INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
SECCIÓN DE ESTUDIOS DE POSTGRADO E INVESTIGACIÓN

MAESTRÍA EN CIENCIAS EN INGENIERÍA DE TELECOMUNICACIONES

Diseño de la Red Inalámbrica para la UPIITA y la UPIBI del Instituto Politécnico Nacional

Tesis que para obtener el grado de Maestro en Ciencias en Ingeniería de Telecomunicaciones presenta el ING. MIGUEL BORZELLI ARENAS

ASESOR
DR. SALVADOR ÁLVAREZ BALLESTEROS

MÉXICO D.F.
2005

CGPI-14

INSTITUTO POLITECNICO NACIONAL

COORDINACION GENERAL DE POSGRADO E INVESTIGACION

ACTA DE REVISION DE TESIS

En la Ciudad de México, D. F. siendo las 11:00 horas del día 4 del mes de Marzo del 2005 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de la E. S. I. M. E. para examinar la tesis de grado titulada:

"DISEÑO DE LA RED INALAMBRICA PARA LA UPIITA Y LA UPIBI DEL INSTITUTO POLITECNICO NACIONAL"

Presentada por el alumno:

BORZELLI	***ARENAS***	***MIGUEL***
Apellido paterno	materno	nombre(s)

Con registro:

B	0	2	1	7	5	0

Aspirante al grado de:

MAESTRO EN CIENCIAS

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACION DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISION REVISORA

Director de tesis

DR. SALVADOR ALVAREZ BALLESTEROS

DR. ROLANDO MENCHACA GARCIA

M. EN C. MARCO ANTONIO ACEVEDO MOSQUEDA

M. EN C. SERGIO VIDAL BELTRAN

DR. HECTOR OVIEDO GALDEANO

M. EN C. MIGUEL SANCHEZ MERAZ

EL PRESIDENTE DEL COLEGIO

DR. FLORENCIO SANCHEZ SILVA

SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION

CARTA SESIÓN DE DERECHOS

En la Ciudad de México, Distrito Federal, el día **23** de **MAYO** del año **2005**, el (la) que suscribe **MIGUEL BORZELLI ARENAS** alumno(a) del Programa de **MAESTRÍA EN CIENCIAS EN INGENIERÍA DE TELECOMUNICACIONES** con número de registro **B 0 2 1 7 5 0**, adscrito a la Sección de Estudios de Posgrado e Investigación de la ESIME Unidad Zacatenco, manifiesta que es autor(a) intelectual del presente Trabajo de Tesis bajo la dirección del **DR. SALVADOR ÁLVAREZ BALLESTEROS** y cede los derechos del trabajo intitulado: ***DISEÑO DE LA RED INALÁMBRICA PARA LA UPIITA Y LA UPIBI DEL INSTITUTO POLITÉCNICO NACIONAL***, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, graficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección: **mborzelli@hotmail.com**.

Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

MIGUEL BORZELLI ARENAS
Nombre y Firma

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Índice de Fotos

RESUMEN

Este trabajo presenta una propuesta de diseño para la red inalámbrica de acceso a la Internet de los campus UPIITA y UPIBI del IPN, para lo cual se revisara la teoría general de las redes inalámbricas, señalaremos los temas necesarios que deben ser considerados para realizar el diseño de la red de manera sencilla. Así mismo, se presentan las pruebas realizadas y sus respectivos resultados, finalizando con las conclusiones y recomendaciones derivadas de la realización de este trabajo.

ABSTRACT

This work presents a design proposal for the wireless local area network for the access to the Internet for the UPIITA and UPIBI of the IPN, for that which the general theory of the wireless networks was revised; we will present the necessary topics that should be considered to carry out the design of the network. The carried out tests and their respective results are presented, concluding with the conclusions and derived recommendations of the realization of this work.

PLANTEAMIENTO DEL PROBLEMA

La constante expansión de las redes de área local y el crecimiento que se viene dando en el desarrollo de las comunicaciones móviles ha motivado la búsqueda de nuevas soluciones de conectividad. Este crecimiento continúa a paso acelerado a medida que se desarrollan mercados emergentes.

Una de las soluciones que comienza a tener auge importante son las Redes Inalámbricas ó Wireless LAN (WLAN), basadas en el estándar IEEE 802.11, una de las principales funciones de este tipo de redes es proporcionar conectividad y acceso a las redes cableadas (Ethernet, Token Ring, etc.), proveyéndoles de la flexibilidad y de la movilidad que ofrecen las comunicaciones inalámbricas. El diseño y la planeación adecuada nos permiten reducir la cantidad de equipos necesarios al momento de implementar la red, por lo tanto se reduce el costo de la implementación y al mismo tiempo se aseguran altos niveles de funcionamiento y una mejor calidad en los servicios que se prestan al usuario.

El propósito de este proyecto es brindar una alternativa de conectividad para los estudiantes y personal docente y administrativo del Instituto Politécnico Nacional, de manera que desde los salones de clases, bibliotecas, o cualquier otra área dentro del campus puedan tener acceso a la Internet. Una consideración importante que debe tenerse presente con este trabajo es que las redes inalámbricas no pretenden sustituir a las redes tradicionales, sino complementarlas. En este sentido, buscamos proporcionar facilidades no disponibles en los sistemas cableados y permitir la coexistencia de ambos tipos de redes.

En nuestro país podemos encontrar redes inalámbricas en las principales universidades privadas, y el Instituto Politécnico Nacional, en su calidad icono de la educación superior, no puede y no debe quedarse atrás en el diseño e implementación de las WLAN, para ello es necesario motivar a los estudiantes a que se involucren en el desarrollo de proyectos relacionados con ellas.

Por lo anterior, se propone este trabajo de tesis, con la finalidad de ampliar y mejorar los servicios de red que ofrece el Instituto Politécnico Nacional.

OBJETIVO

Proponer un diseño para una red inalámbrica, basada en el estándar IEEE 802.11b, para el acceso a la Internet por parte de los estudiantes, profesores y personal administrativo de los campus UPIITA y UPIBI del Instituto Politécnico Nacional.

JUSTIFICACIÓN DEL PROYECTO

La Dirección General pidió a la Dirección de Informática elaborara un proyecto de puesta en operación de una red inalámbrica en el Instituto Politécnico Nacional.

Por tal motivo, la Dirección de Informática invitó al Dr. Salvador Álvarez Ballesteros, profesor de la ESIME Zacatenco, a proponer un diseño de red inalámbrica, basada en el estándar IEEE 802.11b, para brindar el servicio de Internet inalámbrico a la UPIITA y la UPIBI.

Dicha dirección presentó el proyecto "Acceso Inalámbrico a la Red Institucional de Telecomunicaciones" para los campus Zacatenco, Santo Tomas y UPIICSA. Este trabajo de tesis forma parte de la propuesta para el campus Zacatenco.

Sin lugar a dudas la puesta en operación de la red viene a complementar la operación de la red cableada, y a su vez, le permite al IPN ofrecer servicios adicionales con tecnología de punta a sus estudiantes.

PROLOGO

En el primer capítulo revisaremos la teoría concerniente con las redes inalámbricas, sus objetivos, su funcionamiento general, algunos de los diferentes estándares existentes en el mercado. Revisaremos las características del estándar IEEE 802.11b, el cual es la base de este trabajo, daremos una revisión de su funcionamiento. Definiremos que es la tecnología Wi-Fi. Revisaremos conceptos generales sobre la seguridad en las redes inalámbricas, y mencionaremos algunos de los distintos mecanismos de seguridad existentes.

En el segundo capítulo revisaremos la teoría relativa al diseño de las redes inalámbricas, tales como que tipo de red se debe implementar, donde colocar los equipos, la planeación de la capacidad de la red, como seleccionar los puntos de acceso (AP) adecuados, y los equipos de usuarios. También presentamos un modelo de propagación para interiores y su comparación con el modelo de propagación en el espacio libre, y como se relacionan entre ambos. Además, presentamos una serie de consideraciones para el mantenimiento de las redes inalámbricas.

En el tercer capítulo revisaremos las propuestas para la UPIITA y la UPIBI, presentamos los resultados de las encuestas realizadas, así como la propuesta de los posibles lugares donde colocar los AP para dar cobertura a aquellas áreas donde los estudiantes demuestran mayor interés por contar con el servicio de Internet inalámbrico. Listamos los equipos de conexión de red con que cuenta cada unidad, ya que es importante conocer si existe equipo disponible para implementar el servicio. También presentamos las políticas de seguridad que deben ser tomadas en consideración para que el servicio prestado sea seguro.

En el cuarto capítulo presentamos las pruebas teóricas y prácticas que realizamos en la UPIITA y la UPIBI, con la intención de conocer si el modelo de propagación elegido es válido, y conocer cual es el área real de cobertura de los AP colocados de acuerdo a las propuestas mencionadas en el tercer capítulo. También mencionamos las especificaciones de los equipos que utilizamos para realizar las mediciones en el campus.

Al final del trabajo presentamos las conclusiones y recomendaciones que han surgido a raíz de la realización del este proyecto. La primera conclusión de este trabajo es que sin importar del lugar en el que se desee implementar una red inalámbrica, si seguimos una serie de pasos básicos podemos diseñar nuestra red sin mayores complicaciones. De igual manera debemos seguir una política de seguridad a fin de que la red que implementemos sea lo más segura posible, a fin de evitar la pérdida de información vital para la institución, así como evitar el uso de la misma por personas ajenas a la organización.

CAPÍTULO 1
INTRODUCCIÓN A LAS REDES INALÁMBRICAS

En este capítulo revisaremos la teoría concerniente con las redes inalámbricas, sus objetivos, su funcionamiento general, algunos de los diferentes estándares existentes en el mercado. Revisaremos las características del estándar IEEE 802.11b, el cual es la base de este trabajo, daremos una revisión de su funcionamiento. Definiremos que es la tecnología Wi-Fi.

Revisaremos conceptos generales sobre la seguridad en las redes inalámbricas, y mencionaremos algunos de los distintos mecanismos de seguridad existentes.

1.1 INTRODUCCIÓN

Las siglas WLAN es una acepción inglesa que corresponde a Wireless Local Area Network, que en español se traduce como Redes de Área Local Inalámbricas. Este tipo de redes nos proporcionan un sistema de comunicación muy flexible al eliminar por completo la utilización de cables, a diferencia de las otras redes de área local (LAN, siglas en inglés), si bien las redes inalámbricas no intentan sustituir por completo al resto de LAN´s sino que se suelen utilizar como complemento a estas.

Estas permiten una mayor movilidad por parte de los usuarios, ya que no es necesario estar conectado físicamente a la red, sino que podemos desplazar nuestro equipo a diferentes lugares atendiendo así nuestras necesidades. Estas redes están alcanzando un gran auge en universidades, oficinas, etc., de modo que permite la transmisión de la información en tiempo real entre los usuarios mientras estos se desplazan por el área cubierta por la red.

De todas formas, y a pesar de las restricciones técnicas que presentan este tipo de redes, tales como la velocidad de transmisión baja, el corto alcance de los puntos de acceso (AP, siglas en inglés), el restringido número de usuarios por cada AP, aún se cree que lo mejor esta todavía por llegar.

1.2 Antecedentes de las Redes Inalámbricas [1, 2]

En 1864 James Clerk Maxwell fue el primero en trabajar en el campo de las ondas electromagnéticas, al mencionar que estas provienen de un cambio de dirección en la energía eléctrica. Tomando como punto de partida el trabajo realizado por Maxwell, Heinrich Hertz desarrolló un equipo transmisor que le permitió enviar y recibir ondas electromagnéticas a través del aire, este equipo fue capaz de incrementar el número de ondas que se producían en un periodo determinado, su frecuencia y su velocidad de oscilación.

Guglielmo Marconi, basado en los trabajos de Hertz, dio el siguiente paso para desarrollar una aplicación más práctica. Marconi siempre estará relacionado con la radio, pero su primera aplicación fue una forma pionera de la comunicación de datos. Al unir su trabajo junto a los descubrimientos de Samuel Morse, pensó que si era posible transmitir señales binarias (guiones y

puntos) a través de un cable, debería ser posible transmitir la misma señal a través de las ondas electromagnéticas y usarlas como un medio de comunicación.

El mundo de la tecnología inalámbrica ha recorrido un largo camino desde Maxwell, Marconi y otros, desde el tiempo de los sencillos equipos que construyeron en sus laboratorios, hasta nuestros días, hemos visto la proliferación de distintas tecnologías inalámbricas, consideradas como herramientas importantes para obtener eficiencia, seguridad y comodidad personal.

Los primeros sistemas que operaban con tecnología inalámbrica, y que son muy semejantes a las WLAN actuales, aparecieron en 1985, cuando se abrió el mercado para comercializar la tecnología inalámbrica gracias a los cambios en las regulaciones de la Comisión Federal de Telecomunicaciones de los Estados Unidos (FCC, siglas en inglés), y permitieron el uso de radios a través del espectro extendido. Poco tiempo después se crea la Telesystems SLW en Toronto, para explotar este desarrollo.

Telesystems empleó un sistema que se conoce como secuencia directa, donde una señal de banda angosta se extiende a través del ancho de banda determinado al multiplicar el ancho de la señal a través de un conjunto de frecuencias mayor, el resultado de este sistema es similar al del salto de frecuencias, es decir, la señal de banda angosta que se extiende a través de un ancho de banda mas amplio es menos susceptible a las interferencias. De manera muy parecida al salto de frecuencias, la señal de secuencia directa proporcionaba el mismo nivel de seguridad.

En 1988 se introduce al mercado el primer sistema comercial basado en la tecnología de Secuencia Directa en el Espectro Extendido (DSSS, siglas en inglés). Estos sistemas no operaban en bandas de frecuencias que requirieran licencia, sino que trabajan en la banda de frecuencias de 902 y 928 megahertz (MHz) recientemente establecidas por la FCC y que no requerían de licencia de operación. Con DSSS fue posible la operación con otros equipos que tampoco requerían licencia de operación, lo que permitió a los usuarios resolver los problemas de interferencia.

Los primeros productos de Telesystems fueron diseñados como reemplazos del cableado, ya fuera para conectar varías computadoras con una estación central de manera parecida a como funciona

una red ethernet, o para conectar redes en edificios separados. Estos primeros equipos tenían un precio de venta muy elevado por nodo, y brindaban una relación precio desempeño insuficiente para obtener aceptación en el mercado.

Los usuarios se dieron cuenta de las ventajas de la nueva oferta libre de licencias, y comenzó la migración, lo que provocó que a principios de 1991 la compañía Telxon adquiriera a Telesystems SWL, para 1999 había agrupado su equipo de radios en la división Aironet Wireless Communications, misma que fue adquirida meses mas tarde por el gigante de la industria de redes, Cisco Systems.

La operación en Estados Unidos, Canadá y Australia se dio en la banda de 900 MHz pero estaba limitada ya que no se podía operar sin licencia en otras partes del mundo. Para llegar a los mercados ubicados fuera de estas áreas, los fabricantes comenzaron a producir radios que operaban en la banda de 2.4 gigaherts (GHz), que estaba disponible para la operación libre de licencia a lo largo de la mayor parte de Europa y Japón, además de Estados Unidos, Canadá y Australia. Los radios que operaban en la banda de 2.4 GHz. iniciaron su proliferación a medida que la operación libre de licencia comenzó a tener mayor aceptación.

En 1991 diversos grupos interesados en el desarrollo de las WLAN solicitaron al Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, siglas en inglés) autorización para establecer un estándar interoperable para las WLAN. Esta tendencia se inclinó hacia el grupo recién formado en torno a la banda de 2.4 GHz y rechazó la de 900 MHz.

Hacia 1993, los fundamentos para un estándar estaban establecidos, y en junio de 1997, el estándar IEEE 802.11 fue ratificado. Este primer estándar proporcionaba velocidades de datos de 1 y 2 megabits por segundo (Mbps), cifrado de datos, llamado Wired Equivalent Protocol (WEP), transmisión a través de secuencia directa y de salto de frecuencia.

El estándar 802.11 marcó el inicio de una nueva era y estableció los fundamentos para el siguiente estándar, el 802.11b, que fue ratificado en 1999 y ofrece una velocidad de datos de 11 Mbps, aproximadamente la misma velocidad que el estándar Ethernet.

1.3 Definición de una Red Inalámbrica [1]

Una Red Inalámbrica es un sistema flexible de comunicaciones que puede implementarse como una extensión o una alternativa a una red cableada. Este tipo de redes utiliza tecnología de radiofrecuencia minimizando así la necesidad de conexiones cableadas. Esto proporciona al usuario movilidad sin perder conectividad de la red.

El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la eliminación del medio de transmisión cableado. Las WLAN son la alternativa ideal para hacer llegar una red LAN cableada a lugares donde el cableado no lo permite.

1.4 Beneficios de las Redes inalámbricas [1]

El principal beneficio fue la eliminación del cableado entre los distintos equipos existentes dentro de la red, posteriormente se considero incluir otros que le darían mayor proyección, tales como:

- Simplificar la instalación de los sistemas. Conexión de los equipos mediante un procedimiento rápido y sencillo que pueda ser realizado por personal no experto en el área.

- Disminuir el costo de mantenimiento por averías, reposiciones, eliminación e incorporación de nuevas unidades, así como los costos de instalación. Esta característica es importante si se desea tener gran capacidad de penetración en el mercado.

- Dar movilidad a los equipos de forma que se puedan conectar y desconectar de manera sencilla y rápida y se puedan utilizar de forma autónoma.

- Aumentar el alcance de las conexiones con la finalidad de aumentar las características de movilidad de los terminales.

- Integrar la WLAN con otros sistemas de comunicación. La integración es importante para las organizaciones que desean comunicarse con una red de terminales móviles de amplia cobertura geográfica.

1.5 ¿Porque utilizar Redes Inalámbricas? [2]

Es clara la alta dependencia en los negocios de redes de comunicación, por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad, así mismo la red puede ser más extensa sin tener que mover o instalar cables.

Respecto a las redes tradicionales las redes inalámbricas ofrecen las siguientes ventajas:

- **Movilidad**: Información en tiempo real en cualquier lugar de empresa para todo usuario de la red, el que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.

- **Facilidad de instalación**: Evita obras para instalar cableado por muros y techos.

- **Flexibilidad**: Permite llegar donde las redes LAN tradicionales no puede.

- **Reducción de costos**: Cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.

- **Escalabilidad**: El cambio de topología de red es sencillo y trata igual pequeñas y grandes redes.

1.6 Funcionamiento general [3]

Utilizan ondas de radio o rayos infrarrojos para transmitir la información de un punto a otro sin necesidad de un medio físico (cables), las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final, esto es llamado modulación de la portadora por la información que está siendo transmitida, de este modo la señal ocupa más ancho de banda que una sola frecuencia. Varías portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio.

Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de WLAN los AP conectan la red cableada de un lugar fijo mediante cableado normalizado, el AP recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un solo AP puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

El AP es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores (tarjetas de usuario). Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS, siglas en inglés) y las ondas, vía una antena.

La naturaleza de la conexión sin cable es transparente al sistema del cliente.

1.7 Tipos de estándares para las Redes inalámbricas [3]

Existen varios estándares para las redes inalámbricas, los cuales listamos a continuación. Existe una gran diferencia entre cada uno de los estándares, y cada uno ha sido adoptado para brindar servicios y productos específicos.

Algunos de los estándares para WLAN existentes son:

- HomeRF
- BlueTooth
- HiperLAN
- IEEE 802.11

En la tabla 1.1 presentamos las diferentes características de los estándares HomeRF, BlueTooth y 802.11.

	HomeRF	BlueTooth	802.11b
Capa Física	FHSS	FHSS	FHSS, DSSS, IR
Saltos de Frecuencia	50 saltos por segundo	1600 saltos por segundo	2.5 saltos por segundo
Potencia de Transmisión Máxima	100 mW	100 mW	800 mW
Velocidades de Datos	1 o 2 Mbps	1 Mbps	11 Mbps
Número máximo de dispositivos	Hasta 127	Hasta 26	Hasta 256
Seguridad	Formato Blowfish	0, 40 y 64 bits	40 y 28 bits RC4 TKIP MIC, SSN
Rango	150 pies	30 pies	400 pies en exteriores, 1000 pies
Versión actual	V1.0	V1.0	V1.0
Costo	Ni más ni menos costoso	Menos costoso	Más costoso
Tamaño físico	Ni mayor ni menor	El mas pequeño	El mas grande
Alcance exterior al hogar	No	No	Sí

Tabla 1.1 – Estándares y Características.

1.7.1 Estándar HomeRF

Tiene sus raíces en el Digital Enhanced Cordless Telephone (DECT). El estándar soporta el tráfico de voz con calidad de llamada telefónica normal, y esta tomando un camino opuesto a los estándares 802.11 y BlueTooth.

Utiliza una combinación de Carrier Sense Multiple Access / Collision Detect (CSMA/CD) para la transmisión de los datos en paquetes, y acceso múltiple por división de tiempo (TDMA, siglas en inglés) para el tráfico de voz y video con el fin de optimizar el flujo de tráfico sobre una base de prioridad. La capa física emplea modulación por desplazamiento de frecuencia (FSK, siglas en inglés) para proporcionar velocidades entre 800 Kbps y 1.6 Mbps en la banda de 2.4 GHz. La disminución del ancho de banda se efectúa a través del uso de 75 canales de 1 MHz para voz y canales de datos de 1.6 Mbps.

El estándar HomeRF incluye un conjunto de capacidades de voz, por ejemplo, identificador de llamadas, llamadas en espera, y regreso de llamadas entre otras, esto se atribuye a que el origen del estándar se basa en un estándar de voz desarrollado por las compañías telefónicas.

1.7.2 Estándar BlueTooth

Existe la confusión de si compite o no directamente con 802.11 y HomeRF, en resumen, este estándar no compite directamente con 802.11 y solo de manera superficial con HomeRF. La primera razón radica en que BlueTooth tiene como propósito ser un estándar con un rango de operación corto, de aproximadamente 1 a 3 metros de cobertura, su intención es conectar computadoras portátiles con teléfonos celulares, asistentes personales digitales (PDA, siglas en inglés) con computadoras portátiles y teléfonos celulares; La segunda razón es que su velocidad de transmisión le permite proporcionar aproximadamente hasta 1.5 Mbps, lo que equivale a una décima parte de la velocidad de 802.11.

Tiene dos puntos fuertes:

- Tamaño: El tamaño que ofrece BlueTooth le permite conectarse en relojes de mano, PDA, y otros dispositivos pequeños en los que el tamaño es un criterio de diseño importante.

- Ahorro de Energía: Utiliza aproximadamente 30 μA, lo que representa una cantidad mínima de energía.

En términos de seguridad cuenta con un método de cifrado de datos. En cuanto al esquema de espectro extendido por salto de frecuencia (FHSS, siglas en inglés) de 1600 saltos por segundo, además del rango limitado de 1 a 3 metros, hace que sea muy difícil interferir la comunicación a distancia.

1.7.3 Estándar HiperLAN

Es un estándar europeo, opera en la banda de 5 GHz. Define una versión inalámbrica de modo de transferencia asíncrono (ATM, siglas en inglés), cuyos estándares fueron aprobados por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI, siglas en inglés) en febrero de 2000.

Hay dos versiones: HiperLAN1 que permite alcanzar velocidades de hasta 20 Mbps e HiperLAN2 que permite velocidades de hasta 54 Mbps. Incorpora Control de Transmisión de Potencia (TCP, siglas en inglés) que reduce el nivel de potencia al mínimo para alcanzar al usuario más alejado y

evitar problemas con otras señales y Selección Dinámica de Frecuencia (DFS, siglas en inglés) para la selección automática de un canal en el AP para minimizar las interferencias con otros sistemas.

Sus principales características son:

- **Alta velocidad de transmisión**: Ofrece una velocidad de transmisión de hasta 54 Mbps, emplea la técnica de modulación de multiplexación por división de frecuencia ortogonal (OFDM, siglas en inglés) para transmitir las señales.

- **Orientado a conexión**: Los datos son transmitidos en conexiones entre los usuarios y los AP, establecida previamente la comunicación entre ambos. Las conexiones emplean multiplexación por división de tiempo y pueden ser punto a punto o punto a multipunto.

- **Calidad de servicio**: Que el estándar sea orientado a conexión permite proporcionar calidad de servicio, lo que permite establecer a cada conexión variables como el ancho de banda, el retraso, la tasa de errores, etc.

- **Búsqueda automática de frecuencia**: En las redes HiperLAN2, no es necesaria la planificación manual. Los AP seleccionan automáticamente el canal de radio adecuado para las transmisiones, evitando posibles interferencias.

- **Seguridad**: Soporta autenticación y encriptación. Los AP y los usuarios pueden autenticarse unos a otros para asegurar un acceso autorizado y válido a la red operadora.

- **Movilidad**: El usuario puede desplazarse entre la cobertura de dos AP distintos, sin perder por ello conectividad.

- **Bajo consumo**: Se permite el establecimiento entre el usuario y el AP, de periodos de inactividad, en los que el usuario establece un estado de bajo consumo.

1.7.4 Estándar IEEE 802.11

El IEEE adoptó este estándar en 1997 y se convirtió en el primer estándar para redes inalámbricas. El estándar 802.11 debe ser observado con mayor detalle, ya que contiene un conjunto de variantes, y quizás porque es el que ha llamado la atención de los principales proveedores de esta tecnología.

El objetivo del estándar es desarrollar un Control de Acceso al Medio (MAC) y las Especificaciones de la Capa Física (PHY) para la conectividad Inalámbrica para terminales Fijas y Móviles dentro de una LAN.

El estándar define varías funciones específicas, entre las cuales podemos mencionar:

- Describe las funciones y servicios requeridos por el estándar para operar en una red con Topología "Ad-Hoc" y con Topología de "Infraestructura", además de los aspectos de movilidad de estaciones dentro de las redes.

- Define los procedimientos de la capa MAC para soportar el servicio de MAC asíncrono para distribución de servicios MSDU (MAC service data unit).

- Define las técnicas de Señalización y las funciones de interfase (PHY) que son controlados por la capa MAC.

- Describe los procedimientos y requerimientos para proveer privacidad a la transferencia de datos de usuarios sobre medios inalámbricos.

La tabla 1.2 nos muestra un resumen de las versiones del estándar 802.11.

Versión del Estándar	Frecuencia Portadora	Velocidad de Datos	Resumen
802.11a	5.1 – 5.2 GHz 5.2 – 5.3 GHz 5.7 – 5.8 GHz	54 Mbps	La potencia máxima es de 40 mW en la banda 5.1, 250 mW en la banda 5.2 y 800 mW en la banda 5.7
802.11b	2.4 – 2.485 GHz	11 Mbps	Es el estándar que mayor mercado tiene actualmente.
802.11d	N/D	N/D	Múltiples dominios reguladores
802.11e	N/D	N/D	Calidad de servicio
802.11f	N/D	N/D	Protocolo de conexión entre AP
802.11g	2.4 – 2.485 GHz	36 o 54 Mbps	Para redes de alto desempeño, es la próxima generación
802.11h	N/D	N/D	Selección dinámica de frecuencia
802.11i	N/D	N/D	Seguridad

Tabla 1.2 – Versiones del estándar 802.11.

Controla las capas 1 (capa Física) y 2 (capa de Enlace) del modelo de referencia OSI.

La capa 1 (Física) en una red basada en el estándar 802.11 realiza tres funciones esenciales:

- Funciona como interfaz entre la capa de Control de Acceso a Medios (MAC) en dos o más ubicaciones, estas normalmente se encuentran separadas por pequeñas distancias.

- Realiza la detección de los sucesos CSMA/CD que ocurren dentro de la capa MAC.

- Efectúa la modulación y demodulación de la señal entre dos equipos de radio 802.11.

También define una técnica de cambio de velocidad que permite a las redes reducir las velocidades de datos a medida que ocurren cambios en la distancia, calidad e intensidad de la señal del equipo de radio. Las velocidades de datos pueden ir de 1 Mbps y hasta 54 Mbps dependiendo de la técnica de modulación empleada.

La capa MAC es una subcapa de la capa 2 del modelo de referencia OSI (capa de Enlace), controla la conectividad de dos o más puntos a través de un esquema de direcciones, cada computadora o AP tiene asignada una dirección MAC. El estándar 802.11 define la forma en que funciona esta

asignación de direcciones. La capa MAC controla todo lo relacionado con la movilidad en una red basada en el estándar.

El estándar define las siguientes características:

- Las funciones que se requieren en un dispositivo compatible con 802.11 para operar en una red de igual a igual, o integrado a una WLAN existente.

- La operación del equipo 802.11 dentro del rango de otros equipos y la forma en que la tarjeta cliente migraría físicamente de un AP a otro.

- Servicios de control de acceso y entrega de datos a la capa MAC para las capas superiores.

- Privacidad y seguridad en los datos del usuario que se transfieren a través del medio inalámbrico.

La tabla 1.3 muestra algunas de las características más importantes de las tres versiones del estándar 802.11 que se encuentran en el mercado actualmente.

	802.11a	802.11b	802.11g
Frecuencia	5.7 GHz	2.4 GHz	2.4 GHz
OFDM*	Sí	No	Si
Velocidad de datos	54 Mbps	11 Mbps	54 Mbps
Número de canales no traslapados	12	3	3

Tabla 1.3 – Características de las versiones del estándar 802.11.

*(OFDM: multiplexación por división de frecuencia ortogonal, es una técnica de modulación FDM que se usa para transmitir señales al dividir la señal en varías frecuencias en las que transmite de forma simultanea).

En la tabla 1.4 podemos observar algunas ventajas y desventajas de las versiones de estándar, versión 802.11a y versión 802.11g.

	802.11a	802.11g
Desempeño	Ventaja: Emplea OFDM, opera en la banda de 5 GHz y la ausencia de células mixtas proporciona una mejor capacidad de salida.	Desventaja: Soporte para los estándares elevados, células mixtas y la operación en la banda de 2.4 GHz que podría estar potencialmente saturada, lo cual tendría como resultado una capacidad de salida ligeramente menor que la de 802.11a.
Capacidad	Ventaja: Con ocho canales, proporciona una capacidad agregada de 432 Mbps (54 Mbps por cada canal).	Desventaja: Con solo tres canales, proporciona una capacidad teórica agregada de 162 Mbps (54 Mbps por cada canal).
Rango	Desventaja: Una longitud de onda mas corta y restricciones reguladoras en la potencia de transmisión y la ganancia de la antena que deterioran el rango de alcance.	Ventaja: A pesar de que no proporcionará el mismo rango que 802.11b debido a las velocidades de datos mas altas, la física y regulaciones en la banda de 2.4 GHz permiten un rango mayor que cuando se opera en la banda de 5 GHz.
Interferencia	Ventaja: Las WLAN 802.11a operan en las bandas de 5 GHz que son relativamente grandes, pero aun así están saturadas.	Desventaja: Las bandas que no requieren de licencia de 2.4 GHz son relativamente pequeñas y se están saturando con las WLAN, teléfonos inalámbricos, y dispositivos Bluetooth
Migración	Desventaja: Operando a 5 GHz y proporcionando soporte solo para la transmisión OFDM, no proporciona compatibilidad con dispositivos anteriores de 802.11a.	Ventaja: Al operar en la banda heredada de 2.4 GHz y soportar DSSS, proporciona la característica importante de la compatibilidad con productos anteriores 802.11b
Flexibilidad de instalación	Desventaja: Las regulaciones FCC que se aplican a los cuatro canales inferiores de 802.11a restringen a los fabricantes al uso exclusivo de antenas integradas que no se pueden desconectar.	Ventaja: Al igual que 802.11b, permite antenas de 2.4 GHz auxiliares que pueden estar directamente conectadas o conectadas por cables.
Operación a nivel mundial	Desventaja: Operación en los países apegados a FCC y Japón, pero aun no se define en Europa.	Ventaja: La operación libre de licencia, en prácticamente, todo el mundo

Tabla 1.4 – Ventajas y desventajas de las versiones 802.11a y 802.11g.

1.8 Topologías de Red [12, 13]

Las redes inalámbricas basadas en el estándar 802.11 pueden operar bajo dos topologías de red distintas: **Topología Ad-Hoc** y **Topología de Infraestructura**

Dentro de cada una encontramos el Conjunto de Servicio Básico (BSS, siglas en inglés), que consiste de dos o más nodos, también llamados estaciones. Cada nodo o estación es una plataforma individual, como un AP o una tarjeta de usuario (tarjetas PCMCIA). Un BSS cuenta con

dispositivos que reconocen y trabajan en conjunto para minimizar la cantidad de colisiones que existen dentro del dominio del BSS.

Las redes Ad-Hoc también son conocidas como Conjunto de Servicio Básico Independiente (IBSS, siglas en inglés), la palabra independiente se refiere a que no existe un AP dentro del conjunto de servicio. Estas redes tienden a ser temporales, se usan cuando dos o más equipos portátiles se conectan entre ellos para intercambiar información.

La figura 1.1 nos muestra un ejemplo de una red Ad-Hoc.

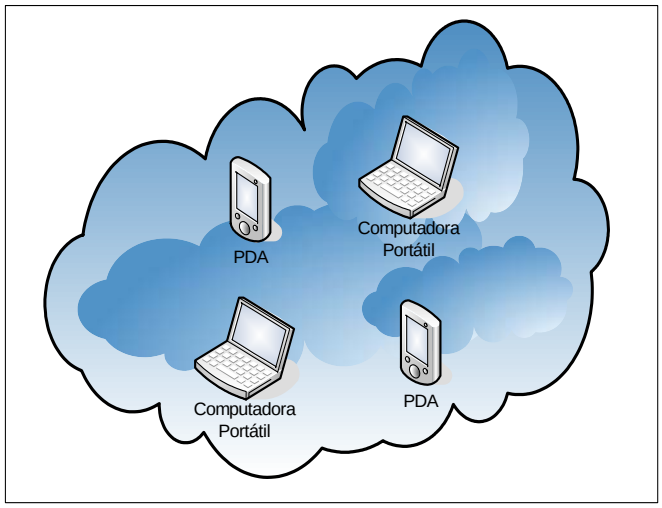


Figura 1.1 – Topología de red Ad-Hoc.

En las redes con topología de Infraestructura puede verse al AP como la extensión base con la que se conectan los usuarios (equipos portátiles), es el dispositivo que controla el tráfico que fluye entre AP y los usuarios. Al conjunto de AP y usuarios se le conoce como Conjunto de Servicio Extendido (ESS, siglas en inglés), todos los equipos provienen de más de un BSS.

La figura 1.2 nos muestra un ejemplo de una red con topología de Infraestructura.

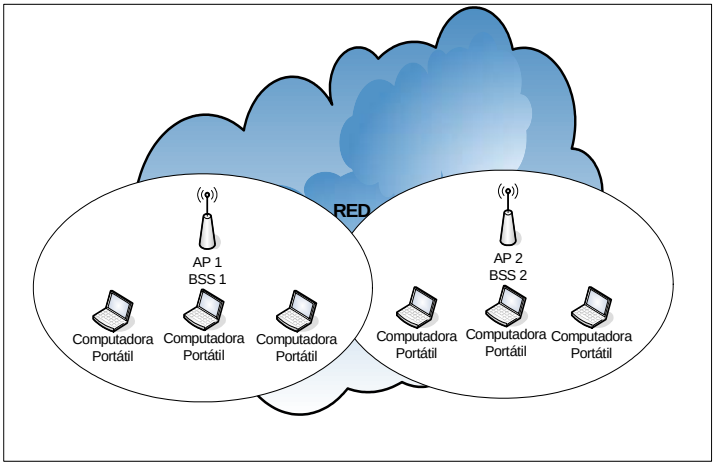


Figura 1.2 – Topología de red de Infraestructura.

1.9 Capa Física (PHY) [12, 13]

Los radios que se usan en 802.11 están compuestos por tres elementos:

- Radio: Genera y recibe la energía que se envía y recibe desde una antena.

- Capa MAC: Controla el flujo de paquetes entre dos o más puntos de una red.

- Antena: Realiza dos funciones esenciales: Mejora el desempeño del equipo de radio y Optimiza el patrón de radiación de la energía radiada.

La capa PHY esta compuesta por dos subcapas: Protocolo de Convergencia de la Capa Física (PLCP, siglas en inglés) y la subcapa Dependiente del Medio Físico (PDM, siglas en inglés). La diferencia entre ambas es que la PLCP se encarga de las técnicas de modulación por Código Complementario (CCK, siglas en inglés), modulación por Fase por Desplazamiento Binario (BPSK, siglas en inglés), modulación por Fase por Desplazamiento en Cuadratura (QPSK, siglas en inglés) y de las técnicas de propagación DSSS o FHSS, mientras que la PMD crea la interfaz hacia la capa MAC para la sensibilidad de la portadora a través de su Comprobación de Canal Libre (CCA, siglas en inglés).

El PLCP esta formado por un preámbulo de 144 bits que se usa para sincronizar los AP con los usuarios, determinar la ganancia del radio y establecer la CCA, el preámbulo esta constituido por 128 bits para la sincronización y seguido de un campo de 16 bits que consiste del patrón 1111001110100000, esta secuencia se usa para marcar el inicio de una trama y se conoce como delimitador de inicio de trama (SFD, siglas en inglés).

Los siguientes 48 bits se conocen en conjunto como el encabezado PLCP, cuenta con tres campos: señal, servicio, y longitud, además de revisión de errores en el encabezado (HEC, siglas en inglés), lo que asegura la integridad del encabezado y del preámbulo. El campo de señal indica la velocidad a la que será transmitida la carga, el campo de longitud incida el tamaño de la carga e incluye los 16 bits de HEC que se efectúa mediante una revisión de redundancia cíclica (CRC, siglas en inglés) y el campo de servicio esta reservado para un uso futuro.

PLCP siempre transmite a 1 Mbps, debido a que la confiabilidad y solidez de la señal son más importantes y tiene prioridad sobre la velocidad, sin embargo, este encabezado no impacta la velocidad general del enlace, debido a que 24 bits de cada paquete se envían a 1 Mbps.

1.9.1 DSSS y FHSS

El estándar 802.11 permite tres técnicas de propagación en la capa PHY: Espectro Extendido de Secuencia Directa (DSSS), Espectro Extendido por Salto de Frecuencia (FHSS) y la transmisión por rayos infrarrojos.

DSSS tiene asignado 11 canales en Estados Unidos, 13 en la mayor parte de Europa y 14 en Japón, pero debido a que la energía del espectro extendido cubre cinco canales distintos a la vez, sólo tres son capaces de no traslaparse.

La figura 1.3 muestra el esquema, por lo tanto como principio básico los dominios de colisión no usan más de tres canales por AP, de esta manera se consiguen velocidades de datos mas altas y un enlace más sólido.

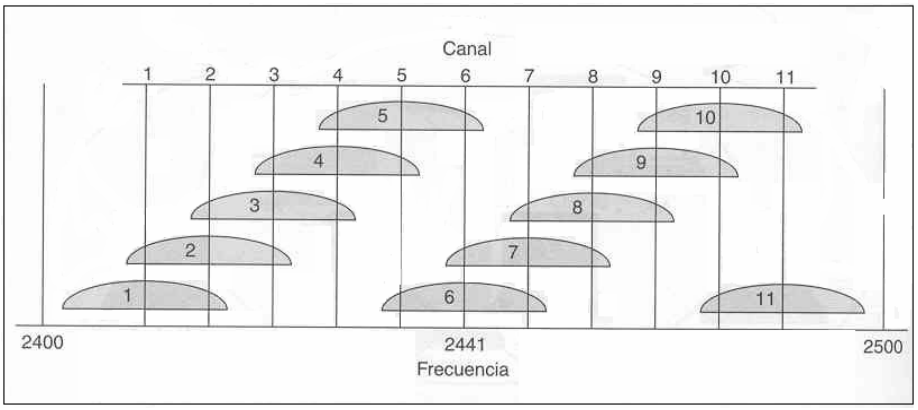


Figura 1.3 – Canales de radio del estándar 802.11.

La técnica DSSS funciona mediante la adquisición del flujo de unos y ceros que conforman el tráfico entre el AP y el usuario, agrupa cada uno de los números individuales en un conjunto de 11 números, conocido como Código Barker ó Secuencia de Fragmentación, esto significa que cada grupo de 11 bits representa un solo bit de flujo de datos, después, los fragmentos son modulados por uno de los esquemas y se envían a través de uno de tres canales no traslapados hacia los usuarios.

FHSS consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo inferior a 400 milisegundos. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia, de esta manera cada tramo de información es transmitida en una frecuencia distinta durante intervalos de tiempo muy cortos.

Cada una de las transmisiones a una frecuencia específica se realiza utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal. El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia pseudoaleatoria que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer. La ventaja de estos sistemas frente a los sistemas DSSS es que con esta tecnología podemos tener más de un AP

operando en la misma zona geográfica sin que existan interferencias, si se cumple que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo.

Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación, el efecto global es que aunque vamos cambiando de canal físico con el tiempo y se mantiene un único canal lógico a través del cual se desarrolla la comunicación. Para un usuario externo a la comunicación la recepción de una señal FHSS equivale a la recepción de ruido impulsivo de corta duración. El estándar 802.11 describe esta tecnología mediante la modulación FSK, y con una velocidad de transferencia de 1 Mbps ampliable a 2 Mbps bajo condiciones de operación óptimas.

La tercera variante, de momento no demasiado utilizada a nivel comercial para implementar WLAN es la transmisión por rayos infrarrojos. Estos sistemas se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades son las mismas que tiene la luz visible. De esta forma los rayos infrarrojos no pueden pasar a través de objetos opacos pero se pueden reflejar en determinadas superficies.

Las longitudes de onda de operación se sitúan alrededor de los 850 - 950 nanómetros, es decir, a frecuencias de emisión que se sitúan entre los $3{,}15 \times 10^{14}$ Hz y los $3{,}52 \times 10^{14}$ Hz.

Los sistemas que funcionan mediante rayos infrarrojos se clasifican según el ángulo de apertura con el que se emite la información en el emisor en:

- **Sistemas de corta apertura**, de haz dirigido o de visibilidad directa que funcionan de manera similar a los controles remotos de los equipos electrónicos. Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse la información.

- **Sistemas de gran apertura**, reflejados o de difusión que radian tal y como lo haría una bombilla, permitiendo el intercambio de información en un rango más amplio.

El estándar 802.11 permite técnicas de modulación tales como BPSK, esta se usa con un cambio de fase por cada bit modulado para asegurar el rango máximo, se alcanza una velocidad de datos cercana a 1 Mbps, es la técnica de modulación más simple que implementa el estándar; La siguiente técnica de modulación implementada es la modulación QPSK, codifica dos bits de la información en la misma cantidad que BPSK y se obtiene un rango mayor; La técnica de modulación más compleja que se implementa en la versión 802.11b es la modulación CCK, esta modulación se basa en una serie de códigos denominados secuencias complementarias.

1.10 Capa de Enlace (MAC) [12, 13]

La principal función de la capa es asegurar que los paquetes no choquen dentro de un dominio, por ejemplo, una WLAN, mediante el control de acceso a los canales de radio asignados y compartidos.

Recordemos que la capa MAC es una de las dos subcapas de la capa de enlace de datos y es la responsable de controlar el flujo de paquetes de un usuario hacia otro a través de un canal compartido, ya sea sobre una red Ethernet o 802.11.

Consiste en dos subcapas:

- Control Lógico de Enlace (LLC, siglas en inglés)

- Control de Acceso al Medio (MAC, siglas en inglés)

La LLC permite la interoperabilidad entre las redes tradicionales cableadas y las redes inalámbricas. La capa MAC es propia del estándar 802.11, aunque en concepto es muy similar a la de las redes ethernet 802.3, debido a que se basa en el principio de que muchos usuarios acceden al mismo y único medio. Debido a la imposibilidad de emplear la misma tecnología Carrier Sense Multiple Access / Collision Detect (CSMA/CD) de las redes ethernet, las redes basadas en el estándar 802.11 emplean una modificación del protocolo denominada Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA).

Esto protocolo evita las colisiones, enviando un paquete de reconocimiento (ACK, siglas en inglés) para confirmar la llegada al receptor del paquete enviado.

CSMA/CA trabaja de la siguiente manera:

- La estación transmisora comprueba el medio, si no detecta ninguna transmisión en curso esperara una cantidad aleatoria de tiempo, si pasado este tiempo, el medio sigue libre comienza la transmisión.

- Si el paquete se recibe intacto, la estación receptora envía un paquete ACK a la estación transmisora. Si este paquete de reconocimiento llega al transmisor, el ciclo se ha completado.

- Si la estación transmisora no recibe el paquete ACK, bien porque el paquete de datos no llegó a la estación receptora o porque se perdió el ACK, se asume que se produjo una colisión, y se esperará de nuevo un tiempo aleatorio para volver a intentar la comunicación.

La capa MAC ofrece dos características que mejoran la robustez del estándar: comprobación de suma CRC y fragmentación de paquetes. Cada paquete lleva asociado un CRC para asegurar que este no se ha degenerado en la transmisión. Esta es una diferencia con respecto a Ethernet, ya que esta dejaba tales comprobaciones a los protocolos de niveles superiores. La fragmentación de paquetes permite enviar pequeños fragmentos de paquete que permiten optimizar las comunicaciones en entornos congestionados o donde la interferencia es un factor a tener en cuenta.

Algunas de las principales funciones de la capa MAC son:

- **Exploración**: Existen dos tipos: Activa y Pasiva. La exploración pasiva es obligatoria, se realiza cuando los usuarios exploran cada uno de los canales disponibles, se efectúa con el fin de encontrar una señal óptima del AP. El propósito principal es asegurar que el usuario se conectará con el AP mas adecuado de la red. La exploración activa es opcional, opera de manera muy similar a la exploración pasiva, la diferencia es que el usuario envía una trama de prueba y todos los AP dentro del rango de emisión responden con una respuesta de prueba.

- **Autenticación**: Es el proceso mediante el cual los usuarios previamente aprobados pueden integrarse a la red. Ocurre antes de la asociación, debido a que es durante este proceso que

las direcciones del protocolo de Internet (IP) son reveladas por el AP y asignadas a los usuarios.

- **Asociación**: Después de que se realiza el proceso de autenticación, el usuario inicia una asociación cuando envía una trama de solicitud de asociación que contiene un identificador de establecimiento de servicio (SSID, siglas en inglés) y las velocidades de datos soportadas, el AP responde mediante una trama que contiene un identificador de asociación, y una dirección IP.

- **Seguridad**: Mediante alguno de los mecanismos de seguridad existentes el usuario cifra el cuerpo de la trama, mas no así el encabezado antes de la transmisión, el AP descifra la trama cuando la recibe usando empleando el mismo mecanismo utilizado por el usuario. Más adelante revisaremos con mayor detalle el proceso de seguridad.

- **RTS/CTS**: Significa Request To Send / Clear To Send. Este protocolo es muy útil cuando existen nodos ocultos, dos o más usuarios, que no se detectan entre ellos debido a que están fuera de sus rangos respectivos. Un usuario envía una trama RTS a un AP antes de la transmisión de un paquete cuando ocurre un exceso en el tiempo predeterminado, luego el AP controlará el tiempo de transmisión al enviar un paquete CTS al usuario que espera la transmisión, cuando el usuario recibe el paquete CTS incluirá un valor de duración en el encabezado de la trama, este valor evita que el AP reciba paquetes de cualquier otro usuario dentro de la red.

- **Modo de Ahorro de Energía**: La capa MAC permite la opción de reducir el consumo de energía.

- **Fragmentación**: Se refiere a la capacidad de un AP para dividir paquetes en tramas más pequeñas. Esto se hace de modo que la interferencia RF solo elimina a los paquetes más pequeños. La fragmentación de paquetes también permite el incremento de tiempo libre en el canal.

Además de evitar las colisiones y pérdidas en la señal, la capa MAC es responsable de identificar las direcciones fuente y destino de los paquetes que se envían dentro de la red.

1.11 ¿Que es Wi-Fi? [2]

Wireless Fidelity (Wi-Fi) es el nombre comercial desarrollado por el grupo de comercio industrial llamado Wi-Fi Alliance. Describe los productos de redes de área local inalámbricos basados en el estándar IEEE 802.11 y esta diseñado para que tenga un nombre más accesible para los usuarios. En principio Wi-Fi fue creado para describir los equipos con velocidades máximas de 11 Mbps que operaban en la banda de frecuencia de 2.4 GHz del espectro de frecuencia y que cumplían con la versión 802.11b del estándar, posteriormente se decidió que debería ser extendido para incluir a todos los equipos con velocidades mayores (velocidades de 54 Mbps), basados en la versión 802.11g del estándar.

1.11.1 Velocidades de datos que soporta Wi-Fi

Comúnmente se promociona una velocidad de datos máxima de 11 Mbps, es importante notar que el estándar 802.11b soporta en realidad cuatro velocidades de datos: 1, 2, 5.5 y 11 Mbps. Estas velocidades están disponibles en el mismo medio físico, específicamente, en una porción de 80 MHz de amplitud del espectro de frecuencia del radio, iniciando en la frecuencia de 2.400 GHz que luego se divide en 11, 13 y 14 canales, dependiendo de la cantidad exacta del espectro asignado por las distintas agencias gubernamentales.

En Ethernet, el medio físico permanece igual cuando las velocidades de datos aumentan o disminuyen, el mismo concepto se aplica para Wi-Fi, aumentar o disminuir el desempeño de la red inalámbrica no es una función de incrementar o disminuir el tamaño de la capa física o cambiar el ancho de banda, por el contrario, es una función del tipo de modulación que se utilice.

Las bases para las cuatro velocidades de datos que proporciona el estándar 802.11b son tres técnicas de modulación distintas:

- Modulación BPSK para proporcionar velocidades de hasta 1 Mbps.

- Modulación QPSK para proporcionar velocidades de hasta 2 Mbps.

- Modulación CCK para proporcionar velocidades de hasta 5.5 y 11 Mbps.

Nos podríamos preguntar porque si la mayor velocidad siempre es mejor, la industria y los estándares se preocupan por proporcionar soporte para cualquier otro tipo de modulación que no sea CCK, la respuesta se resume en una palabra: rango.

Para entender mejor esto, podemos observar la figura 1.4 donde se aprecia como varía la velocidad y el rango dependiendo del tipo de modulación que se utiliza.

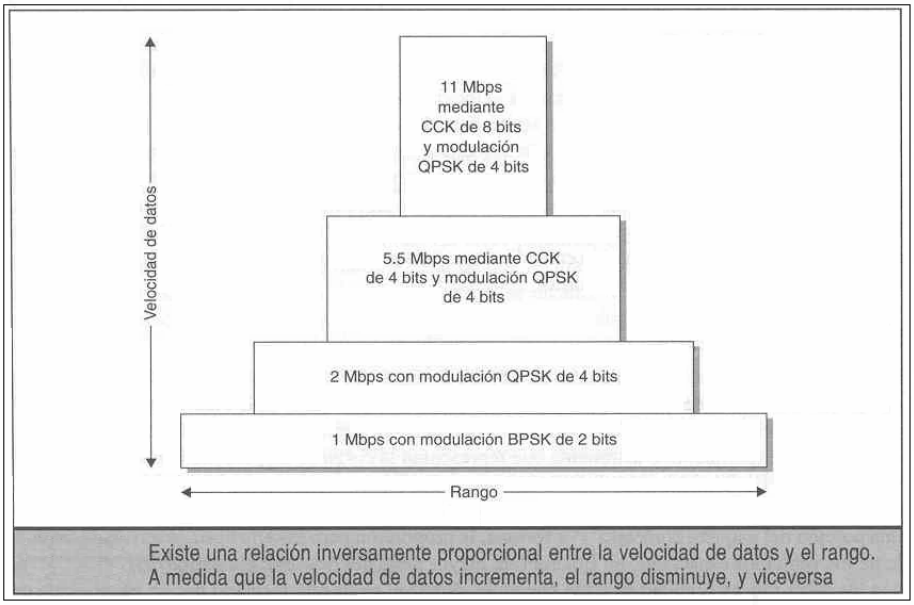


Figura 1.4 – Relación de Velocidad de datos contra Rango de alcance

1.12 Seguridad en las Redes Inalámbricas [9, 10, 11]

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad, la salida de estas señales fuera de los edificios donde está ubicada la red permite que un pirata informático sin poseer un equipo sofisticado, se introduzca en una red empresarial. Y una brecha de seguridad en una red es un grave problema para cualquier empresa. Una vez dentro, el pirata informático puede tener acceso a contraseñas, introducirse en los servidores y robar información, cambiar la página Web de la empresa o hacer que la red entera deje de funcionar.

¿Qué es lo que hace que las redes inalámbricas sean más vulnerables que las redes de cableadas? La respuesta es sencilla: desconocimiento de las herramientas de seguridad disponibles para las redes inalámbricas. El término "seguridad inalámbrica" no tiene porque ser una expresión contradictoria, de hecho son muchas las personas que piensan que es más difícil violar la seguridad en una red cableada que en una red inalámbrica. En el mercado podemos encontrar las herramientas de seguridad, funciones y protocolos para proporcionar una adecuada protección a las WLAN.

Las redes inalámbricas pueden tener un impacto positivo en una empresa cuando el resultado de implementarlas produce mejoras en la eficiencia organizacional, en la toma de decisiones y en la productividad en general, pero pueden tener un impacto negativo cuando pone en riesgo no solo la seguridad de la WLAN, sino de toda la red (cableada e inalámbrica).

Las redes basadas en el estándar IEEE 802.11 presentan un crecimiento espectacular, ello incide en hacer cada vez más necesaria la seguridad de este tipo de redes. El IEEE, consciente de esta necesidad, aprobó en junio de 2001 el estándar IEEE Std 802.1X-2001 que especifica el control de acceso a la red basado en puertos, el cual utiliza las características físicas de las infraestructuras de las redes locales IEEE 802.11 para facilitar una forma de autenticación y autorización de dispositivos conectados a un puerto de la red en modo punto a punto y de impedir el acceso a dicho puerto si falla el proceso de autenticación y autorización.

El objetivo del estándar es especificar un método general de provisión de control de acceso a la red basado en puertos. Entre su contenido cabe destacar que: describe un marco de referencia en el que

se produce la autenticación, define los principios de funcionamiento de los mecanismos de control de acceso, los niveles de control de acceso y el comportamiento asociado a ellos (en cuanto a transmisión y recepción de tramas), los requisitos del protocolo entre Autenticador - Solicitante y entre Autenticador y Servidor de Autenticación. También especifica los mecanismos y procedimientos que soportan control de acceso a la red por medio de protocolos de autorización y autenticación, la codificación de las unidades de datos del protocolo (PDU, siglas en inglés) utilizadas por dichos protocolos, establece los requisitos de gestión del control de acceso basado en puerto y el acceso remoto a las operaciones de administración de la red mediante el protocolo de administración de red simple (SNMP, siglas en inglés).

Explicaremos un escenario típico de autenticación 802.1x. Existen tres actores principales en la autenticación 802.1x: El Solicitante (Usuario), el Autenticador (AP), y el Servidor de Autenticación, en la figura 1.5 se pueden apreciar estos tres actores de acuerdo con una configuración básica de red.

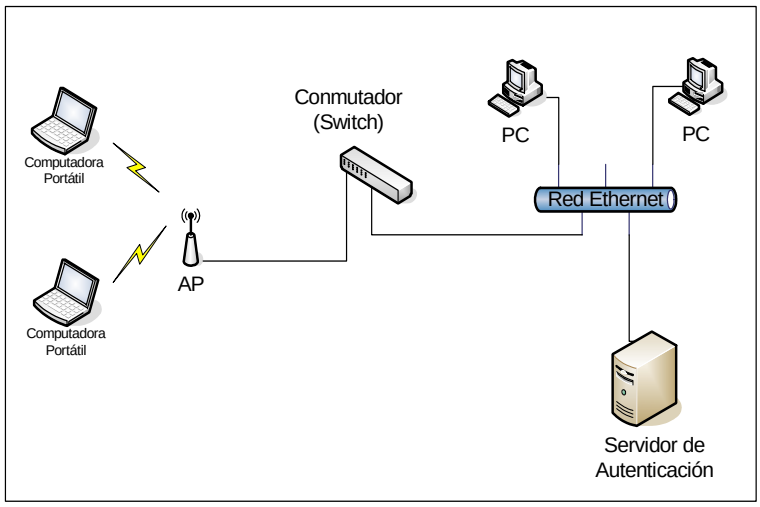


Figura 1.5 – Actores de la autenticación 802.1x.

La comunicación comienza con un solicitante no autenticado que desea conectarse con un AP, el AP responde permitiendo al puerto pasar solamente paquetes del protocolo de Autenticación Extensible (EAP, siglas en inglés) desde el usuario hacia al servidor de autenticación situado en la red cableada, en ese momento pone al puerto en estado de "No Autorizado", el AP bloquea cualquier otro tipo de tráfico como paquetes del protocolo de transferencia de hipertexto (HTTP, siglas en inglés) o POP3.

El usuario envía un paquete EAP-inicio, el AP responde con EAP-solicitud de identidad para obtener la identidad del usuario, este contesta con su identidad y el AP envía este mensaje al servidor de autenticación, la autenticación se realiza de acuerdo con el algoritmo de autenticación seleccionado y el resultado es enviado al AP. Una vez autenticado el usuario, el AP abre el puerto del usuario para otro tipo de tráfico. El estado del puerto pasa a "Autorizado". Para desconectar, el usuario enviará un mensaje EAP-desconexión, con lo que el AP pone el puerto en estado "No Autorizado" nuevamente. Este procedimiento puede apreciarse en figura 1.6.

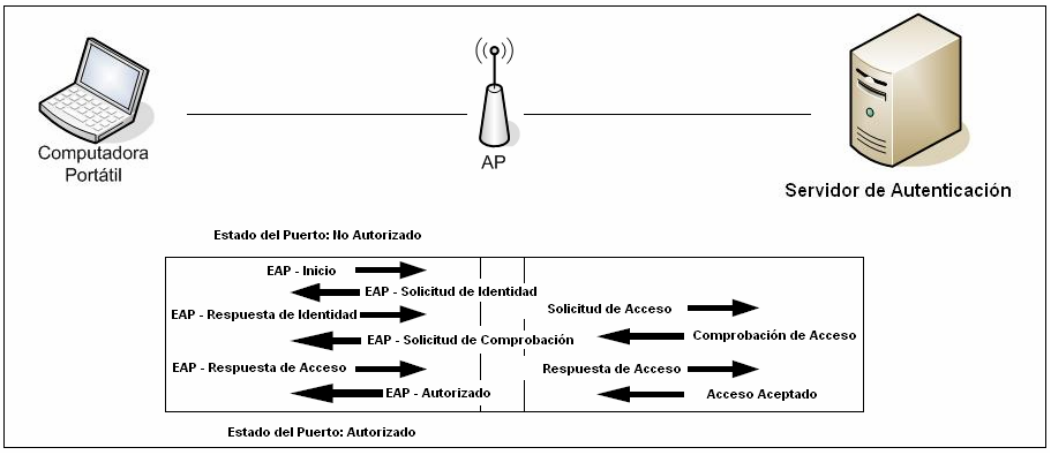


Figura 1.6 – Procedimiento de Autenticación

A continuación se resumen las funciones de las entidades que intervienen:

- **Autenticador (AP)**: Equipo en el extremo de un segmento punto a punto de una LAN que facilita la autenticación de la entidad conectada al otro extremo del enlace.

- **Servidor de Autenticación**: Equipo que facilita servicio de autenticación al autenticador. Puede estar situada junto al autenticador o remotamente, en el se implementa el mecanismo de autenticación.

- **Puerto de Acceso a la Red (Puerto)**: Es el punto de conexión de un sistema a una LAN. Puede ser un puerto físico MAC o un puerto lógico, como una asociación IEEE 802.11 entre un AP y una estación inalámbrica.

- **Extensible Authentication Protocol (EAP)**: Es el protocolo asociado con un puerto. Puede incluir la funcionalidad de autenticador, solicitante o ambas funcionalidades.

- **Solicitante (Usuario)**: Es aquel en un extremo de un segmento LAN punto a punto que está siendo autenticado por un autenticador al otro extremo del enlace.

Como hemos visto, cuando se discuten los sistemas de seguridad, las dos áreas principales son: Autenticación y Cifrado, aunque están interrelacionadas, la veremos por separado ya que constituyen aspectos diferentes de una arquitectura general de seguridad.

La autenticación es el proceso en que se determina que un usuario es quien dice ser. Un ejemplo sencillo de este proceso es por ejemplo un agente que llega a una oficina, primero muestra una tarjeta de identificación con su foto, luego mira a través de un visor que examina el patrón de su retina y por último tiene que teclear una secuencia numérica para poder acceder al edificio.

Los AP pueden configurarse de manera que usen contraseñas, conocidas como SSID, usualmente están compuestos por una sola palabra, y ya vienen predeterminados por el fabricante de los AP. Las herramientas administrativas, como por ejemplo NetStumbler, proporcionan la capacidad de registrar todos los SSID que se pueden recibir en el equipo del usuario y luego permitir que el usuario se asocie al AP seleccionado.

Algunos fabricantes proporcionan la capacidad de deshabilitar los SSID de los AP, por un lado esto resuelve un problema de seguridad, pero por el otro deshabilita la capacidad de que un usuario pueda encontrar la red adecuada con la cual quiere conectarse. Un SSID debe considerarse más como un nombre que como una contraseña, debe actuar como un medio de identificación del AP o como la identificación de toda una WLAN.

La mayoría de los fabricantes proporcionan la capacidad de restringir el acceso a las redes basándose en la tabla de direcciones MAC, la programación de las direcciones MAC son los únicos identificadores numéricos que usan los fabricantes para los equipos de las redes. Mediante esta

característica se puede introducir un rango de direcciones MAC dentro de los AP y solo permitir que los equipos que cuenten con esas direcciones accedan a la red.

A pesar de que este método proporciona cierto nivel de seguridad presenta dos problemas importantes:

- Las direcciones MAC pueden ser falsificadas. Un pirata informático puede usar un analizador de protocolo inalámbrico para revisar el tráfico y encontrar una dirección valida, luego solo debe copiarla en un equipo de usuario y hacerse pasar por un usuario válido.

- Las bases de datos separadas crean problemas administrativos, cada tabla de direcciones que se ubica en AP individuales representa una base de datos separada. Algunos fabricantes proporcionan medios para replicar las tablas de direcciones a lo largo de un grupo de AP, pero esta solución rompe la sincronización y crea problemas de actualización.

1.12.1 Mecanismos de Seguridad

Wired Equivalent Protocol (WEP): El protocolo WEP es un sistema de encriptación implementado en la capa MAC y soportado por la mayoría de los AP. Comprime y cifra los datos que se envían a través de las ondas de radio. Su objetivo es proporcionar confidencialidad, autentificación y control de acceso a las redes WLAN.

Utiliza una misma clave simétrica y estática entre los usuarios y los AP. No contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los equipos de la red, lo que genera varios inconvenientes. Por un lado, la clave está almacenada en todas los equipos, aumentando las posibilidades de que sea comprometida; Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

Open System Authentication (OSA): Es el mecanismo de autenticación por defecto del estándar 802.11, sirve para autenticar todas las peticiones que recibe el AP. El principal problema que tiene

es que no realiza ninguna comprobación del equipo del usuario, además, las tramas de gestión son enviadas sin encriptar, aun habilitando el protocolo WEP, por lo tanto es un mecanismo poco fiable.

Access Control List (ACL): Este mecanismo de seguridad es soportado por la mayoría de los AP, utiliza como mecanismo de autenticación la dirección MAC de cada equipo de usuario, permitiendo el acceso a aquellas direcciones que consten en la lista de control de acceso.
Closed Network Access Control (CNAC): Este mecanismo pretende controlar el acceso a la WLAN y permitirlo solamente a aquellos equipos de usuarios que conozcan el nombre de la red (SSID), actuando este como contraseña.

Wi-Fi Protected Access (WPA): WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Sus principales características son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

- IEEE 802.1X, Proporciona control de acceso a la rede basado en puertos. Con este fin utiliza el protocolo EAP (RFC 2284) y un servidor de autenticación, por ejemplo tipo RADIUS (Remote Authentication Dial-In User Service) (RFC 2058), el cual proveerá de las claves que se utilizarán para cifrar los datos.

- TKIP (Temporal Key Integrity Protocol), es el protocolo encargado de la generación de la clave para cada trama.

- MIC (Message Integrity Code), verifica la integridad de los datos de las tramas.

WPA puede funcionar en dos modos:

- Modo Empresarial: Requiere un servidor de autenticación tipo RADIUS, configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

- Modo de Llave Inicial Compartida (Pre Shared Key, PSK): Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor de autenticación. Utiliza una clave compartida en los usuarios y los AP para poder accesar a la red.

Como hemos visto, la seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la mayoría de las redes inalámbricas instaladas no cuentan con una herramienta de seguridad debidamente configurada o poseen un nivel de seguridad muy débil, con lo cual se pone riesgo la confidencialidad e integridad de la información y de la red.

CAPÍTULO 2
METODOLOGÍA PARA EL DISEÑO

Revisaremos la teoría relativa al diseño de las redes inalámbricas, tales como que tipo de red se debe implementar, donde colocar los equipos, la planeación de la capacidad de la red, como seleccionar el AP adecuado, y los equipos de usuarios.

También presentamos un modelo de propagación para interiores y su comparación con el modelo de propagación en el espacio libre, y como se relacionan entre ambos. Al final de capítulo presentamos algunos lineamientos para brindar un nivel aceptable de seguridad dentro de las redes inalámbricas y algunas consideraciones para el mantenimiento de las redes.

2.1 METODOLOGÍA PARA EL DISEÑO [1, 2]

El primer paso para diseñar cualquier red es determinar el objetivo final de ella, es decir, las necesidades de los usuarios, para el diseño de una red inalámbrica se debe incluir la definición del área de cobertura.

Al inicio de la etapa de diseño se debe determinar las áreas en las que los usuarios estarán ubicados, las rutas comunes entre las ubicaciones principales, como por ejemplo salas de conferencia, salones de clases, laboratorios, etc., para esta etapa es importante contar los planos de las instalaciones donde se desea brindar el servicio a fin de poder estimar el área de cobertura.

También se deben determinar las velocidades mínimas que requieren los usuarios, para esto es necesario conocer las aplicaciones que se ejecutaran, no todas las aplicaciones se ajustan a las WLAN, por lo tanto el diseño de la red requiere que se considere el ancho de banda disponible.

Una primera etapa en el diseño de la WLAN podemos llevarla a cabo contestando las siguientes preguntas, destinas a reconocer que versión del estándar 802.11 (11a, 11b o 11g) es necesaria para implementar nuestra red:

- ¿Cuáles son las aplicaciones que se usaran y cual es su requerimiento de ancho de banda por usuario?

- ¿Planea usar la WLAN para condiciones de Voz sobre IP (VoIP, siglas en inglés) portátiles, y si es así, cuántas conexiones VoIP concurrentes tendrá dentro de un área de cobertura del AP determinada?

- ¿Cuál es la densidad promedio y máxima de los usuarios en un área de cobertura predeterminada, y si es posible que dicha densidad aumente?

- ¿Cuántos AP son necesarios?

- ¿Qué aplicaciones futuras se están considerando y cual es el requerimiento de ancho de banda que se espera?

- ¿A qué área físicas se planea proporcionar el acceso a la WLAN?

- ¿Los AP necesitan estar colocados en el techo o en ubicaciones seguras que no estén al alcance de la vista?

- ¿Qué tipos de equipos de usuarios (tarjetas PCMCIA) se utilizarán?

- ¿Dentro de las instalaciones se emplea algún otro equipo que pueda causar interferencia con el AP, como equipos BlueTooth, teléfonos inalámbricos, hornos de microondas, etc.?

- ¿Cuáles son las regulaciones que rigen el uso del estándar IEEE 802.11 en la región?

También se debe determinar que otras funciones deberán ser consideradas para la puesta en operación del servicio, algunas de estas funciones son VLAN, QoS, Seguridad, Balanceo de cargas, Interoperabilidad, etc.

Las VLAN son una característica relativamente nueva en las WLAN, proporcionan la capacidad de separar el tráfico. Una pregunta válida sería ¿Por qué desearía contar con una VLAN sobre medios inalámbricos? Un ejemplo es el de tráfico de usuarios invitados, normalmente, debe establecerse un sistema de seguridad para los usuarios permanentes de la red, cuando los invitados quieren hacer uso de la red, proveerles de este servicio no es sencillo, ya que deben de establecerse contraseñas y cuentas, y es posible que los invitados cambien regularmente. Mediante el uso de las VLAN se puede proporcionar a los invitados cierto nivel de seguridad y permitir el acceso a la parte de la red a la que se quiere que tengan acceso.

La calidad de servicio (QoS) es un servicio necesario si se intenta proporcionar soporte para VoIP, y también si se desea diferenciar el tráfico por puerto, aplicación o usuario. Actualmente el grupo de trabajo IEEE 802.11e esta trabajando para definir el estándar que de soporte de QoS a las redes inalámbricas.

En cuanto a seguridad, debemos asegurarnos que la solución en seguridad y los equipos que se seleccionen sean compatibles, tomando en cuenta que no tendremos un nivel de seguridad más alto que el del equipo menos sofisticado de la red.

El balanceo de cargas es otro de los elementos que debe tomarse en consideración al momento de diseñar redes con gran cantidad de usuarios y tráfico. Los AP con características para brindar el servicio en grandes empresas proporcionan soporte para esta función, en algunos casos es necesario prestar atención a la forma en que están configurados, sin embargo, hay muchos equipos orientados a redes domesticas y de pequeñas y medianas empresas (PYMES) que por sus bajos costos son elegidos a la hora de implementar las redes, pero no soportan este servicio.

La interoperabilidad también se debe considerar al momento de seleccionar los equipos, debemos asegurarnos que cualquier equipo que seleccionemos cuente con la certificación Wi-Fi, esto proporciona un nivel básico de pruebas y certificación de la interoperabilidad.

Al igual que en cualquier proyecto, el primer paso es establecer los objetivos y luego formular un plan para alcanzarlos. A pesar de que los objetivos específicos de implementación de una WLAN variaran, existe una constante: ***implementar la red en las áreas designadas, que proporcione cobertura confiable y ofrezca el nivel de desempeño esperado sin poner en riesgo la seguridad de la institución.***

2.2 Designación de áreas [1]

En pocos casos se despliega una WLAN a lo largo de toda la organización en un solo esfuerzo de despliegue inicial, una de las razones principales de esto es que puede resultar difícil obtener el financiamiento para implementar una red grande, los responsables de otorgar el financiamiento por lo regular solicitan una muestra de cómo trabajara la red, evaluación de los gastos y recursos del proyecto, la veracidad de la estimación del presupuesto y la recuperación de la inversión.

Se reconoce, además, que todas las tecnologías que se implementan tienen una curva de aprendizaje, por lo tanto la ejecución de un despliegue limitado puede proporcionar un entrenamiento valioso para cuando se vaya a ampliar la red. Por esta razón las organizaciones optan inicialmente por un

despliegue limitado, existen distintos criterios para definir la manera en que pueden estar limitados los despliegues.

2.2.1 Despliegue solo en los lugares en los que se necesita

Esta estrategia se basa en la suposición de que cuando los usuarios que cuenten con computadoras portátiles están en su área de trabajo, por ejemplo, una oficina, cubículo o escritorio, pueden acceder a la red a través de una conexión cableada, por lo tanto la red inalámbrica esta limitada a los lugares donde las personas tienden a congregarse en un área donde no tengan acceso cableado a la red, como salas de conferencia, salas de juntas, cafeterías, salones de clase, laboratorios etc.

Esta estrategia no toma en cuenta el hecho de que las personas son impredecibles y los lugares donde se reúnen a trabajar no son siempre los mismos. Esta falta de precisión aumenta a medida que en las empresas se usan con mayor frecuencia computadoras portátiles o PDA´s. Asimismo, a medida que se comienza a usar la infraestructura de las WLAN para proporcionar soporte de voz local, la expectativa de los usuarios es que la cobertura sea tan completa como la de los teléfonos celulares.

Para algunas organizaciones el despliegue de la red Wi-Fi en salones de clases y auditorios pronostica un despliegue completo, si se desea hacer un despliegue limitado son necesarios otros medios de limitación, lo que nos lleva a la siguiente estrategia.

2.2.2 Despliegue de un edificio a la vez

En los entornos universitarios donde distintos edificios o grupos de edificios tienen asignaciones diferentes es común que se despliegue la red en un edificio a la vez. Este modelo es típico en una universidad donde una facultad despliega una red Wi-Fi en su edificio y les proporciona las tarjetas a los estudiantes de la facultad, o les dan las características que deben tener las tarjetas que adquiera por su cuenta para que puedan acceder a la red.

Resulta más fácil conseguir el financiamiento para implementar una WLAN en un solo edificio que en todo el campus de la universidad, se pueden usar fuentes externas a la universidad, como asociaciones de alumnos, compañías locales asociadas, etc.

Una desventaja de este modelo es que la mayoría de los estudiantes y algunos profesores pasan el día en más de un edificio. La experiencia muestra que cuando se despliega una WLAN en un solo edificio de la universidad se crea la expectativa de que también se implementara la red en el resto del campus, salones de clases, cafeterías, bibliotecas, y otros lugares.

2.2.3 Despliegue entre edificios o grupos de trabajo temporales

Este modelo se despliega no tanto por la movilidad que proporciona al usuario, sino por la movilidad que proporciona a la infraestructura. Es común que grupos de personas que pertenecen a grupos de trabajo diferentes se reúnan en periodos temporales para un proyecto específico, este fenómeno ha impulsado la creación del término redes en movimiento. En ocasiones las organizaciones despliegan la red Wi-Fi para satisfacer estas demandas.

Cuando un edificio se utiliza de manera temporal, no tiene mucho sentido, en cuanto a los gastos, instalar cables a lo largo de todo el edificio para abandonar la instalación posteriormente. Por lo regular estos edificios cuentan con cableado de cobre instalado para dar soporte a los sistemas telefónicos, pero es insuficiente para las redes de información, las soluciones de cableado temporales que implica que los cables cuelguen de los techos entre los edificios o conductos puestos con cinta en las paredes ofrecen una apariencia poco profesional y un riesgo potencial en la seguridad.

Una red Wi-Fi se puede desplegar más rápido a lo largo de un edificio que una red tradicional cableada, además de no requerir mayores gastos, cuando llega el momento de desocupar el edificio, la infraestructura de la red se puede desmontar fácilmente y volver a desplegar en otra locación.

Los grupos de trabajo temporales presentan retos similares a los de un edificio temporal y se ajustan de la misma forma a un despliegue Wi-Fi, las redes se pueden desplegar rápidamente en áreas como cafeterías, tiendas, y demás lugares diseñados para un grupo de trabajo temporal.

2.3 Planeación de la Capacidad [1]

Una vez que se ha definido la estrategia de despliegue, el paso siguiente debe ser la definición del nivel de servicio WLAN que necesita proporcionar a los usuarios. Las WLAN por naturaleza son una tecnología de medio compartido, un AP establece un área de cobertura o celda que proporciona una cantidad de capacidad de salida que es compartida por todos los usuarios dentro de esa celda, asociados a un AP.

En las WLAN la cantidad de usuarios puede variar en la medida en que estos entren y salgan del área de cobertura, además, debido a la transmisión a través de ondas de radio, la capacidad de salida esta sujeta a la variación de factores transitorios como, por ejemplo, la interferencia, los cuales disminuyen la capacidad de salida cuando se presentan en el área de cobertura. Por lo tanto, la planeación de la capacidad para las WLAN está representada por una aproximación.

Una pregunta que debemos plantearnos a la hora de determinar la capacidad es ¿Qué capacidad de salida se deberá, en promedio, proporcionar a cada usuario? Los distintos tipos de usuarios tienen diferentes promedios en los requerimientos de capacidad de salida, los trabajadores de almacenes y puntos de venta que usan lectores de códigos de barra requieren una capacidad de salida modesta a diferencia de los usuarios de oficinas y salones de clase que trasfieren correo electrónico, exploran la Internet e intercambian ocasionalmente archivos de texto, hojas de cálculo o presentaciones, quienes tienen requerimientos de salida más grandes, aunque relativamente pequeños en comparación con los movimientos de información de las grandes organizaciones.

En el caso de las entidades educativas son los estudiantes y el personal docente y administrativo quienes usan principalmente la red. La planeación de la capacidad debe estar enfocada ha satisfacer la necesidad de estos grupos.

Estudiantes accesando al sitio intranet de una universidad durante una conferencia. A pesar de que el protocolo HTTP es bastante eficiente, la transferencia de páginas Web con muchas imágenes requiere de una cantidad sustancial del ancho de banda para obtener un uso aceptable para el usuario. Este requerimiento se vuelve mayor cuando, como parte de una presentación de un instructor, muchos estudiantes deben acceder a la WLAN casi al mismo tiempo.

Un punto importante en la planeación de la capacidad que no debemos olvidar es el reciclamiento de canales. Uno de los enfoques más antiguos para maximizar la cantidad de canales disponibles es el reciclaje de estos.

La figura 2.1 proporciona una muestra de la forma en que se pueden reciclar los canales de forma que se pueda cubrir un área extensa, incluso cuando solo se cuenta con tres canales que no se traslapan.

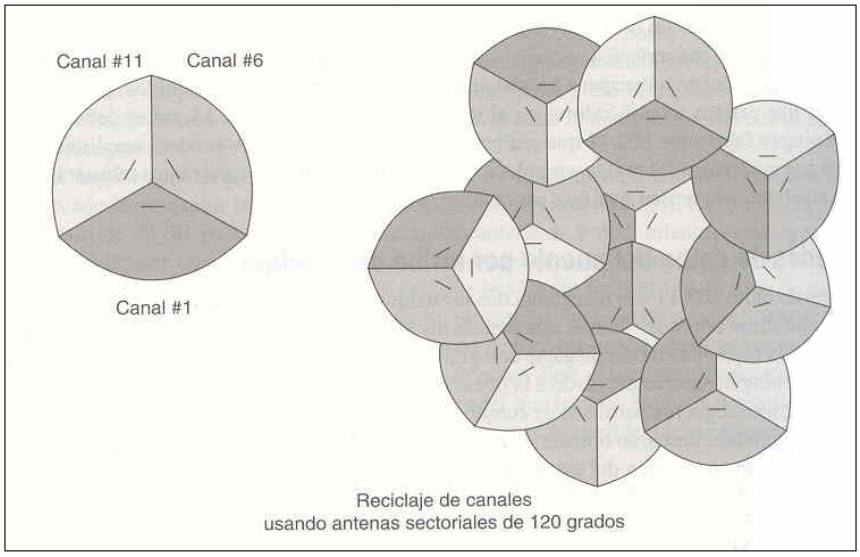


Figura 2.1 – Ejemplo de reciclaje de canales

La asignación de canales de tal forma que no afecten a las células adyacentes es muy importante. También es crítico el uso de la cantidad adecuada de ganancia en las antenas, demasiada ganancia puede ocasionar la pérdida de energía en un canal adyacente.

La elección del área de cobertura, así como la correcta planeación de la capacidad deben ser confirmadas por una evaluación física en el sitio donde se planea implementar el servicio.

2.4 Evaluación física en sitio [1]

Cuando se tiene identificada el área a cubrir y el plan de capacidad, se deben realizar pruebas a fin de validar o invalidar las suposiciones teóricas planteadas. Este es el momento en el que realmente se colocan los AP y las antenas seleccionadas en sus posibles ubicaciones y se comprueba la

cobertura. De la misma manera en que un producto real puede ser muy distinto de lo que especifica su hoja de datos, una construcción puede ser muy distinta de su plano de planta. Además, la propagación en la práctica puede ser muy distinta a la estimada en teoría, por tanto, antes de comprar el equipo e instalarlo es muy recomendable que se realicen pruebas de instalación en la mayoría de las posibles ubicaciones que fueron definidas durante el proceso de la planeación de cobertura.

Es importante contar con los planos del edificio donde se pretende instalar el equipo, dichos planos deben estar dedicados al proyecto, a fin de poder escribir sobre ellos para marcar las ubicaciones de los AP, líneas de corriente y elementos, por ejemplo, columnas o lugares en los que se puedan montar los AP, además, es preciso incluir los conductos que llevaran y protegerán los cables Ethernet y de corriente, desde y hasta los AP. Los planos de construcción también indican las distancias relativas entre las áreas y el tamaño de las habitaciones que se deberán cubrir, esto ayudara a determinar cuantos AP se deben usar y donde localizarlos para obtener un desempeño óptimo.

Además, un recorrido del sitio junto con alguna persona que lo conozca bien permite al equipo de evaluación e instalación estar al tanto de las operaciones que ocurren en los cuartos y pisos adyacentes; Además de sus contenidos, los planos de los edificios normalmente no indican la instalación de equipo y están limitados a planos de planta. Un elemento adicional que se debe considerar cuando se revisan los planos de un edificio, es que no todos los planos reflejan las configuraciones de cómo fueron construidos.

Una evaluación en sitio puede llevarse a cabo en el siguiente orden:

- Estudio de los planos del edifico junto con todo el personal involucrado en el proyecto.
- Identificación de los posibles obstáculos que no se muestran en los planos y marcarlos.
- Contar con los planos de los edificios en el sitio.
- Seleccionar los equipos adecuados.
- Elaborar un informe final.

Después de realizada la evaluación en sitio es recomendable elaborar un informe final que debe, al menos, incluir la siguiente información:

- Ubicación de los AP, como se muestra en los planos de cobertura. Las distancias de por lo menos dos paredes u otros elementos permanentes son necesarias para señalar con exactitud las ubicaciones.

- Características de cada AP.

- Configuración sugerida para cada AP, incluida velocidad, canal y parámetros de seguridad, además de la selección de los protocolos de seguridad.

- Planos de las áreas de coberturas.

- Fotografías de las ubicaciones de los AP y sus montajes.

- Configuración de canales y velocidades de transmisión y recepción.

Una buena razón para crear un informe final con un nivel de detalle y claridad tan excelente como sea posible es que, como ocurre en la mayoría de los casos, la terminación de la instalación no se programa sino hasta después de algunos meses posteriores a la evaluación en sitio.

2.5 Diseño Interno y Externo de los edificios [1]

Entender el efecto que distintos materiales de construcción tienen en la energía de radio representa un buen punto de inicio cuando se evalúa el edificio donde se desea brindar el servicio, por medio de planos o mediante la inspección física directa debemos familiarizarnos con los tipos de materiales de construcción que se encuentran en el edificio.

En general, mientras más denso sea el material de construcción, evitara que la energía de RF pase a través de él, esto se conoce como atenuación de la señal. La madera, paredes de cubículos, compartimientos de habitaciones, etc. contienen una cantidad relativamente alta de aire, mientras que los ladrillos, cemento, piedras y yeso tienen menos aire dentro de ellas y, por tanto, tienden a ser

más sólidas. Los edificios con paredes externas de aluminio, hierro, latón, etc. presentan un problema especial debido a que no solo detienen la señal, sino que la reflejan, propiciando la propagación a través de trayectorias múltiples.

Como podemos observar en la figura 2.2, en la banda de 2.4 GHz existen tres canales no traslapados. Si un edificio se puede cubrir con tres o menos AP, la interferencia entre canales no es un problema, lo cual simplifica la instalación y puesta en funcionamiento del equipo y del servicio.

Con un solo AP o con tres AP se pueden cubrir la mayoría de los pisos de oficinas modernas, las cuales tienden a solo tener paredes parciales en los cubículos en lugar de paredes que vayan desde el piso hasta el techo, las cuales tienen a atenuar la energía de la señal y reducir la cobertura.

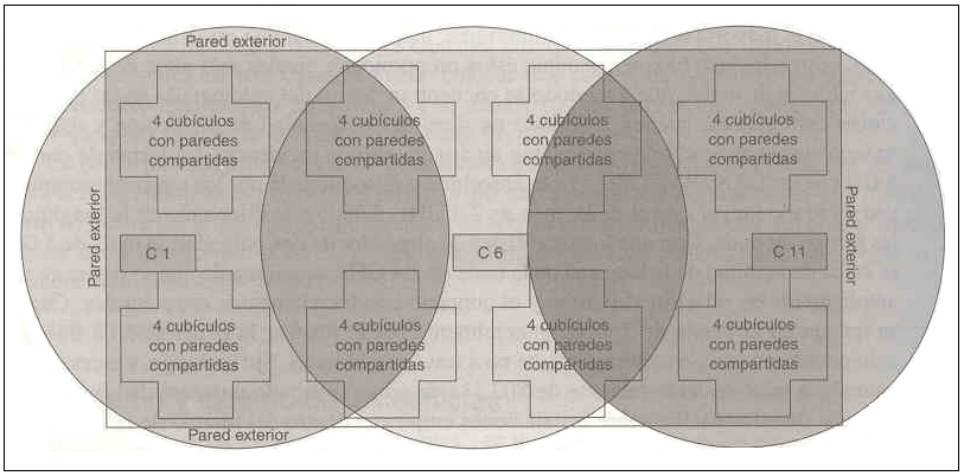


Figura 2.2 – Vista de un piso con la cobertura de los tres canales no traslapados

Para el caso de escuelas o universidades, donde la mayoría de las paredes están hechas de distintos tipos de materiales de construcción podemos optar por un AP con una antena omnidirecional colocada en la pared, de esta manera es posible cubrir dos salones de clase. Dada la alta densidad de usuarios en las escuelas y universidades, la capacidad de salida por usuario ofrecida por este tipo de instalación puede ser bastante baja. Debido a que solo están disponibles tres canales no traslapados, el aislamiento de las células que están en el mismo canal se puede convertir en un problema.

Seleccionar las mejores ubicaciones para la colocación de los AP y de las antenas requiere de la consideración de factores distintos, y algunas veces hasta contradictorios. Las ubicaciones óptimas desde una perspectiva de propagación pueden ser estéticas y económicamente inaceptables, las restricciones en el presupuesto pueden dar como resultado AP con rangos por debajo de los niveles óptimos y reducir las opciones de antenas. Cada edificio presentará distintos parámetros que sugerirán ubicaciones diferentes, sin embargo, se pueden aplicar algunas reglas generales.

La instalación en el techo tiende a funcionar mejor. Al colocar los AP en los techos, podemos configurar células que maximicen el área de cobertura del AP con antenas omnidireccionales, este es el tipo más común que existe. La colocación en el techo hace que los AP y antenas estén lejos de las personas, minimizando el contacto intencional o no intencional. Algunos AP se pueden ocultar por arriba de los techos falsos, donde solo estén visibles las antenas, esta es una característica positiva desde un punto de vista estético. En los edificios con techos falsos es más frecuente colocar un AP diseñado para estas ubicaciones cerca de la antena en lugar de tener pérdidas en costo y cable asociadas con la colocación de AP remotos.

El montaje de los AP en los escritorios o en la parte alta de los muros proporciona beneficios similares a los de la colocación en los techos. Este tipo de instalación es común cuando se trabaja con AP de costo bajo y que no son adecuados para la instalación en el techo, o cuando es probable que la instalación sea temporal.

En las construcciones donde la colocación en el techo es impractica, ya sea porque representa una disrupción inaceptable a las operaciones normales, o se considera un aspecto poco estético, la colocación en las paredes es una opción cada vez es más popular. Cuando se instalan antenas omnidireccionales, los AP montados en las paredes con frecuencia pueden cubrir dos habitaciones. Mediante la colocación de múltiples AP en las paredes, la cobertura completa de las unidades montadas en la pared se puede alcanzar en casi toda las habitaciones.

2.6 Selección del Hardware para el AP [1]

Existen muchos tipos de diseños para los AP en el mercado, tanto en la forma física como en la arquitectura. La selección de la forma principal puede ser crítica a la hora de implementar la red y también para el soporte, mantenimiento, costo general, seguridad y confiabilidad.

Primero consideraremos una arquitectura inteligente del AP como se puede ver en la figura 2.3.

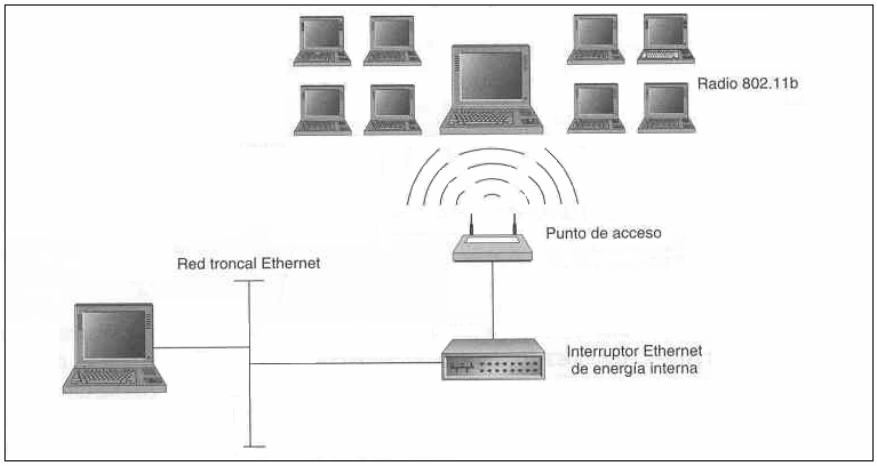


Figura 2.3 – Arquitectura de AP Inteligentes

En esta arquitectura el AP tiene capacidad de procesamiento y usa su "inteligencia" en el extremo de la red, se conecta directamente a la red cableada al mismo tiempo que es un AP independiente, es decir, que no depende de ningún servidor o controlador en la red para mantener la conexión con los usuarios. Cuando un AP falla, solo ese AP queda afectado y los equipos restantes continúan operando normalmente. La desventaja de esta configuración es que en las redes de grandes empresas se requiere de un servidor de administración para proporcionar el soporte, configuración y el mantenimiento de la red.

Los AP "inteligentes" son más fáciles de instalar, pueden integrarse en cualquier lugar de la red que se desee y escalar la red simplemente mediante la adición de más AP.

Una segunda arquitectura que se puede implantar es presentada en la figura 2.4, en este caso se cuenta con un controlador central.

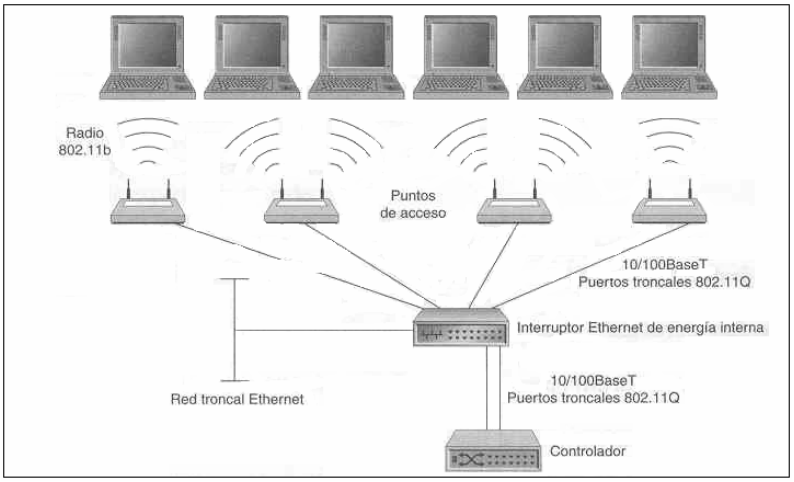


Figura 2.4 – Arquitectura de AP con controlador

En esta configuración de red la "inteligencia" no la da el AP, sino que la soporta el controlador central. Este controlador administra la autenticación, seguridad, archivos de configuración y otros aspectos de la red. La desventaja de esta configuración es que representa un solo punto de falla, es decir, cuando el controlador falla cualquier AP que este conectado a él también fallará.

El controlador da soporte a una cantidad específica de AP, por lo que se deberá tomar en consideración, ya que si solo se desean instalar dos AP con un controlador, el costo del sistema aumentará ya que habrá que comprar un controlador para dar servicio solo a dos AP. En las redes donde se cuente con una gran cantidad de AP (por ejemplo 200 AP) se necesitarán varios controladores (por ejemplo, 4 controladores por cada 100 AP) y, además, se necesitará una estación de administración para manejar los controladores.

2.7 Selección del equipo del usuario [1]

Debido a que la mayoría de las características de la red se encuentran en el AP, hay pocos aspectos que considerar en el lado del usuario. Un aspecto que si se debe considerar es la selección del equipo que utilizarán los usuarios, para poder brindarles un buen servicio.

En el mercado encontramos una variedad de equipos para usuarios y no todos cuentan con las mismas características, esto puede ser un factor importante en la decisión, se deben considerar aspectos como la interoperabilidad, la seguridad y la QoS. Por esta razón, primero debemos seleccionar las características necesarias en la red y a partir de estas seleccionar los equipos de usuario que cumplan con las características del sistema, y proporcionar las características de la red a los usuarios para que estos adquieran sus equipos basados en estas características o en su defecto, indicarles que los equipos que adquieran deberán contar con la certificación de compatibilidad Wi-Fi 802.11.

2.8 Modelos de propagación [4, 5, 7]

El canal de radio es una de las limitantes del óptimo desarrollo de una red inalámbrica. La trayectoria entre el receptor y el transmisor puede variar de muchas maneras, con diferentes tipos de obstrucciones. Esto hace difícil predecir la señal recibida o analizar el canal de radio.

El modelado de un canal de radio se hace típicamente en base a estadísticas, basadas en mediciones realizadas específicamente para ese fin. La mayoría de los modelos de propagación se han realizado para sistemas inalámbricos al aire libre y no toman en consideración la propagación en espacios interiores. Los modelos existentes difieren en su aplicación sobre diferentes tipos de terreno y condiciones ambientales, otros están restringidos a situaciones más específicas. Lo que es cierto es que ningún modelo puede satisfacer todas las situaciones ambientales. La mayoría de los modelos predicen las pérdidas por trayectoria promedio.

Es importante elegir un modelo de propagación adecuado ya que de este va a la estimación de las áreas de cobertura en las cuales se desea brindar el servicio. Los modelos de propagación son usados entre 1 y 5 años por los operadores, mientras se hacen nuevos estudios de propagación. El campo de propagación en interiores es relativamente nuevo y la primera investigación se inicio en la década del 80. La aparición de las WLAN ha hecho necesario contar con modelos para predecir el área de cobertura en espacios interiores.

La figura 2.5 nos permite observar como se comporta la potencia recibida a medida que la distancia entre el transmisor (Tx) y el receptor (Rx) aumenta.

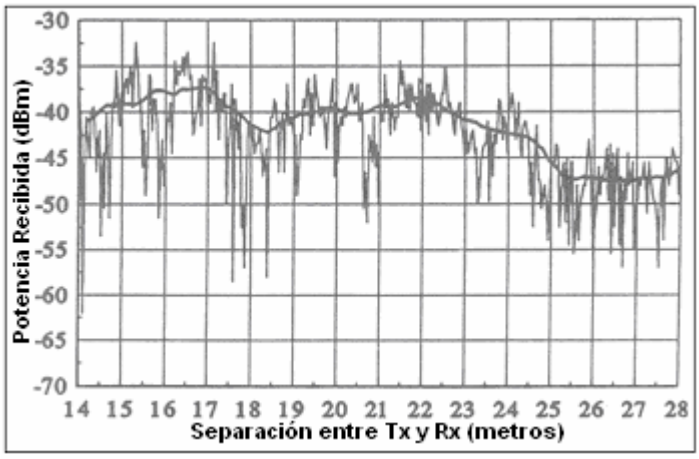


Figura 2.5 – Relación entre la potencia recibida contra la separación del Tx y Rx.

Los mecanismos de propagación influyen directamente en como se comporta la señal al ser transmitida, es por ello que debemos tomarlos en consideración al emplear los modelos de propagación.

Los mecanismos de propagación son:

- **Reflexión**: Ocurre cuando una onda propagada choca contra un objeto que tiene dimensiones mayores que la longitud de onda de la señal. La reflexión tiene lugar en la superficie de la tierra, muros y edificios.

- **Difracción**: Ocurre cuando la trayectoria entre el transmisor y el receptor es obstruida por una superficie que tiene irregularidades. A altas frecuencias tanto la difracción como la reflexión dependen de la geometría del objeto, así como de la amplitud, la fase y la polarización de la onda incidente en el punto de difracción.

- **Dispersión**: Ocurre cuando el medio a través del cual viaja la onda consiste de objetos con dimensiones menores comparadas con la longitud de onda, y donde el número de obstáculos por unidad de volumen es mayor. La dispersión en las ondas es producida por superficies rugosas, pequeños objetos, etc.

La figura 2.6 nos muestra como se comporta la señal a ser afectada por alguno de los mecanismos de propagación

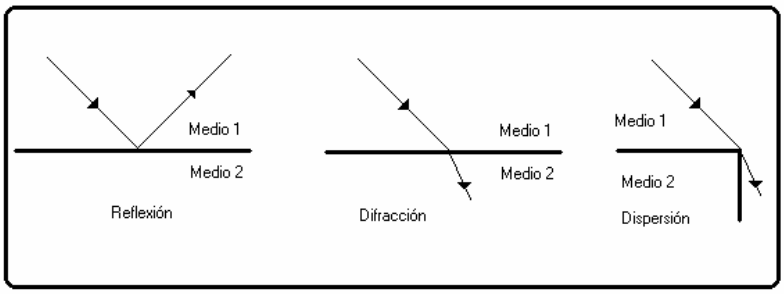


Figura 2.6 – Mecanismos de propagación.

En el análisis de la propagación de las ondas de radio también debemos considerar un fenómeno conocido como Ensombrecimiento (Shadowing). Se conoce como ensombrecimiento al efecto causado por obstrucciones en la trayectoria de las ondas de radio, y puede bloquearla la trayectoria parcial o totalmente.

La variación de la señal inducida por la difracción se relaciona a este fenómeno por medio de una variable aleatoria la cual tiene una distribución log-normal, donde la desviación estándar de esta distribución, σ, caracteriza el fenómeno. En otras palabras, los ensombrecimientos representan la variación estadística de la señal recibida debido a irregularidades en la trayectoria entre el transmisor y el receptor.

Los ensombrecimientos muchas veces son llamados Desvanecimientos Lentos o Desvanecimientos de Larga Duración y son causados por obstrucciones naturales (árboles) o artificiales (paredes) y se caracterizan por tener una distribución log-normal cuya desviación estándar es determinada a partir de mediciones. Así para un ambiente de propagación cuyas pérdidas medias a lo largo de la trayectoria se obtiene determinísticamente por alguno de los modelos de propagación, es posible sobreponer una variación con distribución log-normal correspondiente a este fenómeno.

En general las señales de radio se caracterizan por propagarse en condiciones de multitrayectoría, donde podría existir una trayectoria dominante y un conjunto de rayos retardados.

En el receptor la señal puede sumarse constructiva o destructivamente dependiendo de la fase. Este fenómeno es conocido como: Desvanecimiento Rápido o Desvanecimiento de Corta Duración. Se caracteriza con una distribución Rayleigh o Rice. Cuando existe una trayectoria de línea de vista o dominante sobre las demás, los desvanecimientos son caracterizados con una variable aleatoria tipo Rice, que se muestra abajo.

$$f(x) = \frac{x}{\sigma^2} e^{-\left(\frac{x^2+A^2}{2\sigma^2}\right)} I_0\left(\frac{Ax}{\sigma^2}\right) \qquad (2.1)$$

donde: A = Potencia de la trayectoria dominante.

I_0 = Función modificada de Bessel de primera clase y orden cero.

σ = Desviación Estándar

Mientras que cuando no existe una trayectoria dominante la señal recibida será un conjunto de muestras con diferente fase (multitrayectoria) que ocasionara que en ciertos instantes la señal recibida sea atenuada (desvanecida) casi en su totalidad y este fenómeno se modela con una variable aleatoria de tipo Rayleigh. Para el caso de desvanecimientos de tipo Rayleigh se ha encontrado que los desvanecimientos ocurren cada media longitud de onda de la señal portadora.

Un dato interesante es que la variable aleatoria Rayleigh es un caso particular de la variable aleatoria tipo Rice, cuando la potencia de la señal dominante no existe, es decir, A = 0.

$$f(x) = \frac{x}{\sigma^2} e^{-\left(\frac{x^2}{2\sigma^2}\right)} \qquad (2.2)$$

Además de estos mecanismos de propagación y los fenómenos que se presentan debemos considerar la penetración de la señal, ya que las WLAN por lo regular trabajan en espacios interiores y las paredes, divisiones, puertas y demás afectan su desempeño.

Cuando una señal se propaga a través de un ambiente de interiores puede que se encuentre con muchos obstáculos y deba penetrarlos para continuar con la trayectoria de la señal. Cuando la señal penetra un obstáculo experimenta una pérdida que dependerá del espesor del objeto y del material

con que este construido. La frecuencia de onda electromagnética también influirá en cuánto de la señal pasará a través del objeto.

Las grandes empresas han realizado mediciones con la finalidad de conocer las pérdidas de la señal a través de distintos materiales. En la tabla 2.1 mostramos las medidas presentadas en el "Wireless LAN User's Guide version 4.2" de Ericsson.

Obstáculo	Pérdida
Espacio Abierto	0 dB
Ventana (sin malla metálica)	3 dB
Ventana (con malla metálica)	5 – 8 dB
Pared delgada (plafón)	5 – 8 dB
Pared mediana (Madera)	10 dB
Pared gruesa (6" de grosor)	15 – 20 dB
Pared muy gruesa (12" de grosor)	20 – 25 dB
Piso y Techo (grosor mediano)	15 – 20 dB
Piso y Techo (grosor grueso)	20 – 25 dB

Tabla 2.1 – Valores de pérdidas para diversos materiales.

Además de los mecanismos de propagación y de la penetración, también debemos mencionar que las interferencias y el ruido afectan la propagación de la señal.

Las WLAN comparten la banda de 2.400 – 2.4835 GHz con la industria, la medicina y la Ciencia, ya que dicha banda no requiere en la mayoría de los países permisos para su utilización, por tal motivo es utilizada en la investigación, y es susceptible de interferir con otros equipos que trabajen en la misma banda de frecuencia. El estándar 802.11b permite radiar una potencia máxima de 1 watt mediante técnicas de espectro disperso, lo que facilita que muchos usuarios puedan compartir el mismo espectro.

Los modelos de propagación se han enfocado, tradicionalmente, en predecir la potencia (intensidad) promedio recibida a una distancia dada del transmisor, así como las variaciones de la potencia de la señal en la cercanía espacial de un lugar o punto particular. Los modelos de propagación que predicen la potencia (intensidad) media de la señal para cualquier distancia de separación entre transmisor (Tx) y receptor (Rx) (distancia de separación arbitraria) son útiles para estimar el área de cobertura de radio de un transmisor y se conocen como: Modelos de Propagación de Gran Escala;

Porque modelan o caracterizan la fuerza o potencia de la señal para distancias de separación entre Tx y Rx grandes (varios cientos o miles de metros).

Los modelos de propagación que caracterizan las fluctuaciones rápidas de la fuerza o potencia de la señal recibida, sobre distancias muy cortas (unas cuantas longitudes de onda) o para tiempos de recorrido muy cortos (algunos segundos), se conocen como: Modelos de Propagación de Pequeña Escala.

La predicción del área de cobertura mediante los modelos de propagación es importante ya que nos permite decidir como y en donde debemos colocar los AP para generas las celdas de cobertura, utilizando la misma frecuencia en un área común y sin causar interferencia entre ellos, además de que nos permiten determinar la mayor área de cobertura posible con un AP.

Además, es necesario definir un umbral para conocer en que momento una conexión dejara de ser útil o no permitirá un buen enlace entre el AP y el usuario, este umbral lo podemos definir mediante dos medidas mencionadas en la especificación 802.11b, que son:

- La tasa de error por trama (FER, siglas en inglés) debe tener un máximo de 8×10^{-2}, también puede ser dada por la tasa de error por bits (BER, siglas en inglés), por la tasa de error por paquetes (PER, siglas en inglés) y/o por la tasa de error por símbolos (SER, siglas en inglés).

- La intensidad de la señal recibida debe ser de al menos –76 dBm para la especificación 802.11b trabajando con modulación CCK.

Uno de los retos importantes a la hora de diseñar es contar con un modelo de propagación adecuado. Decidimos utilizar como modelo base el ETSI TR – 101 – 112, este es un modelo de propagación para interiores probado para la tecnología del servicio de telecomunicaciones móvil universal (UMTS, siglas en inglés), y derivado del modelo COST 231 de Paredes Múltiples (MWM).

2.8.1 Modelo COST 231 MWM para Interiores

El modelo permite estimar la pérdida en la trayectoria como la pérdida en el espacio libre más las pérdidas introducidas por las paredes y pisos que tiene que atravesar la señal en la trayectoria directa entre el Tx y Rx. Se ha observado que la pérdida total por pisos es una función no lineal del número de pisos atravesados. La pérdida constante es un valor que resulta cuando las pérdidas a través de las paredes son determinadas de los resultados de las medidas, usando regresiones lineales múltiples.

Descripción del modelo

El modelo esta definido por:

$$L = L_{FS} + L_c + \sum K_{wi} L_{wi} + n^{\left(\frac{(n+1)}{(n+2)-b}\right)} * L_f \qquad (2.3)$$

donde: L_{FS} = pérdida en el espacio libre entre Tx y Rx.

L_c = Constante de pérdida

K_{wi} = Número de paredes penetradas tipo i

L_{wi} = Pérdidas en las paredes tipo i

L_f = Pérdidas entre pisos adyacentes

n = Número de pisos penetrados

b = Constante Empírica

Nota 1: L_c normalmente es igual a 37 dB.

Nota 2: n = 4 para la mayoría de los ambientes interiores. Cuando se desee realizar el cálculo para un ambiente muy difícil n puede ser igual con 3.

En la tabla 2.2 presentamos los valores de las pérdidas contempladas en el modelo.

Tipo de Pérdida	Descripción	Valor (dB)
L_f	Tipos de pisos para oficinas Concreto reforzado Piso delgado < 30 cm. Mosaicos y/o azulejos	18.3
L_{w1}	Paredes internas delgadas Plafón Paredes con muchas ventanas	3.4
L_{w2}	Paredes internas gruesas Concreto y/o ladrillo	6.9

Tabla 2.2 – Valores de pérdidas del modelo.

Sustituyendo valores en la ecuación 2.3, el modelo queda de la siguiente manera:

$$L(R) = 37 + 30Log(R) + 18.3n^{\left(\frac{(n+1)}{(n+2)-0.46}\right)}dB \qquad (2.4)$$

donde: R = Distancia entre Tx (AP) y Rx (usuario), dada en metros.

n = Cantidad de pisos en la trayectoria

Si nos interesa solamente considerar la propagación en una sola área interior sin paredes que la dividan, la parte del modelo concerniente a la penetración entre paredes y pisos puede eliminarse, dejando al modelo de la siguiente manera:

$$L(R) = 37 + 30Log(R)dB \qquad (2.5)$$

2.8.2 Modelo de Propagación en Espacio Libre

Las WLAN que se pretendan poner en operación en áreas que se encuentren libres de obstáculos que atenúen la señal, tal como exteriores (áreas verdes) e interiores (salas, bibliotecas), pueden valerse de este modelo para su diseño.

Se utiliza para predecir la potencia de la señal cuando entre el Tx y el Rx hay una línea de vista clara o "LOS" (no hay obstáculos en la línea de vista). En este modelo, la potencia recibida disminuye en función de la distancia entre Tx y Rx, es decir, a medida que aumenta la distancia, disminuye la potencia.

El modelo de propagación en espacio libre esta dado por la Ecuación de Friis:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \qquad (2.6)$$

donde: Pr(d) = potencia recibida

Pt = potencia transmitida

d = separación entre Tx y Rx

At o Gt = ganancia de la antena Tx (cantidad adimensional)

Ar o Gr = ganancia de la antena Rx

L = pérdida del sistema (debido a atenuación en líneas de transmisión, pérdidas por filtros, y pérdidas en las antenas). Cuando L = 1, significa que no hay pérdida en el sistema

λ = longitud de onda

La pérdida en la trayectoria representa la atenuación de la señal, como una cantidad positiva, medida en dB. Esta definida como la diferencia en dB entre la potencia efectiva transmitida y la potencia recibida.

El modelo para la pérdida en la trayectoria cuando se conocen las ganancias de las antenas esta dado por:

$$P(dB) = 10Log\left(\frac{P_t}{P_r}\right) = -10Log\left(\frac{G_t G_r \lambda^2}{(4\pi)^2 d^2}\right) \qquad (2.7)$$

El modelo para la pérdida en la trayectoria cuando la ganancia de las antenas se asume unitaria esta dado por:

$$P(dB) = 10Log\left(\frac{P_t}{P_r}\right) = -10Log\left(\frac{\lambda^2}{(4\pi)^2 d^2}\right) \qquad (2.8)$$

Cuando la potencia recibida a una distancia (d_0 = distancia de referencia) es conocida, la siguiente ecuación puede usarse para encontrar la potencia a una distancia mucho mayor:

$$P_r(d) = P_r(d_0) + 20Log\left(\frac{d_0}{d}\right) \qquad (2.9)$$

Esta ecuación puede convertirse para la pérdida en la trayectoria fácilmente, quedando de la siguiente manera:

$$P(d) = P(d_0) + 20Log\left(\frac{d}{d_0}\right) \qquad (2.10)$$

2.8.3 Relacionando el Modelo de Pérdida en la Trayectoria para Interiores

Podemos ver que hay una relación aparente entre los dos modelos. Ambos operan con un punto de referencia y tienen una pérdida en la trayectoria logarítmica desde el punto de referencia:

$$P(d) = P(d_0) + 20Log\left(\frac{d}{d_0}\right) \rightarrow P(R) = 37 + 30Log(R) \qquad (2.11)$$

La pérdida en la trayectoria para el punto de referencia es:

- El modelo de pérdida en el espacio libre: $20Log(R)$

  donde R = distancia en metros, si d_0 = 1 metro.

- El modelo de pérdida en la trayectoria para interiores: $30Log(R)$

  donde R = distancia en metros

2.9 Realización de Encuesta

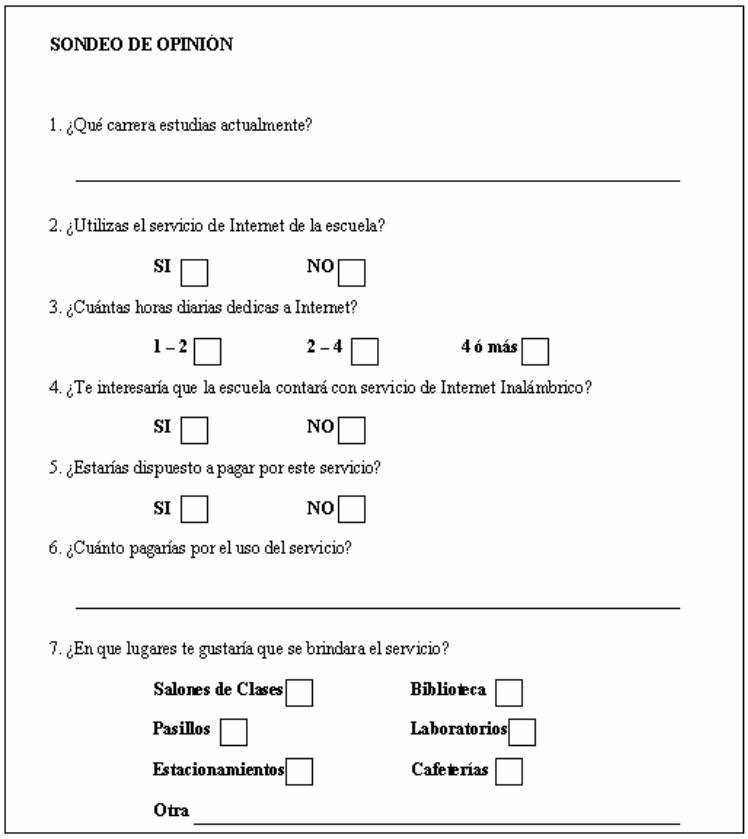
Es importante conocer las distintas inquietudes que puede generar la puesta en servicio de una red inalámbrica en una organización (empresas, entidades educativas, etc.), ya que afectara de manera directa el diario quehacer del personal que asiste y trabaja en ellas, y finalmente son ellos quienes utilizaran el servicio. Para ello es recomendable realizar un sondeo de opinión para conocer sus expectativas para con el proyecto.

En el caso de las entidades educativas, las siguientes preguntas pueden ser de valiosa ayuda al momento de diseñar y planear la red:

- ¿Qué carrera cursas actualmente?
- ¿Cuántas horas diarias dedicas a navegar en Internet?
- ¿Te interesaría que la Escuela contara con servicio de acceso inalámbrico a Internet?
- ¿Estarías de acuerdo a pagar por el servicio?
- ¿Dónde te convendría que existiera cobertura del servicio?

Al tener una idea de cual es el interés de los estudiantes y del personal docente y administrativo, podremos dirigir el diseño de la WLAN para satisfacer en la medida de lo posible sus necesidades.

En la figura 2.7 presentamos el cuestionario para el sondeo de opinión.


SONDEO DE OPINIÓN

1. ¿Qué carrera estudias actualmente?

_____

2. ¿Utilizas el servicio de Internet de la escuela?

SI ☐ NO ☐

3. ¿Cuántas horas diarias dedicas a Internet?

1 – 2 ☐ 2 – 4 ☐ 4 ó más ☐

4. ¿Te interesaría que la escuela contará con servicio de Internet Inalámbrico?

SI ☐ NO ☐

5. ¿Estarías dispuesto a pagar por este servicio?

SI ☐ NO ☐

6. ¿Cuánto pagarías por el uso del servicio?

_____

7. ¿En que lugares te gustaría que se brindara el servicio?

Salones de Clases ☐ Biblioteca ☐

Pasillos ☐ Laboratorios ☐

Estacionamientos ☐ Cafeterías ☐

Otra _____

Figura 2.7 – Cuestionario para sondeo de opinión.

2.10 Pasos básicos para brindar seguridad en una Red Inalámbrica [11]

El propósito de asegurar correctamente un AP es limitar el acceso desde el exterior a usuarios ajenos a nuestra red. Una red inalámbrica es por definición más difícil de proteger que una red convencional entre otras cosas porque el medio de transmisión es el aire, y en principio, en una WLAN se puede acceder desde cualquier lugar donde se cuente con cobertura.

A pesar de esto siempre se pueden establecer una serie de medidas básicas para impedir el acceso a la mayoría de los usuarios no autorizados.

Para establecer un nivel básico de seguridad podemos seguir los siguientes pasos:

1. **Colocación del AP**: El primer paso para cerrar el acceso no autorizado a nuestro AP es colocarlo de manera que limite el alcance a nuestra área de trabajo.

2. **Implementar un mecanismo de seguridad**: Por ejemplo WAP, que permite cambiar aleatoriamente la clave compartida entre AP y usuario que se utiliza para cifrar los datos de la red inalámbrica.

3. **Cambiar el SSID:** El SSID es la cadena de identificación usada por los clientes de un AP para ser capaces de iniciar una conexión. Este identificador viene predefinido por el fabricante y cada uno viene con una palabra por defecto. Los usuarios ilegales que conozcan estas palabras pueden acceder con relativa facilidad a una WLAN. Por cada AP que instalemos se debe seleccionar un SSID complejo.

4. **Deshabilitar el servicio DHCP**: En un principio puede parecer extraño pero en una WLAN es más importante de lo que parece. Mediante este paso un usuario puede descifrar nuestra dirección IP, máscara de subred, y otros parámetros TCP/IP relevantes, con los cuales podría obtener acceso a nuestra WLAN.

5. **Deshabilitar o modificar la configuración SNMP**: Si el AP soporta SNMP deberemos deshabilitar o cambiar tanto la cadena privada como la pública. Un usuario podría obtener información relevante sobre nuestra red mediante este servicio.

6. **Usar listas de control de acceso**: Para un control más efectivo de nuestra red es importante el uso de listas de control de acceso (ACL). Esta es una opción que no todos los AP ofrecen, por lo que deberemos de tenerla en cuenta a la hora de comprar el equipo.

La salida de las ondas de radio fuera del entorno donde esta ubicada la red permite la exposición de los datos a posibles intrusos, quienes podrían obtener información sensible a la institución. Varios son los riesgos derivables de esta situación, por ejemplo: Se podría realizar un ataque por inserción, ya sea de un usuario no autorizado o por la ubicación de un AP ilegal más potente que capte a los

usuarios en vez del AP de la institución, interceptando de esta manera, la red inalámbrica. Los AP pueden ser víctimas de un ataque de fuerza bruta para tratar de conseguir las contraseñas, por los que una mala configuración facilitaría la irrupción de la red por parte de los usuarios no autorizados.

Se podrían hacer varías recomendaciones para el diseño de una red inalámbrica y tratar de impedir en la medida de lo posible la mayoría de los ataques que suelen recibir por parte de las personas ajenas a la red.

Como primera medida, se debe separar la red de la institución en un dominio público y otro privado. En el dominio público tendrán acceso los usuarios de la red inalámbrica. Así mismo se deben implementar mecanismos de autenticación entre la red inalámbrica y la red cableada institucional, lo ideal sería aplicar un nivel de seguridad distinto según el tipo de usuario que quiera accesar a la red y dependiendo del tipo de aplicación que quiera utilizar.

A pesar de que suene contradictorio, es recomendable no utilizar normas de seguridad excesivas, ya que podría reducir la rapidez y la capacidad de la red.

También se pueden tomar medidas de seguridad en la construcción del edificio o en el área donde se pretende brindar el servicio de la red inalámbrica, se pueden utilizar materiales que atenúen la señal hacia el perímetro exterior. Mencionamos algunas de estas medidas:

- Utilizar cobertura metálica en las paredes exteriores.
- Colocar vidrio aislante térmico (atenúa las señales de radiofrecuencia).
- Instalar persianas metálicas en vez de plásticas.
- Colocar los AP lejos de las paredes exteriores.
- Utilizar pintura metálica en las paredes exteriores.
- Limitar la potencia de salida del AP.

2.11 Mantenimiento de las Redes inalámbricas [8]

No solo es importante contar con un buen diseño de la red inalámbrica, sino también contar con las políticas de mantenimiento para la red, ya que sin estas todo el trabajo realizado sería en vano.

A continuación presentamos un análisis del problema de mantenimiento y se exponemos algunos consejos para reducir su impacto.

Las principales áreas que se deben tomar en cuenta para dar mantenimiento en las WLAN son:

- **Entorno radio**: Esta área es exclusiva de los entornos inalámbricos y no existe en redes cableadas. Comprende los problemas que generan las interferencias entre los equipos de la propia red o con otras redes, perturbaciones radioeléctricas de otros equipos (hornos microondas, radares, teléfonos celulares, etc.) y redes de otras tecnologías (por ejemplo Bluetooth). En múltiples ocasiones la fuente de perturbaciones sólo emite potencia apreciable durante un breve periodo de tiempo, generando mal funcionamientos aleatorios que complican su identificación, en otras, la implementación de una nueva red con excesiva potencia en las cercanías y operando en la misma frecuencia o una muy próxima, obliga a una replanificación de las frecuencias, tarea que puede ser compleja si se dispone de una gran cantidad de AP.

- **Equipamiento**: AP, antenas, cableado (coaxial, estructurado, eléctrico), etc. requieren de cuidado regular. Las actualizaciones de los controladores de los equipos deberán ser realizadas cuando el personal técnico así lo considere. En el caso de instalaciones exteriores, se debe tener en cuenta la aceleración de la degradación de los equipos por las inclemencias del tiempo y los casos de robos y vandalismo lo cual suele afectar sobre todo a antenas, cableado y AP.

- **Seguridad**: Periódicamente es necesario cambiar las claves si son estáticas; las altas, bajas y modificaciones de usuarios deberán introducirse en el servidor de administración de la red; las direcciones MAC también deberán ser declaradas; las aplicaciones deberán actualizarse para cerrar posibles agujeros de seguridad; analizar posibles intrusiones, etc. Aunque estas

tareas parecen de mayor volumen que para el caso de redes fijas, si estas últimas están adecuadamente configuradas, entonces el mantenimiento es análogo.

2.11.1 Recomendaciones para el Mantenimiento

Para que el mantenimiento de una red no sea una tarea compleja y constante fuente de problemas es aconsejable seguir las siguientes recomendaciones:

- Realizar un buen diseño inicial: Estudio exhaustivo previo de posibles fuentes de interferencias externas e internas para minimizar su impacto; análisis de cobertura, potencia de señal y planificación de frecuencias para conseguir una buena recepción interna y reducir su emisión externa; estimaciones adecuadas de uso; etc.

- Realizar un mantenimiento interno periódico para detectar degradaciones de la señal, saturación de usuarios en los AP, intrusiones por usuarios no autorizados, dentro de la red.

- Ejecutar la adecuada actualización de controladores, reparaciones, análisis de las causas de interferencias o degradaciones detectadas, planificación del crecimiento y ejecutar la ampliación de la red de manera correcta.

Una red debidamente implementada y mantenida puede generar gran satisfacción a sus usuarios, incrementar la productividad y reducir costos, así como requerir un mantenimiento bajo. Por el contrario, si no se le da la importancia que requiere, la red sufrirá de continuas incidencias, generará malestar en los usuarios y se acabará abandonando o utilizando como una curiosidad ocasional.

2.12 Pasos para el Diseño de la Red Inalámbrica

Para llevar a cabo el diseño óptimo de la red podemos seguir los siguientes pasos, mismos que se derivan de la teoría presentada y analizada en este capítulo, y que nos pueden guiar durante el proceso de diseño:

1. Realizar un Sondeo de Opinión. Esta encuesta debe cubrir, en la medida de lo posible, todos los requerimientos de los usuarios.

2. Designación del área donde se pretende brindar el servicio. Estas áreas deben ser designadas de acuerdo a las necesidades reales de los usuarios.

3. Planear la capacidad de la red. Tomando en consideración cuantos usuarios utilizarán la red en un mismo momento, y cuantos AP son necesarios para soportar a todos los usuarios.

4. Tomar en consideración el diseño interno y externo del área donde se pretende brindar el servicio.

5. Seleccionar el hardware apropiado de acuerdo a las necesidades reales de la red, y seleccionar los equipos para los usuarios de acuerdo con las características necesarias para trabajar en la red.

6. Propuesta para el modelo de propagación. Es importante considerar la propagación de la señal de acuerdo a las áreas donde se pretenda brindar el servicio.

7. Establecer políticas de seguridad para la red inalámbrica. De manera que solo aquellos usuarios válidos puedan accesar a ella.

8. Puesta en operación del equipo y evaluación de la red inalámbrica, mediante el monitoreo y análisis del comportamiento de la red.

CAPÍTULO 3
PROPUESTAS UPIITA Y UPIBI

En este capítulo revisaremos las propuestas para la UPIITA y la UPIBI del I.P.N., presentamos los resultados de las encuestas realizadas, así como los posibles lugares donde colocar los AP para dar cobertura a aquellas áreas donde los estudiantes demuestran mayor interés por contar con el servicio de Internet inalámbrico. Listamos los equipos de conexión de red con que cuenta cada unidad, ya que es importante conocer si existe equipo disponible para implementar el servicio.

Además, presentamos los diagramas de las posibles soluciones que proponemos para brindar el servicio. También mencionamos las políticas de seguridad que se deben tomar en consideración para que el servicio sea el más seguro posible.

3.1 PROPUESTA PARA LA UNIDAD PROFESIONAL INTERDISCIPLINARIA EN INGENIERÍA Y TECNOLOGÍAS AVANZADAS (UPIITA)

La UPIITA cuenta con tres edificios (Planta Baja, Primer y Segundo Piso respectivamente) que albergan a los salones de clases, oficinas administrativas, biblioteca, laboratorios y salas de computo, además de un área destinada a la cafetería, y al servicio de apoyo estudiantil, una cancha de baloncesto, el área de estacionamientos y se iniciaron los trabajos de construcción para un nuevo edificio que albergara salones de clases.

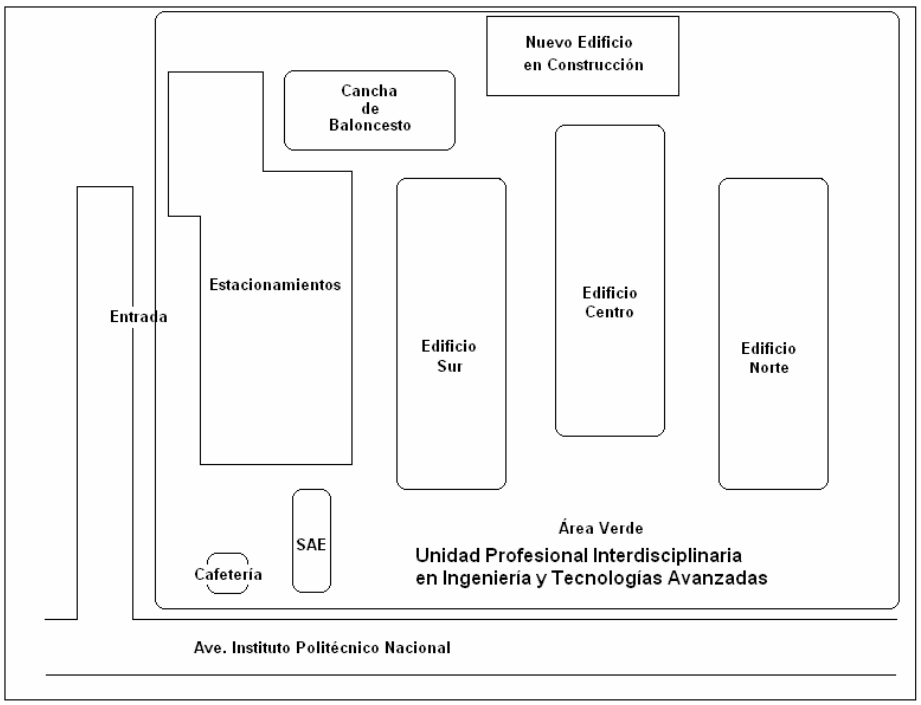


Figura 3.1 – Mapa de UPIITA

Para conocer con que equipos cuenta actualmente la unidad, realizamos una visita a los cuartos de equipos, donde se encuentran los equipos de conexión de red, la UPIITA cuenta con tres cuartos de equipos, uno en cada edificio, a continuación presentamos una lista de los equipos que se encuentran en cada uno:

- Edificio Norte: Switch Enterasys Vertical Horizon 2402S2
  Switch Cisco Catalyst 2900

Con estos equipos dan servicio a la planta baja y al primer piso solamente, cuentan con puertos disponibles para poder conectar el AP.

- Edificio Centro: Switch Enterasys Vertical Horizon 2402S2

  Con este equipo dan servicio a todo el edificio, y cuenta con puertos disponibles.

- Edificio Sur: Switch Enterasys Vertical Horizon 2402S2

  Con estos equipos dan servicio a la planta baja y al primer piso solamente, cuentan con puertos disponibles.

Se realizo este inventario con la finalidad de conocer si la unidad contaba con el equipo suficiente para soportar el servicio de la red inalámbrica o si se requeriría adquirir equipo adicional. En el caso de la UPIITA no es necesario adquirir equipo adicional, ya que el existente puede soportar la implementación de la red inalámbrica.

De acuerdo con la teoría presentada en el capítulo 2, relativo al diseño de la red, presentamos nuestra solución para implementar una red inalámbrica para acceso a la Internet para el Campus UPIITA, de acuerdo con los pasos presentados al final del segundo capítulo.

3.1.1 Sondeo de Opinión

El día martes 28 de septiembre de 2004 realizamos la encuesta en el Campus UPIITA, se encuestaron 154 estudiantes, que representan aproximadamente un 10% de la población estudiantil del campus.

A continuación presentamos los resultados obtenidos con la encuesta.

En la primera figura observamos como fue la distribución de la encuesta entre las distintas carreras y el número de estudiantes que participaron.

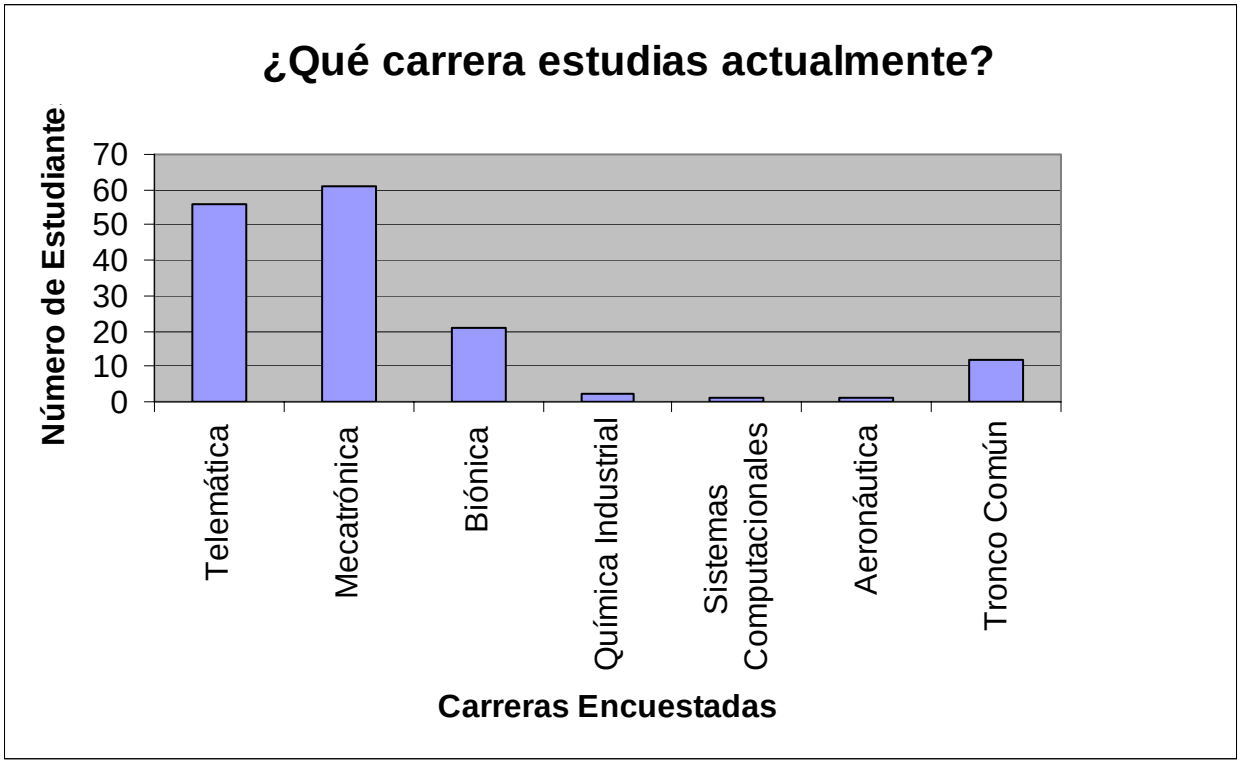


Figura 3.2 – ¿Qué carrera estudias actualmente?

Nota: La unidad ofrece tres carreras (Telemática, Mecatrónica y Biónica), pero en los cuestionarios encontramos que algunos estudiantes respondieron que estudiaban carreras diferentes a las impartidas en la unidad.

Es importante conocer si los estudiantes presentan interés para que la escuela brinde el servicio de Internet inalámbrico.

Del resultado obtenido podemos observar que la gran mayoría de la muestra tiene interés en que se brinde el servicio, esto debido a la naturaleza de las carreras impartidas en el campus, además, se pudo observar que un gran número de estudiantes cuentan con computadoras portátiles, lo que nos indica que la gran mayoría utilizaría el servicio.

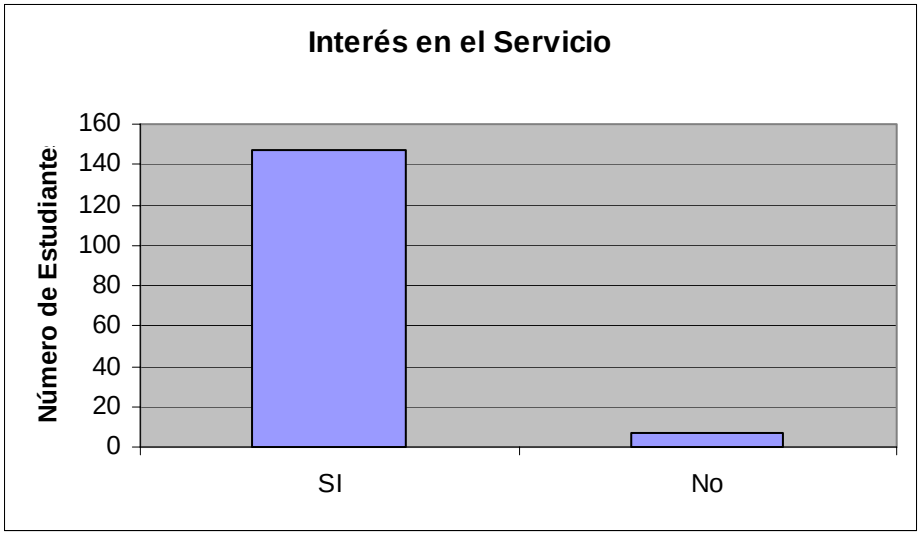


Figura 3.3– Interés en el servicio.

Una importante interrogante del proyecto es conocer si los estudiantes estuviesen dispuestos o no a pagar alguna cantidad de dinero por el uso del servicio, dicha cantidad debe ser destinada al mantenimiento de los equipos y para poder expandir la red en caso de ser necesario. Del resultado obtenido podemos observar que la opinión se encuentra dividida, aunque el número de estudiantes dispuestos a pagar fue mayor que aquellos que no les gustaría pagar por el servicio.

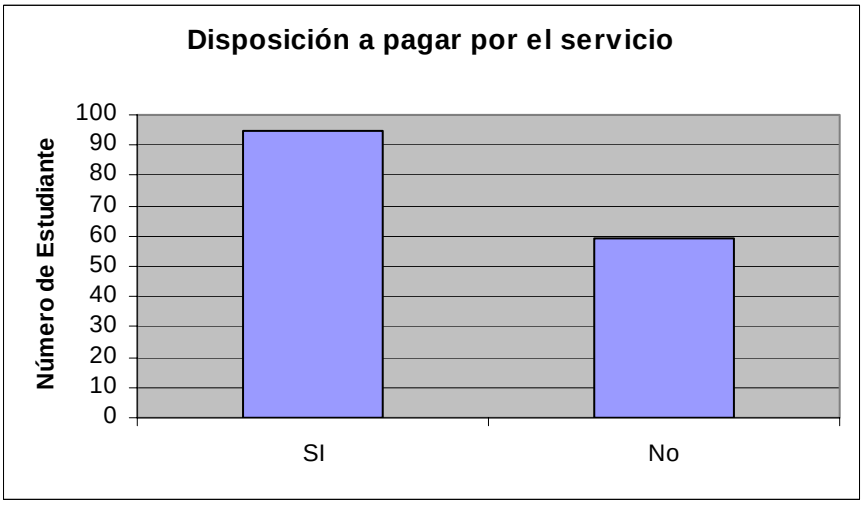


Figura 3.4 – Disposición a pagar.

Para satisfacer la demanda de los posibles usuarios preguntamos en que lugares les gustaría que se les brindara el servicio. A esta pregunta obtuvimos resultados diversos, pero dejaron claro cuales son las tres principales áreas donde les gustaría poder utilizar el servicio.

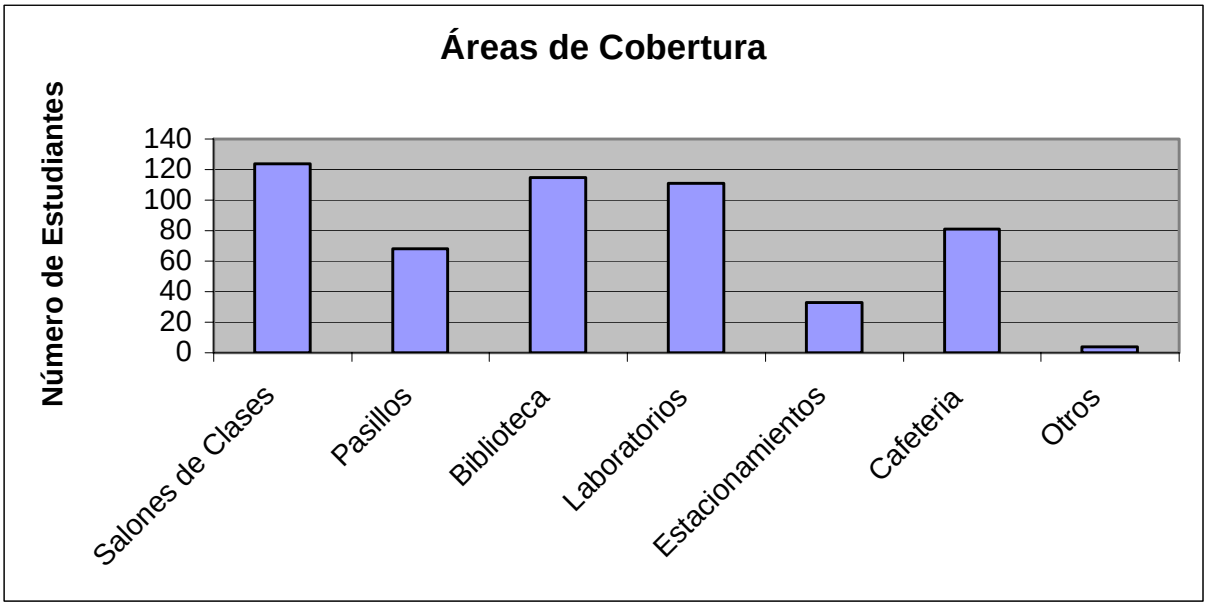


Figura 3.5 – Áreas de cobertura.

De acuerdo con los resultados de la encuesta, a la mayoría de los estudiantes les gustaría contar con el servicio de la red inalámbrica principalmente en los salones de clases, biblioteca y laboratorios.

3.1.2 Designación del Área a Cubrir

Por la forma en que se encuentran distribuidos los laboratorios, salones de clases, y biblioteca de la UPIITA y de acuerdo a los resultados obtenidos en la encuesta con relación a en que áreas les gustaría contar con el servicio, podemos utilizar la estrategia de brindar el servicio en un edificio a la vez. En este caso el edificio a cubrir sería el Edificio Centro, mismo que alberga la Biblioteca y los laboratorios de la UPIITA.

Proponemos que en una primera fase de diseño se brinde cobertura a la biblioteca y a los laboratorios, ya que en estas áreas se concentran una gran cantidad de estudiantes que usarían el servicio. Posteriormente, en una segunda etapa considerar si es conveniente o no brindar el servicio en los salones de clases.

Propuesta 1: Colocar un AP en la biblioteca, destinado a cubrir principalmente esta área, y de manera adicional cubrir los laboratorios que se encuentran en la planta baja, las oficinas administrativas y pasillos de la planta baja.

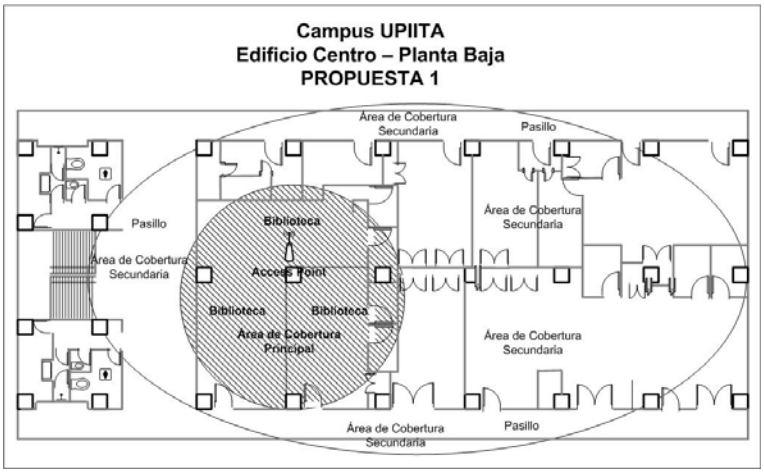


Figura 3.6 – Propuesta 1, Planta Baja.

El segundo y tercer AP serían colocados respectivamente en el primer y segundo piso del Edificio Centro, para brindar el servicio.

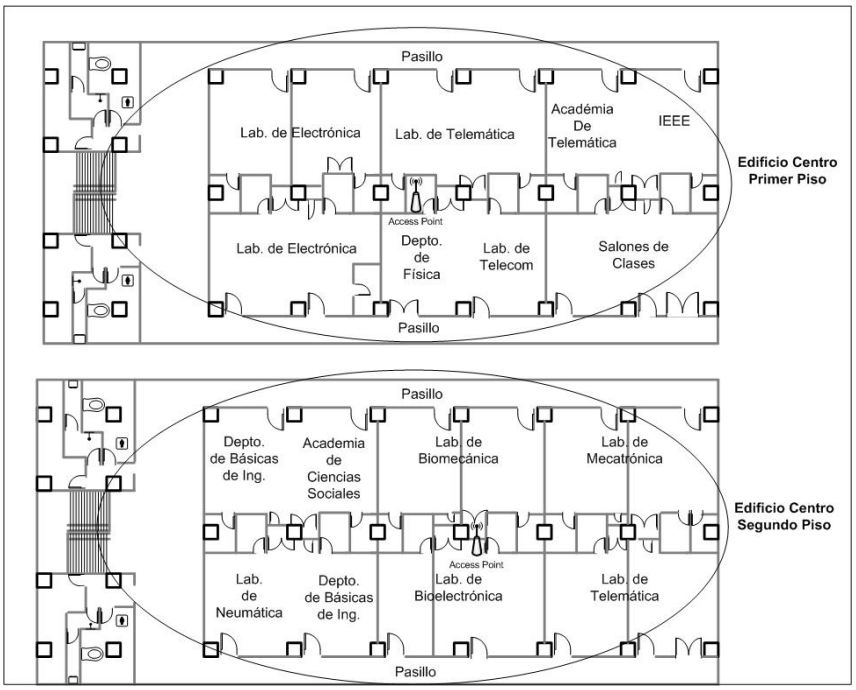


Figura 3.7 – Propuesta 1, Primer y Segundo Piso.

3.1.3 Planeación de la Capacidad

¿Qué capacidad de salida se deberá, en promedio, proporcionar a cada usuario? Distintos tipos de usuarios tienen diferentes promedios en los requerimientos de capacidad de salida, en nuestro caso, nos enfocaremos a satisfacer las necesidades de los estudiantes.

El número de usuarios simultáneos que puede soportar un AP depende principalmente de la cantidad de tráfico de datos en un momento dado. Debemos recordar que el ancho de banda es compartido entre los usuarios.

Para estimar la capacidad podemos utilizar la siguiente formula:

$$C_u = \frac{A_b}{Usuarios} \qquad (3.1)$$

donde: C_u = Capacidad de salida para cada usuario.

A_b = Ancho de banda de la red, para las WLAN basadas en el estándar 802.11b es de 11 Mbps.

Usuarios = Cantidad de usuarios que soportará un AP.

Para el caso de la UPIITA, asumimos que cada AP brindará servicio a 50 usuarios al mismo tiempo, empleando la ecuación 3.1, podemos estimar que capacidad podrá obtener cada usuario.

$$C_u = \frac{11Mbps}{50usuarios}$$

$$C_u = 220Kbps$$

En teoría, cada uno de los 50 usuarios esperados, podría disponer de 220 Kbps para operar dentro de la WLAN al mismo tiempo. Es importante recordar que en la medida en que se conecten o desconecten los usuarios de la red, este valor podrá disminuir o aumentar en igual proporción. Los usuarios dispondrán de servicios de HTTP (páginas Web), FTP (transferencia de archivos), y POP3 (correo electrónico).

La planeación de la capacidad de salida para cada usuario puede ser calculada empleando la velocidad de operación de la versión G del estándar IEEE 802.11, la cual es de 54 Mbps, con este valor, cada usuario dispondría de mayor capacidad.

Además de estimar la capacidad para cada usuario, también debemos recordar que en caso de utilizar más de tres AP para cubrir un área específica es necesario planear la reutilización de los canales de operación, tal como se observo en el segundo capítulo. En el caso de la UPIITA proponemos la utilización de tres AP, por lo que cada AP puede operar en los canales 1, 6 y 11 respectivamente sin causar interferencia entre ellos.

3.1.4 Consideraciones sobre el diseño interno y externos del Edificio Centro.

En relación a las consideraciones sobre el diseño interno y externo del Edificio Centro podemos mencionar que las paredes exteriores del edificio están construidas con tabiques y concreto con un espesor no mayor a 12 centímetros, las paredes interiores y divisiones de las distintas oficinas están construidas con tabla roca y vidrio, lo que permite que la señal del AP pueda penetrarlas fácilmente.

El edificio cuenta con pisos falsos, para albergar los distintos tipos de cables y tuberías que se extienden a lo largo de la estructura, además de contar con un recubrimiento metálico para brindar mayor soporte.

3.1.5 Selección del Hardware para los AP y para los equipos de los Usuarios

En el mercado existen una gran variedad de AP disponibles, para nuestra propuesta consideramos que el Enterasys AP3000 sería apropiado para implementar la WLAN en la UPIITA, ya que cuenta con características y especificaciones con las cuales sería factible obtener un buen desempeño de la red inalámbrica.

La decisión de utilizar tres AP la tomamos en base a las especificaciones técnicas del AP Enterasys AP 3000, el cual en teoría nos permitiría tener un radio de cobertura de hasta 60 metros en ambiente de interiores trabajando a una velocidad de 11 Mbps. Con estas especificaciones sería suficiente para cubrir satisfactoriamente el Edificio Centro.

También al proponer utilizar tres AP en vez de uno solo con una antena externa estaríamos ahorrando en el costo de esta y triplicando el número de usuarios que podrían disponer del servicio.

La tabla 3.1 presenta las distancias que se pueden cubrir utilizando un AP, operando en espacios Exteriores o en espacios Interiores, de acuerdo a la velocidad de operación en la que se encuentre trabajando. Estos datos fueron obtenidos de las especificaciones técnicas del AP Enterasys AP 3000.

Ambiente / Velocidad / Distancia	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Exteriores	300 metros 984 pies	465 metros 1525 pies	500 metros 1639 pies	515 metros 1689 pies
Interiores	60 metros 197 pies	70 metros 230 pies	83 metros 272 pies	85 metros 279 pies

Tabla 3.1 – Velocidad de transmisión vs. Área de cobertura.

Presentamos algunas características del Enterasys RoamAbout AP3000:

- Equipo: Enterasys RoamAbout AP3000
- Número de Canales: 1 a 11 canales
- Número de Usuarios: 250 usuarios sin usar encriptación y / o autenticación
  120 usando encriptación y / o autenticación
- Velocidad de Transmisión: 1, 2, 5.5, 11 Mbps
- Tipos de Modulación: CCK, BPSK, QPSK
- Frecuencia de Operación: 2.4 – 2.4835 GHz.
- Seguridad: Encriptación vía WEP a 64, 128 y 152 bits.
  Puerto de Autenticación IEEE 802.11x
  Wi-Fi Protected Access (WAP)
- Potencia de Transmisión: 2.412 y 2.472 GHz. - 15 dBm
  2.417 – 2.467 GHz. 16 dBm

Figura 3.8 – AP Enterasys AP3000

Esta y otra información puede observarse con mayor detalle en la Guía de Instalación del Access Point 3000 de Enterasys.

A los estudiantes que quieran utilizar el servicio de la red inalámbrica se les debe recomendar que sus equipos deben ser compatibles con el estándar IEEE 802.11b, y certificados como equipos Wi-Fi. De esta manera aseguramos que puedan utilizar el servicio de manera satisfactoria.

3.1.6 Propuesta de Modelo de Propagación

Para nuestro proyecto proponemos la utilización del modelo ETSI TR – 101 – 112, este es un modelo de propagación para interiores probado para la tecnología UMTS, para la transmisión de datos en medios inalámbricos, y derivado del modelo COST 231 MWM, ver Capítulo 2, sección 2.8.

Ya que nuestra propuesta de solución contempla brindar el servicio de la red inalámbrica, tanto en áreas abiertas, como en espacios interiores, con la utilización de este modelo podemos estimar la potencia recibida para ambas áreas, y estimar el área de cobertura de cada AP.

3.1.7 Políticas de Seguridad para la red inalámbrica de la UPIITA

Las políticas de seguridad podemos dividirlas en políticas de seguridad física, es decir, políticas referentes a la integridad del hardware (AP) y políticas de seguridad lógica, referentes a la seguridad de la red inalámbrica.

Recomendamos la aplicación de las siguientes políticas de seguridad de manera que red inalámbrica sea segura:

- La señal del AP debe confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo configurando adecuadamente la potencia de transmisión de los AP.

- Proponemos la utilización de los protocolos WPA y ACL. Recomendamos la utilización del protocolo WPA ya que soluciona en gran medida las debilidades conocidas del protocolo WEP y es considerado suficientemente seguro.

  Utilizar listas de control de acceso basadas en ACL, ya que utiliza como mecanismo de autenticación la dirección MAC de los equipos de los usuarios, de esta manera podemos crear una base de datos en cada AP con las direcciones MAC de los equipos de usuarios que son validos para accesar a la red. Este mecanismo es útil cuando trabajamos con pocos AP en la red.

- Inhabilitar la función de DHCP para la asignación de direcciones IP, estas deben ser fijas. De esta manera evitamos que un usuario ajeno pueda descifrar una dirección valida, y accesar a la red.

- Cambiar o no utilizar el SSID de la red, de manera que no pueda dar una idea de cual es la contraseña para accesar al AP. El SSID es una identificación configurable que permite la comunicación entre los usuarios y el AP y en algunos casos funciona como la contraseña de acceso a la red.

- Actualizar regularmente los controladores de los AP, con la finalidad de solucionar posibles fallas causadas por problemas en la configuración de los mismos.

- Proporcionar un ambiente físicamente seguro a los AP, es decir, resguardarlos de las inclemencias de las condiciones ambientales, y del maltrato y abuso por parte de los

usuarios. Así mismo, desactivarlos cuando se presenten periodos de inactividad prolongados.

Esta propuesta de políticas de seguridad es valida para la red inalámbrica de la UPIITA operando como una red local, pero al mismo tiempo se deben tomar en cuenta las políticas de seguridad de la red inalámbrica de todo el IPN.

3.1.8 Puesta en operación del equipo y evaluación de su comportamiento

La puesta en operación de la red inalámbrica y su posterior evaluación de comportamiento quedará a cargo del Departamento de Comunicaciones y Cómputo de la UPIITA, en coordinación con la Dirección de Informática del IPN.

3.2 PROPUESTA PARA LA UNIDAD PROFESIONAL INTERDISCIPLINARIA DE BIOTECNOLOGÍA (UPIBI)

La UPIBI esta conformada por los siguientes edificios: Dos edificios (planta baja y primer piso) que albergan la mayoría de los salones de clases, y algunos laboratorios, además, al lado del Edificio 2 se encuentra la biblioteca, el edificio de Gobierno o Talleres, un pabellón con tres salones de clases, el edifico de la Planta Piloto donde se encuentran varios laboratorios y algunas aulas, la cancha de baloncesto, el área de estacionamientos y el área donde se inicio la construcción de un nuevo edificio.

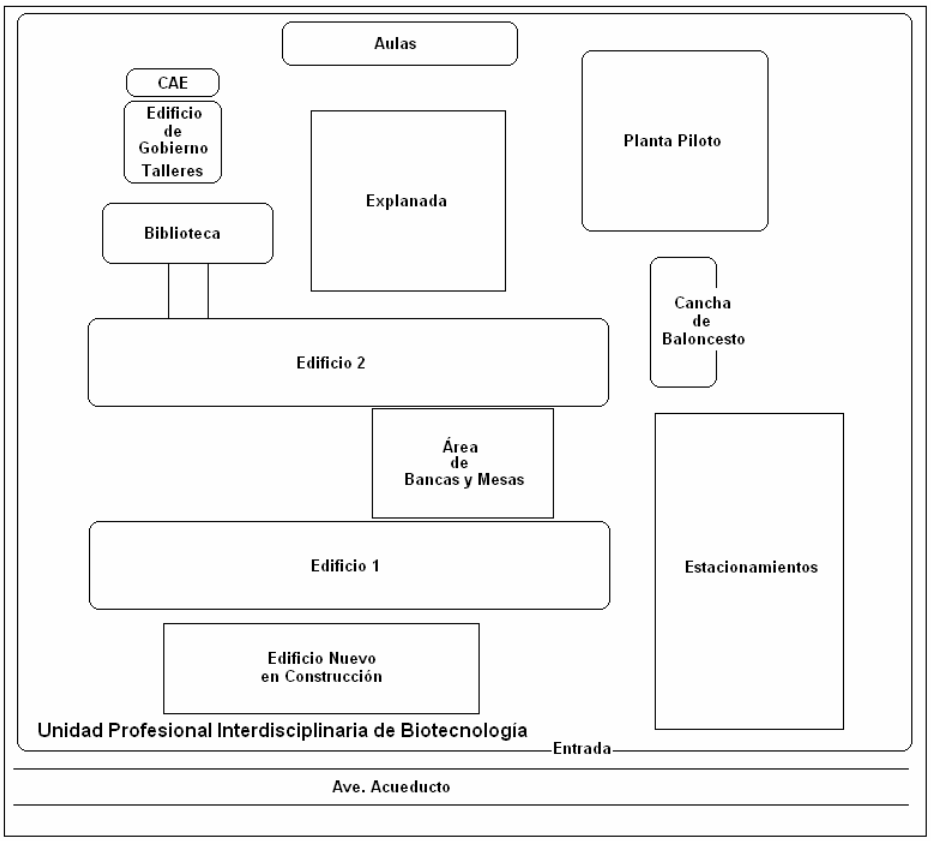


Figura 3.9 - Mapa de UPIBI

Al igual que en el caso de la UPIITA, realizamos una visita a los cuartos de equipos para conocer con que capacidad cuentan, la UPIBI tiene distribuidos sus cuartos de equipos de la siguiente manera:

- Edificio 1: Switch Enterasys Vertical Horizon 2402S2
  Switch 3COM 10/100

  Con estos equipos dan servicio a todo el edificio 1 y cuentan con puertos disponibles.

- Edificio 2: Switch Enterasys Vertical Horizon 2402S2

  Con este equipo se da servicio al edificio 2 y además se cubre la biblioteca, no hay puertos disponibles, por lo que se tendría que pensar un colocar otro switch en caso de ser necesario.

- Almacén: Hub Cisco FastHub 100

  Con este equipo se da servicio a las oficinas administrativas de gobierno y del taller.

- Edificio Planta Piloto: Switch Enterasys Vertical Horizon 2402S2
  Switch 3COM 16Plus
  Switch 3COM 12

Con el equipo Enterasys se da servicio a toda la planta baja, mientras que con los equipos 3COM se cubre el primer piso, cada uno cubre una parte del piso, y solo hay puertos disponibles en el 16Plus.

Siguiendo los pasos planteados en el segundo capítulo, presentamos nuestra propuesta de solución para implementar una red inalámbrica para acceso a la Internet para la UPIBI.

3.2.1 Sondeo de Opinión

El día jueves 30 de septiembre de 2004 realizamos la encuesta en la UPIBI, encuestamos a 4 profesores y 102 estudiantes, que representan aproximadamente un 10% de la población estudiantil del campus.

A continuación presentamos los resultados obtenidos de la encuesta.

En la primera figura se puede observar como fue la distribución de la encuesta entre las distintas carreras y el número de estudiantes que participaron, además de los profesores encuestados.

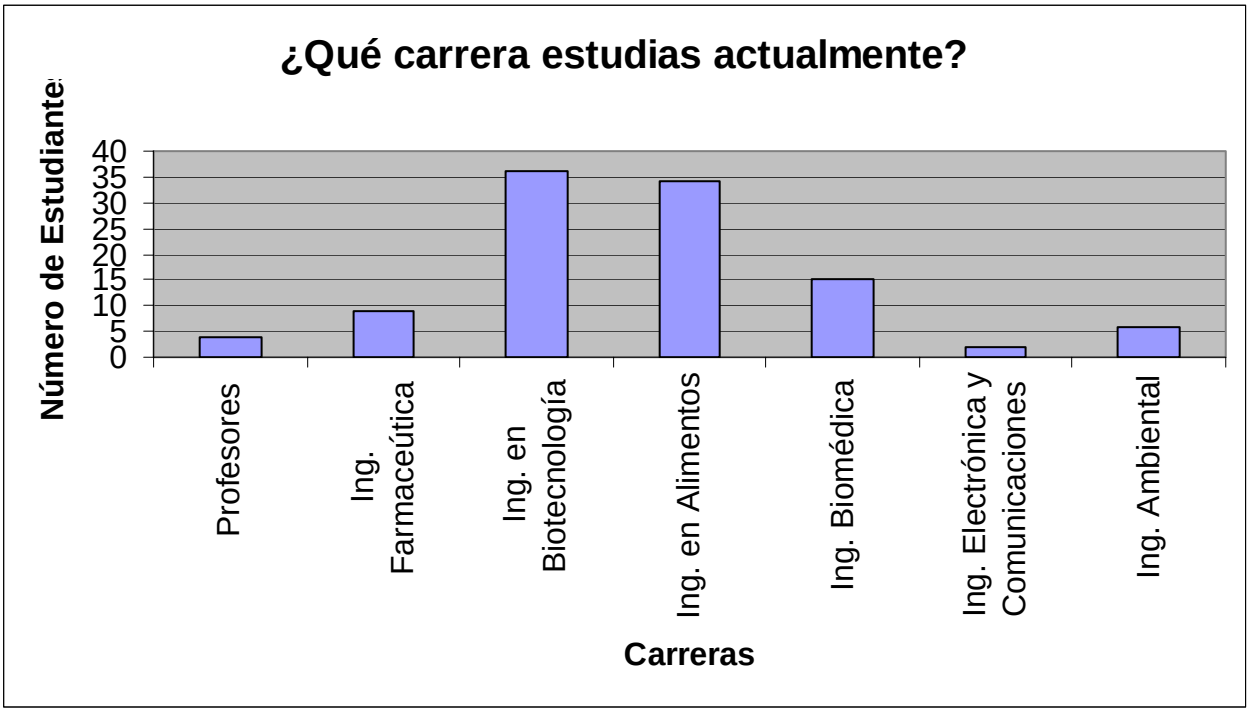


Figura 3.10 – ¿Qué carrera estudias actualmente?

Nota: La unidad ofrece cinco carreras (Farmacéutica, Biotecnología, Ing. en Alimentos, Biomédica e Ing. Ambiental), pero en los cuestionarios encontramos que algunos estudiantes respondieron que estudiaban carreras diferentes a las impartidas en la unidad.

Es importante conocer si los estudiantes presentan interés para que la escuela brinde el servicio de Internet inalámbrico. Del resultado obtenido podemos observar que la mayoría de la muestra tiene interés en que se brinde el servicio.

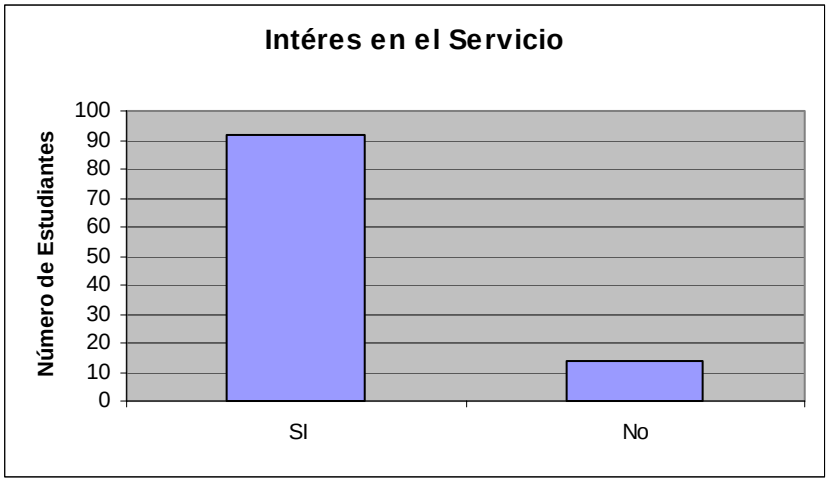


Figura 3.11 – Interés en el servicio.

Una importante interrogante del proyecto es conocer si los estudiantes estuviesen dispuestos o no a pagar alguna cantidad de dinero por el uso del servicio, dicha cantidad debe ser destinada al mantenimiento de los equipos y para poder expandir la red en caso de ser necesario. Del resultado obtenido podemos observar que la opinión se encuentra dividida, aunque el número de estudiantes dispuestos a pagar fue mayor que aquellos que no les gustaría pagar por el servicio.

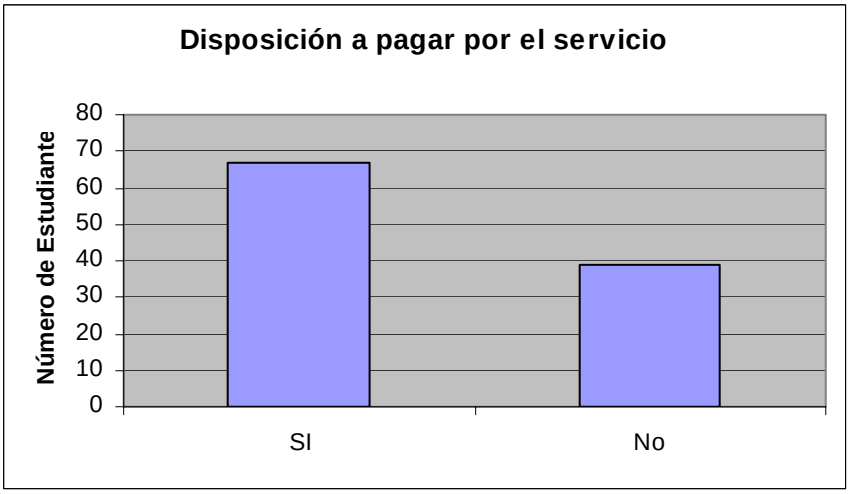


Figura 3.12 – Disposición a pagar por el servicio.

Para satisfacer la demanda de los posibles usuarios preguntamos en que lugares les gustaría que se les brindara el servicio. A esta pregunta obtuvimos resultados diversos, pero dejaron claro cuales son las tres principales áreas donde les gustaría poder utilizar el servicio.

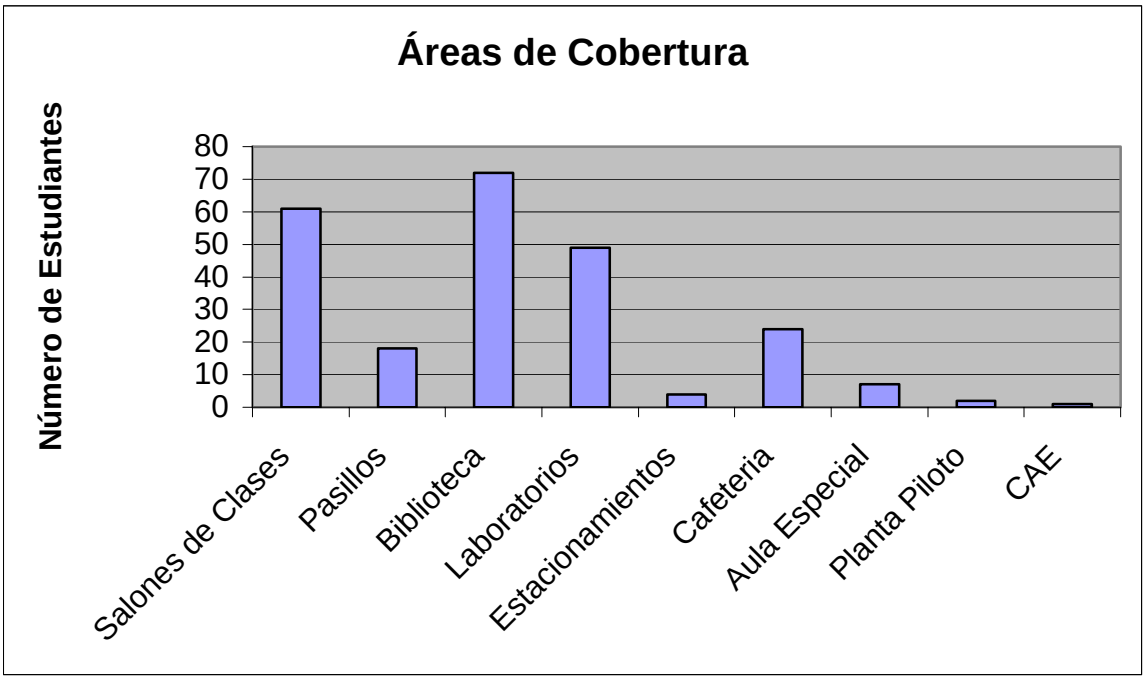


Figura 3.13 – Áreas de cobertura.

De los resultados obtenidos en la encuesta queda claro que las tres principales áreas donde a los estudiantes les gustaría que se les brindara el servicio son: la Biblioteca, Salones de Clases y Laboratorios.

3.2.2 Designación del Área a Cubrir

Para el caso de la UPIBI decidimos utilizar la primera estrategia presentada para la designación de áreas, solamente brindar el servicio en los lugares que se necesite.

Propuesta: En una primera etapa brindar el servicio de red inalámbrica en la Biblioteca y en el Jardín ubicado entre los Edificios 1 y 2.

Proponemos utilizar un AP para dar cobertura a la biblioteca, suponemos que podemos cubrir un área mayor, esta suposición deberá ser avalada o desmentida mediante las mediciones realizadas en el sitio. Y utilizar un AP para cubrir el jardín entre los edificios 1 y 2, zona donde se congregan la mayoría de los estudiantes para realizar distintas actividades.

Al considerar utilizar dos AP para cubrir estas áreas estamos previendo poder brindar el servicio a un mayor número de usuarios, pues contaríamos con dos zonas de cobertura inalámbrica dentro del campus. Estas áreas pueden ser apreciadas con mayor detalle en las fotos presentadas en el Anexo 2.

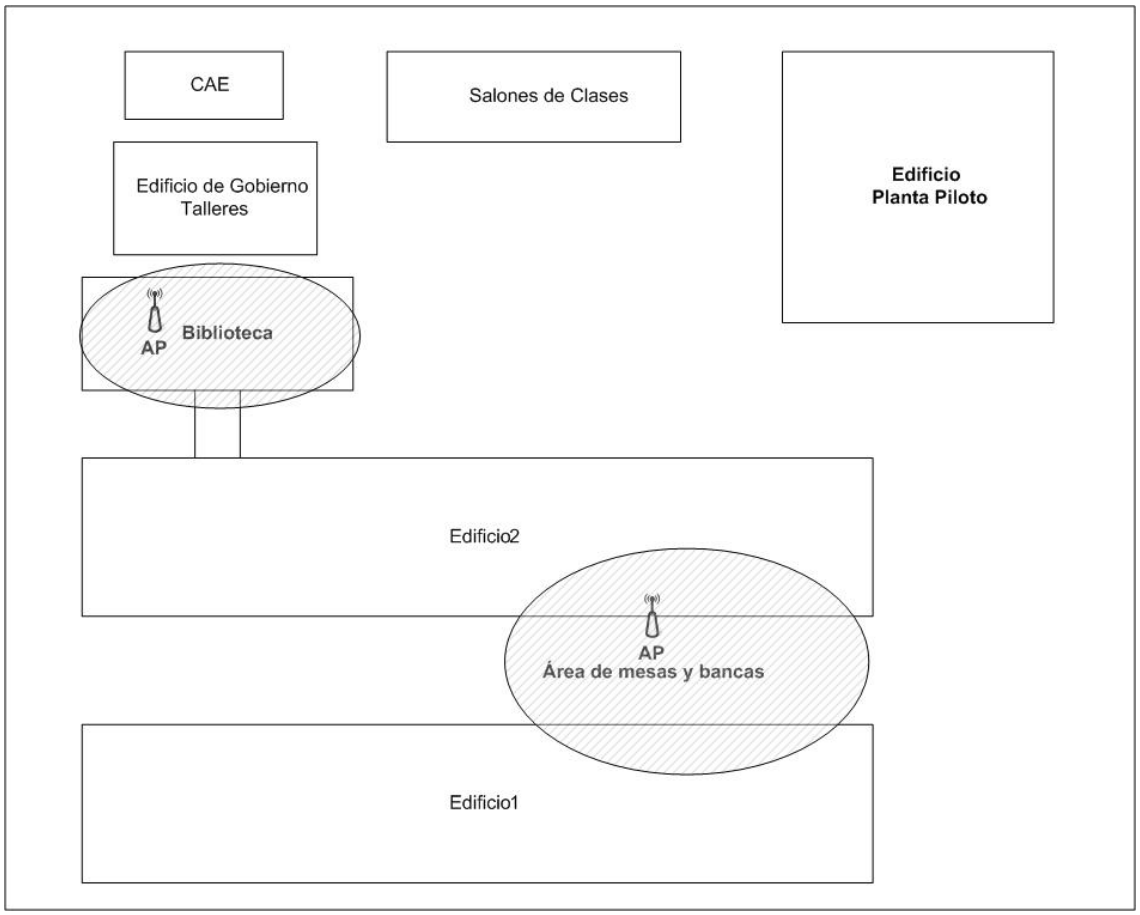


Figura 3.14 – Propuesta UPIBI

En una segunda etapa estudiar si resulta conveniente brindar el servicio de red inalámbrica en otras áreas de la UPIBI.

3.2.3 Planeación de la Capacidad

En el caso de la UPIBI, por ser esta unidad destinada a carreras de biotecnología, esperamos un máximo de 25 usuarios trabajando al mismo tiempo en la WLAN.

Empleando nuevamente la ecuación 3.1 podemos estimar la capacidad para cada usuario.

$$C_u = \frac{11Mbps}{25usuarios}$$

$$C_u = 440Kbps$$

En teoría, cada uno de los 25 usuarios esperados, podría disponer de 440 Kbps para operar dentro de la WLAN al mismo tiempo. Esta capacidad podrá variar en la medida en que se conecten o desconecten los usuarios de la red.

La planeación de la capacidad de salida para cada usuario puede ser calculada empleando la velocidad de operación de la versión G del estándar IEEE 802.11, la cual es de 54 Mbps, con este valor, cada usuario dispondría de mayor capacidad.

La propuesta para la UPIBI, basada en utilizar dos AP para brindar el servicio de WLAN en dos zonas distintas de la unidad nos permite que cada AP opere en cualquiera de los canales que no se traslapan, sin causar interferencia entre ellos, por lo que en esta primera etapa no es necesario realizar una planeación sobre la reutilización de los canales de operación de los AP.

3.2.4 Consideraciones sobre el diseño interno y externo de la Biblioteca y el Jardín.

Para el caso de la UPIBI debemos considerar el diseño interno y externo del edificio que alberga a la Biblioteca. La biblioteca de la UPIBI cuenta con paredes exteriores construidas con tabiques y concreto y ventanas amplias, esto permitiría que el AP colocado en esta ubicación para brindar el servicio de la red inalámbrica, pudiera además proveer cobertura en un área mayor a la esperada.

Para brindar el servicio de la WLAN, en el jardín ubicado entre los Edificios 1 y 2, donde se encuentran mesas y bancas utilizadas por los estudiantes para realizar distintas actividades, debemos tomar en cuenta que la ubicación del AP debe ser tal que se pueda cubrir la mayor área posible, esto se determinara colocando el AP en varias posiciones hasta determinar la más óptima.

3.2.5 Selección del Hardware para los AP y para los equipos de los Usuarios

Proponemos la utilización del AP Enterasys AP3000 ya que cuenta con características y especificaciones con las cuales sería factible obtener un buen desempeño de la WLAN para la UPIBI.

Como podemos observar en la tabla 3.1, de acuerdo a las especificaciones técnicas del equipo podemos brindar en servicio de la WLAN en las áreas previamente establecidas a la velocidad máxima de operación.

A los estudiantes se les debe recomendar que sus equipos deben ser compatibles con el estándar IEEE 802.11b, y certificados como equipos Wi-Fi. De esta manera aseguramos que puedan utilizar el servicio de manera satisfactoria.

3.2.6 Propuesta de Modelo de Propagación

Con la utilización del modelo ETSI TR – 101 – 112, modelo de propagación para la transmisión de datos en medios inalámbricos, y derivado del modelo COST 231 MWM, (Capítulo 2, sección 2.8), podemos estimar la potencia recibida para las áreas en las que se propone brindar el servicio de la red inalámbrica.

3.2.7 Políticas de Seguridad para la red inalámbrica de la UPIBI

Las políticas de seguridad podemos dividirlas en políticas de seguridad física, es decir, políticas referentes a la integridad del hardware (AP) y políticas de seguridad lógica, referentes a la seguridad de la red inalámbrica.

Para el caso de la UPIBI proponemos implementar políticas de seguridad similares a las propuestas para el caso de la UPIITA, ya que ambas unidades académicas son bastante similares en cuanto a cantidad de AP para desplegar la red.

A continuación listamos las políticas de seguridad que se deben implementar:

- La señal del AP debe confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo configurando adecuadamente la potencia de transmisión de los AP.

- Proponemos la utilización de los protocolos WPA y ACL. Recomendamos la utilización del protocolo WPA ya que soluciona en gran medida las debilidades conocidas del protocolo WEP y es considerado suficientemente seguro.

  Utilizar listas de control de acceso basadas en ACL, ya que utiliza como mecanismo de autenticación la dirección MAC de los equipos de los usuarios, de esta manera podemos crear una base de datos en cada AP con las direcciones MAC de los equipos de usuarios que son validos para acceder a la red. Este mecanismo es útil cuando trabajamos con pocos AP en la red.

- Inhabilitar la función de DHCP para la asignación de direcciones IP, estas deben ser fijas. De esta manera evitamos que un usuario ajeno pueda descifrar una dirección valida, y acceder a la red.

- Cambiar o no utilizar el SSID de la red, de manera que no pueda dar una idea de cual es la contraseña para acceder al AP. El SSID es una identificación configurable que permite la comunicación entre los usuarios y el AP y en algunos casos funciona como la contraseña de acceso a la red.

- Actualizar regularmente los controladores de los AP, con la finalidad de solucionar posibles fallas causadas por problemas en la configuración de los mismos.

- Proporcionar un ambiente físicamente seguro a los AP, es decir, resguardarlos de las inclemencias de las condiciones ambientales, y del maltrato y abuso por parte de los usuarios. Así mismo, desactivarlos cuando se presenten periodos de inactividad prolongados.

Esta propuesta de políticas de seguridad es valida para la red inalámbrica de la UPIBI operando como una red local, pero al mismo tiempo se deben tomar en cuenta las políticas de seguridad de la red inalámbrica de todo el IPN.

3.2.8 Puesta en operación del equipo y evaluación de su comportamiento

La puesta en operación de la red inalámbrica y su posterior evaluación de comportamiento quedará a cargo del Departamento de Cómputo de la UPIBI, en coordinación con la Dirección de Informática del IPN.

CAPÍTULO 4
PRUEBAS Y RESULTADOS

En este capítulo presentamos las pruebas teóricas y practicas que realizamos para la UPIITA y la UPIBI, con la finalidad de confirmar si las propuestas presentadas en el capítulo 3 son adecuadas para brindar el servicio de red inalámbrica en ambas unidades académicas.

Además, presentamos los equipos y sus respectivas especificaciones que utilizamos para realizar las mediciones en las unidades académicas.

4.1 Cálculos Teóricos

El primer cálculo teórico que realizamos para estimar la potencia de la señal recibida en los equipos de los usuarios, fue empleando el modelo de propagación en el espacio libre, en este caso la frecuencia (longitud de onda) de la señal afecta la pérdida en la trayectoria.

Existe una diferencia en el rango de frecuencia que emplea UMTS y las WLAN, en Europa UMTS opera en las bandas de frecuencia de 1920 – 1980 MHz. y 2110 – 2170 MHz. mientras que las WLAN operan en la banda de frecuencia de 2.4000 – 2.4835 GHz.

Para ilustrar la magnitud de la diferencia en la pérdida en la trayectoria debido a la diferencia entre ambas bandas de frecuencia seleccionamos algunos valores de frecuencia por las dos tecnologías. Para UMTS usamos la frecuencia de 2.0 GHz. mientras que para WLAN usamos 2.4 GHz., además, asumimos una ganancia unitaria para las antenas, y una distancia de 1 metro entre el usuario y el AP, usando la ecuación (2.8) $P(dB) = -10Log\left(\frac{\lambda^2}{(4\pi)^2 d^2}\right)$ tenemos:

$$\text{Para UMTS: } P(dB) = -10Log\left(\frac{(0.15)^2}{(4\pi)^2 d^2}\right) = 38.46dB$$

$$\text{Para WLAN: } P(dB) = -10Log\left(\frac{(0.125)^2}{(4\pi)^2 d^2}\right) = 40.04dB$$

Realizamos el mismo cálculo variando la distancia, ya que este parámetro es el que varía cuando el usuario se desplaza por el área de cobertura y con él varía la potencia recibida en su equipo. La tabla 4.1 nos muestra los valores teóricos obtenidos.

Tecnología / Distancia	5 m	10 m	15 m	20 m	25 m
UMTS	52.44 dB	58.46 dB	61.98 dB	64.48 dB	66.42 dB
WLAN	54.02 dB	60.04 dB	63.56 dB	66.06 dB	68.00 dB

Tabla 4.1 – Valores teóricos en el espacio libre (Modelo de Propagación en el Espacio Libre).

Se puede observar que la diferencia debido a la frecuencia es de 1.58 dB. Como vemos la diferencia entre ambos valores es mínima, por lo tanto podemos utilizar el modelo para estimar la potencia de la señal recibida en los equipos de los usuarios en el espacio libre valores de nuestra WLAN.

De igual manera realizamos el cálculo empleando la ecuación (2.5) $L(R) = 37 + 30Log(R)dB$, derivada del modelo ETSI TR – 101 – 112 (Sección 2.8), para estimar la potencia de la señal recibida en el espacio libre. En este caso la frecuencia de operación no influye en las pérdidas por la trayectoria. Cuando la distancia (R) entre el usuario y el AP es de 1 metro tenemos:

$$L(R) = 37 + 30Log(1) = 37dB$$

La tabla 4.2 nos muestra los valores obtenidos al variar la distancia para conocer la potencia estimada en el equipo del usuario.

Distancia / Potencia	5 m	10 m	15 m	20 m	25 m
	58 dB	67 dB	72 dB	76 dB	79 dB

Tabla 4.2 – Valores teóricos en el espacio libre (Modelo ETSI TR – 101 -112)

Ahora, debemos estimar los valores de la potencia recibida en los equipos de los usuarios cuando la señal del AP debe cubrir varias áreas interiores, en nuestro caso sería para brindar el servicio en los distintos laboratorios y salones de clases.

Para esto, empleamos la ecuación (2.4) $L(R) = 37 + 30Log(R) + 18.3n^{\left(\frac{(n+1)}{(n+2)-0.46}\right)}dB$, misma que toma en cuenta la cantidad de paredes que debe atravesar la señal del AP y la distancia entre el AP y el usuario. Asumiendo n = 1, y R = 1, tenemos:

$$L(R) = 37 + 30Log(1) + 18.3*(1)^{\left(\frac{(2)}{(3)-0.46}\right)} = 46.86dB$$

Realizamos el cálculo para distintos valores de n y R, la tabla 4.3 nos muestra los resultados obtenidos cuando la señal debe propagarse en interiores.

Distancia / Número de paredes	1 m	5 m	10 m	15 m	20 m	25 m
n = 1	46.86 dB	67.83 dB	76.86 dB	82.14 dB	85.89 dB	88.80 dB
n = 2	58.13 dB	79.10 dB	88.13 dB	93.41 dB	97.16 dB	100.07 dB
n = 5	100.01 dB	120.98 dB	130.01 dB	135.30 dB	139.04 dB	141.95 dB

Tabla 4.3 – Valores teóricos para propagación en interiores (Modelo ETSI TR – 101 -112).

Debemos mencionar que la mayoría de las veces los resultados obtenidos con los modelos de propagación varían en comparación con los resultados obtenidos mediante las mediciones, esto se debe a que los modelos de propagación no toman en consideración todos los fenómenos que pueden afectar la propagación de la señal.

Una vez conociendo los posibles valores teóricos que podíamos esperar debemos realizar las mediciones en los sitios donde nos interesa brindar el servicio.

Para esto utilizamos un AP de la casa 11Wave (caso UPIITA), un AP de la casa Belkin (caso UPIBI), una tarjeta PCMCIA marca Linksys, modelo WPC54G, una computadora portátil con sistema operativo Windows XP. Adicionalmente utilizamos los siguientes software: DFU Utility para la configuración del AP y el Wireless-G Notebook Adapter Utility para medir la intensidad de la señal recibida.

Presentamos las especificaciones técnicas del AP y de la tarjeta PCMCIA.

IEEE 802.11b Wireless Access Point 11Wave

- Estándares Soportados: 802.11b y 802.3
- Velocidad de Operación: 11, 5.5, 2, y 1 Mbps
- Sistemas Operativos: Windows 9x / ME / 2000 / XP / NT y LINUX
- Canales de Operación: 1 – 11 (FCC), 1 – 11 (IC), 1 – 13 (ETSI) y 1 – 14 (MKK)
- Frecuencia de Operación: 2.4000 – 2.4835 GHz. (FCC y ETSI) y 2.4000 – 2.497 GHz. (MKK)

- Tecnología de Radio: Direct Sequence Spread Spectrum (DSSS)
- Seguridad: 64 / 128 bits WEP y 802.1x
- Modo de Operación: Access Point, Bridge, Repetidor
- Potencia de Transmisión: 18 dBm ±1 dBm
- Antena: Dipolo dual con función de diversidad, ganancia de 2 dBi
- Administración: Win Server, SNMP, TFTP, CDP
- Puertos: 1 RJ-45 (LAN), 1 DC-Jack (Voltaje), 1 USB-B (Configuración)

IEEE 802.11b Wireless Access Point Belkin

- Estándares Soportados: 802.11b y 802.11g
- Velocidad de Operación: 54 Mbps
- Frecuencia de Operación: 2.4000 – 2.4835 GHz. (FCC y ETSI)
- Seguridad: Encriptación WEP 64 / 128 bits
- Puertos: 4 10 / 100 Base T Ethernet, 1 Conexión de MODEM
- Sistemas Operativos: Windows / LINUX / UNIX

Tarjeta PCMCIA modelo WPC54G

- Estándares Soportados: IEEE 802.11b, 802.11g
- Modulación: 802.11b – CCK (11 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps) y 802.11g – OFDM
- Canales de Operación: 1 – 11 (FCC), 1 – 11 (IC), 1 – 13 (ETSI) y 1 – 14 (MKK)
- Interfase: CardBus
- Velocidad de Operación: Hasta 54 Mbps
- Seguridad: 64 / 128 bits WEP, AES, TKIP, 802.1x
- Indicadores: Encendido / Apagado, Enlace RF, Enlace LAN

Primero procedimos a configurar el AP con las condiciones necesarias para que su funcionamiento sea de acuerdo a nuestro interés, ya que viene configurado de fábrica con ciertas funciones que no van de acuerdo a nuestra propuesta, la figura 4.1 nos muestra la ventana inicial con la configuración inicial del AP.

Como se puede apreciar el AP viene con la opción de seguridad WEP deshabilitada, la clave WEP viene configurada con una secuencia numérica muy sencilla por lo cual la cambiamos, las direcciones IP, máscara de subred y puerta de enlace (Gateway) no corresponden a la red donde deseamos instalar el equipo, la opción de enviar a todos los equipos el SSID del AP y la opción de DCHP deshabilitada (son algunas de las opciones que no cambiamos).

También se puede observar que el equipo nos permite seleccionar la velocidad de transmisión, el canal en el cual debe trabajar, el modo de operación para el equipo (AP, Puente, Repetidor, etc.), entre otras opciones.

Figura 4.1 – Configuración de fábrica del AP.

Una vez que configuramos el equipo de acuerdo a nuestras características de funcionamiento, ver figura 4.2, procedimos a constatar que el AP fuera un elemento válido de la red, para esto utilizamos

el comando “ping” para comprobar que el equipo se encontrara bien conectado y configurado en nuestra red, ver figura 4.3

Figura 4.2 – Configuración del AP para nuestra red.

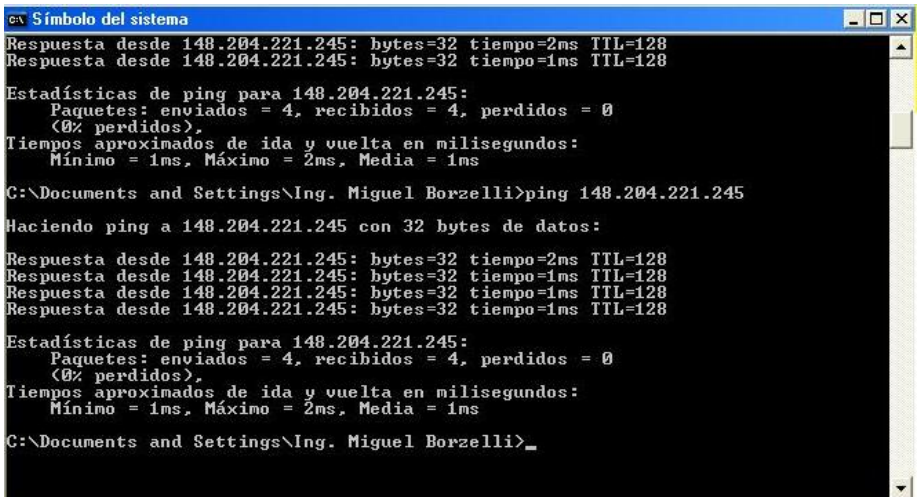


Figura 4.3 – “Ping” al AP.

4.2 Caso UPIITA

Para la UPIITA, la primera serie de mediciones las realizamos en la biblioteca, para esto colocamos el AP en la columna central de la biblioteca, sobre el cielo raso, y procedimos a realizar las mediciones. En la tabla 4.4 presentamos los valores obtenidos dentro de la biblioteca (1, 2, y 5 metros) y los obtenidos fuera de ella (15 metros).

Distancia / Grados	1 metro	2 metros	5 metros	15 metros
0°	-35 dBm	-39 dBm	-40 dBm	-53 dBm
45°	-37 dBm	-41 dBm	-43 dBm	-50 dBm
90°	-29 dBm	-37 dBm	-39 dBm	-52 dBm
135°	-39 dBm	-39 dBm	-44 dBm	-52 dBm
180°	-37 dBm	-36 dBm	-46 dBm	-63 dBm
225°	-42 dBm	-40 dBm	-39 dBm	-65 dBm
270°	-41 dBm	-43 dBm	-45 dBm	-67 dBm
315°	-39 dBm	-40 dBm	-40 dBm	-63 dBm
360°	-37 dBm	-38 dBm	-41 dBm	-55 dBm

Tabla 4.4 – Valores de intensidad de señal dentro y fuera de la biblioteca de la UPIITA.

Las siguientes tres figuras nos muestran como la computadora portátil detecta al AP y nos presenta la intensidad de señal que recibe, el nivel de ruido, así como también la velocidad de transmisión del AP, así como otra serie de características.

Figura 4.4 – Estado de la conexión entre el usuario y el AP.

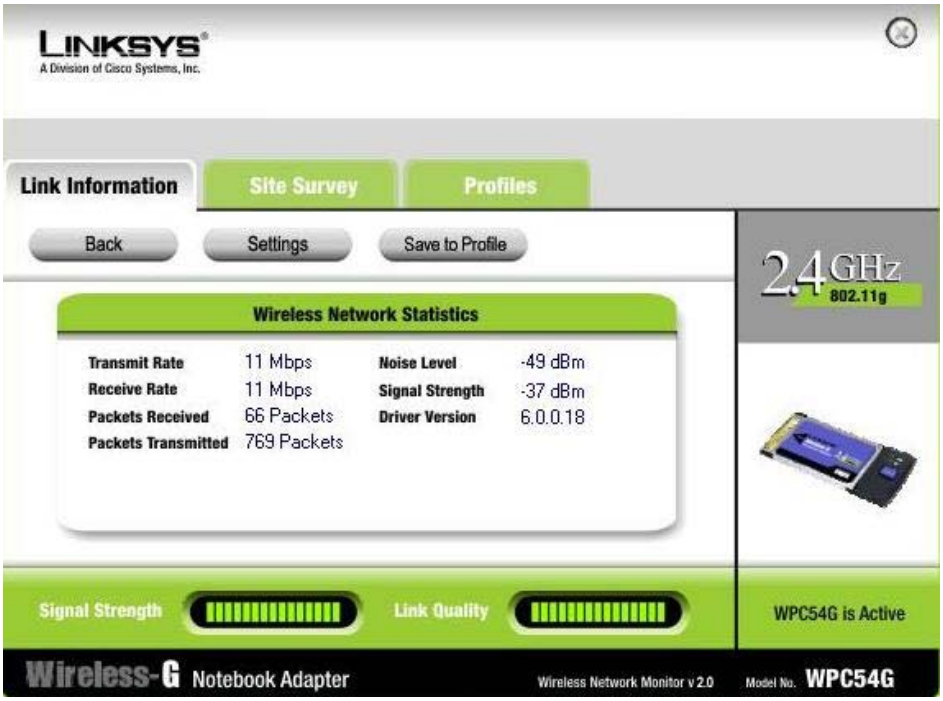


Figura 4.5 – Estadísticas de la conexión entre usuario y AP.

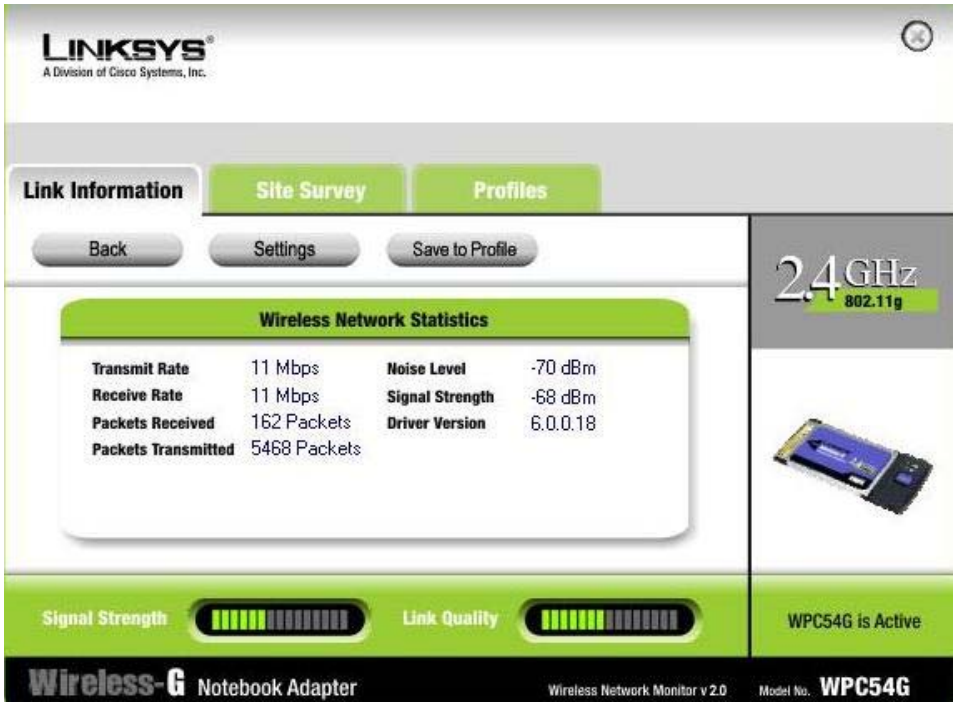


Figura 4.6 – Estadísticas de la conexión entre usuario y AP.

Con el AP colocado en esa posición podemos dar cobertura a toda la biblioteca, que es nuestra principal área de interés. Adicionalmente, nos desplazamos con el equipo por el área exterior, alrededor de la biblioteca y observamos que es factible cubrir satisfactoriamente casi toda la planta baja, comprendida entre el Edificio Centro (donde se encuentra la biblioteca) y los Edificios Norte y Sur, dando cobertura a las áreas verdes que se encuentran entre los edificios, además, de las oficinas, algunos laboratorios y salones de clases que se encuentran en dicha planta.

La figura 4.7 nos muestra la cobertura que obtuvimos para la primera serie de mediciones realizadas.

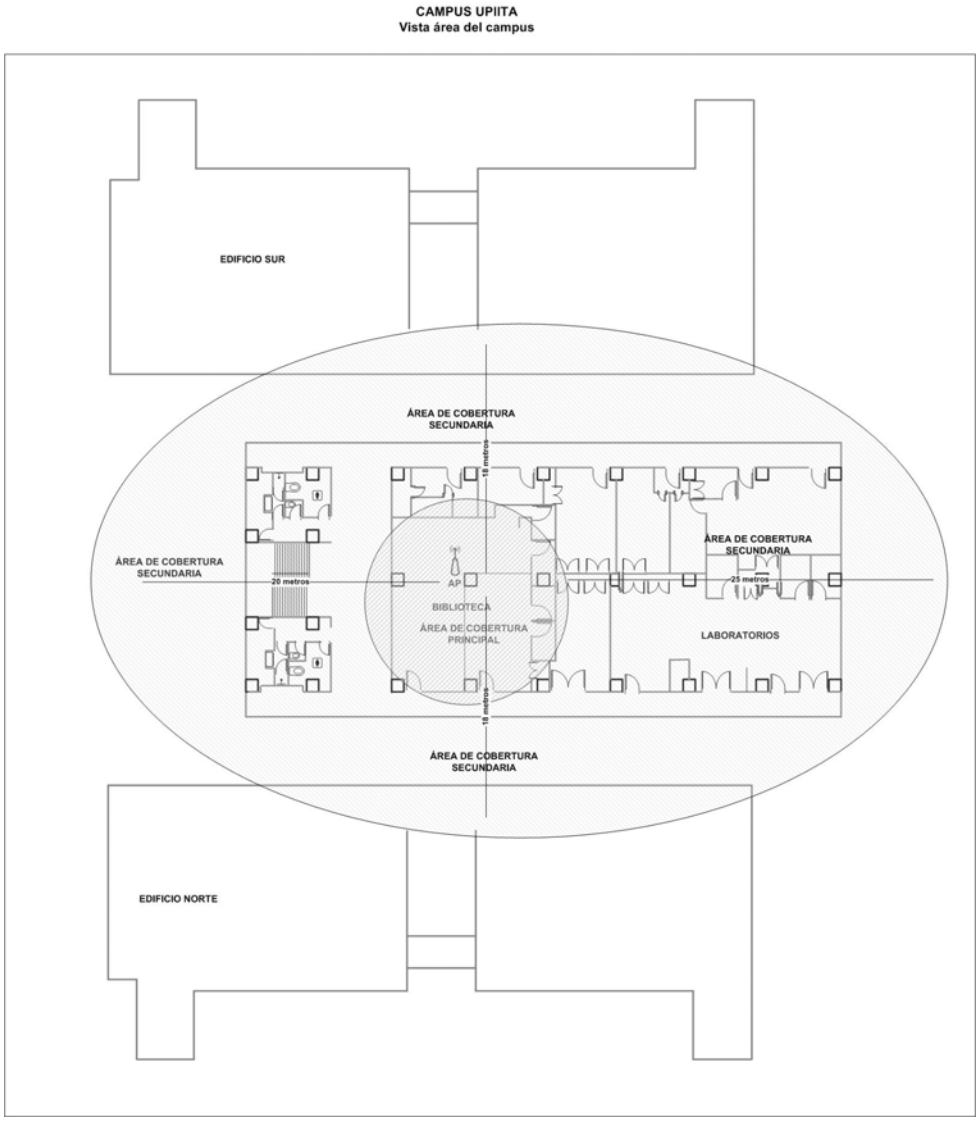


Figura 4.7 – Cobertura obtenida para la propuesta de la planta baja, UPIITA.

La segunda serie de mediciones que realizamos fue con el AP colocado en el primer piso, en el Departamento de Física, la tabla 4.5 nos muestra los valores de potencia obtenidos para las diferentes distancias a las que realizamos las mediciones. En el área de las escaleras y los sanitarios no realizamos medidas ya que en estos lugares no son los más comunes para que los estudiantes utilicen el servicio.

Ubicación	Intensidad de Señal	Distancia
Laboratorios de Electrónica 1	-55 dBm	10 metros
Departamento de Física	-35 dBm	Ubicación del AP
Laboratorio de Telecomunicaciones	-39 dBm	5 metros
Salón de Clases 1	-56 dBm	10 metros
Salón de Clases 2	-58 dBm	15 metros
Laboratorio de Electrónica 2	-57 dBm	10 metros
Laboratorio de Telemática 1	-38 dBm	Ubicación del AP
Laboratorio de Telemática 2	-47 dBm	5 metros
Academia de Telemática	-60 dBm	10 metros
Cubículo de IEEE	-65 dBm	17 metros

Tabla 4.5 – Valores de intensidad de señal en Laboratorios y Oficinas del primer piso, edificio Centro.

La figura 4.8 nos muestra el área de cobertura aproximada que se obtuvo en el primer piso del edificio Centro.

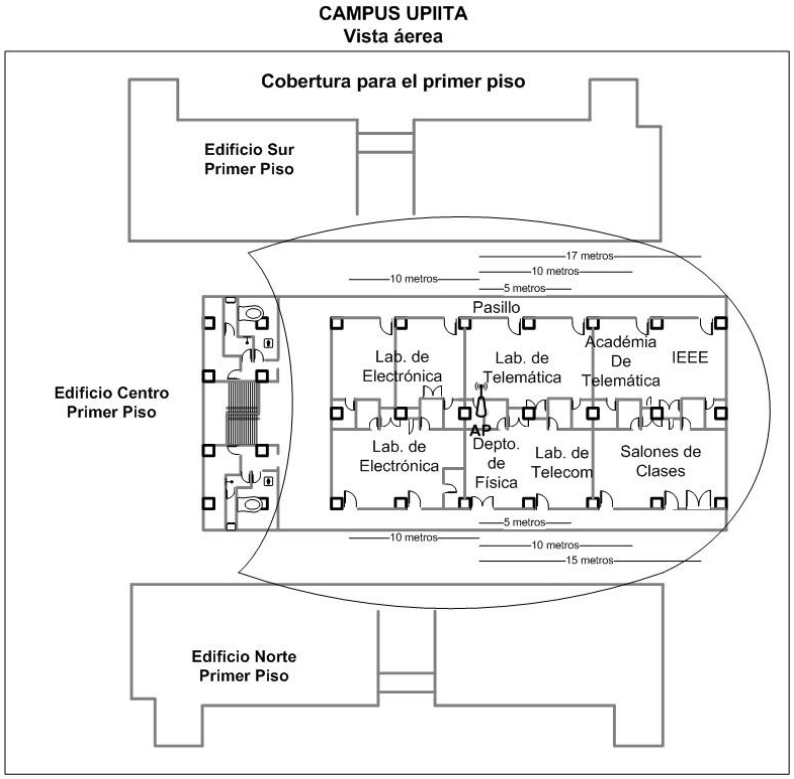


Figura 4.8 – Cobertura obtenida en el primer piso, edificio Centro.

Con el AP colocado en esta posición se puede cubrir satisfactoriamente todo el primer piso del edificio Centro. Basados en los resultados obtenidos en la primera serie de mediciones (el AP colocado en la biblioteca), asumimos que sería factible cubrir el primer piso de los edificios Sur y Norte, pero la potencia de la señal del AP no fue suficiente para brindar una cobertura satisfactoria a los salones de clases y oficinas administrativas de dichos edificios.

Algunos de los valores que obtuvimos cuando nos desplazamos al primer piso de los edificio Sur y Norte fueron de –74 dBm, -71 dBm, -75 dBm, -73 dBm, mismos que se encuentran muy cerca del umbral de operación establecido previamente, estos valores fueron medidos en los pasillos de ambos edificios, al realizar las mediciones dentro de los salones de clases y oficinas administrativas no se recibía señal alguna.

Para la tercera serie de mediciones que realizamos en el edificio Centro, colocamos el AP en los laboratorios de Bioelectrónica y Biomecánica, ubicados en el segundo piso del edificio, y obtuvimos resultados parecidos a los obtenidos en el primero piso, se puede cubrir de manera satisfactoria todo el piso.

La tabla 4.6 nos muestra los resultados obtenidos con el AP colocado en el segundo piso del edificio Centro.

Ubicación	Intensidad de Señal	Distancia
Laboratorio de Neumática	-62 dBm	10 metros
Academia de Básicas de Ingeniería	-58 dBm	5 metros
Laboratorio de Bioelectrónica	-43 dBm	Ubicación del AP
Laboratorio de Telemática	-63 dBm	10 metros
Departamento de Básicas de Ingeniería	-67 dBm	12 metros
Academia de Ciencias Sociales	-62 dBm	7 metros
Laboratorio de Biomecánica	-41 dBm	Ubicación del AP
Laboratorio de Mecatrónica	-65 dBm	12 metros

Tabla 4.6 – Valores de intensidad de señal obtenidos en el segundo piso, edificio Centro.

La figura 4.9 nos muestra el área de cobertura aproximada que se obtuvo en el segundo piso del edificio Centro.

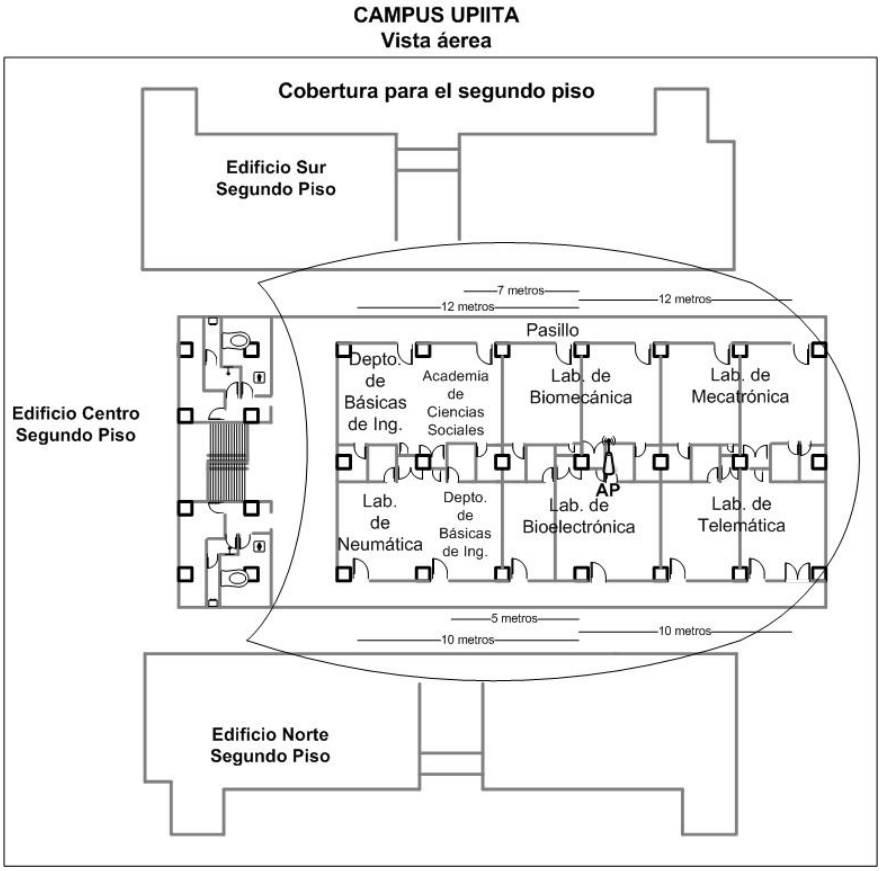


Figura 4.9 – Cobertura obtenida en el segundo piso, edificio Centro.

Nuevamente realizamos mediciones en el segundo piso de los otros dos edificios, obteniendo resultados similares a los obtenidos en el primer piso.

Con esto terminamos las mediciones realizadas en el campus de la UPIITA.

4.3 Caso UPIBI

De acuerdo con la propuesta para brindar el servicio de la WLAN en la UPIBI, presentamos los resultados obtenidos.

Para la propuesta de brindar el servicio en la Biblioteca de la UPIBI, realizamos dos series de mediciones para comprobar la cobertura, los primeros valores obtenidos pueden ser observados en la tabla 4.7, estos valores fueron obtenidos dentro de la biblioteca.

Grados	Intensidad de Señal	Distancia
0°	-47 dBm	6 m
45°	-52 dBm	10 m
90°	-45 dBm	8 m
135°	-58 dBm	20 m
180°	-60 dBm	22 m

Tabla 4.7 - Valores de intensidad de señal dentro de la Biblioteca de la UPIBI.

Posteriormente realizamos mediciones alrededor de la biblioteca para conocer si es factible brindar el servicio en las áreas circundantes de la misma. Los valores obtenidos pueden ser observados en la tabla 4.8.

Grados	Intensidad de Señal	Distancia
45°	-63 dBm	15 m
90°	-60 dBm	12 m
135°	-68 dBm	25 m
180°	-72 dBm	30 m
225°	-67 dBm	25 m
270	-56 dBm	12 m
315°	-53 dBm	10 m

Tabla 4.8 - Valores de intensidad de señal alrededor de la Biblioteca de la UPIBI.

Con el AP colocado en la Biblioteca podemos brindar el servicio de la WLAN de manera satisfactoria dentro de la misma y al mismo tiempo brindar el servicio en el pasillo que se encuentra entre la biblioteca y el Edificio 2, y en el jardín que se encuentra en la parte de atrás de la biblioteca. Estas áreas pueden observarse en la figura 4.10.

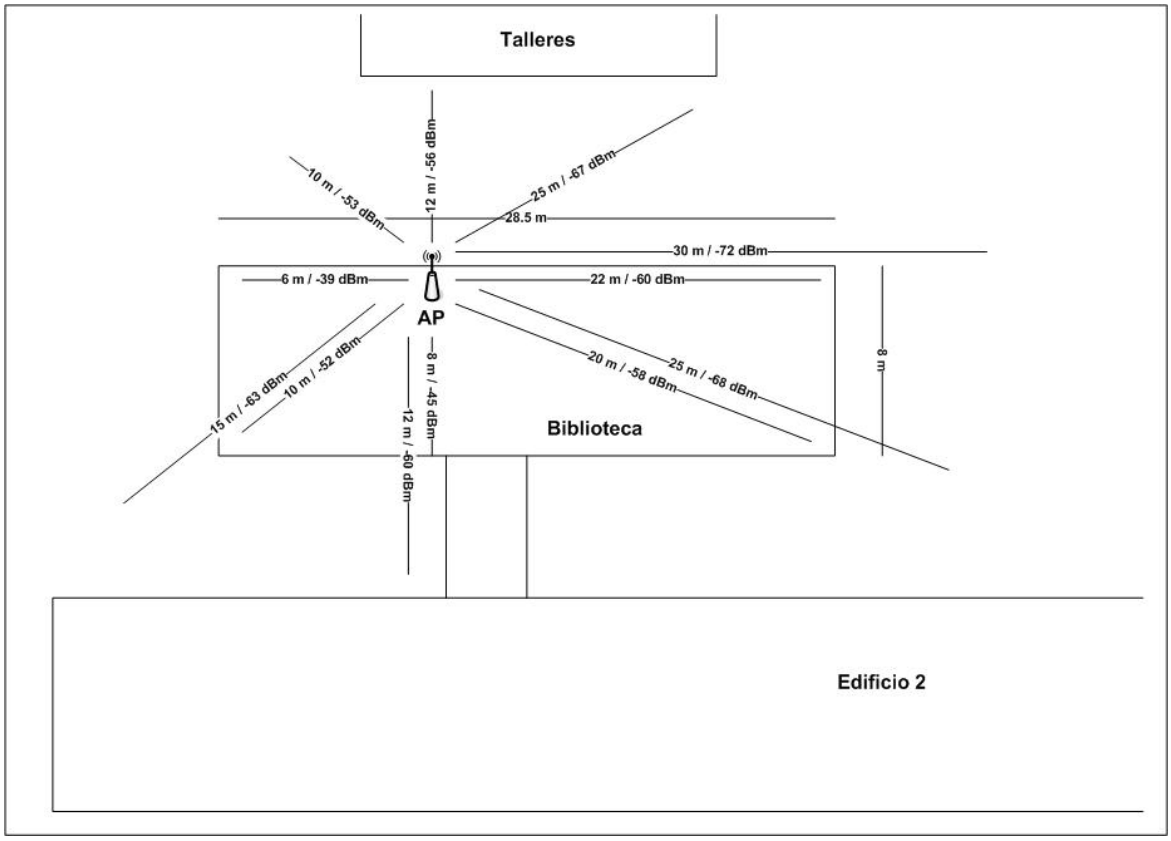


Figura 4.10 – Cobertura interna y externa en la Biblioteca de la UPIBI.

Así mismo, realizamos mediciones para conocer si es factible brindar el servicio de la red inalámbrica en el primer piso del edificio donde se encuentra ubicada la biblioteca, pero los valores de intensidad de señal (-77 dBm, -80 dBm, -79 dBm) recibidos en el equipo portátil están por encima del umbral de operación definido para tener un buen enlace entre Usuario y AP, por lo que no es posible brindar el servicio a estas áreas con el AP colocado en la Biblioteca.

La segunda área de cobertura propuesta para la UPIBI es el jardín ubicado entre los Edificios 1 y 2, a continuación presentamos los resultados de las dos series de mediciones que realizamos. La primera serie de mediciones la realizamos con el AP colocado en la parte exterior del Laboratorio de Microbiología.

La tabla 4.9 muestra los valores obtenidos.

Grados	Intensidad de Señal	Distancia
0°	-61 dBm	12 m
15°	-65 dBm	18 m
45°	-68 dBm	20 m
60°	-70 dBm	28 m
90°	-69 dBm	30 m
120°	-73 dBm	32 m
135°	-70 dBm	28 m
165°	-65 dBm	20 m
180°	-58 dBm	8 m

Tabla 4.9 – Valores obtenidos con el AP colocado afuera del Laboratorio de Microbiología.

En la figura 4.11 podemos observar con mayor detalle el resultado obtenido.

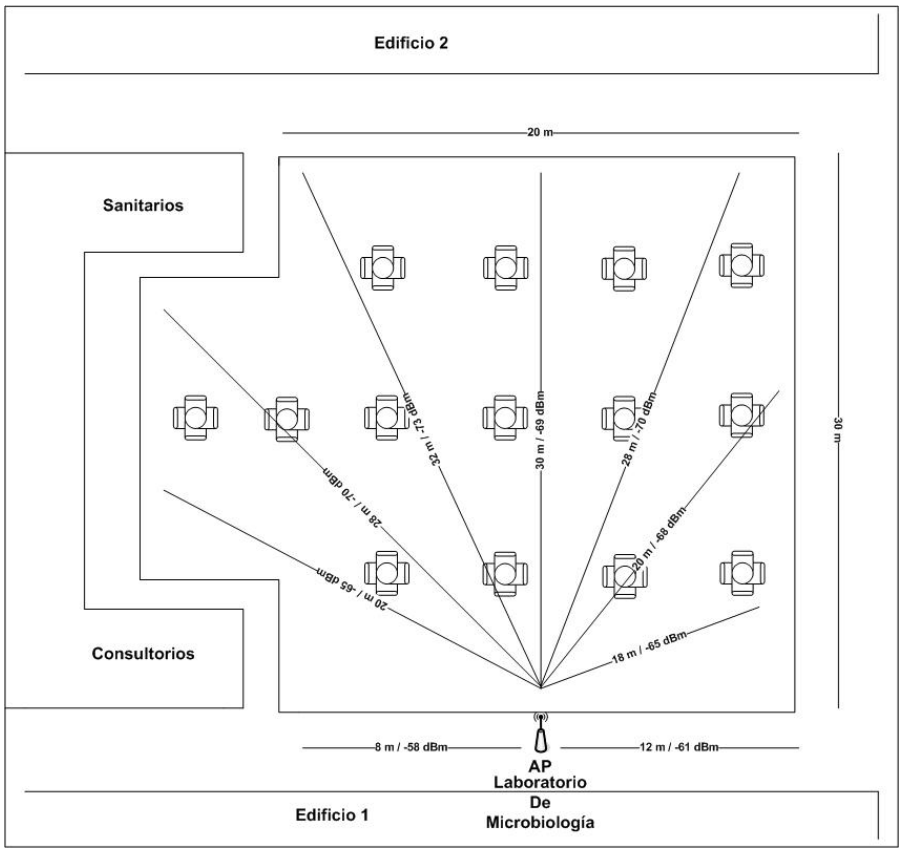


Figura 4.11 – Resultados con el AP colocado afuera del Laboratorio de Microbiología.

Decidimos cambiar la posición del AP hacia otra ubicación con la intención de conocer si podíamos obtener un mejor desempeño y mejores valores de intensidad de señal. Colocamos el AP en la parte exterior de los consultorios médicos, en esta posición obtuvimos los siguientes resultados.

La tabla 4.10 muestra los valores obtenidos.

Grados	Intensidad de Señal	Distancia
0°	-46 dBm	5 m
15°	-66 dBm	20 m
45°	-69 dBm	25 m
90°	-70 dBm	32 m
135°	-68 dBm	25 m
165°	-55 dBm	10 m
180°	-49 dBm	5 m

Tabla 4.10 – Valores obtenidos con el AP colocado afuera de los Consultorios Médicos.

Esto puede ser observado en la figura 4.12.

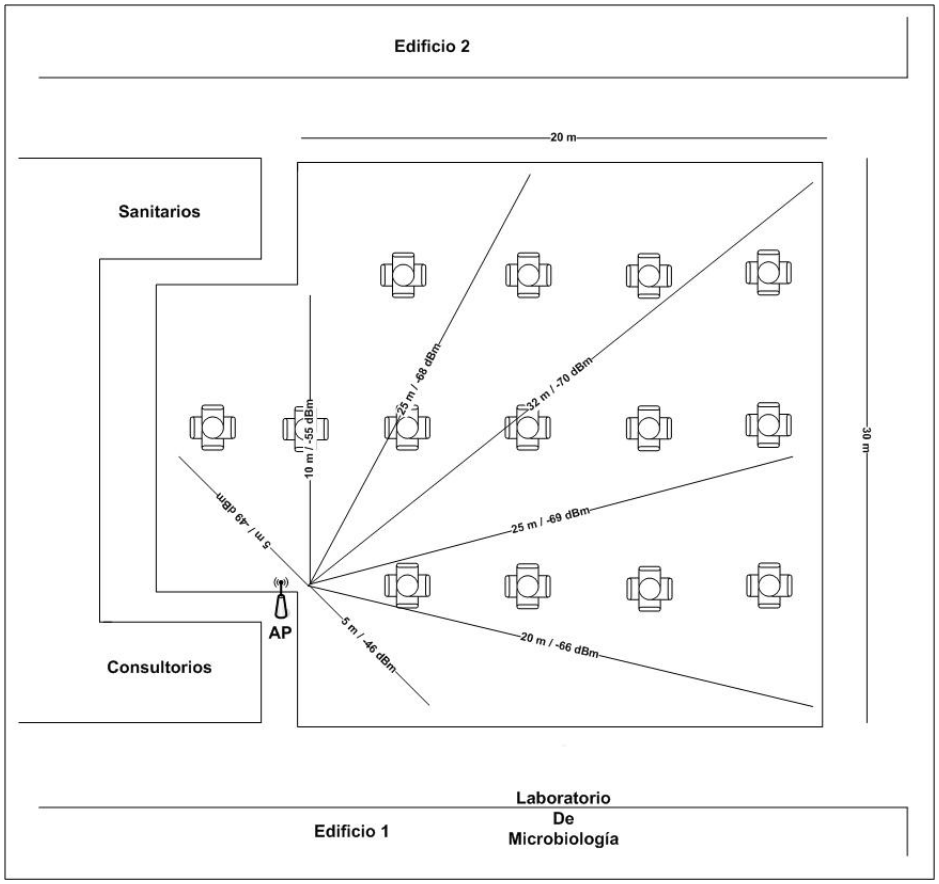


Figura 4.12 – Resultados obtenidos con el AP colocado afuera de los Consultorios Médicos.

De estos resultados podemos apreciar que colocar el AP afuera de los Consultorios Médicos nos permitiría tener un área de cobertura con mejor desempeño, que colocándolo afuera del Laboratorio de Microbiología.

Con esto damos por terminado el Capítulo 4 referente a las pruebas y resultados que llevamos a cabo para validar nuestra propuesta.

CONCLUSIONES Y RECOMENDACIONES

A continuación presentamos las conclusiones y recomendaciones que surgen a raíz de la realización de este trabajo.

Siguiendo los pasos propuestos en la metodología podemos determinar el diseño de una red inalámbrica, realizar la planeación de la capacidad de salida por usuarios, establecer que políticas de seguridad son necesarias para que la red sea segura y evitar que personas ajenas a ella tengan acceso a la misma, y elegir el hardware (AP) apropiado de acuerdo con las características de nuestra red.

La elaboración de un buen diseño y la correcta planeación de la WLAN nos permiten determinar la cantidad de AP necesarios para desplegar la red y brindar el servicio a los usuarios. Así mismo, la propuesta elaborada debe ser confirmada mediante pruebas realizadas en las áreas en las cuales se pretende ofrecer el servicio, ya que en algunas ocasiones las propuestas teóricas no consideran todas las características que podemos encontrar en el sitio propuesto, y no reflejan como se comportara la red una vez instalada y puesta en funcionamiento.

De acuerdo a la propuesta presentada en el Capítulo 3 para la UPIITA, de emplear un AP por piso en el Edificio Centro para desplegar la red inalámbrica, y después de realizadas las pruebas en los sitios comprobamos que nuestra propuesta es valida.

Obtuvimos un área de cobertura adicional a la esperada en la planta baja del edificio, ya que con el AP colocado en la Biblioteca cubrimos de manera satisfactoria toda la planta baja (biblioteca, laboratorios y oficinas administrativas) y los pasillos y jardines ubicados entre los edificios contiguos al Edificio Centro. (Ver fotos de UPIITA en anexo 2).

Para que dichas áreas sean aprovechadas al máximo recomendamos la instalación de las tomas de corriente necesarias para que los estudiantes puedan conectar sus equipos y así poder trabajar mas tiempo en las áreas donde se puede brindar el servicio de Internet de manera inalámbrica.

Una desventaja que presenta la estructura de los edificios de la UPIITA es que los pisos / techos cuentan con un recubrimiento metálico, el cual no permite que la señal del AP los atraviese, por lo que no es factible reducir el numero de AP de tres a dos para brindar el servicio de la WLAN en el Edificio Centro.

La UPIBI, por ser una Unidad Académica destinada a carreras biológicas no requiere que la red inalámbrica desplegada sea muy grande ni que soporte a un elevado numero de usuarios. Por lo anterior, se propuso brindar el servicio en la Biblioteca del campus, y crear una zona de conexión inalámbrica al aire libre en el jardín ubicado entre los Edificios 1 y 2 del campus.

Las pruebas realizadas con el AP colocado en la biblioteca confirmaron nuestra suposición de que se puede desplegar la red para cubrir esta área y de manera adicional cubrir las áreas contiguas a la biblioteca.

De las pruebas realizadas en el jardín, resulto factible cubrirlo con un solo AP. En este trabajo presentamos dos posibles lugares para colocar el AP para obtener un buen desempeño de la red y la mejor área de cobertura posible. Para que el jardín pueda ser utilizado por los estudiantes es necesario que se coloquen las tomas de corriente necesarias para que los estudiantes puedan trabajar en esta zona durante mayor tiempo con sus equipos portátiles.

La planeación de la capacidad de salida por usuario tanto para la UPIITA como para la UPIBI se realizo empleando la versión "b" del estándar IEEE 802.11. Ya que la versión "g" opera en la misma banda de frecuencia, seria factible realizar nuevamente esta planeación de capacidad y obtener una mayor capacidad de salida por usuario de la WLAN.

Los AP que podemos encontrar en el mercado hoy día brindan mejores desempeños en cuanto a velocidad de operación y alcance de cobertura, por lo que los resultados presentados en este trabajo pueden variar al realizar pruebas con diferentes tipos de AP.

Las redes inalámbricas han evolucionado vertiginosamente, han pasado solo algunos años desde que apareció el estándar IEEE 802.11, al momento de escribir este trabajo ya podemos encontrar tecnologías como las llamadas Redes de Área Metropolitana Inalámbricas (WPAN, siglas en inglés) o llamadas WIMAX, basadas en el estándar IEEE 802.16, la cual permitirá desarrollar celdas de cobertura de varios kilómetros con la utilización de un solo AP. Están destinadas a operar en grandes zonas geográficas con alta densidad de usuarios, y sin la necesidad de que exista línea de

vista entre el usuario y el AP. Operarán en la banda de 2 a 11 GHz y se espera que mas adelante opere también en la banda de 66 GHz, ofreciendo velocidades de hasta 280 Mbps.

También encontramos las llamadas Redes de Área Personal Inalámbricas (WPAN, siglas en inglés) basadas en el estándar IEEE 802.15, con las cuales se pretende conectar de manera inalámbrica los distintos equipos que puede emplear un usuario, tales como computadoras, impresoras, scanners, cámaras de video, teléfonos celulares, agendas digitales, etc. Los primeros ejemplos de este tipo de redes son las conexiones entre teléfonos celulares y computadoras portátiles, que se realizan mediante la tecnología inalámbrica Bluetooth, basada en el estándar IEEE 802.15.1, el cual trabaja con velocidades de operación de hasta 1 Mbps y opera en la banda de 2.4 GHz, y próximamente el estándar 802.15.3a con una velocidad de operación de hasta 100 Mbps y operando en la frecuencia de 7.5 GHz.

Debemos recordar que las redes inalámbricas no pretenden sustituir a las redes cableadas tradicionales, sino servir como una extensión de estas para brindar los servicios de red en aquellos lugares en los que resulta complicado o costoso llevar el cableado.

ANEXO 1

ANTENAS

Introducción

Una antena es un dispositivo que permite la emisión y recepción de ondas electromagnéticas (ondas de radio). Esto quiere decir que las antenas convierten las señales eléctricas en ondas electromagnéticas y viceversa.

La mayoría de los AP incorporan antenas, no obstante, cuando se desea que el área de cobertura del AP sea mayor resulta conveniente sustituir la antena incorporada al AP por una exterior con mayor ganancia. El obtener un buen resultado en la colocación de antenas exteriores depende no solo del conocimiento técnico que se tenga sobre los distintos tipos de antenas, de cómo instalarlos, sino que, además, es necesaria cierta experiencia.

La razón para que no existan reglas absolutas para el diseño y localización de las antenas es que son muchas las variables que afectan la propagación de la señal, además, con las WLAN debemos considerar que los usuarios son móviles y las condiciones ambientales cambian constantemente. Esto significa que el problema de colocar una antena exterior requiere de cierta experimentación hasta encontrar una posición óptima.

Con una buena antena externa, la señal del AP puede alcanzar varios kilómetros, siempre que no existan obstáculos entre el AP y el usuario.

Ganancia

La ganancia representa la relación entre la intensidad de campo que produce una antena en particular en un punto determinado y la intensidad de campo que produce una antena omnidireccional (isotrópica) en el mismo punto y en las mismas condiciones.

Las antenas de los AP suelen ser antenas omnidireccionales, estas tienen una ganancia mayor a las antenas de los adaptadores de usuario (Tarjetas PCMCIA por ejemplo), pero bastante menor que la ganancia de una antena externa direccional. Las antenas direccionales concentran la energía radiada en una sola dirección, por lo que se consigue que la energía alcance una mayor distancia, aunque sea en una sola dirección.

Relación Señal / Ruido

En los sistemas de radio cuando se emite la señal, no solo se emiten los datos, sino que, además, se emite ruido, de la misma forma, cuando se recibe los datos, también se recibe ruido. Una transmisión se recibirá mejor cuanto más potente sea la señal de los datos en comparación con el ruido.

Al resultado de dividir el valor de la intensidad de la señal de la información por el valor de la intensidad del ruido, se le conoce como relación Señal / Ruido (S/N siglas en ingles). Cuanto mayor sea este valor, mejor será la comunicación.

Patrón de radiación y apertura del haz

El patrón de radiación es un diagrama polar sobre el que se representa la intensidad del campo electromagnético radiado por una antena. La forma del patrón depende del modelo de antena. Puede ser representado en dos planos perpendiculares conocidos como azimut y elevación.

La figura A.1 nos muestra ambos diagramas.

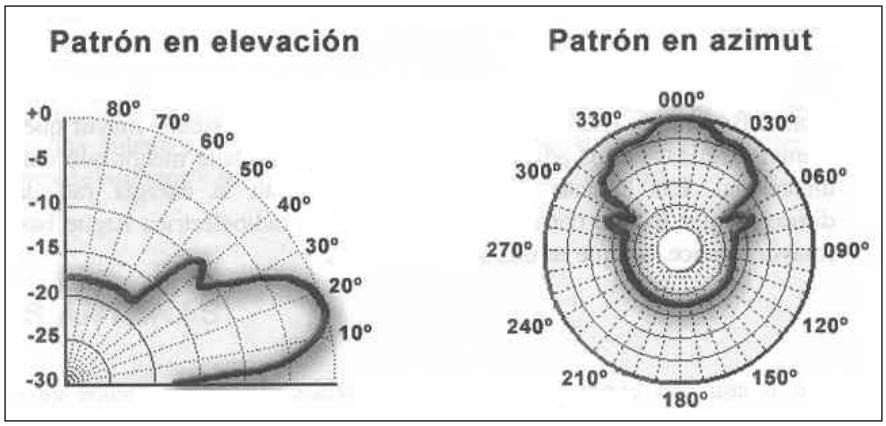


Figura A.1 – Ejemplo de un patrón de radiación de una antena

Otro valor que esta relacionado con el modelo de radiación es la apertura del haz. Este valor representa la separación angular entre los dos puntos del lóbulo principal del patrón de radiación, donde el valor de la energía es la mitad de la original (-3 dB). La apertura del haz suele representarse en el plano horizontal, aunque no siempre es así.

Polarización

La polarización de la antena describe la orientación de los campos electromagnéticos que irradia o recibe la antena. Las formas de polarización más comunes son:

- **Vertical**: Cuando el campo eléctrico generado es vertical con respecto al horizonte terrestre.
- **Horizontal**: Cuando el campo eléctrico generado es paralelo al horizonte terrestre.
- **Circular**: Cuando el campo eléctrico generado rota de vertical a horizontal, y viceversa, creando movimientos circulares.
- **Elíptica**: Cuando el campo eléctrico generado se mueve como en la polarización circular, pero con desigual fuerza en las distintas direcciones.

La polarización de las antenas en ambos extremos del enlace de comunicación debe ser la misma para minimizar la pérdida de ganancia.

Tipos de Antenas

Existen varios tipos de antenas en el mercado, yagui, dipolo, sectoriales, parabólicas, etc., no obstante los tipos de antenas pueden agruparse en dos tipos principales: omnidireccionales y direccionales.

Las antenas omnidireccionales son aquellas que radian en todas direcciones y también pueden captar la señal procedente de todas direcciones. Por el contrario, las antenas direccionales concentran su radiación en una sola dirección y solo pueden captar la señal procedente de la misma dirección. Estas últimas tienen mayor alcance y ganancia que las primeras, a costa de concentrar la energía en una sola dirección.

La figura A.2 nos muestra algunos de los tipos de antenas existentes.

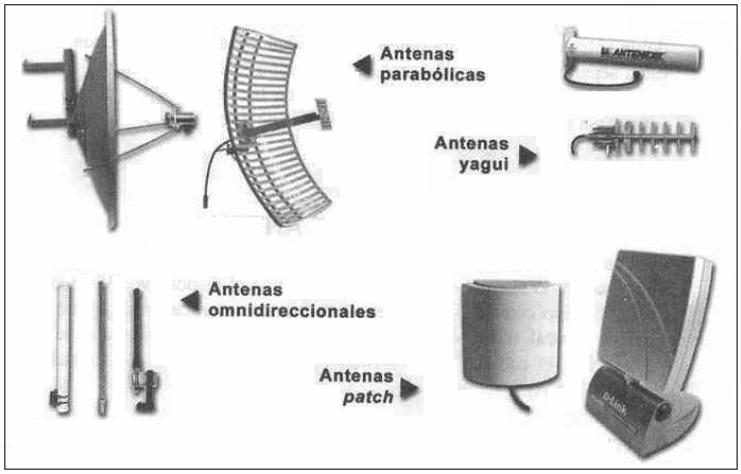


Figura A.2 – Tipos de Antenas

En los AP que se utilizan para implementar las WLAN se suelen utilizar las antenas omnidireccionales para la cobertura en interiores y las antenas direccionales para la cobertura de exteriores.

Las antenas direccionales concentran la energía en una sola dirección, incrementando el alcance. Mientras más direccional sea la antena, mayor será el alcance. Existen distintos modelos de antenas direccionales, entre los más importantes tenemos:

- **Antena Yagui**: Antena direccional con apertura de haz de entre 15 y 60 grados. Su ganancia varía entre los 6 y 21 dBi. Suelen venir montadas en el interior de una cobertura cilíndrica.
- **Antena tipo Patch**: Antena plana para ser montada en la pared. Emite energía siguiendo un modelo semiesférico. Su ganancia varía entre 12 y 22 dBi. Su principal desventaja es que al ser plana, puede sufrir por la acción del viento cuando se coloca exteriores.
- **Antena Parabólica**: Antena en forma de disco cóncavo con la que se consigue haces direccionales. Muy útil para comunicaciones punto a punto. Su ganancia puede llegar hasta los 27 dBi.

Además de las anteriores, existen otros tipos de antenas que pueden ser utilizados con los AP. En cualquier caso, siempre es bueno asegurarse que la antena este construida para funcionar en la banda

de frecuencia de 2.4 GHz. La mayoría de los AP vienen equipados con una antena doble, esta se utiliza para obtener diversidad en la recepción. Cada antena puede recibir la señal en distintas condiciones en cada momento, el equipo elige la mejor de las señales en cada momento, evitando de esta forma problemas de mala recepción.

Hemos visto los conceptos generales relacionados con las antenas, ahora debemos decidir cual es la más adecuada para dar solución a nuestras necesidades.

Donde situar la antena

La especificación 802.11b presenta dos retos importantes desde el punto de vista de la transmisión: el primero es que utiliza un rango de frecuencias que es utilizado por una gran variedad de dispositivos, y el segundo es que la especificación limita la potencia con la que los AP pueden emitir su señal.

Las interferencias son producidas generalmente por distintos equipos en funcionamiento cerca del AP, por lo que debemos tratar de colocarlo en un lugar donde no existan demás dispositivos trabajando en la misma banda de frecuencias.

Construcción de una antena

La mayoría de las antenas comerciales existentes en el mercado tienen un costo elevado, lo que puede elevar considerablemente el presupuesto destinado al diseño e implementación de la WLAN, por lo que en algunas ocasiones conviene construir la antena.

Conceptos teóricos

Como sabemos, las ondas radioeléctricas tienen forma senoidal, esto quiere decir que la onda aumenta y diminuye su amplitud en forma cíclica. La onda tiene al final de cada ciclo la misma amplitud. El tiempo que tarda la onda en completar cada ciclo se conoce como periodo. La distancia que recorre la señal en un ciclo como longitud de onda.

La figura A.3 nos muestra la forma de una onda de radio frecuencia

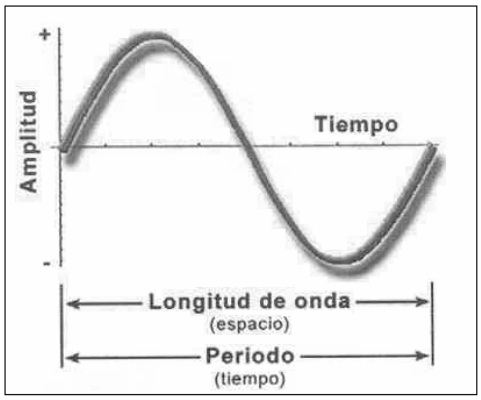


Figura A.3 – Onda de radio frecuencia.

El Hertz en la unidad de medida del número de ciclos que completa la onda en un segundo. Una frecuencia (f) de 10 Hz significa que la onda completa 10 ciclos en un segundo, esto quiere decir que tarda una décima de segundo en completar cada ciclo, por lo tanto, el periodo es de 0.1 segundo.

El periodo se calcula con la siguiente fórmula: $periodo = \frac{1}{frecuencia}$

donde el periodo esta expresado en segundos y la frecuencia en Hertz.

Teniendo en cuenta que las señales radioeléctricas se desplazan a la velocidad de la luz (c), es fácil calcular la longitud de onda (λ) si conocemos el periodo por medio de la fórmula:

$$\lambda = \frac{c}{f}$$

Mencionamos esto ya que el funcionamiento y construcción de las antenas esta directamente relacionado con la longitud de onda de la frecuencia a la que trabajara la antena. De esta variable depende la mayoría de las mediciones de la antena.

Construcción de una antena direccional

Se pueden encontrar un sin fin de modelos y tipos de antenas para incrementar el alcance de los AP, pero sin importar que tipo de antena decidamos construir, hay que tener presente que lo más importante a la hora de construirla, son sus medidas.

Con el modelo de antena que presentamos, en teoría, se podría conseguir una ganancia de 12 dB y cubrir una distancia de hasta 1 Km, no obstante estos datos son teóricos, y debemos recordar que el alcance no depende solo de la antena, sino que influyen otros factores, tales como las condiciones climatológicas, el entorno en donde se encuentre el AP, los equipos que puedan causar interferencias, etc.

A la hora de construir una antena no siempre podemos contar con las herramientas, equipos y experiencia necesaria, por lo que el resultado de la antena tal vez no sea el esperado, pero podemos dar por bueno el haber construido una antena que nos de una ganancia de entre 6 y 9 dB, y que alcance a cubrir una distancia de hasta 500 metros transmitiendo a una velocidad relativamente buena.

Los materiales que necesitamos para construir la antena son los siguientes:

- 1 tubo de cartón o plástico rígido no muy grueso con un diámetro de 73 mm y longitud de 230 mm y cerrado en un extremo (servirá como cobertura para el arreglo).
- 1 tapa de plástico para el cilindro.
- 1 disco plástico de 73 mm de diámetro exterior.
- 1 conector de antena, se puede utilizar un conector hembra tipo N. En el se conectara el cable que une la antena con el AP.
- 1 varilla roscada de 3 mm de diámetro, y 20 cm de largo, (no se usara toda la varilla).
- 2 tuercas plásticas que enrosquen en la varilla.
- 5 arandelas de 25 mm de diámetro exterior, 1.5 mm de espesor y que el diámetro interior sea el suficiente para pasar por la varilla (algo mas de 3 mm).
- 1 tubo de aluminio de 6 mm de diámetro, y 15 cm de largo, (no se usara todo el tubo).
- Cable de cobre grueso de un solo hilo, aproximadamente 50 mm de longitud.

Lo primero es cortar el tubo de aluminio en 4 pedazos de 31 mm de largo. Luego cortamos la varilla a una longitud de 143 mm, la longitud de la varilla debe ser suficiente para albergar las 5 arandelas, los 4 tubos de aluminio y las 2 tuercas.

A continuación, debemos hacer un agujero en el centro a la tapa de plástico para que pase la varilla, y el disco de plástico, al que hay que cortar con un diámetro exterior de 73 mm y hacerle un agujero en el centro de 6 mm para que quepa el tubo de aluminio.

Luego debemos ensamblar el tubo, quedando la antena como mostramos mas adelante. El ensamblaje consiste en poner una tuerca en un extremo de la varilla e ir introduciendo por el otro extremo el resto de las piezas, en el siguiente orden: tapa de plástico, arandela, tubo, arandela, tubo, arandela, tubo con el disco de plástico, arandela, tubo, arandela, y por último colocar la otra tuerca al final de la varilla. De ser necesario debemos limar el resto de la varilla que haya sobrado.

El cable de cobre debe soldarse al conector, y el conector debe fijarse a la pared del tubo, el resultado debe ser que el cable de cobre llegue justo al centro del tubo. Como podemos encontrar distintos tipo de conectores es posible que la longitud de cable pueda variar. En general deberá estar alrededor de 27 a 38 mm del centro del tubo.

El cable deberá estar recto y bien soldado al conector. Para fijar el conector se deben hacer agujeros en un lado del tubo, de forma que el cable quede justo delante de la varilla sin tocarla. Esto supone situar al conector a unos 85 mm desde la base del tubo.

Por último, montamos la varilla en el tubo, conectamos el conector al AP mediante un cable adecuado, y listo, tenemos una antena direccional para nuestra WLAN.

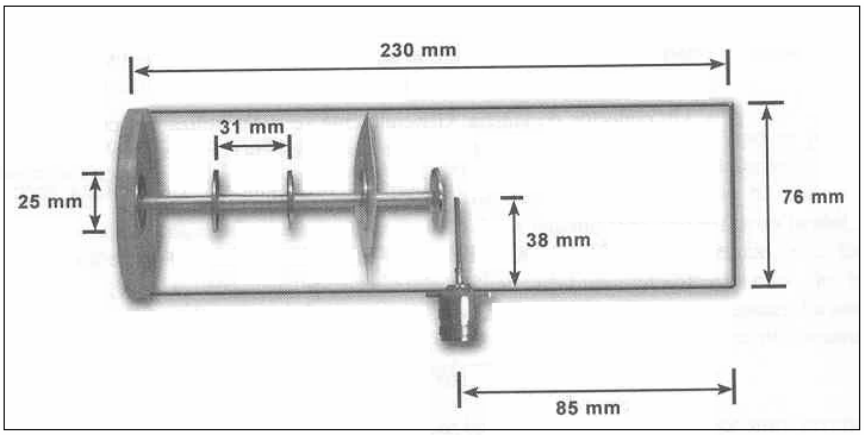


Figura A.4 – Esquema de construcción de antena direccional

Una vez montada la antena, las arandelas actúan como amplificadores de la señal. Lo que hace que esta antena sea apta para nuestra red es la distancia entre las arandelas, esta distancia esta relacionada con la frecuencia mediante la siguiente fórmula:

$$L = \frac{75}{f}$$

donde L = longitud de los tubos de aluminio (1/4 de longitud de onda), f = frecuencia de operación, y 75 es una constante dada.

Si hacemos el cálculo para dos frecuencias de operación de las WLAN, (por ejemplo 2.412 y 2.462 GHz), vemos que la longitud de los tubos de aluminio pueden variar desde lo 31.1 y 30.46 mm. En cualquier caso podemos utilizar la longitud de 31 mm para cada tramo de tubo y nos debe funcionar correctamente.

ANEXO 2

FOTOS DE LA UPIITA Y LA UPIBI

Presentamos algunas fotos de las áreas donde se propone brindar el servicio para darnos una idea de cómo son y como se ven físicamente.

Fotos UPIITA

Foto A.1 – UPIITA

Fotos de los Edificios UPIITA

Foto A.2 - Edificios Centro y Norte

Foto A.3 - Edificios Sur y Centro

Fotos de Edificios UPIITA

Foto A.4 - Edificios Centro y Sur

Fotos de Edificios UPIITA

Foto A.5 - Edificio Norte

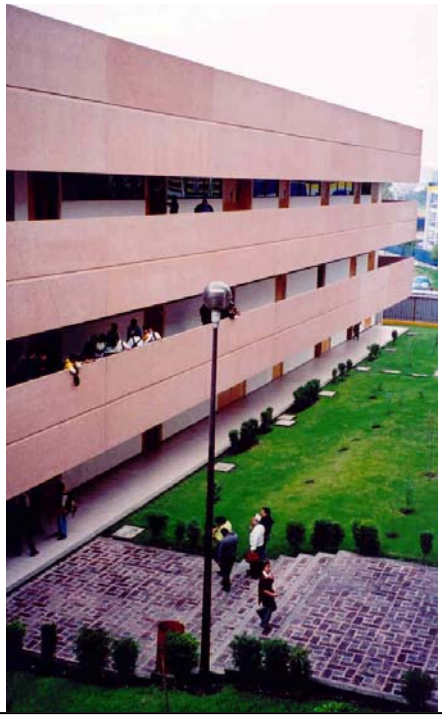


Foto A.6 - Edificio Centro

Fotos de Laboratorios UPIITA

Foto A.7 – Laboratorio de Biónica.

Foto A.8 – Laboratorio de Telemática

Fotos Laboratorios UPIITA

Foto A.9 – Laboratorio de Telecomunicaciones.

Foto A.10 - Biblioteca UPIITA

Foto A.11 - Biblioteca UPIITA

Presentamos algunas fotos del Campus UPIBI para darnos una idea de cómo se ven físicamente las áreas en las que se desea brindar el servicio.

Fotos UPIBI

Foto A.12 – UPIBI.

Fotos de Biblioteca UPIBI

Foto A.13 - Biblioteca UPIBI, vista exterior.

Foto A.14 - Biblioteca UPIBI, vista interior

Foto A.15 - Biblioteca UPIBI, vista interior

Foto A.16 - Biblioteca UPIBI, vista interior

Zona de bancas y mesas

Foto A.17 – Áreas verdes

Foto A.18 – Áreas verdes

Foto A.19 – Áreas verdes

BIBLIOGRAFÍA

Libros

- [1] Reid, Neil y Seide, Ron. 802.11 (Wi-Fi) Manual de Redes Inalámbricas. McGraw – Hill Interamericana, México, D.F. 2004.

- [2] Carballar, José A. Wi-Fi. Como construir una red inalámbrica. Alfaomega – Ra-Ma. México, D.F. 2004.

- [3] Dayem, Rifaat A. Mobile Data and Wireless LAN Technologies. Prentice Hall, United States of America. 1997.

- [4] Parsons, J. D. The Mobile Radio Propagation Channel. Pentech Press. London. 1994.

- [5] Saunders, Simon R. Antennas and Propagation for Wireless Communication Systems. John Wiley & Sons, Ltd. New York, U.S.A.

- [6] RoamAbout, Enjoy the freedom of wireless networking. 802.11 Wireless Networking Guide. Enterasys Networks.

Tesis

- [7] Quino C., Juan M. Análisis de Propagación Electromagnética dentro de Edificios Educativos del I.P.N. en la banda de 800 MHz. Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica, Sección de Estudios de Postgrado e Investigación. 2002.

- [8] Hay R., Francisco E. Diseño e Implementación de una Red Inalámbrica en el Campus Panamá de la Universidad Católica Santa Maria La Antigua. Universidad Católica Santa Maria La Antigua, Facultad de Ciencias y Tecnología, Escuela de Ingeniería Electrónica. 2003.

Artículos

- [9] Pau Oliva Fora. (In)Seguridad en redes 802.11. Universidad Politécnica de Mataró.

- [10] Alapont M., Vicent. Seguridad en Redes Inalámbricas. Universitat de València.

- [11] Guillermo Ibáñez Fernández. Aspectos de Seguridad en Redes Locales e Inalámbricas: Acceso a la Red controlado por puerto (IEEE 802.1X). Universidad Carlos III.

Estándares IEEE

- [12] ANSI/IEEE Std 802.11, 1999 Edition

- [13] IEEE Std 802.11b, 1999 Edition

Páginas de Internet

- http://www.idg.es/comunicaciones/pdf/3com4.pdf
- http://www.ictnet.es/novedades/articulos/155.htm
- http://www.lucent.com/livelink/161940_Whitepaper.pdf
- http://www.domotica.net/802.11b.htm
- http://www.oreillynet.com/cs/weblog/view/wlg/448
- http://www.qsl.net/n9zia/wireless
- http://www.wimaxforum.org
- http://www.ieee802.org/15

GLOSARIO

ACL: Lista de Control de Acceso

AP: Punto de Acceso

BER: Tasa de Error por Bit

BPSK: Modulación de Fase por Desplazamiento Binario

BSS: Conjunto de Servicio Básico

CCA: Comprobación de Canal Libre

CCK: Modulación de Código Complementario

CNAC: Control de Acceso a la Red Cerrado

CRC: Revisión de Redundancia Cíclica

CSMA / CA: Carrier Sence Multiple Access / Collision Avoidance

CSMA / CD: Carrier Sence Multiple Access / Collision Detect

DFS: Selección Dinámica de Frecuencia

DHCP: Protocolo de Configuración Dinámica de Usuario

DSSS: Espectro Extendido de Secuencia Directa

ESS: Conjunto de Servicio Extendido

ETSI: Instituto Europeo de Estándares de Telecomunicaciones

FCC: Comisión Federal de Comunicaciones de Estados Unidos

FER: Tasa de Error por Trama

FHSS: Espectro Extendido por Salto de Frecuencia

FSK: Frecuency Shift Keying

HEC: Revisión de Errores en el Encabezado

HTTP: Protocolo de Transferencia de Hipertexto

IBSS: Conjunto de Servicio Básico Independiente

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos

IP: Protocolo de Internet

LAN: Red de Área Local

LLC: Logical Link Control

MAC: Capa de Control de Acceso al Medio

MIC: Messagge Integrity Code

MSDU: MAC Service Data Unit

OFDM: Multiplexación por División Ortogonal de Frecuencia

OSA: Sistema de Autenticación Abierto

PCMCIA: Personal Computer Memory Card International Association

PDA: Asistente Personal Digital

PDU: Protocol Data Unit

PHY: Capa Física

PLCP: Protocolo de Convergencia de la Capa Física

POP3: Post Office Protocol

QoS: Calidad de Servicio

QPSK: Modulación por Fase de Desplazamiento en Cuadratura

RADIUS: Remote Autenticación Dial In User Service

SER: Tasa de Error por Símbolo

SFD: Delimitador de Inicio de Trama

SKA: Autenticación por Llave Compartida

SNMP: Protocolo de Administración de Red Simple

SSID: Identificadores de Establecimiento de Servicio

TCP: Control de Potencia de Transmisión

TKIP: Temporal Key Integrity Protocol

TDMA: Acceso por Multiplexación de División de Tiempo

UMTS: Sistema de Telecomunicaciones Móvil Universal

UPIBI: Unidad Profesional Interdisciplinaria de Biotecnología

UPIITA: Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías Avanzadas

VLAN: Red de Área Local Virtual

VoIP: Voz sobre Protocolo de Internet

WEP: Wired Equivalent Protocol

WLAN: Red de Área Local Inalámbrica

WPA: Protocolo de Autenticación Inalámbrico