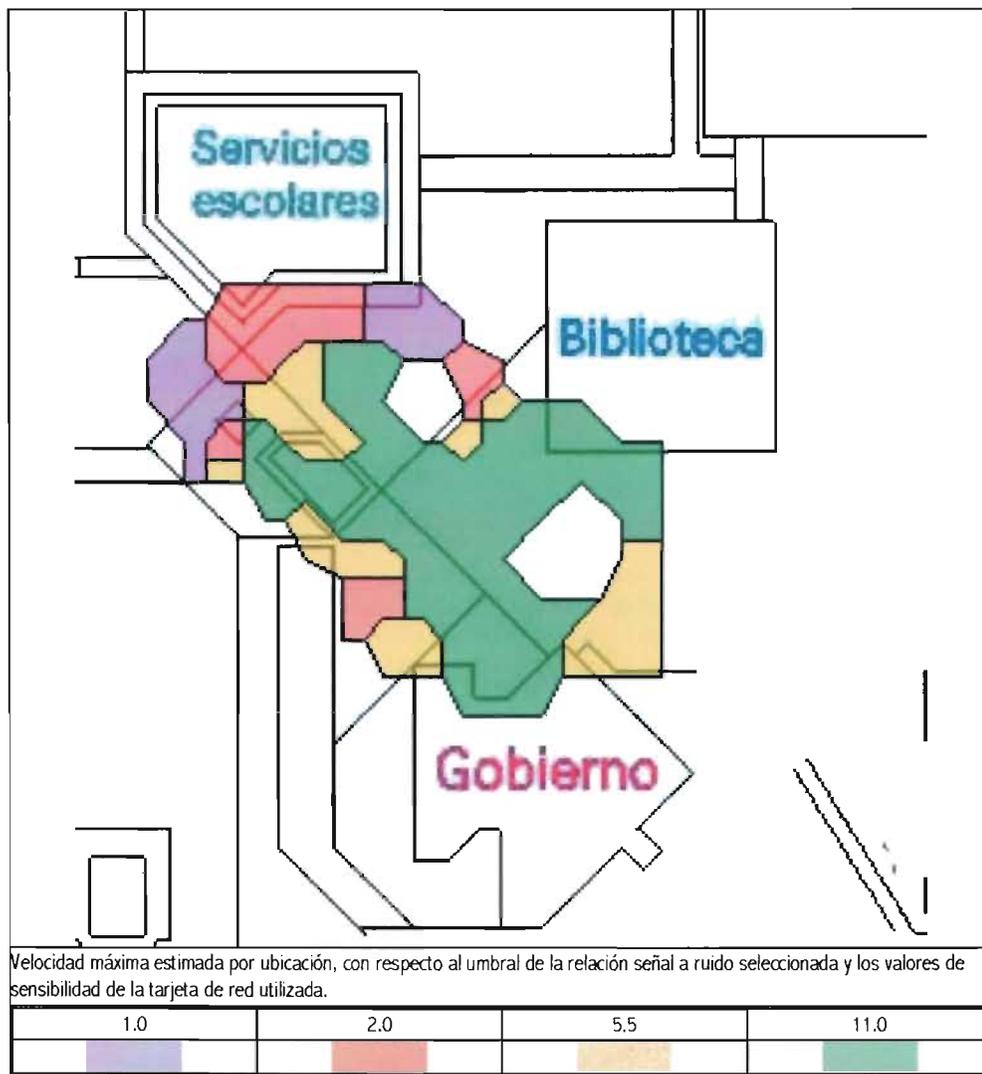
Cuenta de Access Point

146



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Velocidades de Datos



147

De estas pruebas podemos concluir que la mejor ubicación del equipo para el Biblioteca es al centro, al lado del pilar.

Y para cubrir la explanada es necesario colocar una antena externa al equipo con el fin de proporcionarle mayor ganancia a la señal, para que pueda radiar toda la zona deseada.

IV.2.4 [Carta de aceptación del proyecto]

Se presenta una propuesta formal en donde se describe lo que se va a realizar al implementar la red, con el fin de que el cliente este enterado y de acuerdo por si tiene algún cambio u objeción antes de instalar.



UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

México D.F., 20 de abril de 2005.

ING. MOISES HERNÁNDEZ DUARTE
JEFE DEL CENTRO DE CÓMPUTO.
F.E.S CUAUTILÁN

PROPUESTA TÉCNICA PARA LA IMPLEMENTACIÓN DE LA RED INALÁMBRICA

De acuerdo con los estudios realizados y las necesidades requeridas, propongo instalar dos equipos inalámbricos para cubrir la planta alta de la Biblioteca y la explanada central.

La ubicación de los equipos quedará de la siguiente manera: el equipo destinado a cubrir el interior de la biblioteca, se instalará en el pilar que se encuentra al centro de la misma. El equipo destinado a cubrir la explanada se ubicará en una de las paredes de la escalera, con el fin de que la distancia entre la antena y el equipo sea la menor posible.

El equipo ubicado en el interior de la biblioteca no necesitará una antena externa, pero el equipo destinado a cubrir la explanada requerirá de una, para que la señal alcance el área deseada. La antena que se instalará será una antena omnidireccional y se fijará en la fachada principal de la biblioteca, con un soporte metálico a 20cm de la pared y una altura de 6 metros.

Para que los equipos estén conectados a la red cableada se requerirá de un nodo de red o un puerto de un switch, si es necesario se instalará el cableado desde el IDF hasta cada uno de los equipos.

Una vez instalado todo, se configurarán los equipos y se harán pruebas de conexión.

Atentamente,

Miriam Garrada Hernández.

Aceptación
Ing. Moisés Hernández Duarte

■ IV.3 [Planeación]

■ IV.3.1 [Selección del hardware]

Debido a que las pruebas se realizaron con un equipo de la marca Linksys WRT54G Wireless-G Bridge, y que este equipo tiene las características necesarias para cubrir las necesidades del cliente, además de su fácil administración, configuración y su costo es relativamente bajo, se optó por seleccionarlo para la instalación de la red inalámbrica.

Tabla de especificaciones y características principales del equipo (de acuerdo con lo publicado por el fabricante).

Ruteador de banda ancha Wireless-G

WRT54G



Wireless-G es el novedoso estándar de red inalámbrica de 54Mbps que proporciona una velocidad casi 5 veces superior que los populares productos Wireless-B (802.11b) para el hogar, la oficina y establecimientos públicos con conexiones inalámbricas de todo el país. Los dispositivos Wireless-G comparten una banda de radio común de 2.4 GHz, por lo que también funcionan con equipos Wireless-B de 11Mbps existentes. Ya que ambos estándares son incorporados, puede aprovechar la inversión realizada en infraestructura 802.11b y migrar al novedoso y velocísimo estándar Wireless-G a medida que aumentan sus necesidades.

Características:

- El módem ADSL de alta velocidad ofrece una conexión rápida e ininterrumpida a Internet
- Conecte los PC mediante el ruteador y el conmutador de 4 puertos incorporados para crear una red Ethernet y compartir la conexión a Internet en toda la casa
- Además, el punto de acceso Wireless-G (802.11g) incorporado le permite conectarse sin necesidad de cables
- Las funciones de firewall y seguridad avanzadas ofrecen protección para los PC, los datos y su familia

El ruteador de banda ancha Wireless-G de Linksys supone, en realidad, tres dispositivos en uno. En primer lugar, el punto de acceso inalámbrico, que permite conectar dispositivos Wireless-G o Wireless-B a la red. También incorpora un conmutador 10/100 de cuatro puertos de dúplex completo para conectar dispositivos Ethernet con cables. Puede conectar cuatro PC directamente o encadenar en margarita varios concentradores y conmutadores para crear una red que satisfaga sus requisitos. Por último, la función de ruteador une todos los elementos y permite compartir una conexión a Internet DSL o por cable de alta velocidad en toda la red.

Para proteger datos y privacidad, la puerta de enlace ADSL Wireless-G cuenta con un avanzado firewall que detiene los ataques e intrusiones desde Internet. Las transmisiones inalámbricas pueden protegerse mediante una compleja encriptación de datos. Puede proteger a su familia mediante funciones de control parental como la limitación de tiempo de acceso a Internet y el bloqueo mediante palabras clave. La configuración es sencillísima y se puede realizar con cualquier explorador Web.

Además Wireless-G puede encriptar todas las transmisiones inalámbricas. El ruteador puede funcionar como servidor DHCP, dispone de tecnología NAT de protección contra intrusos, admite paso a través VPN y se puede configurar para filtrar el acceso a Internet de los usuarios internos. La utilidad de configuración basada en explorador Web hace de ésta una tarea sencillísima.



Los productos verificados de Linksys se han probado con Intel. Centrino. Tecnología móvil para la compatibilidad y la interoperabilidad, realizando más su experiencia inalámbrica futura.

LINKSYS®
A Division of Cisco Systems, Inc.

The All-In-One Wireless-G Networking Solution



Verified Linksys products have been tested with Intel® Centrino™ Mobile Technology for compatibility and interoperability, further enhancing your wireless experience.

The Linksys Wireless-G Broadband Router is really three devices in one box. First, there's the Wireless Access Point, which lets you connect both screaming fast Wireless-G (802.11g at 54Mbps) and Wireless-B (802.11b at 11Mbps) devices to the network. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices together. Connect four PCs directly, or attach more hubs and switches to create as big a network as you need. Finally, the Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

Once your computers are connected to the Router and the Internet, they can communicate with each other too, sharing resources and files. All your computers can print on a shared printer connected anywhere in the house. And your computers can share all kinds of files -- music, digital pictures, and documents. Keep all your digital music on one computer, and listen to it anywhere in the house. Organize all of your family's digital pictures in one place, to simplify finding the ones you want, and easing backup to CD-R. Utilize extra free space on one computer when another's hard drive starts to fill up.

To protect your data and privacy, the Wireless-G Broadband Router can encode all wireless transmissions with up to 256-bit encryption, and supports both Wired Equivalent Privacy (WEP) and the industrial-strength wireless security of Wi-Fi Protected Access™ (WPA). The Router can serve as a DHCP Server, has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks, supports VPN pass-through, and can be configured to filter internal users' access to the Internet. Configuration is a snap with the web browser-based configuration utility.

With the Linksys Wireless-G Broadband Router at the center of your home or office network, you can share a high-speed Internet connection, files, printers, and multi-player games with the flexibility, speed, and security you need!

All-in-one Internet-sharing Router, 4-port Switch, and Wireless-G (802.11g) Access Point

Wireless data rates up to 54Mbps—5 times as fast as Wireless-B (802.11b)

Shares a single Internet connection and other resources with Ethernet-wired and Wireless-G and B devices

High security: Wi-Fi Protected Access™ (WPA), wireless MAC address filtering, powerful SPI firewall

Wireless-G Broadband Router

Product Data

Model No. **WRT54G**

CISCO SYSTEMS



Wireless-G Broadband Router

Features

- Complies with 802.11g and 802.11b (2.4GHz) Standards
- Unsurpassed Wireless Security with Wi-Fi Protected Access™ (WPA)
- Enhanced Internet Security Management Functions including Internet Access Policies with Time Schedules
- All LAN Ports Support Auto-Crossover (MDI/MDIX) - No Need for Crossover Cables



Linksys
A Division of Cisco Systems, Inc.
9502 Teller Avenue
Folsom, CA 95762 USA
E-mail: sales@linksys.com
support@linksys.com
Web: http://www.linksys.com
Linksys products are available in more than 100 countries, supported by 12 Linksys Regional Offices throughout the world. For a complete list of local Linksys Sales and Technical Support contacts, visit our Worldwide Web Site at www.linksys.com.

Specifications

Model Number	WRT54G
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Channels	11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
Ports/Buttons	Internet: One 10/100 RJ-45 Port LAN: Four 10/100 RJ-45 Switched Ports One Power Port One Reset Button
Cabling Type	UTP CAT5
LEDs	Power, DMZ, WLAN, LAN (1, 2, 3, 4), Internet
RF Power Output	18 dBm
WiFi cable/cert	None
Security Features	Stateful Packet Inspection (SPI) Firewall, Internet Policy
Wireless Security	Wi-Fi Protected Access™ (WPA), WEP, Wireless MAC Filtering

Environmental

Dimensions	7.32" x 1.89" x 7.87" W x H x D (186 mm x 48 mm x 200 mm)
Unit Weight	1.7 oz. (0.48 kg)
Power	External, 12V DC, 1.0A
Certifications	FCC, IC-03, CE, Wi-Fi (802.11b, 802.11g), WPA
Operating Temp.	32°F to 104°F (0°C to 40°C)
Storage Temp.	-4°F to 158°F (-20°C to 70°C)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Warranty	3 Years Limited

Minimum Requirements

- 200 MHz or Faster Processor
- 64 MB of RAM
- Internet Explorer 4.0 or Netscape Navigator 4.7 or Higher for Web-based configuration
- CD-ROM Drive
- Windows 98SE, Me, 2000, or XP
- Network Adapter

Package Contents

- Wireless-G Broadband Router
- Setup CD-ROM with Symantec Internet Security
- User Guide on CD-ROM
- Power Adapter
- Ethernet Network Cable
- Quick Installation Guide
- Registration Card

Linksys and the Linksys logo are trademarks of Cisco Systems, Inc. Linksys is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and various other countries. Copyright © 2004 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

WRT54G-02-05-0339X-01

Product Data

Model No. **WRT54G**

De igual forma se utilizó un equipo WAP11 de la marca Linksys, para radiar la explanada externa, este Access Point no brinda las características de ruteo ofrecidas por el WRT54G Wireless-G Bridge, por lo que se conecto a uno de los puertos del ruteador para poder brindar DHCP (direcciones IP automáticas a los que se conectaran a la red)

Tabla de características y especificaciones de acuerdo con la información proporcionada por el fabricante.

Wireless Access Point	
	<p>WAP11</p>
<p>Características:</p> <ul style="list-style-type: none"> • Proporciona punto de acceso inalámbrico o puente • Filtrado de MAC y cliente DHCP • Antenas ajustables que proporcionan una configuración física sencilla • Extensas áreas de funcionamiento de hasta 350 metros en exteriores • Configuración basada en navegador Web fácil de usar • Hasta 256 bits de seguridad WEP 	<p>No deje que los cables le enreden. Con Wireless Access Point de Linksys podrá configurar su red a su manera. La utilización de la tecnología inalámbrica de última generación le permite configurar sus estaciones de trabajo como nunca había imaginado que fuera posible; sin cables, lo que significa menos gastos y menos quebraderos de cabeza.</p> <p>Las potentes antenas de Wireless Access Point abarcan un área de funcionamiento de más de 90 metros en interiores, lo que proporciona una itinerancia perfecta en toda la infraestructura de LAN inalámbrica. La característica avanzada de autenticación del usuario garantiza un alto nivel de seguridad en la red. Wireless Access Point es fácil de instalar (conectar y listo) y de usar. Las herramientas de diagnóstico y estadísticas basadas en Windows le aseguran el control en todo momento.</p> <p>Reúna todas estas características en una unidad compacta, ligera y potente, y obtendrá lo último en redes flexibles: Wireless Access Point de Linksys.</p>

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA



Instant Wireless® Series Wireless Network Access Point

Connect to your home or office network, without wires!

Set your network free! The Wireless Access Point from Linksys connects wireless computers to your wired network, so you can add PCs to the network with no cabling hassle. Create a "wireless bubble" in that hard-to-wire office space, and save the time, hassle, and expense of running cables. Plus, notebook PCs can travel around your home or office and stay connected wherever they go.

You can also use the Wireless Access Point as a kind of "cable-less cable" to connect remote areas together. Maybe Shipping is all the way across the warehouse from Receiving. Or maybe you want to set up a home office in your detached garage. With a Wireless Access Point in the garage, and another one (or the Linksys Wireless Ethernet Bridge) in the house, you're connected—with no cable to run.

For even more versatility, the Wireless Access Point can act as a Repeater. If you're already using one WAP11, you can extend your wireless network's range by installing a second one that "bounces" received data further down the line. The repeating Access Point can be installed nearly anywhere, because it works entirely by radio—no data cable is necessary.

Whichever mode you use, the dual antenna configuration provides "antenna diversity", for exceptional signal sensitivity and increased useable range. To protect your data and privacy, the Wireless Access Point can encrypt all wireless transmissions. The MAC Address filter lets you decide exactly who has access to your wireless network. Configuration is a snap with web browser-based configuration.

The Linksys Wireless Access Point is the simple, versatile way to add wireless capabilities to your network.



Wireless Network Access Point
Model Number: WAP11 ver. 2.6

Benefits

- Create an 11Mbps Wireless-G (802.11g) network in your home or office
- Also wirelessly bridges multiple wired networks across rooms, floors, or buildings
- Advanced features: AP Client, Point-to-Point or Point-to-Multipoint Bridging, and Repeater Mode
- Up to 128-bit encryption and wireless MAC address filtering protect your network and data

Features

- High-Speed Data Transfer Rates of up to 11Mbps
- Compatible with IEEE 802.11b, 2.4GHz Compliant Equipment
- Supports Wireless Bridging, Wireless Repeater, MAC Address Filtering, and Event Logging
- Setup Wizard for Easy Installation
- Built-in Web-based Utility for Easy Configuration from any Web Browser
- Wireless Security with Up to 128-bit WEP Encryption

Specifications

Standards	802.11b, 802.3
Port	One 10BaseT RJ-45 Port
Button	1 x Reset Button
Cabling Type	RJ-45
LEDs	1 x Power, 1 x Activity, 1 x Link
Security Features	MAC filtering, WEP, SSID Broadcast enable/disable
WEP Key Bits	64/128-bit

Environmental

Dimensions	7.32" x 6.06" x 1.89" (186 mm x 154 mm x 48 mm)
Unit Weight	16 oz. (0.45 kg)
Power	DC 5V, 2.5 A
Certifications	FCC Class B, CE Mark
Operating Temp.	0°C to 40°C
Storage Temp.	-20°C to 70°C
Operating Humidity	10% to 80%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing

Package Contents

Wireless Network Access Point

- Wireless Network Access Point
- Detachable Antennas
- Power Adapter
- Setup CD-ROM with User Guide
- Quick Installation
- Ethernet Network Cable
- Registration Card

Minimum Requirements

PC with the following:

- 200MHz or Faster Processor
- 64MB RAM Memory Recommended
- Internet Explorer 4.0 or Netscape Navigator 4.7 or Higher for Web-based Configuration
- CD-ROM Drive
- Windows 98/Me/2000/XP
- 802.11b Wireless Adapter with TCP/IP Protocol Installed per PC
or
Network Adapter with Ethernet (UTP CAT 5) Cabling and TCP/IP Protocol Installed per PC

Linksys

World Headquarters:
17401 Armstrong Ave.
Irvine, CA 92614 USA

E-mail: sales@linksys.com
support@linksys.com

Web: <http://www.linksys.com>

Linksys products are available in more than 50 countries, supported by 12 Linksys Regional Offices throughout the world. For a complete list of local Linksys Sales and Technical Support contacts, visit our Worldwide Web Site at www.linksys.com.



Specifications are subject to change without notice. Instant Wireless, Linksys, and the Linksys logo are registered trademarks of Linksys Group, Inc. Other brands and product names are trademarks or registered trademarks of their respective holders. Copyright © 2003 Linksys. All rights reserved.
WAP11-22-03-10004-0

Puesto que se necesita de una antena externa para brindar cobertura inalámbrica a la explanada, se utilizó una antena omnidireccional de la marca Maxrad modelo Xtreme Wave MFB24008, que ofrece una ganancia de 8 dBi. La antena esta encapsulada en un empaque de fibra de vidrio que la protege de los rayos UV, lo que la hace mucho más duradera, además de que está diseñada para soportar las inclemencias del tiempo y las corrientes de aire.

Tiene un conector tipo N-hembra, es de polarización vertical, mide 50cm aproximadamente y pesa 230gr.

La cantidad de equipos que se instalen en una determinada red depende de dos factores importantes, el tamaño del área que se requiere cubrir y la densidad de usuarios que utilizarán dicha red.

Tabla de características y especificaciones de acuerdo con el fabricante.

XtremeWave™ MFB Series

MAXRAD

PCS, 2.4 GHz ISM and MMDS Omnidirectional Base Station Antenna Series

The XtremeWave™ wireless broadband omnidirectional antennas are designed to provide maximum performance and reliability under the toughest weather conditions. These antennas feature a UV stable, vented radome that provides ultimate protection against weather elements. They can be mast, wall or ceiling mounted.

General Specifications:

Radome Material:

UV resistant pultruded fiberglass

Polarization:

Vertical

Lightning Protection:

Not standard, but all models can be ordered with DC grounding. Add a "DC" suffix to the part number to choose the DC grounded version of the antenna.

Nominal Impedance:

50 Ohms

Mounting Base Diameter:

1.25 inches (all models except MFB24012)
1.5 inches (model MFB24012)

Mounting Method (sold separately):

MMK1924 - L bracket mount for wall or pipe mount (all models, except MFB24010 and MFB24012)

MMK8A - Aluminum extruded bracket for mast mounting (all models, except model MFB24012)

MMK11 - Ceiling mount bracket (for MFB24004, MFB24006 and MFB24008 only)

MMK12 - Heavy duty bracket for mast mounting the MFB24012

MMK14 - Light duty mounting clamp for MFB24012

Termination:

II female standard with all models, except MFB24012

II female, reverse polarity and reverse threaded connectors optional

16" RG-213 pigtail with II female connector for model MFB24012 only

II male connector option available with models MFB24010, MFB24008, MFB24006 and MFB19008. To order, add "IM" to part number.

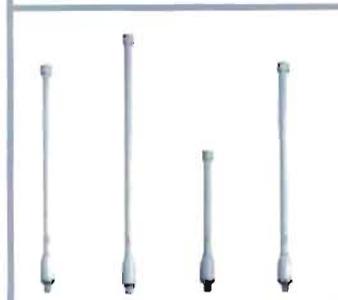
Features and Benefits:

- UV stable, pultruded fiberglass radome. Allows outdoor installation even in harsh climates.
- Vented system design (all models except MFB24012). Provides reliable performance by protecting the electrical design against extreme moisture and/or temperatures.
- Thread relief on connector (all models, except MFB24012 which has a pigtail). Improved accessibility for taping reduces installation time and improves overall effectiveness.
- Internal o-ring seal in the base of the antenna with integrated connector at the base. Assures a watertight seal to prevent water from migrating into the antenna connector (all models, except MFB24012 which has a pigtail.)
- Electrical downtilt options on select models. Provide system planners flexibility in challenging operating environments.

PCTEL Antenna Products Group, Inc. ORDER (800) 323-9122



XtremeWave™ MFB24012



XtremeWave™ Models 25007 MMDS, MFB19008A PCS, MFB24006 and MFB24008 2.4 GHz FSM Antennas



MFB24010 and MFB24012

Specifications

Electrical Specifications

Model #	Frequency Range	Gain	Bandwidth @ 1.5:1 VSWR	Vertical Beam-width @ 1/2 Power	VSWR	Maximum Power	Downtilt
MFB19008A	1850-1990 MHz	8 dBi	140 MHz	12°	< 1.5:1	25 Watts	N/A
MFB24004	2400-2483.5 MHz	4 dBi	100 MHz	30°	< 1.5:1	25 Watts	N/A
MFB24006	2400-2483.5 MHz	6 dBi	100 MHz	20°	< 1.5:1	25 Watts	N/A
MFB24008	2400-2483.5 MHz	8 dBi	100 MHz	13°	< 1.5:1	25 Watts	N/A
MFB24008DT3	2400-2483.5 MHz	8 dBi	100 MHz	13°	< 1.5:1	25 Watts	3°
MFB24008DT5	2400-2483.5 MHz	8 dBi	100 MHz	13°	< 1.5:1	25 Watts	5°
MFB24008DT7	2400-2483.5 MHz	8 dBi	100 MHz	13°	< 1.5:1	25 Watts	7°
MFB24008DT12	2400-2483.5 MHz	8 dBi	100 MHz	13°	< 1.5:1	25 Watts	12°
MFB24010	2400-2483.5 MHz	10 dBi	100 MHz	9°	< 1.5:1	25 Watts	N/A
MFB24012	2400-2500 MHz	12 dBi	100 MHz	7°	< 1.5:1	25 Watts	N/A
MFB25007	2500-2700 MHz	7 dBi	200 MHz	13°	< 1.5:1	25 Watts	N/A
MFB25007DT3	2500-2700 MHz	7 dBi	200 MHz	13°	< 1.5:1	25 Watts	3°

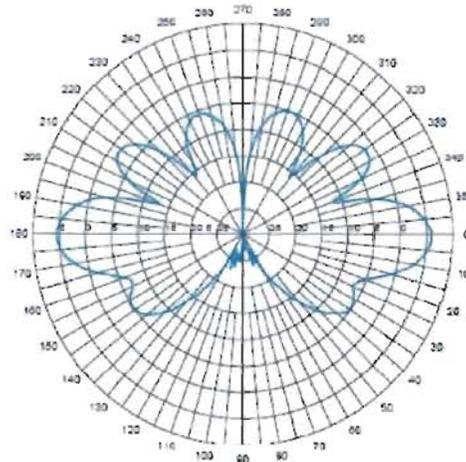
Mechanical Specifications

Model #	Wind Survival	Equivalent Flat Plate Area	Lateral Thrust @ Rated Wind	Bending Moment @ Rated Wind	Height	Weight
MFB19008A	125 mph	.07 ft ²	5.9 lbs	5.7 ft-lbs	24.0" (609.6 mm)	0.70 lbs (0.318 kg)
MFB24004	125 mph	.02 ft ²	2.1 lbs	0.7 ft-lbs	8.1" (205.7 mm)	0.34 lbs (0.154 kg)
MFB24006	125 mph	.04 ft ²	3.0 lbs	1.4 ft-lbs	11.6" (294.6 mm)	0.38 lbs (0.172 kg)
MFB24008	125 mph	.06 ft ²	5.2 lbs	4.4 ft-lbs	20.2" (513.1 mm)	0.50 lbs (0.226 kg)
MFB24008DT3	125 mph	.06 ft ²	5.2 lbs	4.4 ft-lbs	20.2" (513.1 mm)	0.50 lbs (0.226 kg)
MFB24008DT5	125 mph	.06 ft ²	5.2 lbs	4.4 ft-lbs	20.2" (513.1 mm)	0.50 lbs (0.226 kg)
MFB24008DT7	125 mph	.06 ft ²	5.2 lbs	4.4 ft-lbs	20.2" (513.1 mm)	0.50 lbs (0.226 kg)
MFB24008DT12	125 mph	.06 ft ²	5.2 lbs	4.4 ft-lbs	20.2" (513.1 mm)	0.50 lbs (0.226 kg)
MFB24010	125 mph	.11 ft ²	10.1 lbs	14.7 ft-lbs	36.0" (914.4 mm)	0.65 lbs (0.295 kg)
MFB24012	125 mph	.25 ft ²	22.4 lbs	41 ft-lbs	44.0" (1,118 mm)	3.00 lbs (1,400 kg)
MFB25007	125 mph	.06 ft ²	5.2 lbs	4.4 ft-lbs	20.2" (513.1 mm)	0.50 lbs (0.226 kg)
MFB25007DT3	125 mph	.06 ft ²	5.2 lbs	4.4 ft-lbs	20.2" (513.1 mm)	0.50 lbs (0.226 kg)

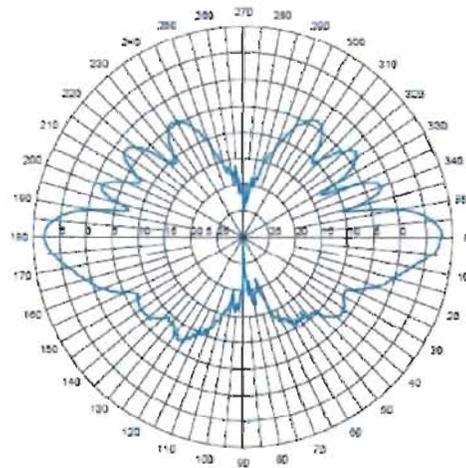


IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Patterns



MFB24006 Elevation Cut



MFB24008 Elevation Cut



IV.4 [Ejecución]**IV.4.1 [Instalación]**a) Instalación de la antena

Se montó un soporte metálico para fijar la antena en la fachada del edificio, a una distancia aproximada de 20cm de la pared del mismo, a una altura de 6mts



Foto 1. Para montar el soporte para la antena



Foto 2. Se atornilla la antena al soporte

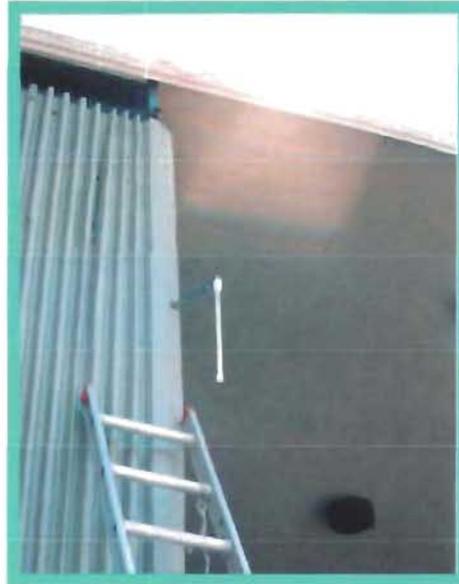


Foto 3. Antena montada a unos 20cm aprox. del edificio.

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

La antena se instaló en el AP 2 (exterior). Fue necesario fabricar un pigtail[□] que tuviera por un lado un conector Tipo N macho y por el otro un conector Tipo TNC (BNC roscado) hembra, se requirió además de un cable coaxial LMR-400 con conector Tipo N Macho (del lado de la antena) y N hembra (del lado del pigtail) con el fin de montar solo la antena fuera del edificio, pues el equipo no puede estar a la intemperie.



Foto 4. Conector Tipo N del coaxial a la antena.



Foto 5. Pigtail, conector Tipo TNC (del lado del equipo)

Para proteger los conectores de la antena y el coaxial con el fin de evitar la corrosión por el ambiente se cubrió la unión con 3 o 4 vueltas con cinta vulcanizada y después se recubrió con cinta de aislar.



Foto 6. Cinta vulcanizada



Foto 7. Cinta de aislar

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA



Foto 8. Conectores cubiertos



Foto 9. Cable coaxial LMR-400 que atraviesa el muro por el plafón en el techo del edificio.

b) Instalación del cableado

Se utilizaron 69mts de UTP categoría 6 para cablear desde el IDF ubicado en la planta baja de la biblioteca, hasta el AP1 en la planta alta, reutilizando una tubería de aluminio galvanizado ya existente, con el fin de proporcionar la conexión a Internet al ruteador inalámbrico.



Foto 10. Bobina de cable UTP categoría 6

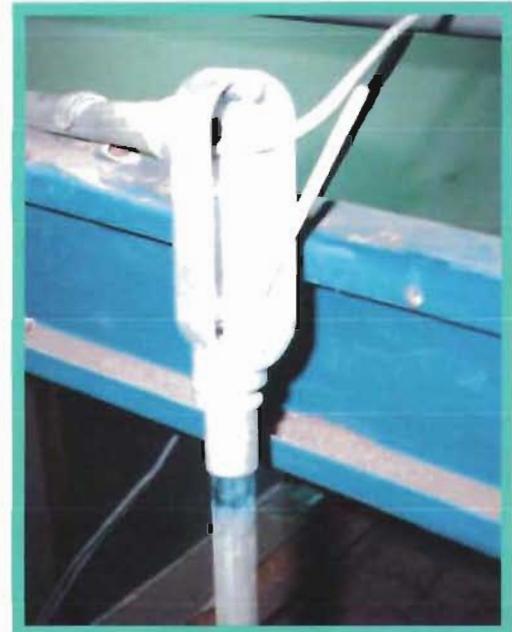


Foto 11. Se reutilizó la tubería existente para cablear desde el IDF ubicado en la PB hasta el AP1 en la PA.

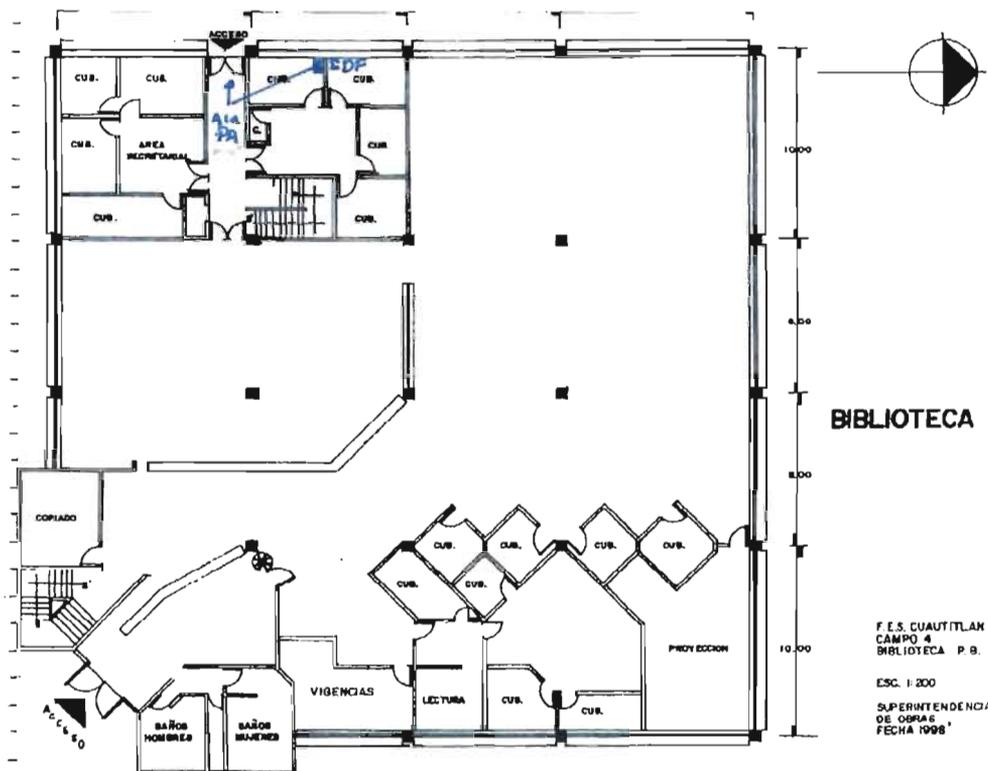
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Se utilizaron 37mts de UTP de uso rudo para interconectar al AP1 (ruteador inalámbrico) con el AP2 (Access Point), con el fin de proporcionar a este último la conexión a Internet y la posibilidad de dar DHCP (asignación de direcciones IP automáticas) por medio del ruteador.

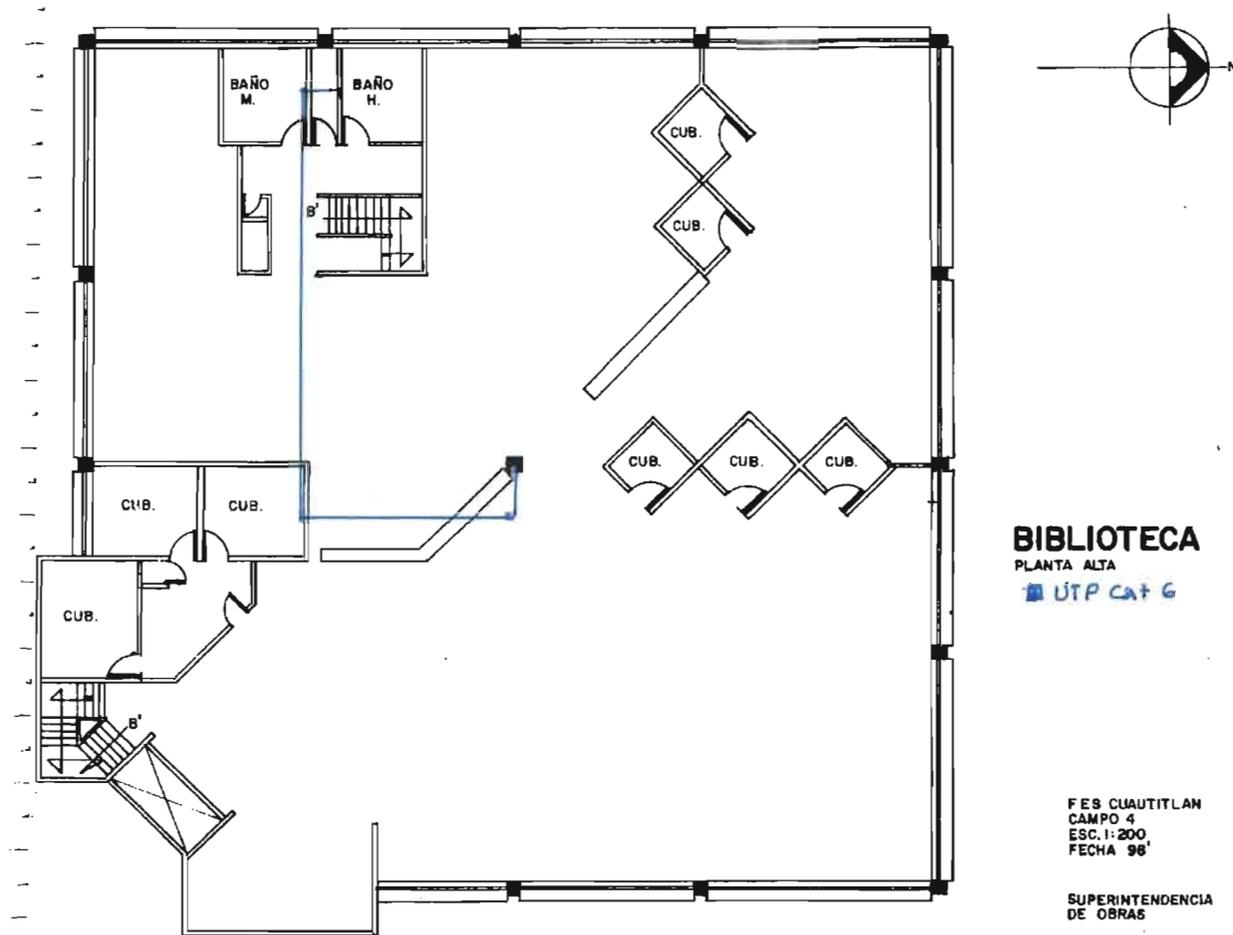


Foto 12. Bobina de cable UTP de uso rudo

La ruta de cableado que se siguió fue la siguiente:



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA



c) Instalación de los equipos

Para instalar el AP 1 (equipo ubicado en el pilar), se reutilizó un soporte existente, solo se le añadió una base de maderas y se colocó sobre esta base el equipo, no fue necesario poner una toma de corriente, puesto que se ocupó una toma previamente instalada.



Foto 13. AP 1 montado en la base y en el pilar.

Para instalar el AP2 (equipo que da servicio a la explanada), fue necesario sujetarlo a una pared en el área de las escaleras del edificio cerca de las ventanas, con el fin de que la distancia del cable coaxial no fuera muy larga, pues las pérdidas de la señal se incrementan con la longitud del cable. También fue necesario colocar una extensión desde los cubículos hasta el AP, para suministrarle corriente eléctrica.



Foto 14. Instalación del AP 2.

■ IV.4.2 [Configuración]

Se capturan todos los datos que se configuraron en el equipo, como: la dirección IP para la red interna, la dirección IP de la WAN, las direcciones MAC de los equipos, el nombre de la red, los canales, etc. Puesto que publicar toda la información de la configuración podría comprometer la seguridad de la red instalada para la FES Cuautitlán Campo 4, solo haré referencia a los parámetros que no afectan de alguna manera su integridad.

La configuración de los equipos quedo como sigue:

AP1 - Configuración del equipo WRT54G (Ruteador) Ubicado en el pilar central de la biblioteca en la Planta Alta.

Router Name: CUAUTITLAN
Internet setup: AUTOMATIC DHCP
DHCP Server: ENABLE

WIRELESS

Wireless Mode: B-ONLY
Wireless Network Name (SSID): cuauti_wifi
Wireless Channel : 11 – 2.462GHz
Wireless SSID Broadcast: ENABLE
Security Mode: DISABLE
Encryption Function: DISABLE

AP2 – Configuración del equipo WAP11 (Access Point) Ubicado en la pared de las escaleras.

AP Name: ap2_exterior
SSID: cuauti_wifi
Channel: 1
WEP: DISABLE
Mode: Access Point
SSID Broadcast: ENABLE

La selección de canales se hizo en base a que se detecto una señal en el canal 6, y puesto a que solo se pueden utilizar tres canales en la banda de 2.4GHz, se eligieron los dos canales restantes: el canal 11 para el interior de la biblioteca y el canal 1 para el exterior con el fin de evitar interferencias.

El nombre de la red, debe ser el mismo en ambos equipos para que pueda llevarse a cabo el roaming, y extender el DHCP. Se recomienda que el SSID se escriba en minúsculas siempre, pues algunas tarjetas inalámbricas tienen problemas para encontrar la red o conectarse si el SSID si este se encuentra con mayúsculas.

Se decidió no poner ninguna clave WEP (seguridad deshabilitada), pues la FES Cuautitlán considera que mientras la red se hace popular entre el alumnado y el profesorado, no es necesario. Pero es posible que en unos meses se implementen otras medidas de seguridad como la autenticación; todo dependerá de la demanda y la respuesta que tenga este nuevo servicio entre los alumnos y profesores.

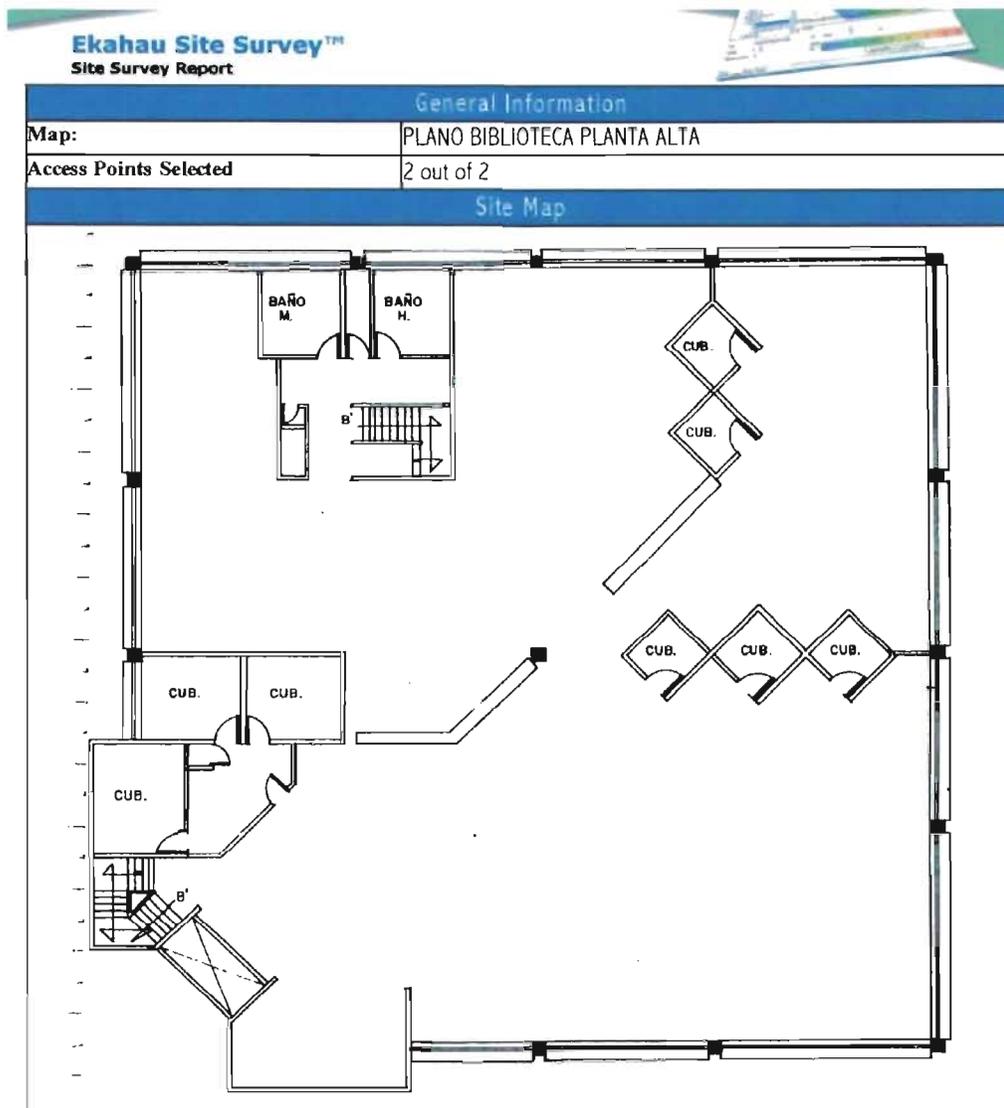
■ IV.4.3 [Pruebas]

a) Site Survey

Una vez instalada la red se realizaron de nuevo pruebas de propagación, para verificar que la ubicación de los equipos y la elección de las antenas son correctas. En caso de que las pruebas no arrojen los resultados esperados, se deberán reubicar los equipos y las antenas hasta obtener el efecto deseado. Es por esta razón que se realiza un estudio previo, para evitar el reubicar un equipo una vez instalado.

La razón más importante de realizar un Site Survey es para asegurarse que la WLAN no deje zonas muertas de cobertura (huecos).

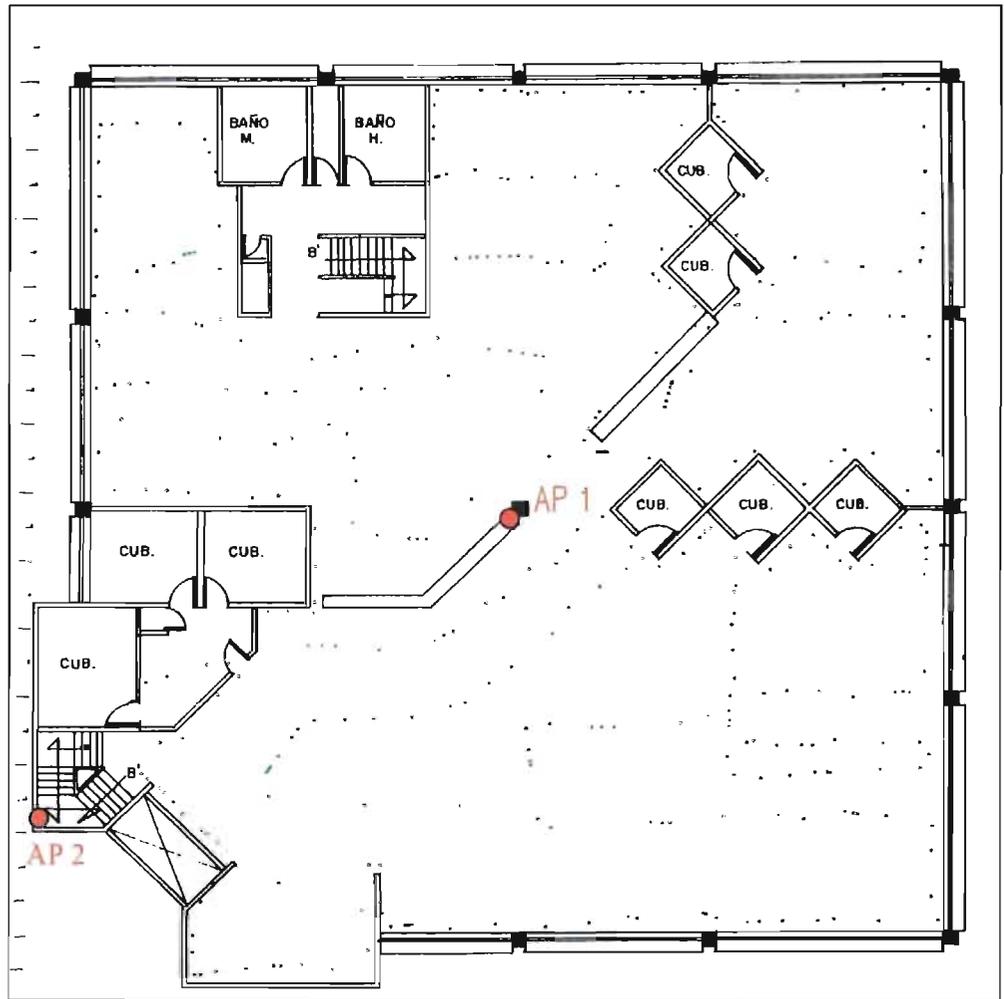
Prueba interior de la biblioteca planta alta.



Access Points Seleccionados

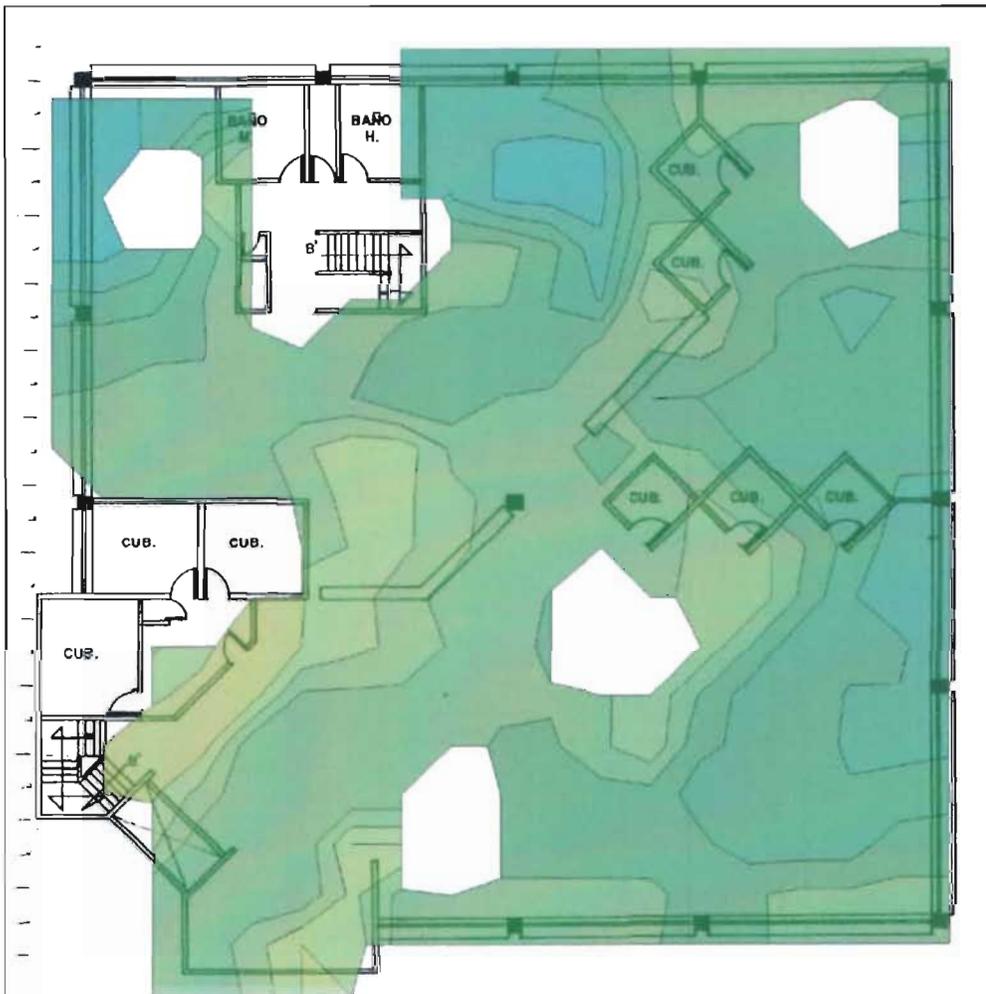
ESSID	Name	Band / Channel	Privacy
cuauti_wifi	00:13:10:2A:CC:DB	802.11b / 11	No
cuauti_wifi	00:0C:41:67:F8:49	802.11b / 1	No

Puntos Muestreados y Ubicación del Access Point



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Fuerza de la Señal



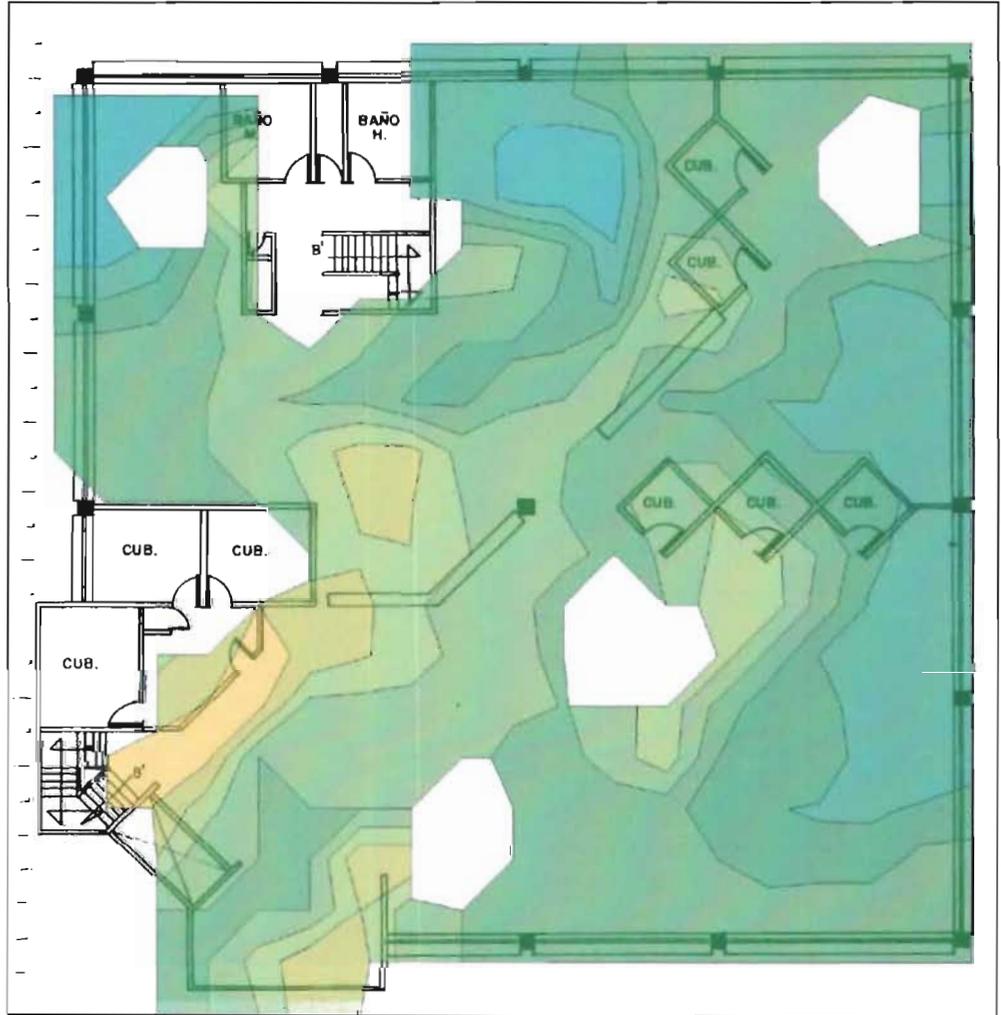
Cobertura de la fuerza de la señal (RSSI) de los Access Points seleccionados. Se muestra la mayor intensidad por ubicación

-100.0..-95.0	-95.0..-90.0	-90.0..-85.0	-85.0..-80.0	-80.0..-75.0	-75.0..-70.0	-70.0..-65.0
-65.0..-60.0	-60.0..-55.0	-55.0..-50.0	-50.0..-45.0	-45.0..-40.0	-40.0..-35.0	-35.0..-30.0
-30.0..-25.0	-25.0..-20.0	-20.0..-15.0	-15.0..-10.0	-10.0..-5.0	-5.0..0.0	



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Relación Señal a Ruido

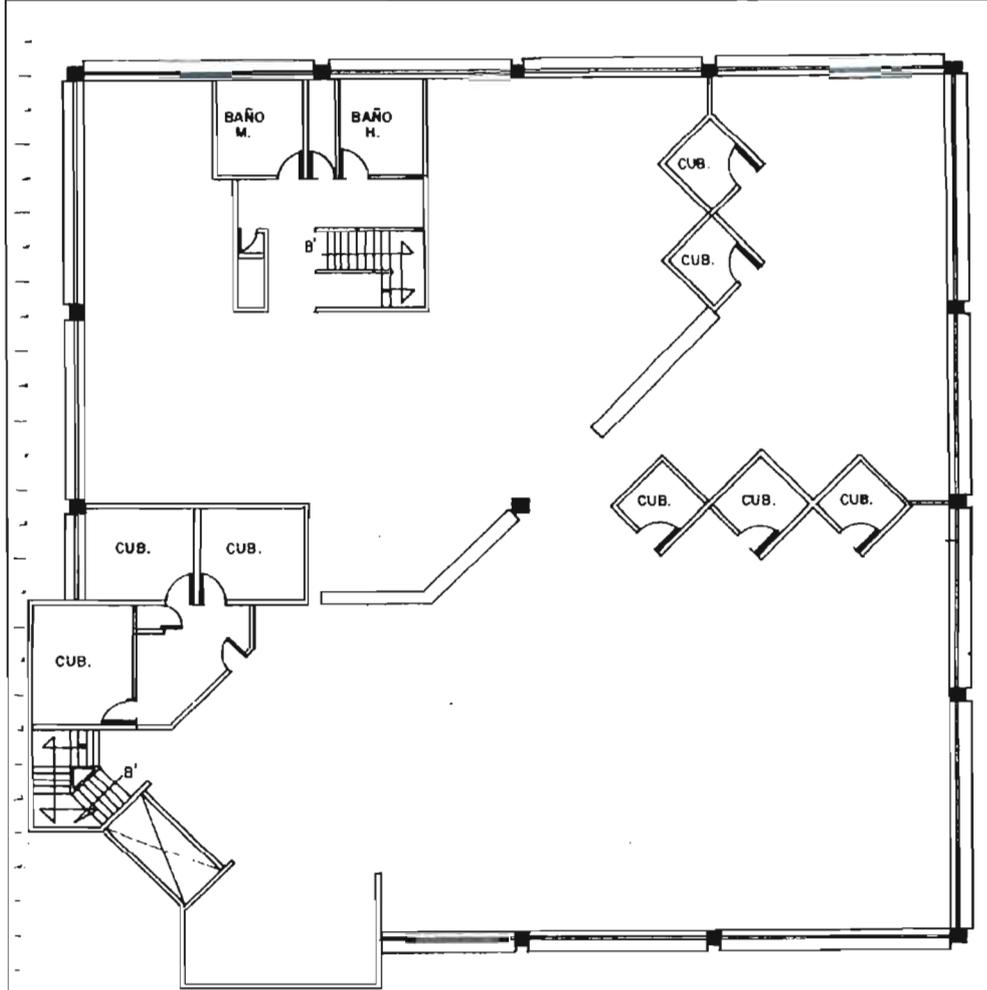


Relación señal a ruido calculada. Formula simplificada: $SNR = [Fuerza\ de\ la\ Señal] - [Interferencia]$

0.0..5.0	5.0..10.0	10.0..15.0	15.0..20.0	20.0..25.0	25.0..30.0
30.0..35.0	35.0..40.0	40.0..45.0	45.0..50.0	50.0..55.0	55.0..60.0
60.0..65.0	65.0..70.0	70.0..75.0	75.0..80.0		

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Interferencia



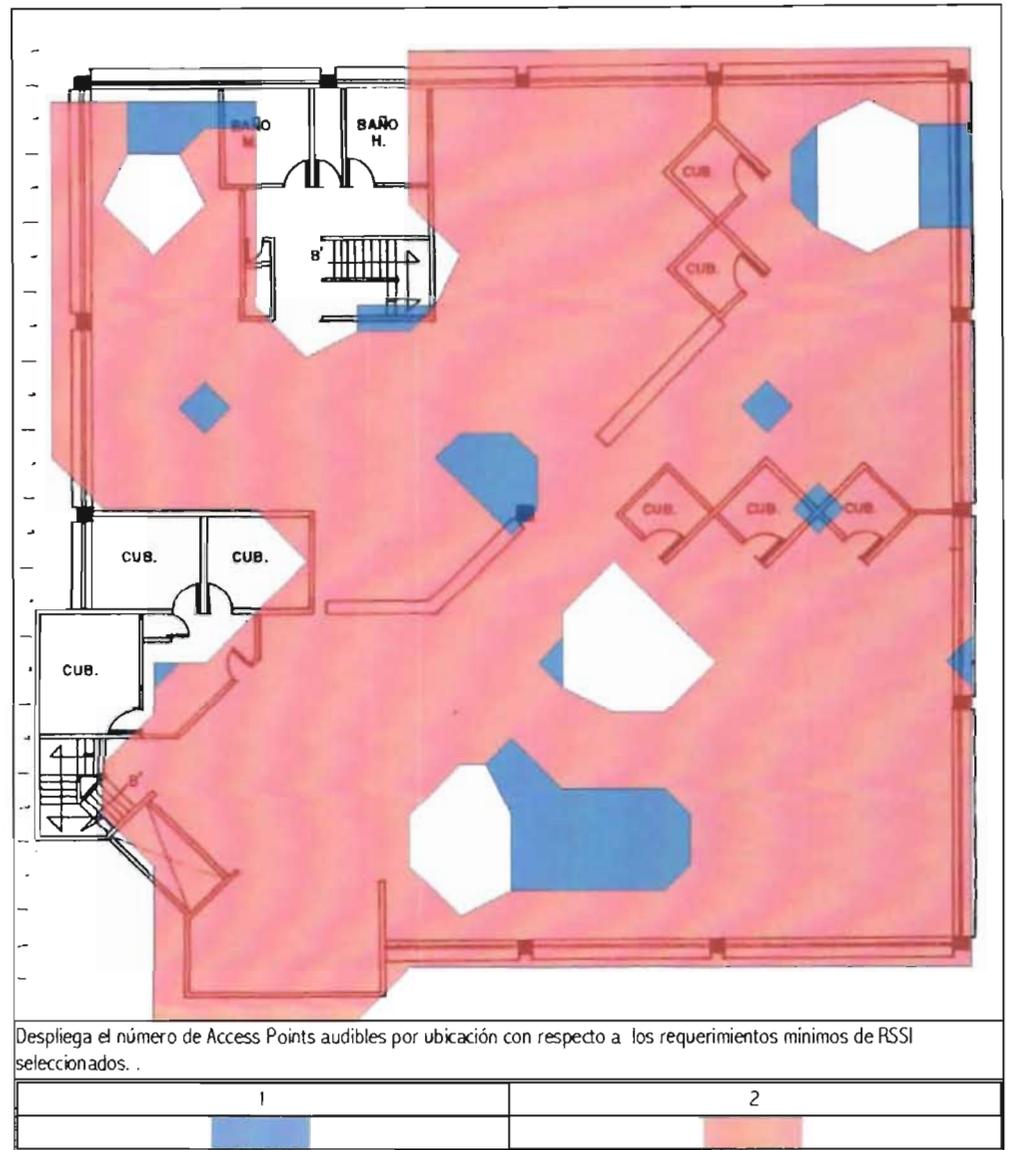
Interferencia calculada.

-100.0..-95.0	-95.0..-90.0	-90.0..-85.0	-85.0..-80.0	-80.0..-75.0	-75.0..-70.0	-70.0..-65.0
-65.0..-60.0	-60.0..-55.0	-55.0..-50.0	-50.0..-45.0	-45.0..-40.0	-40.0..-35.0	-35.0..-30.0
-30.0..-25.0	-25.0..-20.0	-20.0..-15.0	-15.0..-10.0	-10.0..-5.0	-5.0..0.0	



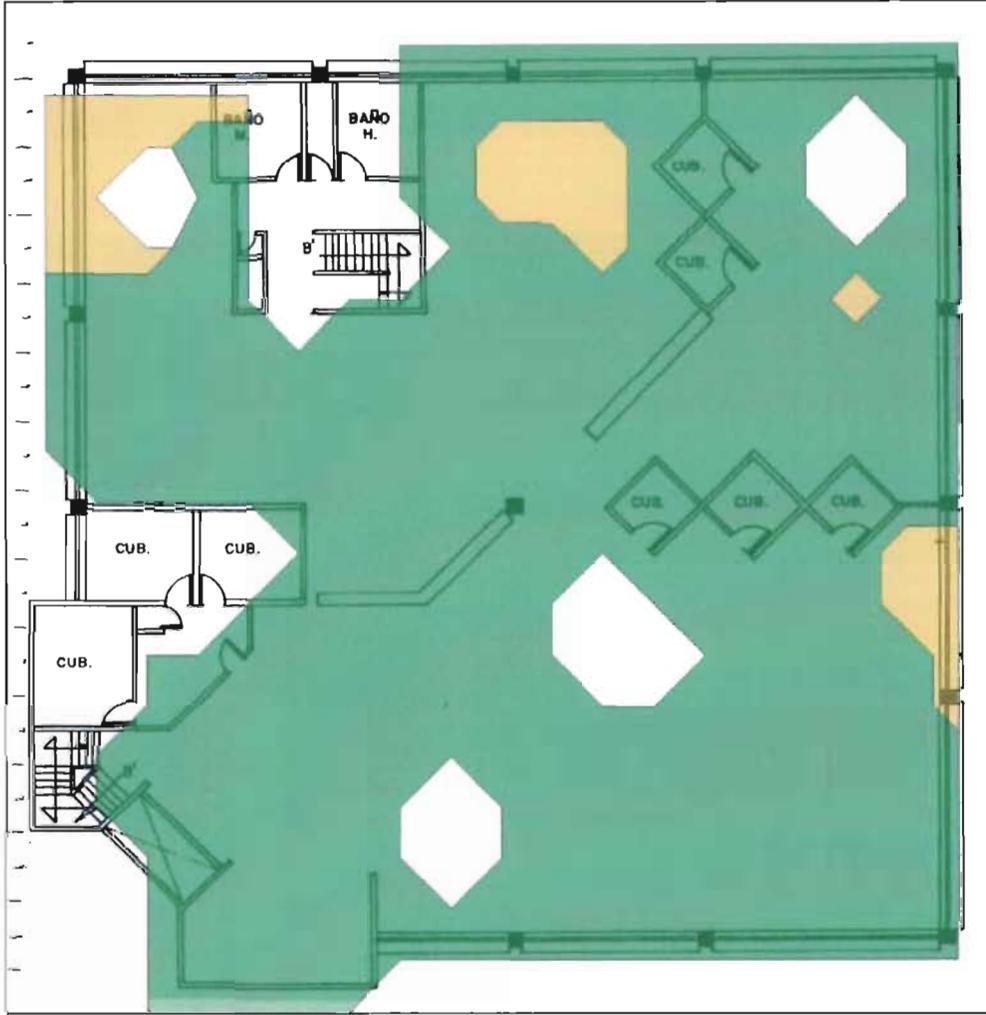
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Cuenta de Access Points



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Velocidades de Datos



Velocidad máxima estimada por ubicación, con respecto al umbral de la relación señal a ruido seleccionada y los valores de sensibilidad de la tarjeta de red utilizada.

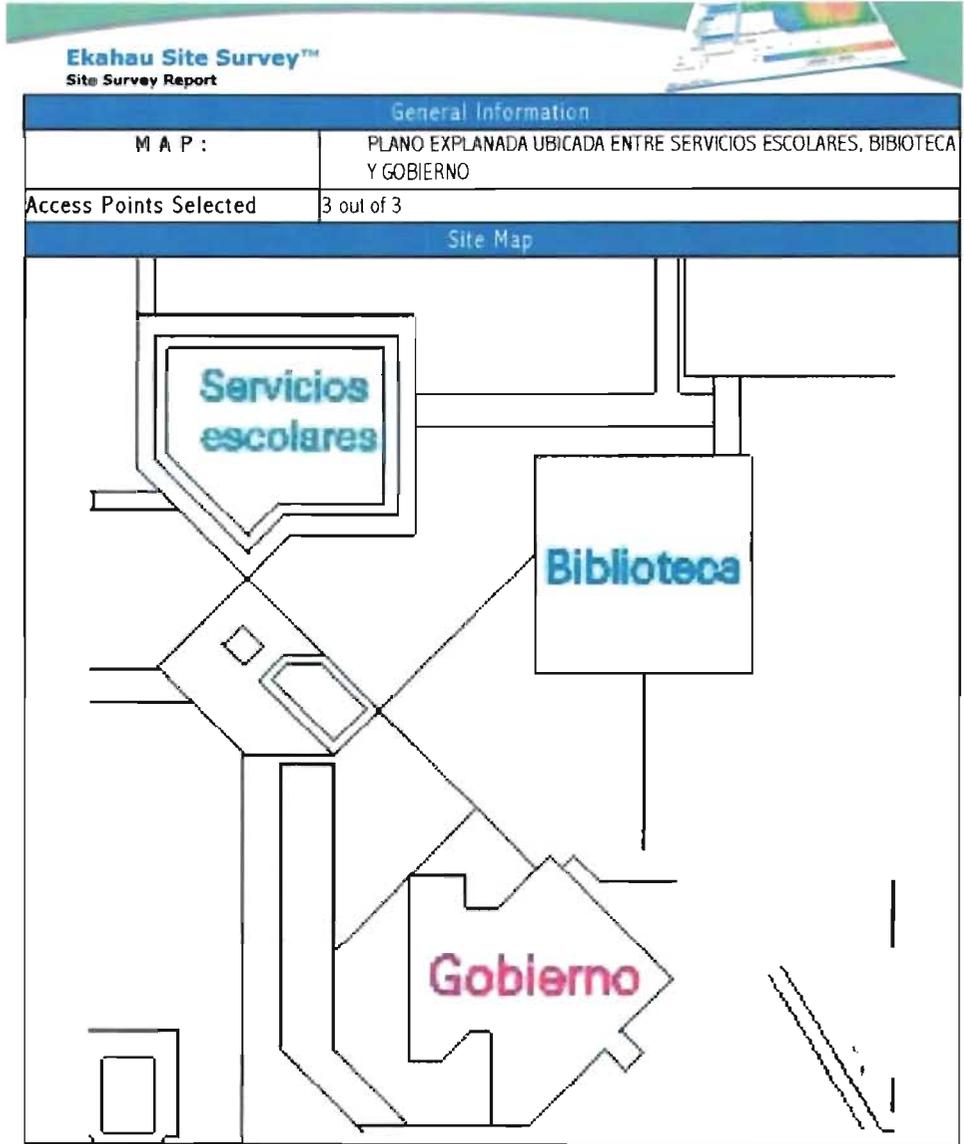
1.0	2.0	5.5	11.0



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

172

Prueba exterior de la explanada.

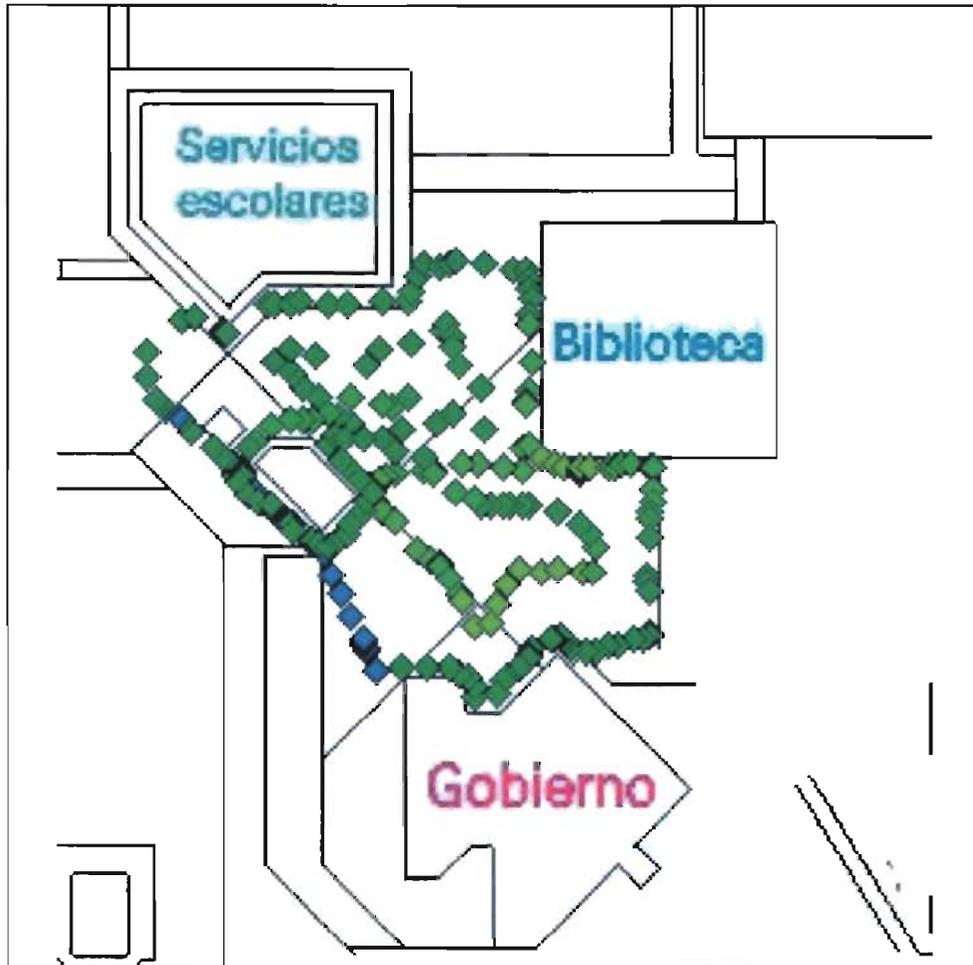


IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Access Points Seleccionados

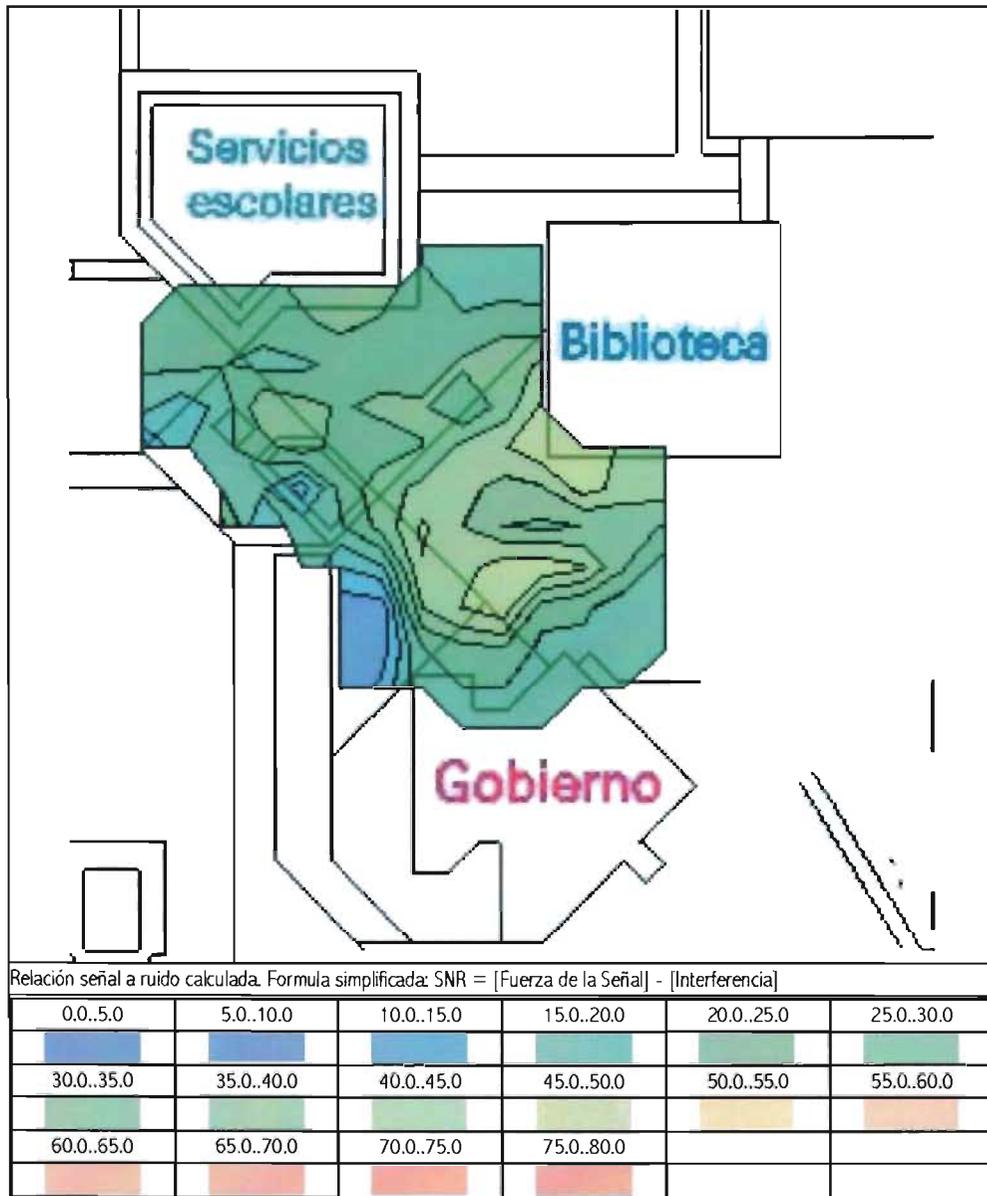
ESSID	Name	Band / Channel	Privacy
cuauti_wifi	00:13:10:2A:CC:DB	802.11b / 11	
cuauti_wifi	00:0C:41:67:F8:49	802.11b / 1	
suvimex	00:40:96:57:B2:33	802.11b / 6	WEP

Puntos Muestreados y Ubicación del Access Point



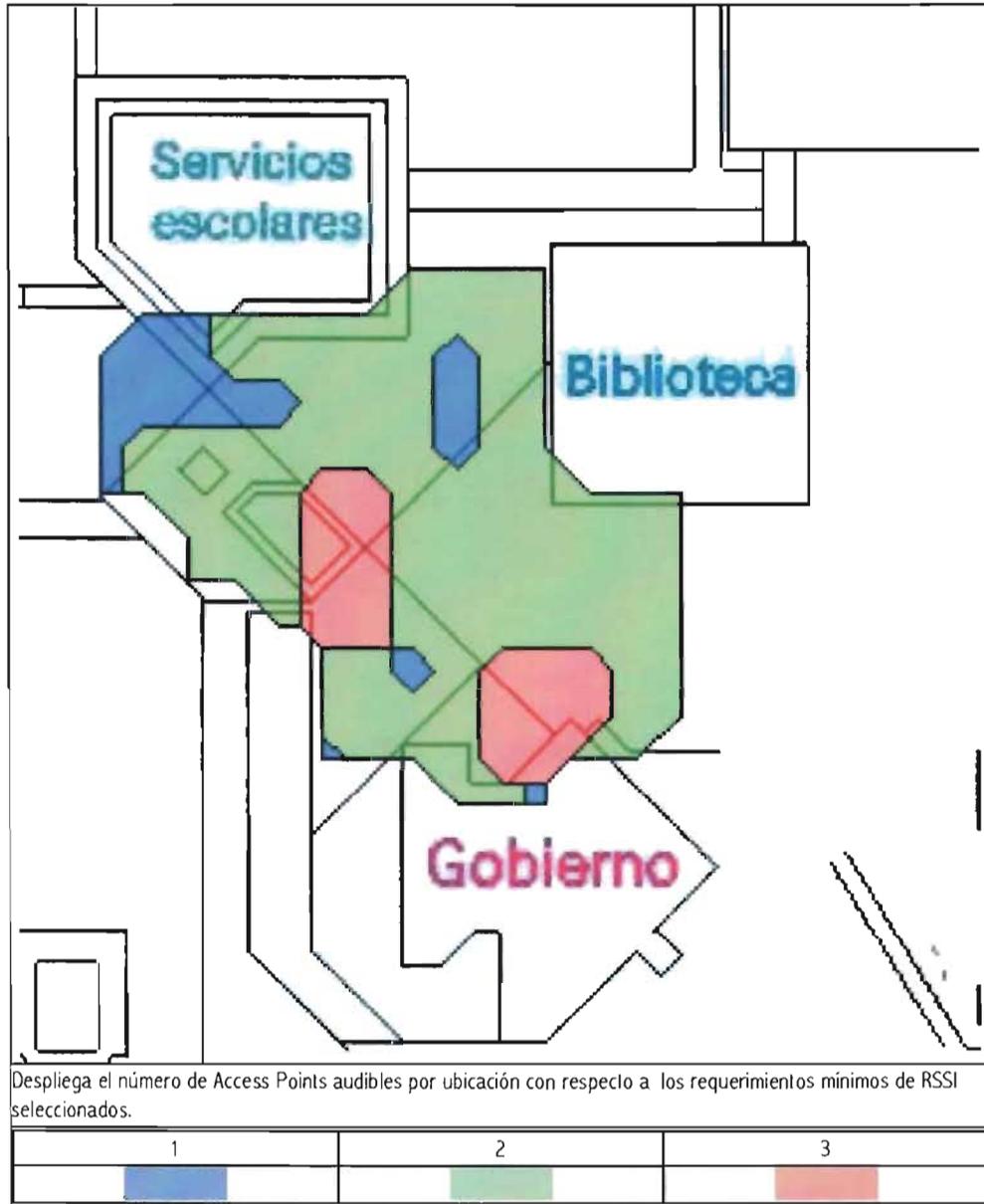
IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Relación Señal a Ruido



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

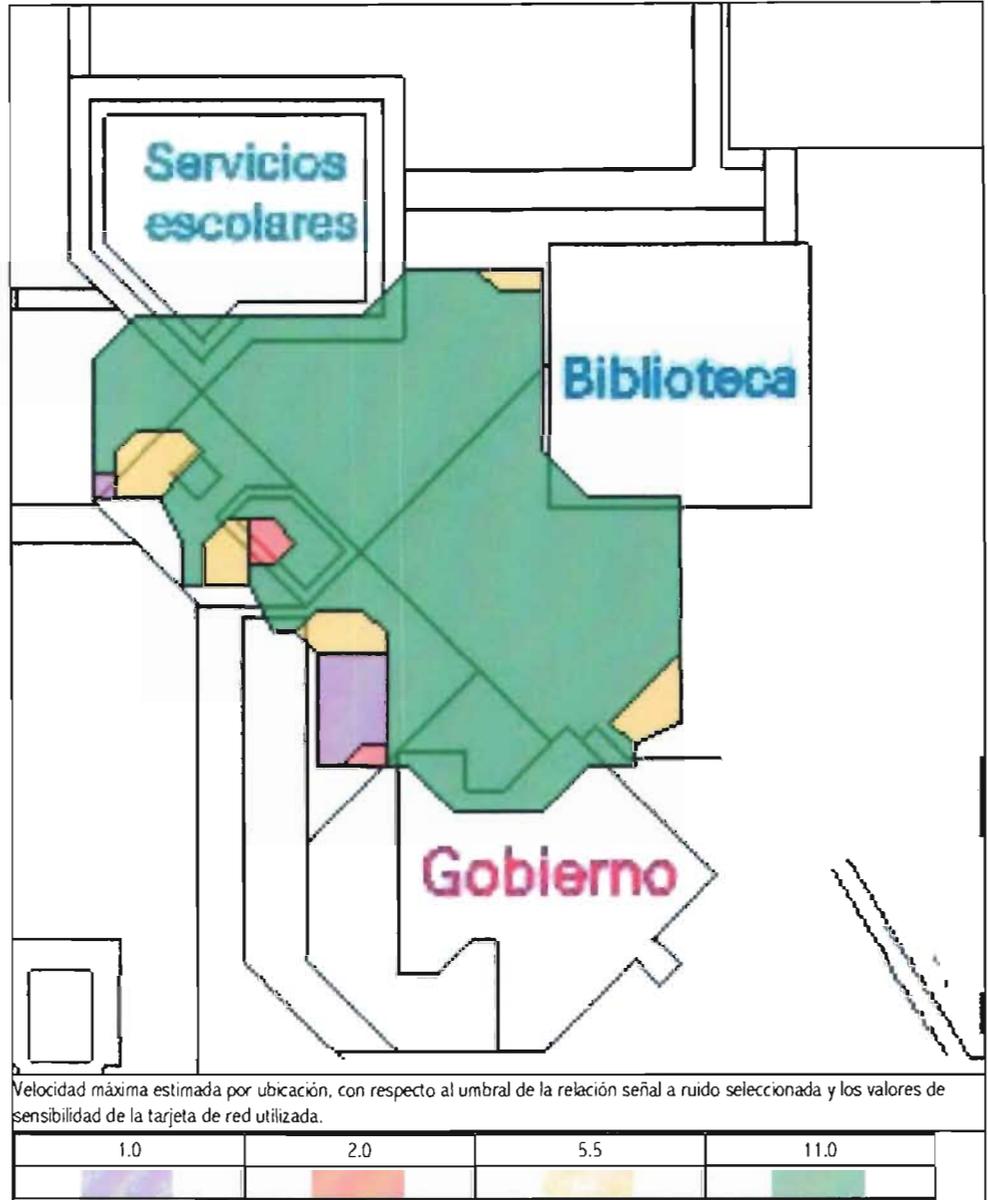
Cuenta de Access Point



IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

Velocidades de Datos

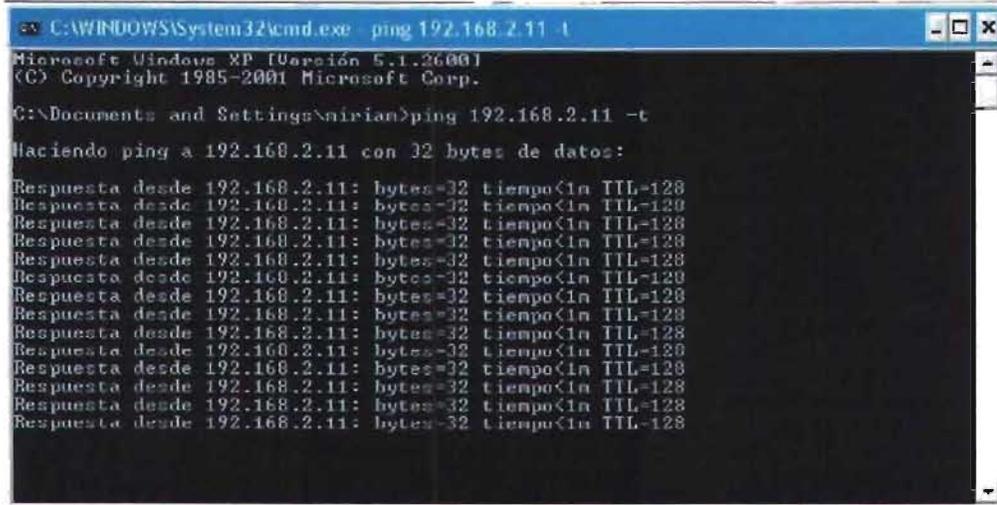
178



c) Pruebas de conexión

PING

Se realizaron pruebas de ping para comprobar que había comunicación entre dos equipos, esta es la prueba más sencilla que existe para comprobar que haya conectividad entre los equipos.

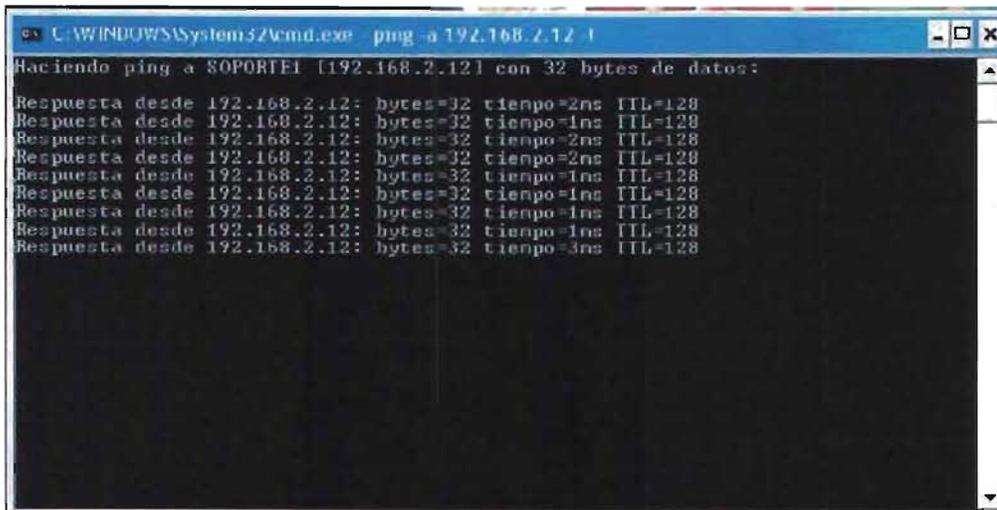


```
C:\WINDOWS\System32\cmd.exe ping 192.168.2.11 -t
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Nirvan>ping 192.168.2.11 -t

Haciendo ping a 192.168.2.11 con 32 bytes de datos:

Respuesta desde 192.168.2.11: bytes=32 tiempo<1n TTL=128
```



```
C:\WINDOWS\System32\cmd.exe ping -a 192.168.2.12 -t
Haciendo ping a SOPORTE1 [192.168.2.12] con 32 bytes de datos:

Respuesta desde 192.168.2.12: bytes=32 tiempo=2ns TTL=128
Respuesta desde 192.168.2.12: bytes=32 tiempo=1ns TTL=128
Respuesta desde 192.168.2.12: bytes=32 tiempo=2ns TTL=128
Respuesta desde 192.168.2.12: bytes=32 tiempo=2ns TTL=128
Respuesta desde 192.168.2.12: bytes=32 tiempo=1ns TTL=128
Respuesta desde 192.168.2.12: bytes=32 tiempo=3ns TTL=128
```

Se probó también la conexión a Internet, intentando acceder a diversas páginas y se descargó un software.



■ IV.4.4 [Cierre]

Acta de entrega.

Una vez instalado y probado todo se hace la entrega formal del proyecto.



UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

México, DF, a 28 de abril del 2005

ING. MOISES HERNÁNDEZ DUARTE
JEFE DEL CENTRO DE CÓMPUTO
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FES CUAUTTLÁN

ACTA DE ENTREGA / RECEPCIÓN DE INSTALACION

PROYECTO: PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA.

DE CONFORMIDAD CON EL LA PROPUESTA TÉCNICA SE ENTREGA A SATISFACCIÓN DE **UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**, LOS EQUIPOS QUE CONFORMAN EL PROYECTO ASI COMO TODA LA INSTALACIÓN.

SUMINISTRO E INSTALACION DE:

ACCESS POINT

PUNTO DE ACCESO MARCA LINKSYS MODELO WAP11 , QUE OPERA EN LA FRECUENCIA DE 2.4GHZ BAJO EL ESTÁNDAR 802.11B. SOPORTA FILTRADO DE DIRECCIONES MAC Y CLIENTE DHCP. CUENTA CON ANTENAS AJUSTABLES Y DESMONTABLES.

SU SISTEMA DE CONFIGURACION ESTA BASADO EN NAVEGADOR WEB LO QUE LO HACE MUY FACIL DE USAR.

SOPORTA ENCRIPCION DE 256 BITS

RUTEADOR INALÁMBRICO

RUTEADOR INALAMBRICO MARCA LINKSYS MODELO WRT54G, QUE OPERA EN LA FRECUENCIA DE 2.4GHZ Y SOPORTA TANTO EL ESTÁNDAR 802.11b COMO 802.11G.

EL RUTEADOR PUEDE FUNCIONAR COMO SERVIDOR DHCP, DISPONE DE TECNOLOGÍA NAT DE PROTECCIÓN CONTRA INTRUSOS, ADMITE PASO A TRAVÉS VPN Y SE PUEDE CONFIGURAR PARA FILTRAR EL ACCESO A INTERNET DE LOS USUARIOS INTERNOS. LA UTILIDAD DE CONFIGURACIÓN BASADA EN EXPLORADOR WEB HACE DE ÉSTA UNA TAREA SENCILLÍSIMA.

ANTENA OMNIDIRECCIONAL

ANTENA OMNIDIRECCIONAL MARCA MAXRAD, MODELO XTREMEWAVE MFB2400B.

PROPORCIONA UNA GANANCIA DE 8 DBI. LA ANTENA ESTA ENCAPSULADA EN UN EMPAQUE DE FIBRA DE VIDRIO QUE LA PROTEGE DE LOS RAYOS UV, LO QUE LA HACE MUCHO MÁS DURADERA, ADEMÁS

IV. PROYECTO PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

DE QUE ESTÁ DISEÑADA PARA SOPORTAR LAS INCLEMENCIAS DEL TIEMPO Y LAS CORRIENTES DE AIRE.
TIENE UN CONECTOR TIPO N-MEMBRA, ES DE POLARIZACIÓN VERTICAL, MIDE 50CM APROXIMADAMENTE Y PESA 230GR

PIGTAIL

PIGTAIL CON CONECTOR N-MACHO EN UN EXTREMO Y TNC ROSCADO EN EL OTRO.

CABLEADO

SE INSTALARON 69 MTS UTP CATEGORÍA 6 PARA CABLEAR DESDE EL IDF UBICADO EN LA PLANTA BAJA DE LA BIBLIOTECA, HASTA LA PLANTA ALTA, REUTILIZANDO UNA TUBERÍA DE ALUMINIO GALVANIZADO YA EXISTENTE
SE UTILIZARON 37MTS DE UTP DE USO RUDO PARA INTERCONECTAR LOS DOS EQUIPOS.

RECIBE
UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO
FES CUAUTITLÁN


ING. MOISES HERNÁNDEZ DUARTE

ENTREGA


MIRIAM CARRADA HERNÁNDEZ.

Debido a que la tecnología siempre esta en constante crecimiento, es necesario evolucionar junto con ella y tratar de aprovechar lo que esta tecnología nos pueda brindar para mejorar nuestro entorno.

Las redes inalámbricas nos brindan comodidad (flexibilidad) y movilidad, además que nos permiten llegar a lugares donde es difícil llevar a cabo una red cableada, ya sea por la distancia, el diseño arquitectónico o el costo. Dependiendo del problema que tengamos que resolver, es necesario hacer un análisis de que es lo más viable y lo que más se adapta a nuestras necesidades.

La implementación de la red inalámbrica en la Facultad de Estudios Superiores Cuautitlán Campus 4 es el primer paso que se da en este campus, para brindar un servicio inalámbrico que permita a los alumnos aprovechar los recursos ofrecidos para tener nuevas herramientas de estudio y fuentes de información.

Conforme vaya popularizándose este servicio, y dependiendo de la demanda es posible que pueda extenderse a otros edificios (salones de clase), lo que ayudaría o auxiliaría a los profesores en su cátedra.

Es difícil determinar el número de usuarios que utilizarán la red, pues es el primer Hot spot inalámbrico que se implementa en la esta Facultad. Esperemos que poco a poco se abran más oportunidades para implementar este tipo de servicios en la UNAM, pues considero que es una herramienta importante y útil, además que es una tecnología que puede brindar muchos beneficios aparte del aquí desarrollado.



[A]

ANCHO DE BANDA – Es la cantidad de información que puede ser transmitida en un canal.

AP – (Access Point) Punto de acceso; dispositivo que normalmente conecta a los dispositivos del cliente con la porción Ethernet de una LAN, y maneja las comunicaciones de todos los dispositivos que forman la red inalámbrica.

ASCII – Código normalizado americano para el Intercambio de Información. Este código asigna a cada letra número o signo empleado por los ordenadores, una determinada combinación de ceros y unos.

ATENUACIÓN – Reducción en la densidad de potencia con la distancia de la fuente, conforme se aleja un frente de onda de la fuente, el campo electromagnético radiado se dispersa.

ATM – Modo de transferencia asíncrono, es una tecnología de transmisión de datos de alta velocidad, que puede transmitir diferentes tipos de información (voz, datos, video, audio, etc.)

AUTENTICAR – Verificar la identidad de algún equipo.

[B]

BIT – Es la unidad más pequeña de información, que puede asumir solo dos valores, 1 o 0.

BFSK – (FSK) Modulación de frecuencia por desplazamiento binario; envía un 1 a través de una frecuencia y un 0 por medio de otra frecuencia.

BPS – Bits por segundo, es la unidad de medida de la velocidad de transmisión de datos.

BPSK – Modulación de fase por desplazamiento binario; enviará un 1 con una fase y un 0 a través de otra fase.

BRIDGE – Puente. Un puente de red une dos segmentos de una misma red. Un AP puede actuar como puente entre una los segmentos de una red inalámbrica y una red cableada.

BYTE – Unidad de información conformada por 8 bits.

[C]

CLIENTE – Dispositivo de red que es total que depende de algún otro dispositivo, en una red Wi-Fi el cliente es una computadora (laptop) PDA u otro dispositivo que se comunique con la red a través de un AP. También recibe el nombre de estación.

COLISIÓN – Resultado de la transmisión de dos nodos al mismo tiempo. Las tramas de cada dispositivo se impactan y se dañan cuando se encuentran en un medio físico



[D]

DHCP – (Dynamic Host Configuration Protocol) Protocolo de configuración dinámica del Host; técnica que permite a un equipo asignar direcciones IP de manera automática a los ordenadores conectados a él, de manera que las direcciones se puedan reciclar cuando un equipo ya no la necesite.

DIFRACCIÓN – redistribución de energía, dentro de un frente de onda cuando pasa cerca del extremo de un objeto opaco. Cuando la señal se encuentra una obstrucción, se dobla pasar al alrededor de la obstrucción.

DIRECCION IP – Es una serie de números que identifica a los equipos conectados para las comunicaciones que se realizan en la red. Existen dos tipos de direcciones IP, las públicas (INTERNET) y las privadas

DIRECCION MAC – Es un número único que asignan los fabricantes a los dispositivos de red. Este número es permanente y viene grabado en el dispositivo para permitir identificarlo. Las direcciones MAC están formadas por 12 caracteres alfanuméricos

DNS – (Domain Name Server) Sistemas de nombre de dominio; traduce los nombre de dominio (www.unam.mx) a direcciones IP (132.248.10.7)

DS – Sistema de Distribución, se refiere a la topología de la red cableada que se conecta a los APs con el fin de proveer diferentes servicios y obtener acceso a recursos de la red cableada.

[E]

EIRP – Potencia de radiación isotrópica efectiva. Expresa el desempeño de un sistema de transmisión en una dirección específica. Se expresa en Watts o dBw.

ETSI – Instituto Europeo de Normas de Telecomunicaciones, fue creado en marzo de 1989, y se encarga de regular las telecomunicaciones en Europa.

[F]

FCC – Comisión Federal de Comunicaciones, agencia gubernamental de Estados Unidos que supervisa, controla y otorga licencias sobre los estándares de transmisión electrónica y electromagnética.

FIREWALL – Es un direccionador o servidor de acceso que tiene la tarea de funcionar como búfer entre cualquier red pública conectada y una red privada. Controla los accesos a una red local desde el exterior (dispositivo de seguridad)

FRECUENCIA. Es la alternancia o ciclos por tiempo. La amplitud oscila de cero a un límite máximo y de regreso. El número de tiempos que el ciclo se repite en un segundo recibe el nombre de frecuencia.

FTP – Protocolo de transferencia de archivos; es un protocolo de Internet que permite transferir archivos de un ordenador a otro.

[G]

GATEWAY – Dispositivo que conecta y pasa paquetes entre dos segmentos de red que usan el mismo protocolo de comunicación. Los gateways operan en la capa de enlace de datos del modelo de referencia OSI. El filtraje, reenvío o rechazo de la trama dependerá de la dirección MAC de dicha trama.

[H]

HOST – Dispositivos que se conectan directamente a un segmento de red, por ejemplo una PC, una impresora, un servidor, etc.

HOTSPOT – es un punto de acceso público a Internet, normalmente se encuentran en restaurantes, salas de espera en terminales aeroportuarias, en el lobby de un hotel, universidades, etc.

HTTP – Protocolo de transporte de hipertexto, se utiliza en Internet para transferir la información Web.

[I]

IEEE – Institute of Electrical and Electronics Engineers; organización que aprueba y desarrolla estándares por una amplia variedad e tecnologías de computación.

ÍNDICE DE REFRACCIÓN – Sirve para calcular la diferencia entre el ángulo de incidencia y el de refracción del haz, también se conoce como la relación entre la velocidad de la luz en el vacío y el medio.

INTERFERENCIA – Cuando dos o más ondas electromagnéticas se combinan de tal forma que el funcionamiento del sistema se degrada. Consiste en la presencia no deseada de señales (de la misma naturaleza que la que se está utilizando) que interrumpen el normal funcionamiento del sistema, o impiden que la comunicación se pueda establecer.

IRRADIAR – Transmitir, propagar, difundir.

ISP – Proveedor de Acceso a Internet, es cualquier empresa que preste el servicio de acceso a Internet a sus clientes o usuarios.

[M]

MAC – Control de Acceso a medios, es la inferior de las subcapas de la capa de enlace de datos del modelo de referencia OSI. Controla el acceso a los medios compartidos.

MODEM – Modulador / Demodulador, dispositivos que convierte señales digitales de tal forma que se puedan transmitir a través de un equipo de comunicación análogo, y ya en su destino las señales análogas se vuelven a convertir a su forma digital.

MODULACIÓN – es la variación de una señal ya sea en su amplitud, en su frecuencia o en su fase con el fin de poderla transmitir. Existen dos tipos de modulación: modulación digital y modulación analógica.



[N]

NAT – Traducción de direcciones de red. Es un estándar que permite a las redes locales conectadas a Internet utilizar su propio sistema de numeración IP privado, compartiendo una misma dirección IP pública.

NIC – Tarjeta interfaz de red, se necesita una tarjeta de red para que cualquier equipo pueda conectarse cableada o inalámbricamente a una red LAN.

[O]

ORIENTADO A CONEXIÓN – Establecer previamente una trayectoria antes de transmitir información.

ORIENTADO A NO-CONEXIÓN – No se establece una trayectoria previa antes de transmitir información; la información se enruta conforme transita a través de la red.

[P]

PAQUETE – Agrupamiento lógico de información que incluye un encabezado que contienen la información de control y los datos del usuario.

PING TEST – es una de las pruebas mas utilizadas para comprobar la función más básica de una red IP, la entrega de un solo paquete. Consiste en que se envían datos cortos en un solo paquete, y se espera la contestación de la estación receptora. Sirve para comprobar comunicación entre dos estaciones.

POP – Protocolo de Oficina de correos, este protocolo permite a los usuarios acceder a un host y transferir a su computadora todo el correo recibido, dirigido a ellos.

PROTOCOLO – Reglas que gobiernan el intercambio de información entre los dispositivos de una red.

[Q]

QPSK – Modulación de fase por desplazamiento en cuadrante. Tiene cuatro estados de fase representados por las combinaciones binarias ya sea 00, 01, 10, 11. Todos mantienen la onda portadora con la misma amplitud y frecuencia. Codifica 2 bits de la información en la misma cantidad de espectro que BPSK.

QAM – Modulación de amplitud del cuadrante; modula la frecuencia portadora de onda tanto en su fase como en su amplitud.

QoS – (Quality of Service) Calidad de servicio, característica de algunos protocolos de red que trabajan con distintos tipos de tráfico, para asegurar los niveles requeridos de confiabilidad y latencia.

[R]

RADIAR – Difundir por medio de las ondas electromagnéticas sonidos e imágenes

REFLEXIÓN – Acto de reflejar; ocurre cuando una onda incidente choca con alguna barrera, una parte de la onda penetra el medio, y la parte que no penetra el medio se refleja con un ángulo

diferente al de inducción.

REFRACCIÓN – Cambio de dirección de un rayo conforme pasa oblicuamente, de un medio a otro, con diferentes velocidades de propagación. (Doblamiento de la señal) La refracción ocurre siempre que una onda de radio pasa de un medio a otro medio de diferente densidad.

RELACION SEÑAL A RUIDO – En una comunicación de radio es el resultado de dividir el valor de la fuerza de la señal de los datos por el valor de la fuerza del ruido. Generalmente, se expresa en dB y se utiliza como indicativo de la calidad de comunicación; cuanto mayor sea este valor mejor será la comunicación.

RUIDO – Señal ajena que interfiere con la señal que transporta la información.

ROAMING – Capacidad que permite a un dispositivo desplazarse de un lugar a otro sin perder la conexión inalámbrica.

ROUTER – Dispositivo utilizado para transferir datos entre dos redes que utilizan un mismo protocolo.

[S]

SERVIDOR – Software que permite ofrecer servicios remotos a sus usuarios, también recibe el nombre de servidor el equipo en el que está instalado el software servidor.

SSID – Es un distintivo del nombre de red. Nombre de la red.

[T]

TELNET – Es una aplicación que permite el acceso remoto a otros equipos, y permite trabajar como si fuese un usuario local.

TCP / IP – Protocolo de control de transmisión / Protocolo de Internet.

TFTP – Protocolo de transferencia de archivos trivial; versión simplificada de FTP que permite la transferencia de archivos de un equipo a otro a través de la red.

[U]

UDP – (User Datagram Protocol) es un protocolo de comunicaciones que ofrece una cantidad limitada de servicio cuando se intercambian mensajes entre computadoras, en una red que utiliza el protocolo de Internet (IP). Es una alternativa al protocolo de transmisión TCP (Transmission Control Protocol). UDP utiliza IP para recibir una unidad de datos (llamada datagrama) de una computadora a otra. Al contrario de TCP, UDP no proporciona el servicio de dividir un mensaje en paquetes y volverlo a ensamblar en el otro lado.

USB – Bus serie universal, interfaz que permite conectar dispositivos a una velocidad de 1, 5 o 12Mbps, sin necesidad de apagar el ordenador y es muy práctico para conectar y desconectar dispositivos.



[V]

VELOCIDAD DE LA LUZ – La velocidad de la luz en el vacío es de 300×10^6 m/s.

VLAN – Red de área local virtual, grupo de clientes que están ubicados en distintos lugares pero que se comunican entre ellos como si pertenecieran al mismo segmento LAN.

VPN – Red privada virtual; es un enlace privado que reside entre dos partes, pero viaja a través de redes públicas.

[W]

WEP – Protocolo equivalente al cableado, se utiliza para proteger las comunicaciones inalámbricas de robo de información y de espionaje.

WLAN – Red de área local inalámbrica.

189

[Z]

ZONAS FRESNEL – Volúmenes elipsoides que residen en el espacio entre una antena transmisora y una receptora. La regla general para los enlaces de transmisión rectilínea directa es dejar 60 por ciento de la parte ubicada más al centro de la primera zona de Fresnel que esté libre de obstáculos.

[1]

10BaseT – Especificación de Ethernet 10-Mbps banda base usando dos pares de cable trenzado (categoría 3, 4, o 5): un par para los datos que se transmiten y el otro para recibir datos. - 10Base T, que es parte de la especificación de IEEE 802.3, tiene un límite de la distancia de aproximadamente 100 metros por el segmento.

■ [Libros]

Aguilar Delgado, Silvia. Sistema de enlace de la Dirección General de Obras (DGOC) con sus subdependencias vía inalámbrica.

Tesis, Facultad de ingeniería, Junio 2003

152 páginas

Brisbin, Shelly. Buid your own Wi-Fi network

New-York: Mc Graw Hill/Osborne, 2002

237 páginas.

Calzada Ríos, Carlos. Redes inalámbricas.

Tesis, Facultad de Ingeniería. Noviembre 2003

180 páginas.

Carballar, José A. Wi-Fi, como construir una red inalámbrica.

España, México: Alfaomega / Ra-Ma

249 páginas.

Cisco Systems. Cisco Airones Access Point Software Configuration guide 340 and 350 Series. Software Release 12.03T.

USA: Cisco Systems. Agosto 2003

382 páginas.

Dowes, Ford, Spainer, Stevenson, Lew. Internetworking Technologies handbook.

Second Edition. USA: Cisco Press, 1998

850 páginas.

Engs, Adam. Introducción a las redes inalámbricas.

Madrid: Anaya Multimedia. Febrero 2003

384 páginas

García Tomás, Jesús. Redes para proceso distribuido.

2a Edición. Madrid: Editorial RAMA, 2001

763 páginas

Habraken, Joe. Practical Cisco Routers.

Missouri: QUE Corporation. 1999

400 páginas

Hayden, Matt. Aprendiendo Redes en 24Hrs

México: Prentice Hall, 1999

425 páginas

Henríquez Campos, Gabriela. Redes inalámbricas.

Tesis, ENEP Aragón. Octubre 2003

147 páginas



Lowe, Rouge. Redes para dummies.
5a Edición. Panamá: ST Editorial Inc, 2001
442 páginas.

Network Associates. Ethernet Network Análisis and Troubleshooting.
Sniffer University.

Nortel Networks. Training Programe Module Frame Relay
1999 38 páginas.

Olvera Basilio, Oswaldo. Propuesta de diseño e implementación de una aplicación WLAN infrarroja punto a punto.
Tesis, Enep Aragón. Septiembre 2002
140 páginas.

Ovellet, Eric; Padjen, Robert. Building a CISCO Wireless LAN
USA, Syngress Publishing 2002
501 páginas

Ramírez Guridí, Julio Cesar. Análisis de la operación de las redes privadas virtuales.
Tesis, ENEP Aragón. Septiembre 2003
118 páginas.

Reid, Neil; Seide, Ron. Manual de redes inalámbricas 802.11 (Wi-Fi)
Mc GrawHill / Interamericana de México. Febrero 2004
364 páginas

Rivera Mera, Rosa del Pilar. Redes locales inalámbricas.
Tesis, ENEP Acatlán. Enero 2003
225 páginas.

Rojas Leal, Gabriel Andrés. Propuesta de un modelo de implementación de una red local inalámbrica para un edificio histórico.
Tesis, FES Cuautitlán. Julio 2001
55 páginas.

Sánchez y López. Redes inalámbricas Iniciación y Referencia
Madrid, México: Mc Graw Hill
Junio 2000. 336páginas.

The Home RF Technical Committee. Home RF specification.
Home RF Working Group. Revisión 2.01 Julio 2002
526 páginas

Thibodeau, Jan. The Basic Guide to Frame Relay Networking
Fremont, California: FrameRelay Forum 1988
86 páginas

- Tolluch Match. Microsoft Encyclopedia of Security.
Washington, USA; Microsoft Press 2003
414 páginas.
- Tomasi, Wayne. Sistemas de Comunicaciones Eléctricas
Segunda Edición. México, Prentice Hall Hispanoamericana 1998
858 páginas.
- Truenet, ADC. Sistema de Cableado Estructurado.
Diapositivas del Curso Truenet 2001
- Truenet, ADC. Sistema de Cableado Estructurado.
Diapositivas del Curso Truenet 2005
- Vargas Jiménez Jonathan. Tendencias de las redes inalámbricas en México WPAN WLAN WMAN
WWAN.
Tesis ENEP Aragón. Noviembre 2004
136 páginas
- Walter, Bruce. Wireless LAN end to end.
New-York: Hungryminds. 2002
382 páginas.
- Zacker, Craig. Redes Manual de Referencia
Madrid-México: McGraw Hill, 2002
346 páginas

■ [Revistas]

- Iglesias, Iván
"Sanborns Unplugged"
En Solo para ti
México Año 2 No. 4 Noviembre 2003
Pags 54-57
- Janowski, Davis. Chang, Stephanie.
"El panorama inalámbrico"
En PC MAGAZINE en Español
México No.8 Agosto 2003
Pags 38-51
- Molina, Arce, Torres
"Wi-Fi transforma su conexión"
En PC MAGAZINE en Español
México No.9 Septiembre 2003
Pags. 56-67



Varshney, Upkar
"The status and future of 802.11-Based WLANs"
En COMPUTER IEEE-Computer Society
Georgia State. No.6 June 2003
Pags. 102-105

Wi-Fi
En Popular Mechanics en Español
México Edición Especial Julio 2004
Pág. 97

■ [Web]

3Com
Redes inalámbricas en edificios históricos
Buenos Aires, Argentina
14 junio 2004
<http://lat.3com.com/lat/news/pro3/mar01034.html>

Arno, Nicolás
Principales diferencias entre 802.11b, 802.11a, 802.11g
6 Febrero 2004
<http://debaser.ath.cx/pipermail/freebaires/20036-February/002819.html>

Brain
Cableado Estructurado
México
5 Diciembre 2003
<http://www.brain.com.mx/soluciones/cableado.htm>

Bricolaje PC
Montaje de una red wireless Ad-Hoc
13 Abril 2004
http://www.baluma.com/bricolaje/wireless_adhoc/home.asp

Bruce Mc Murdo
Cisco Fast Secure Roaming
USA 24 Enero 2004
<http://www.cisco.com>

Cisco Systems
Cisco Technology Helps Keep Passengers Planes, and Luggage on Schedule at Sydney Airport
Mayo 2004
http://business.cisco.com/servletw3/filedonloader/19prd/106018/106018_kbns.pdf

Cisco Systems
Wireless Bridges Keep Egg Data Flowing for Hidden Villa Ranch
19 Mayo 2004
<http://www.cisco.com/warp/public/cc/cisco/mkt/gen/cprof/>

Crow
6 pasos para asegurar una WLAN
3 Diciembre 03
<http://www.seguridadysistemas.com>

Curso sobre redes I
3 Noviembre 2003
<http://www.lpis.com/ayudas/redes1.html>

Eamon Myers
Home RF Overview and Market Positioning
Ireland
Mayo 2004
<http://www.palowireless.com/homerf/>

Enterasys Networks
Roamabout Access Point 2000 and high rate PC card datasheet
18 septiembre 2003
www.entersys.com

Gigabit Ethernet Alliance
Gigabit Ethernet 1000 Base T (Whitepaper)
California
5 enero 2004
<http://www.gigabit-ethernet.org>

Gigabit Ethernet Alliance
Running 100BaseT: Gigabit Ethernet over cooper (Whitepaper)
5 Enero 2004
<http://www.gigabit-ethernet.org>

Göran Malmgren
HiperLAN Type 2.- An emerging world wide WLAN Standard
Sweden, Ericsson Research Access Networks
14 Mayo 2004
http://www.issis_council.org/proc00/papers/6_3.pdf

Hipelan2 Global Forum
HiperLAN 2. The Broadband Radio transmission Technology Operating in the 5GHz Frequency Band.



6 Mayo 2004
<http://www.hiperlan2.com>

Historia de las redes inalámbricas
25 Febrero 2005
<http://www.tecnotopia.com.mx/redes/redinalambricas.htm>

Hotspot Internacional Wireless High Speed Internet Access.
América latina
Diciembre 2003
<http://www.hotspotinternational.com>

IEEE
802.11G 2003 Standard for IT-Telecommunications and Information exchange between systems LAN/
MAN
Septiembre 2004
<http://standards.ieee.org/getieee802/download/802.11g-2003.pdf>

Intel
How Fast wireless networks help your business to grow
Agosto 2004
<http://developer.intel.ru/download/network/pdf/802.11a.pdf>

Jim Zyren
IEEE 802.11g Explained
Intersil Corporation
6 mayo 2004
http://www.techonline.com/pdf/pavillions/standards/intersil_80211g.pdf

Las tecnologías alámbrica e inalámbrica de telecomunicaciones. Orígenes y Desarrollo
16 Febrero 2005
<http://lanic.utexas.edu/la/México/Telecom/cap1.html>

Linksys, Jim Harrington
Antenna Basics
17 Diciembre 2004
<http://www.linksys.com/products/images/antennawhtpaper.pdf>

Matínez, Evelio
Bluetooth afila sus dientes
Facultad de Ciencias de la universidad Autónoma de Baja California
18 Febrero 2004
<http://www.spain-telecom.net/Informes%203.htm>

MaxRad
XtremeWave MFB Series
26 Marzo 2005
http://www.maxrad.com/cgi/maxrad_products_ind.cgi?product=10068&catalog=10002

Microsistemas INC.
El ABC de una red doméstica
Caracas
27 Abril 2004
<http://www.mssimplex.com/red.htm>

Microsoft
Tecnologías para redes LAN inalámbricas y Windows XP
12 Marzo 2004
<http://www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/intro.asp>

Pierre Trudeau
Building Secure Wireless Local Area Networks (Whitepaper)
Colubris Networks Inc.
19 Febrero 2004
<http://colubris.com>

Pierro, Kate
Securing HOTSPOTS with RADIUS. Interlink Networks (Whitepaper)
3 Mayo 2004
<http://www.interlinknetworks.com>

Pejman, Rochan
802.1x authenticates 802.11 wireless
2 Febrero 2004
<http://www.nwfusion.com/news/tech/2001/0924tech.html>

Redes inalámbricas
27 Octubre 2003
<http://www.cybercursos.net/article.php?sid=20>

Redes WAN
3 Diciembre 2003
<http://www.geocities.com/nicaraocalli/Redes/WAN/wan1.htm>

Serrano David
Redes inalámbricas WLAN
Universidad de Alcalá de Henares
Diciembre 2003
<http://www.arrakis.es/~sergilda/wlan>



Split
Bluetooth: el futuro de las comunicaciones
<http://hispace.com/conttuto.asp>

Telcel
¿Que es GSM?
5 Mayo 2004
<http://telcel-gsm.com/pages/gsm.html>

Texas Instruments
IEEE 802.11g New draft Standard Clarity Future of Wireless LAN
6 mayo 2004
http://www.ss-mag.com/pdf/802_11_g_whitepaper.pdf

Torben Rune
HiperLAN the Approaching standard for Wireless LANs
14 junio 2004
http://www.netplan.dk/hip.lhtm#_toc390228496

Vocal Technologies, Ltd
IEEE 802.11a standard (Whitepaper)
6 Mayo 2004
http://www.vocal.com/white_paper/ieee_802.11a_standard_wp1.pdf

Vocal Technologies, Ltd
IEEE 802.11b Whitepaper
6 Mayo 2004
http://www.vocal.com/white_paper/iee_802.11b_wp1.pdf

Webopedia
Wi-Fi
2 Marzo 2004
<http://www.webopedia.com/term/w/wi-fi.html>

WiFi Alliance
Securing Wi-Fi in the Enterprise Whitepaper
12 Marzo 2004
http://www.wi-fi.org/opensection/pdf/whitepaper_wi-fi_enterprise2-06-03.pdf

Wikipedia
Wi-Fi
2 Marzo 2004
<http://www.wikipedia.org/wiki/wi-fi>

BIBLIOGRAFÍA

Wireless
18 Octubre 2003
<http://searchnetworking.techtarget.com>
<http://searchmobilecomputing.techtarget.com>

