Universidad Autónoma de Baja California

Facultad de Ingeniería Ensenada

Maestría y Doctorado en Ciencias e Ingeniería

METODOLOGÍA PARA EL DISEÑO DE REDES DE ÁREA LOCAL INALÁMBRICAS, IEEE 802.11a/b/g

Caso de Estudio: Universidad Autónoma de Baja California campus Ensenada

TESIS

que para obtener el grado de

MAESTRO EN INGENIERÍA

Presenta:

ADRIÁN ENCISO ALMANZA

Ensenada, B.C. a Octubre de 2008

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
FACULTAD DE INGENIERÍA
UNIDAD ENSENADA

METODOLOGÍA PARA EL DISEÑO DE REDES DE ÁREA LOCAL INALÁMBRICAS, IEEE 802.11a/b/g

Caso de Estudio: Universidad Autónoma de Baja California

TESIS

Que para obtener el grado de maestría en ingeniería presenta:

ADRIÁN ENCISO ALMANZA

Aprobada por:

M.C. EVELIO MARTÍNEZ MARTÍNEZ
Director de tesis

DR. JUAN IVÁN NIETO HIPÓLITO
Miembro del comité

M.C. ELITANIA JIMÉNEZ GARCÍA
Miembro del comité

M.C. CHRISTIAN XAVIER NAVARRO COTA
Miembro del comité

Ensenada Baja California, México. Octubre de 2008

La familia que crece unida permanece unida... para siempre.

A la mujer que adoro, mi esposa Lizbeth

A mi encanto, mi hija Daiana

A mi orgullo, mi hijo Axel

AGRADECIMIENTOS

Un agradecimiento muy especial al maestro Evelio Martínez Martínez por su dirección y asesoría en la elaboración de este trabajo, por su paciencia.

A mis padres por sus palabras de aliento.

A todos los que me apoyaron.

RESUMEN

En este trabajo presentaremos una metodología para el diseño de redes de área local inalámbricas - IEEE 802.11a/b/g, mediante la cual podemos implementar una WLAN en cualquier lugar de una manera óptima y segura, analizaremos cada una de sus componentes que la integran, tales como: protección, cobertura, equipamiento, gestión, aplicaciones, y ancho de banda. La metodología podrá adaptarse a las necesidades de cualquier organización que tenga el interés de hacer un diseño e implementar una red inalámbrica. Se analizará como caso de estudio la red inalámbrica con la que cuenta la Universidad Autónoma de Baja California campus Ensenada y se utilizará la metodología para poder evaluar su desempeño.

INDICE

INDICE (continuación)

INDICE (continuación)

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE FIGURAS (continuación)

LISTA DE FIGURAS (continuación)

LISTA DE FIGURAS (continuación)

LISTA DE FIGURAS (continuación)

LISTA DE FIGURAS (continuación)

Capítulo I

1. INTRODUCCIÓN

1.1 Introducción a las WLAN

Las redes inalámbricas en los últimos años han ganado mucha popularidad en el mercado, particularmente las redes locales de datos inalámbricas (WLAN), tecnología que ha tenido mucha aceptación en oficinas, universidades, hogares, así como en áreas públicas como hoteles, aeropuertos, restaurantes, quienes estos últimos ven esto como una estrategia para traer clientes al ofrecer Internet gratis dentro de sus negocios.

La tecnología Wi-Fi, cómo se le conoce comúnmente a las WLANs, usan tecnología de radio frecuencias (RF) para trasmitir y recibir datos a través del aire. Proveen los mismos beneficios y recursos que ofrece una red LAN tradicional pero sin la limitación de estar conectada a través de un cable [1]. Una WLAN es un sistema de comunicación de datos flexible implementada como una extensión o una alternativa de una red de área local cableada

permitiendo además incrementar la productividad y eficiencia de las actividades diarias de la empresa [2].

Las WLAN no vienen a sustituir las LAN cableadas, sino más bien, vienen a expandir su cobertura. Las conexiones inalámbricas pueden extender su cobertura a aquellas zonas en las que es difícil cablear. De este modo, el tener una extensión inalámbrica de una LAN podría ser de mucha importancia para alcanzar las posibilidades de conexión que nos brindan las WLAN.

Una de las características por la que las WLAN se identifican es su fácil implementación. Es precisamente esta lo que las hace un blanco fácil para ataques externos e incluso internos. Recordemos que el medio por el cual se comunican los dispositivos inalámbricos es el aire, y que cualquier espía con los dispositivos necesarios puede interceptar las señales que viajan por él, y utilizar la WLAN para actos no autorizados.

Durante la década de los 90's nacieron dos estándares que vinieron a revolucionar el mercado de las WLAN a nivel mundial, el estándar 802.11 de la IEEE (Institute of Electrical and Electronics Engineers) y el estándar europeo HiperLAN de la ETSI (European Telecommunications Standards Institute), ambos manejan un ancho de banda entre 1 Mbps y 2 Mbps en sus primeras versiones. Esto fue suficiente para que este mercado de las WLAN fuera explotado al máximo por los usuarios finales.

Sin embargo, el estándar que ha dominado el mercado de las WLAN es el de la IEEE 802.11 y sus diferentes variantes, como lo son: 802.11a, 802.11b, 802.11g y 802.11n.

Estos estándares operan en las bandas de frecuencias reservadas para el espectro disperso en los 2.4 GHz y 5 GHz. Estas bandas de frecuencias son consideradas de uso libre. En la tabla I, se muestran otras características técnicas que describiremos más adelante.

Tabla I: Comparación de estándares IEEE 802.11

Tabla 1. Comparación entre los estándares 802.11a, b y g			
Parámetro	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Frecuencia/Ancho de banda	5 GHz (300 MHz)	2.4 GHz (83.5 MHz)	2.4 GHz (83.5 MHz)
Modulación	OFDM	DSSS	OFDM
Ancho de banda por canal	20 MHz (6 canales utilizables)	22 MHz (3 canales)	22 MHz (3 canales)
Tasa de transmisión	54 Mbps	11 Mbps	54 Mbps
Cobertura interior/exterior	30/50 metros	50/150 metros	30/50 metros
Potencia máxima	200 mW, 1 W, 4 W	1 mW/MHz	200 mW, 1 W, 4 W
Usuarios simultáneos	64	32	50

El auge que han tenido este tipo de redes WLAN y los costos tan bajos de los dispositivos en el mercado, han hecho que los usuarios finales sean al mismo tiempo los administradores de la red inalámbrica, lo cual ha ocasionado que la WLAN presenten problemas de seguridad con intrusos, pérdidas de información, problemas con la cobertura de la señal, problemas de administración de accesos y recursos, y de equipos obsoletos que no incorporan los nuevos protocolos que ayudan a mejorar el desempeño de la WLAN.

La planeación y el diseño de este tipo de redes es un reto para las organizaciones que deciden implementarla. Aspectos muy importantes se tienen que tomar en cuenta como: la seguridad

de la información, no solo de la red inalámbrica si no de la información que viaja a través de la red cableada, desgraciadamente este tipo de redes son muy susceptibles al ruido. Otro aspecto importante es que es difícil asegurar un ancho de banda real, debido a que la señal es afectada por diversos factores que vamos a explicar más adelante.

Principalmente éstas fueron las razones que me motivaron hacer este trabajo y poder aportar un procedimiento que ayude a realizar la planeación y un diseño que cumpla con las expectativas de la organizaciones, de esta manera evitar invertir esfuerzo y dinero en un trabajo que no tenga satisfechos a los usuarios ni a la organización misma.

1.1.1 Redes inalámbricas en universidades

Cada día es mayor la inquietud en las universidades por implementar redes inalámbricas. Varias universidades han implementado sus propias redes inalámbricas, y muchas otras están considerando implementarlas. Algunos puntos importantes y beneficios de la implementación de estas redes en las universidades son:

- La utilización de los recursos y servicios que ofrece la LAN universitaria desde cualquier parte del campus: salones de clase, bibliotecas, laboratorios, audiovisuales, etc.

- Una herramienta de apoyo para la docencia.
- Llegar a lugares de difícil acceso.
- Disminuir costos de instalación de cableado estructurado en edificios.
- Delegar la responsabilidad de configuración y conexión a la red a los usuarios que cuentan con sus computadoras portátiles [3].

Muchas universidades han encontrado en las redes inalámbricas ahorro en costos, especialmente en redes para nuevos edificios o reconstruidos. Algunas universidades han optado por implementar redes inalámbricas en edificios que no cuentan con cableado estructurado, los costos por cablear e instalar una red tradicional (cableada), son mucho mayores que implementar una red inalámbrica en un 75%.

Es muy caro el mantenimiento de los equipos y la administración de un aula de cómputo para los estudiantes para que puedan utilizar Internet y otros servicios. Los estudiantes por lo regular deben esperar para hacer uso de una computadora en el laboratorio, lo cual interrumpe sus actividades.

De otra forma las redes inalámbricas dan a los estudiantes acceso a estos recursos utilizando su propia computadora desde cualquier lugar del campus a cualquier hora, aún cuando las aulas de cómputo se encuentren cerradas.

En los Estados Unidos las universidades han tomado muy en serio el papel que juegan las redes WLAN en la educación, tan es así, que hoy en día la universidad de Cornell en Nueva York, ha iniciado la instalación de la *Red Enterprise,* la WLAN más grande de los Estados

Unidos que alberga más de 20,000 estudiantes y 14,000 empleados, incluyendo académicos y administrativos. Una vez que esté terminada la red WLAN incluirá 4,500 puntos de acceso interior y exterior, para cubrir más de 745 acres, así mismo esta universidad utilizará dispositivos del pre-estandar 802.11n para la conexión inalámbrica.

Compañías como Extricom, un fabricante de tecnologías de WLAN, en el 2007 puso en marcha un programa llamado *K-12 School* para colegios y universidades, el cual tiene el propósito de donar un total de un millón de equipos inalámbricos WLAN a las universidades. Estos equipos serán concedidos a aquellas universidades públicas o privadas que demuestren la "necesidad inmediata de la tecnologías WLAN". Según Extricom la escuela moderna es conducida cada vez más por la tecnología, apoyando el proceso educativo. Además las WLAN desempeñan un papel importante en la infraestructura, permitiendo servicios de red de manera rápida y en cualquier punto del campus [4].

Según un informe de la consultora y analista de mercados Pyramid Research, fechado en julio de 2003, alrededor de 50 millones de usuarios utilizan redes WLAN en todo el mundo, y se prevé que para 2008 esta cifra crezca de forma exponencial. El número de usuarios llegará a los 700 millones [5]. Ver la figura 1.1.

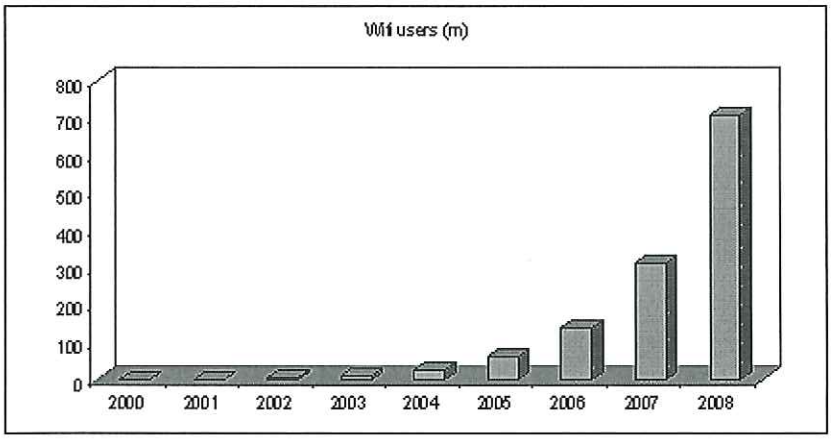


Figura 1.1: Estimación del número global de usuarios Wi-Fi, 2000-2008

(FUENTE: Pyramid Research)

Del mismo modo, Gartner Inc., prevé, refiriéndose al mercado y aplicaciones de uso público, que durante el 2003 hubo más de 80,000 puntos de acceso Wi-Fi en todo el mundo. Según Gartner Inc, el número de puntos de acceso Wi-Fi en todo el mundo se dobló antes del 2006, ver figura 1.2.

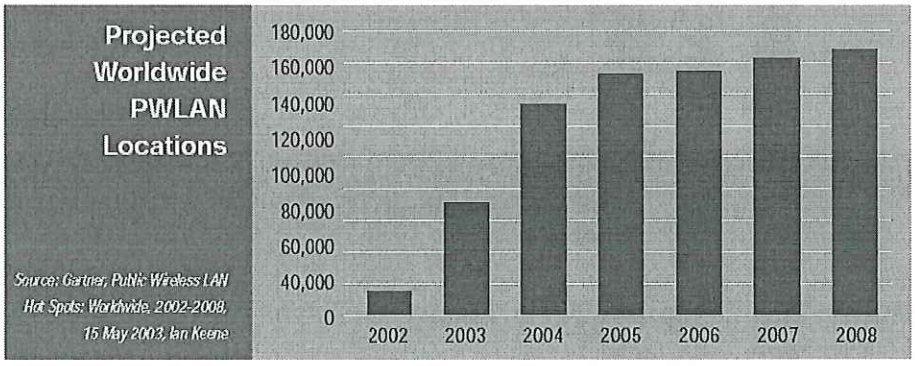


Figura 1.2: Previsiones de puntos de acceso (FUENTE: Gartner Inc.)

1.2 Planteamiento del problema

Como mencionamos anteriormente, debido a la fácil instalación, el bajo costo de los dispositivos y el incremento en la velocidad de transmisión, las redes de área local inalámbricas WLAN han tenido un gran auge entre los usuarios. Es por esto que las WLAN se han convertido para muchas organizaciones, instituciones académicas, establecimientos públicos y hogares, en una opción para realizar tareas comunes como es el acceso a Internet, correo electrónico, mensajería instantánea, transferencia de archivos, entre muchas otras actividades.

Algunas de éstas organizaciones optan por contratar a grandes corporativos que realicen el estudio y hagan el diseño de la WLAN acordé a sus necesidades, sin embargo el costo es muy alto, lo cual para algunas de ellas no les es posible solventar. Otras optan por crear e implementar su propia WLAN realizando sus propios diseños, basados en lo que ellos consideran se debe cubrir como mínimo para obtener las bondades que ofrecen este tipo de redes. Estas últimas en la mayoría de los casos se ven afectadas en la práctica, y no cumplen con lo mínimo necesario para proporcionar un buen servicio.

Instalar y configurar una WLAN puede ser proceso sencillo pero, precisamente esto, lo convierte en un blanco fácil de ataques externos e internos que pueden poner en riesgo a la organización, ya que este tipo de redes utilizan el aire para su comunicación, estando expuestas a cualquier espía que con los dispositivos necesarios pueden interceptar la señal y utilizar los recursos de la red para su beneficio.

Esto se debe a la falta de planeación y un diseño pobre ante las amenazas de los usuarios intrusos que siempre están en la espera de un error durante la implementación de la WLAN.

> *Hasta el 2006, el 70 por ciento de los ataques exitosos a redes inalámbricas de área local WLAN se deberán a una configuración errónea de los puntos de acceso-AP y a la paquetería de los clientes.*
> *---GARTNER---*

Algunos programas de cómputo ayudan a predecir el comportamiento de la señal (análisis de propagación), y realizan un análisis de cobertura de acuerdo a las características del inmueble, éstos además que son costosos, solo contemplan el parámetro cobertura de la señal. De manera aislada existen procedimientos que ayudan a establecer un mecanismo de seguridad aceptable para una WLAN. Sin embargo, no existen hoy en día una metodología o algún procedimiento que integre e indique durante el proceso de planeación los parámetros a considerar antes de implementar una red WLAN, como son: protección, cobertura, ancho de banda, aplicaciones, gestión, y equipos. Es a través de estos parámetros que se define una ruta crítica a seguir que ayude a construir un diseño óptimo de acuerdo a las características de la organización y del inmueble.

1.2.1 Caso de estudio

En la actualidad la Universidad Autónoma de Baja California (UABC) campus Ensenada cuenta con una Red Inalámbrica WLAN. Para fines de este trabajo será el objeto de estudio y se pretende hacer una comparación entre el diseño actual del campus Ensenada, la cual ya está en funcionamiento a partir de junio del 2006, y el diseño de la red inalámbrica que será construida en base a la metodología que este trabajo propone. En la figura 1.3 se muestra el mapa de cobertura de la red WLAN con la que cuenta la Universidad Autónoma de Baja California campus Ensenada.

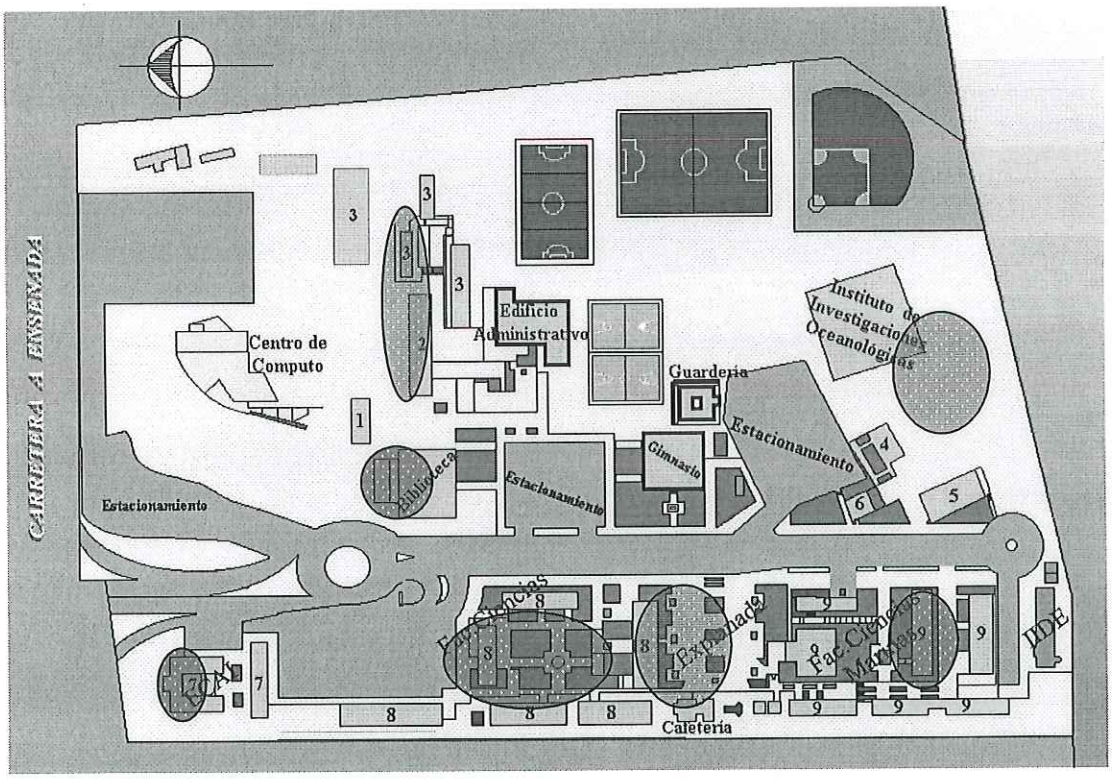


Figura 1.3: Red WLAN actual de la UABC campus Ensenada

1.3 Objetivos

1.3.1 Objetivo General

Elaborar una metodología que permita diseñar redes de área local inalámbricas del tipo IEEE 802.11, mediante la cual podamos implementar una WLAN en cualquier lugar de una manera óptima y segura.

1.3.2 Objetivos particulares

- Establecer la confiabilidad de la metodología realizando un comparativo entre el diseño elaborado por la metodología propuesta y una Wireless LAN existente: Caso de estudio de la *Universidad Autónoma de Baja California campus Ensenada.*

- Elaborar un documento que sirva como base al Departamento de Información Académica de la UABC, para realizar posibles modificaciones y adiciones a la red inalámbrica de la UABC, campus Ensenada.

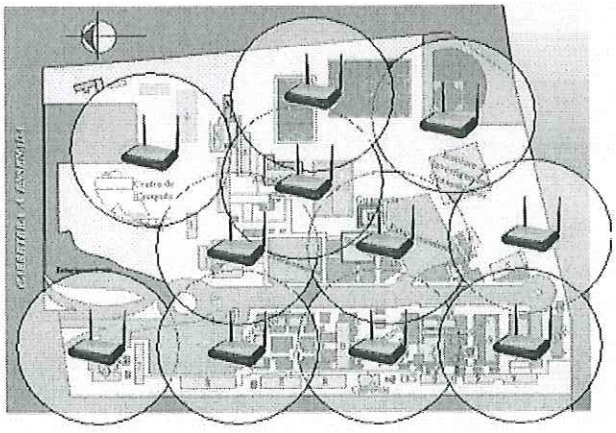


Figura 1.4: Distribución de los AP's en la UABC campus Ensenada.

1.4 Importancia del estudio

En un estudio realizado en la Facultad de Ciencias de la UABC entre el periodo 2003-2 al 2004-2, se identificaron varios factores que tendrían que considerarse en el diseño y planeación de una red WLAN. A continuación se hace un listado de éstos.

1. Ancho de banda y velocidad de transmisión.
2. La frecuencia de operación.
3. Aplicaciones que correrán sobre la WLAN.
4. Máximo número de usuarios.
5. Área de cobertura.
6. Material con el que están construidos los edificios.
7. Conexión de la WLAN con la red cableada.
8. Disponibilidad de productos en el mercado [3].

Estos factores fueron la base para establecer los seis componentes que este trabajo propone para elaborar una metodología, que nos permita poder diseñar redes de área local inalámbricas para cualquier lugar donde se requiera. Las necesidades reales de la organización se encuentran determinadas en solo seis componentes que define esta metodología, en base a estos componentes, se establece un diseño y se procede a su implementación. Ver figura 1.5.

Figura 1.5: Componentes que integra la metodología.

Es de suma importancia contar con un diseño confiable que permita implementar una WLAN que cumpla con las expectativas de los usuarios, y a su vez, reflejar la importancia que tiene el uso de esta tecnología en el trabajo diario de la organización.

Con este trabajo se pretende proponer una metodología que cualquier organización, empresa, institución educativa, hogar, etc, puedan utilizar durante el proceso de planeación y diseño de una Red Inalámbrica. Esta metodología que se propone contempla los elementos o parámetros necesarios que se tienen que consideran para que se tenga un diseño confiable, seguro, con una cobertura real, fácil gestión, con un ancho de banda que debe ser compartido para todos, aplicaciones acordes a las requeridas por la organización, y equipos modernos con capacidad para soportar los nuevos estándares que permitan que lo anterior sea posible.

1.4.1 Importancia del caso de estudio

El departamento de información académica (DIA) de la UABC está totalmente convencido que se requiere de una propuesta de diseño que ayude al crecimiento ordenado de la red inalámbrica actual, con una planeación y definiendo los criterios que nos ayuden en un futuro a contar con una administración y un control adecuado. Es necesario también contar con estadísticas que coadyuven al valoramiento y desempeño de la red inalámbrica actual, la cual fue implementada en junio del 2006, y de la cual no se han evaluado sus resultados. Durante la investigación de este trabajo se aplicó una encuesta a los usuarios (alumnos, maestros, investigadores, técnicos, administrativos) para establecer un juicio real del uso y el desempeño de esta red del campus Universitario.

1.5 Limitaciones del estudio

- Se tomará como objeto de estudio la red inalámbrica con la que cuenta la UABC para el c*ampus* Ensenada (*km. 103 Carretera Tijuana - Ensenada*). El cual puede quedar como prototipo para extenderse y replicarse posteriormente a otros campus universitarios de la UABC en el estado.

- Se utilizarán equipos ya existentes para realizar los estudios de cobertura y poder mostrar resultados comparativos entre AP's de diferentes compañías.

- Se utilizarán herramientas de uso libre, adicionales al software de los equipos para medir la potencia de la señal en puntos estratégicos.

- Existen diferentes estándares que permiten implementar este tipo de redes, para este estudio se limitará al estándar IEEE 802.11b.

1.6 Organización de la tesis

La organización de esta tesis estará dada primero con un estudio del estado del arte referido a redes inalámbricas y un análisis de los modelos de propagación en redes inalámbricas. Posteriormente se establecen los mecanismos de seguridad que hasta el día de hoy son utilizados para contrarrestar las vulnerabilidades que presentan las redes inalámbricas. Enseguida se establecen los parámetros que integra esta metodología. Para comprobar el diseño, se trabajara con la red inalámbrica la UABC y se compararán los diseños.

El capítulo 2 está dedicado a mostrar una introducción de los conceptos básicos de las redes inalámbricas. En él se definen los fundamentos teóricos que influyen en la propagación de señales de radiofrecuencia.

El capítulo 3 realiza una visión general del estado del arte de los sistemas utilizados. Para ello, se han seleccionado un conjunto de modelos que son representativos, los cuales son utilizados para la preedición de la señal en espacios abiertos y cerrados. De cada uno de estos sistemas, se lleva a cabo una pequeña descripción de sus características.

En el capítulo 4 se analiza detalladamente cada uno de los mecanismos de seguridad, presenta una visión clara del funcionamiento de cada mecanismo. Se describe las modificaciones que a lo largo de la evolución del estándar 802.11 se le han hecho para hacerlo menos vulnerable.

En el capítulo 5 se describirá el la metodología que se propone, así como cada uno de sus componentes que lo conforman. Esta metodología plantea una ruta crítica que el diseño debe contemplar para su buen desempeño.

En el capítulo 6 se realiza un análisis geográfico del inmueble, se presentan gráficas de cobertura de la señal de la red inalámbrica, se presentan los resultados de las encuestas realizadas sobre el uso y desempeño de la red inalámbrica instalada actualmente en el campus Ensenada.

En el capítulo 7 se realiza un comparativo entre el diseño actual de la red WLAN de la Universidad Autónoma de Baja California, campus Ensenada y el diseño que se propuso en base a esta metodología que se plantea en este trabajo. De acuerdo a los resultados se evalúa su confiabilidad.

El capítulo 8 nos enfocaremos a las conclusiones recomendaciones y trabajo futuro.

Capítulo II

2. REDES INALÁMBRICAS WLAN

2.1 Introducción

El uso de las redes ha crecido y se ha extendido por todas partes del mundo de forma notoria, todo esto debido a que son eficaces ya que todos los usuarios que están conectados a una red, ya sea pública o privada, pueden utilizar y compartir los mismos datos, lo que ahorra dinero y mejora la productividad en las organizaciones.

Anteriormente los cables que conectaban a los equipos eran difíciles de colocar, resultaban antiestéticos, pero actualmente con las redes inalámbricas todo esto se ha vuelto mucho más sencillo y barato.

WLAN (Wireless Local Area Network) es una tecnología de acceso inalámbrico a redes de comunicaciones electrónicas de ámbito reducido o de área local. El término Wi-Fi (Wireless Fidelity) surge como marca de certificación de conformidad con estándares WLAN. En los últimos tiempos el término Wi-Fi se ha popularizado y en muchos casos se utiliza para

referirse directamente al acceso al Internet inalámbrico de alta velocidad, como un sinónimo de WLAN.

La tecnología WLAN surge como catalizador de los avances en las redes de alta velocidad de acceso a Internet. Las tecnologías inalámbricas abren inmensas posibilidades con su capacidad de permitir compartir fácilmente el ancho de banda de acceso a Internet.

Los elementos básicos para formar una red inalámbrica WLAN son:

- Tarjeta de Red (NIC) con acceso inalámbrico: El NIC es la interfase entre los clientes del sistema y el punto de acceso (AP), para crear una conexión transparente a la red.

- Punto de Acceso (AP): El punto de acceso es un equipo inalámbrico similar al Hub, un AP es típicamente conectado la LAN cableada a través de un cable estándar Ethernet y se comunica con los dispositivos inalámbricos por medio de una antena. El punto de acceso se encarga de establecer las conexiones de los clientes que se encuentran a través de su área de cobertura permitiendo o negando el tráfico hacia el interior de la red.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles (computadoras personales, laptops, teléfonos celulares, PDAs). Ver figura 2.1. Esto permite al usuario viajar a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) sin perder el acceso a los datos de la red.

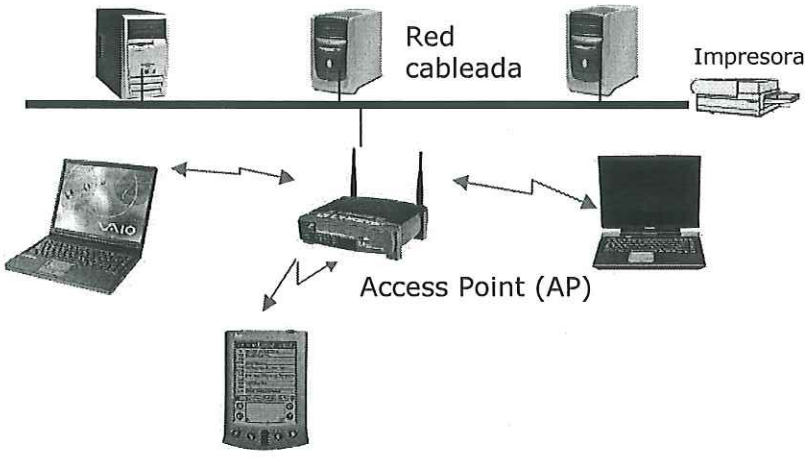


Figura 2.1: Red de Área Local Inalámbrica (WLAN).

En síntesis, frente a las redes tradicionales, las redes inalámbricas tienen algunas ventajas en cuanto a productividad, comodidad y costos. Algunas de estas ventajas o beneficios se listan a continuación:

- **Movilidad:** información en tiempo real en cualquier lugar de la organización o 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 tirar cable por muros y techos.
- **Flexibilidad:** permite llegar donde el cable 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.

2.1.1 Evolución histórica de las WLAN

En los principios de los años 80' tanto la industria como universidades descubrieron los beneficios y eficiencias de la redes de computadoras. El compartir información entre computadoras aumentó las posibilidades de hacer negocio, realizar proyectos inter-disciplinarios, comunicación a través de aplicaciones tales como correo electrónico, por mencionar algunas de las ventajas que ofrece la conectividad entre computadoras.

Sin embargo, no todas las redes de computadoras eran compatibles entre sí, ya que fabricantes lanzaban al mercado diferentes protocolos o formas de comunicar propietarias que de alguna manera no era viable la comunicación entre diferentes redes. Todo esto llevó a que se reunieran grupos de trabajo de diferentes fabricantes, líderes en el ramo, para estandarizar protocolos de comunicación para que las redes fueran compatibles y pudiese existir mayor demanda, productividad, desarrollo y eficiencia hacia el usuario final.

El estándar que actualmente predomina en el mercado de las Redes de Área Local es Ethernet, que fue adoptado por la misma gente (estándar de facto) debido a que es muy fácil de implementar, bajo costo, entre otras características. El protocolo Ethernet esta definido en el estándar IEEE 802.3. El protocolo que actualmente predomina es TCP/IP, que de igual manera que Ethernet se ganó el mercado debido a sus características de fácil implementación, aunque hay que recordar que el diseño de TCP/IP es vulnerable a ciertos ataques, eso no importó para que fuera el dominante de las redes de comunicación. En la década los 90's se vio un gran avance con estas dos tecnologías (Ethernet y TCP/IP) que ahora apunta al futuro

de la nueva generación tecnológica, es decir, la integración de tecnologías estará basada en el protocolo IP [7].

Por otro lado, a finales de la década de los 90's comenzó el fenómeno de las redes de área local inalámbricas (WLAN). En esta década dos avances tecnológicos ayudaron su crecimiento, ancho de banda y alcance de comunicación entre los dispositivos.

Así como existieron protocolos de comunicación propietarios que no permitían la comunicación entre diferentes redes, sucedió lo mismo con las nuevas redes inalámbricas. Es por eso que el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) comenzó a desarrollar estándares para las comunicaciones inalámbricas para asegurar la interoperabilidad entre dispositivos de diferentes fabricantes.

La IEEE es una organización que participa en el desarrollo de estándares para los sistemas de transmisión de datos ha logrado desarrollar la familia de estándares 802.x para estandarizar las comunicaciones en redes de área local (LAN).

Así como las redes de computadoras cableadas (LAN), la tecnología de redes inalámbricas (WLAN, por sus siglas en ingles) ha evolucionado de un modelo propietario a uno estandarizado. La mayoría de los estándares utilizados en WLAN están basados en los estándares desarrollados para las LAN.

En 1997 la IEEE hace público el estándar 802.11 para WLAN, esta versión ofrece velocidades de transmisión de 1 Mbps y 2 Mbps. Debido a la necesidad de mayor velocidad

de transmisión y ancho de banda que las aplicaciones demandaban y que los mismos usuarios necesitaban, la IEEE ratifica un nuevo estándar llamado 802.11b de alta velocidad para transmisión de datos hasta de 11 Mbps.

Sin embargo, en 1999 la IEEE ratifica otro nuevo estándar conocido como 802.11a que alcanza velocidades hasta los 54 Mbps permitiendo así el uso de aplicaciones que utilizan gran ancho de banda y ofreciendo más conectividad de usuarios.

Pero no todo el trabajo es por parte de la IEEE, es decir, líderes de la industria en redes inalámbricas se unieron para formar la WECA (Wireless Ethernet Compatibility Allieance) hoy conocida como Wi-Fi Alliance (Wireless Fidelity Alliance) que en Octubre del 2002 adquirió el nuevo nombre [8][9]. La Wi-Fi Alliance es una organización no-lucrativa que certifica la interoperabilidad de equipos para red inalámbrica basados en los estándares 802.11 de la IEEE [8]. Algunos fabricantes de equipo para WLAN's que pertenecen a la Wi-Fi Alliance son: 3Com, Aironet, Apple, Breezecom, Cabletron, Compac, Dell, Fujitsu, IBM, Intersil, Lucent Technologies, NoWires Hended, Nokia, Samsung, Symbol Technologies, Wayport, y Zoom [10].

En la primavera del 2003 la IEEE ratificó el estándar 802.11g que tiene como característica principal el tomar lo mejor de los estándares 802.11a y 802.11b. Este nuevo estándar es una variante del estándar 802.11b, ya que trabaja en la misma frecuencia de 2.4 GHz del estándar 802.11b y utiliza el mismo tipo de modulación y las mismas velocidades de transmisión del estándar 802.11a.

Tabla II. Familia de Estándares IEEE 802.11

Estándar	Definición
IEEE 802.11	WLAN estándar original para la banda 2.4 GHz soporta de 1Mbps a 2 Mbps
IEEE 802.11a	WLAN estándar de alta velocidad para la banda 5 GHz soporta hasta 54 Mbps
IEEE 802.11b	WLAN estándar llamado Wi-Fi par la banda 2.4 GHz soporta hasta 11Mbps
IEEE 802.11c	Cruce sin cables
IEEE 802.11d	"Modo mundial", adaptación a los requerimientos regionales
IEEE 802.11e	QoS y extensiones en la transferencia entre 802.11a/g/h
IEEE 802.11f	Define la Comunicación entre puntos de acceso (AP)
IEEE 802.11g	WLAN estándar de alta velocidad para la banda 2.4 GHz soporta 54 Mbps
IEEE 802.11h	Define la técnica de manejo del espectro para el 802.11a
IEEE 802.11i	Funciones específicas para WLAN que operan en combinación con el 802.1x y encriptación AES
IEEE 802.11j	802.11a con canales adiciones por encima de 4.9 GHz, "11a Japón"
IEEE 802.11k	Intercambio de información de capacidad entre clientes y puntos de acceso
IEEE 802.11m	Mantenimiento publicación de actualizaciones del estándar
IEEE 802.11n	Nueva generación de WLAN, de al menos 100 Mbps

La próxima generación de WLAN espera ofrecer velocidades de hasta 162 Mbps, el comité IEEE 802.11 trabaja sobre este nuevo estándar el 802.11n. Este sistema usa tres antenas de transmisión/recepción para incrementar la transferencia de información. MIMO (entrada múltiple / salida múltiple) es el nombre de la tecnología que hace posible este incremento en la velocidad, existen algunos prototipos de compañías que se adelantaron y sacaron sus equipos, sin embargo se espera que este nuevo estándar sea ratificado en el 2008[11]. En la tabla II, se muestra un resumen histórico de la evolución del estándar 802.11 con todas sus variantes.

2.1.2 Arquitectura.

Como todos los estándares 802.x de la IEEE, el estándar 802.11 se basa en los dos niveles más bajos de modelo OSI, la capa física y la capa de enlace de datos, ver Figura 2.2. Cualquier aplicación de red, sistema operativo de red o protocolo, incluyendo TCP/IP y Novell Netware, son soportados por el 802.11 tal como se hace con Ethernet [12].

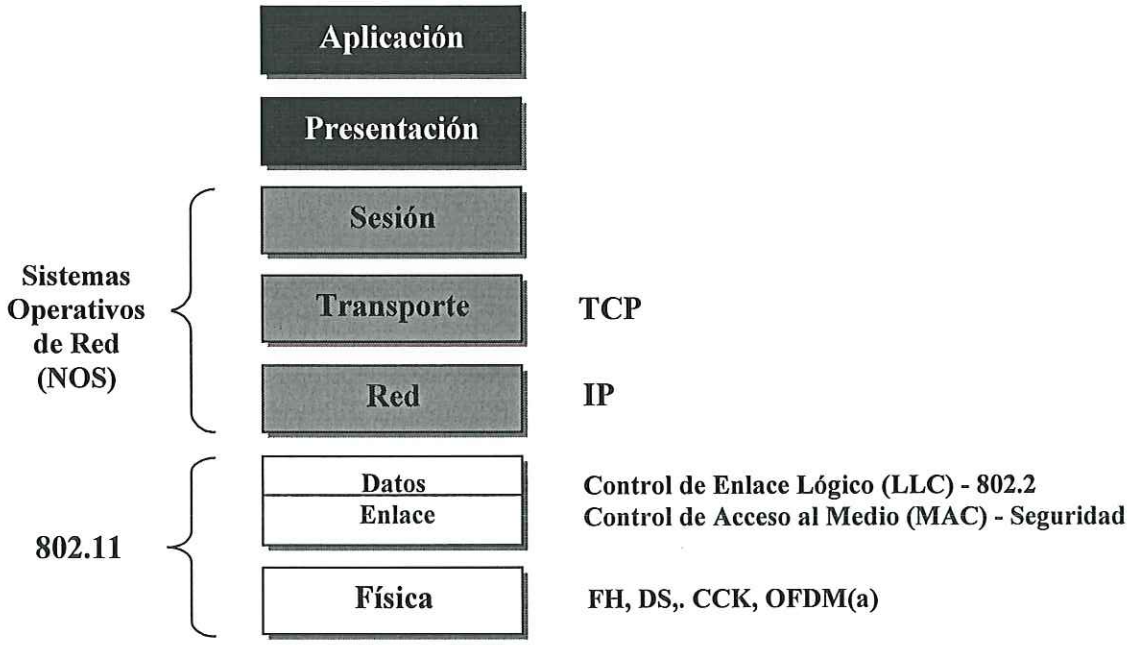


Figura 2.2: Representación del estándar 802.11 en el modelo OSI

El estándar 802.11 define dos tipos de equipos esenciales, una estación inalámbrica, que usualmente es una PC equipada con una interfase de red inalámbrica (NIC), y un punto de acceso (AP), el cual actúa como puente entre la red inalámbrica y la cableada. Un punto de acceso usualmente consiste de un radio, una interfaz Ethernet (802.3), y un software de puente conforme al estándar 802.1d. El punto de acceso actúa como la estación base para la

WLAN, dando acceso a múltiples estaciones inalámbricas a la LAN. La estación final en una WLAN podrían ser tarjetas 802.11 para laptop (PCMIA), antenas externas USB, PCI, o ISA.

2.1.2.1 Capa física

La capa física de cualquier red define la modulación y la señalización características de la transmisión de datos. Como se ha mencionado anteriormente, los métodos de RF operan en la banda de frecuencia de 2.4 GHz, ocupando aproximadamente 83 MHz de ancho de banda entre los 2.400 y 2.483 GHz. El nivel de potencia máximo permitido en este rango de frecuencias varía de un país a otro, según sus normas regulatorias. Así en Estados Unidos la FCC (Federal Communication Commission) limita la radiación de antena a 1W de potencia. La IEEE 802.11 define tres posibles opciones para la elección de la capa física para la transmisión y recepción de tramas 802.11:

- Espectro disperso por secuencia directa o DSSS (Direct Sequence Spread Spectrum)
- Espectro disperso por salto de frecuencias o FHSS (Frequency Hopping Spread Spectrum)
- Luz infrarroja en banda base -sin modular-.

En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación por un lado, y prestaciones y fiabilidad por otra.

Espectro disperso por salto de frecuencia (FHSS)

La tecnología de espectro disperso por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamado *dwell time* inferior a 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo, ver figura 2.3.

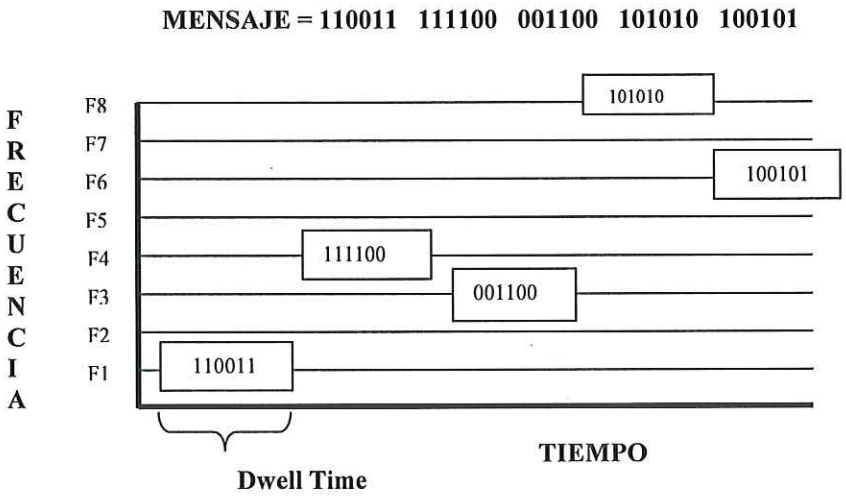


Figura 2.3: Trama transmitida por FHSS

El orden en los saltos en frecuencia se determina según una secuencia pseudo aleatoria almacenada en unas tablas, que tanto el emisor y el receptor deben conocer. Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en el tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación.

Espectro disperso por secuencia directa (DSSS)

DSSS es el segundo nivel físico soportado por el 802.11 y el único especificado en el 802.11b, soportando velocidades de transmisión de 5.5 y 11 Mbps. En el caso de Estados Unidos y Europa, la tecnología DSSS utiliza un rango de frecuencias que va desde los 2.4 GHz hasta los 2.4835 GHz, lo que permite tener un ancho de banda total de 83.5 MHz. Este ancho de banda se subdivide en canales de 5 MHz, lo que hace un total de 14 canales independientes. Cada país esta autorizado a utilizar un subconjunto de estos canales. En Europa existen 13 canales disponibles (excepto en Francia) aunque tan solo 3 non están traslapados. En el a 802.11 debe existir una separación de 30 MHz entre las frecuencias centrales de los canales si las celdas se traslapan y/o son adyacentes para no causar interferencias. En 802.11b la separación se reduce a 25 MHz. Esto significa que pueden existir 3 celdas con zonas traslapadas y/o adyacentes sin causar interferencias entre ellas, tal y como se muestra en la Figura 2.4.

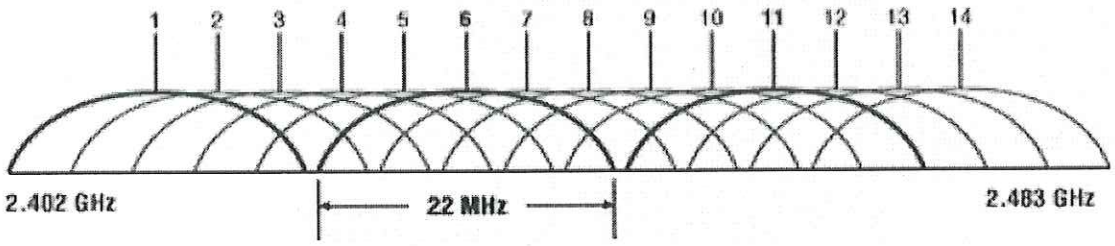


Figura 2.4: Canales DSSS

El estándar 802.11b utiliza DSSS en la banda de 2.40 GHz y la estructura de canales diseñada en el estándar 802.11. La principal diferencia entre los dos estándares está en que 802.11b utiliza modulación CCK (Complementary Code Keying) para las velocidades de 5.5 Mbps y

11 Mbps. El 802.11b soporta también las velocidades de 1 Mbps y 2 Mbps, por lo que tiene compatibilidad hacia atrás con dispositivos 802.11.

Modulación por división ortogonal de frecuencias (OFDM)

La Multicanalizacion por división de frecuencia ortogonal (OFDM, Orthogonal Frecuency División Multiplexing – por sus siglas en ingles), se utiliza para transmitir datos en la banda de frecuencia de 5 GHz. Este tipo de modulación no solo provee una velocidad de transmisión alta, si no que también, mejora el eco y distorsión de la transmisión que resulta de la propagación de multitrayectorias y la interferencia de la frecuencia de radio.

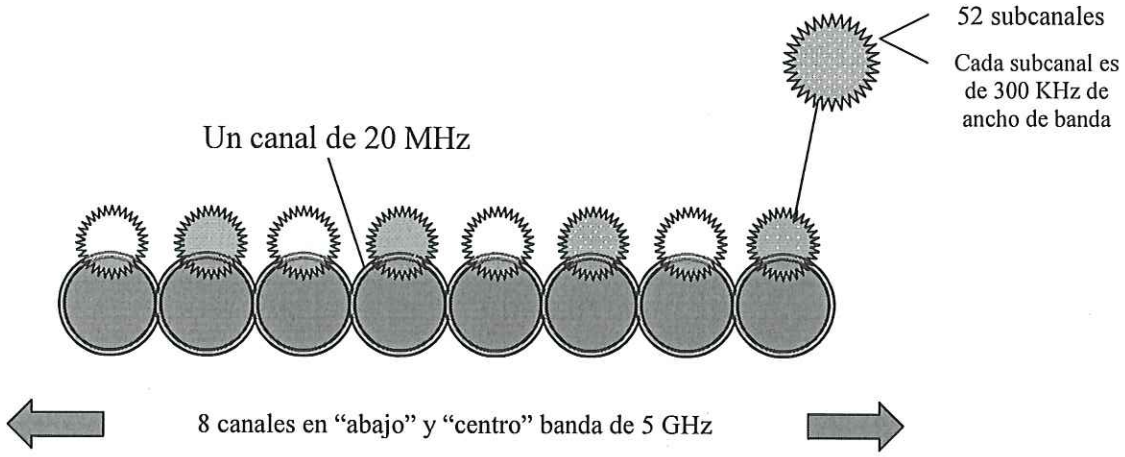


Figura 2.5: OFDM, 8 canales de 20 MHz

El radio espectro es dividido en ocho canales o segmentos de red de 20 MHz. Cada canal puede soportar un cierto número de usuarios. Cada usuario individualmente puede comunicarse con cualquier otro usuario del segmento de red. La red soporta 54 Mbps de

caudal eficaz por canal para compartir dispositivos en el mismo canal en cualquier punto del tiempo. Ver figura 2.5.

Las tecnologías 802.11a y 802.11b definen una capa física diferente. Los emisores 802.11b transmiten a 2.4 GHz y envían datos a tasas tan altas como 11 Mbps usando modulación DSSS; mientras que los emisores 802.11a y 802.11g transmiten a 5 y 2.4 GHz respectivamente y envían datos a tasas de hasta 54 Mbps usando OFDM.

OFDM es una tecnología de modulación digital, una forma especial de modulación multi-portadora (multi-carrier) considerada la piedra angular de la próxima generación de productos y servicios de radio frecuencia de alta velocidad, para uso tanto personal como corporativo. La técnica de espectro disperso de OFDM distribuye los datos en un gran número de portadoras (carriers) que están espaciados entre sí en distintas frecuencias precisas. Ese espaciado evita que los demoduladores vean frecuencias distintas a las suyas. OFDM tiene una alta eficiencia de espectro y menor distorsión de multitrayectorias. Actualmente OFDM no sólo se usa en las redes inalámbricas LAN 802.11a y 802.11g, si no también en comunicaciones de alta velocidad por vía telefónica como ADSL y en difusión de señales de televisión digital terrestre en Europa, Japón y Australia.

2.1.2.2 Control de acceso al medio (MAC)

La capa de acceso al medio en 802.11 se encarga de proporcionar un servicio de datos fiable a los usuarios de esta capa (es decir, a los protocolos de capas superiores) y al mismo tiempo permitir un acceso equitativo al medio inalámbrico compartido. Para la descripción de esta capa consideraremos un servicio básico compuesto por un punto de acceso y diferentes estaciones asociadas al mismo.

Para proporcionar un acceso fiable, el estándar 802.11 define un protocolo para el intercambio de tramas de información [13]. La secuencia mínima en este intercambio consistiría en el envío de una trama de información del origen al destino y un reconocimiento (ACK - *Acknowledgment*) enviado por el destino en el caso de que la primera trama haya sido recibida correctamente. Todas las tramas a nivel MAC incorporan un campo de control de errores (FCS - *Frame Check Sequence*, IEEE 32-bit CRC) que es comprobado en cada recepción. Si la fuente no recibe el reconocimiento o el campo de control falla, la trama es reenviada. Aunque este mecanismo consume cierto ancho de banda, permite hacer frente a los posibles errores provocados por el medio inalámbrico.

Adicionalmente a este mecanismo básico de intercambio de tramas, existe una alternativa que proporciona una mayor robustez al protocolo y permite afrontar el problema de los 'nodos ocultos'. Este mecanismo es conocido por las siglas de las tramas que utiliza, RTS/CTS. Una estación que estuviese haciendo uso de este mecanismo debería mandar una trama RTS (*Request To Send*) al destino antes de transmitir cualquier trama de datos (MSDU – *MAC Service Data Unit*). Una vez que el destino recibe esta trama correctamente entonces debe

responder con otra trama llamada CTS (*Clear To Send*). A partir de este momento la fuente podría comenzar a mandar las tramas MSDU ver figura 2.6.

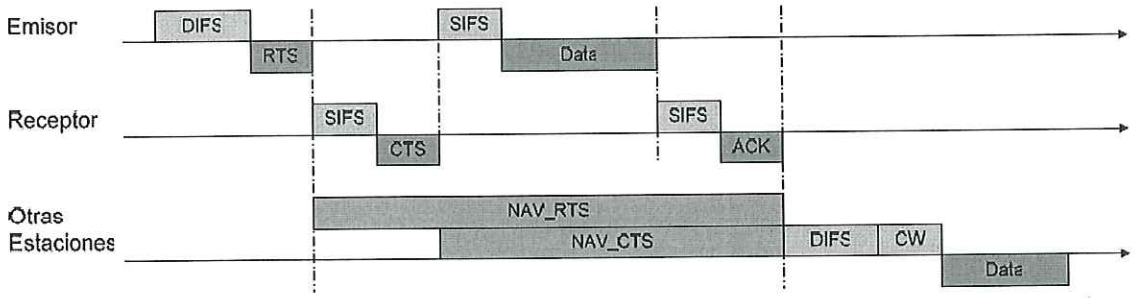


Figura 2.6: Problema RTS/CTS.

Todas las tramas, incluidas las RTS y CTS, contienen información sobre la duración de la transmisión MSDU/ACK. De forma que basándose en esta información todas las estaciones presentes pueden actualizar un contador interno llamado NAV (*Network Allocation Vector*) y retrasar cualquier transmisión hasta que el contador expire. Aunque una estación oculta no pueda escuchar la trama RTS enviada por la fuente, será capaz de recibir la trama CTS con la que responde el destino de forma que pueda actualizar el contador NAV adecuadamente

2.1.3 Topologías

El estándar 802.11 de la IEEE soporta tres tipos de topologías básicas para las WLAN's

IBSS (Independent Basic Service Set).

BSS (Basic Service Set).

ESS (Extended Service Set).

2.1.3.1 Topología IBSS

La topología IBSS consiste en una configuración independiente o red de tipo ad-hoc. Lógicamente la configuración IBSS es similar a una red punto a punto en la cual ninguno de los nodos requiere funcionar como un servidor. La topología IBSS incluye n nodos o estaciones inalámbricas las cuales se comunican directamente una con otra utilizando las bases de ad-hoc pero sin utilizar un punto de acceso (AP) o cualquier tipo de conexión con cable. Ver figura 2.7. Es usualmente fácil y rápido de configurar una red de este tipo en cualquier lugar donde no exista una red de tipo infraestructura y donde no se requieran tantos servicios, tales como centro de convenciones, aeropuertos o cualquier lugar donde no se tenga acceso a una red cableada. Generalmente esta topología cubre un área limitada.

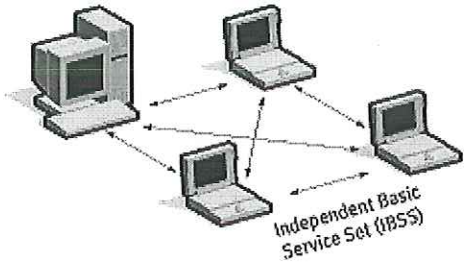


Figura 2.7: Conjunto de Servicios Básicos independientes (IBSS)

2.1.3.2 Topología BSS

La topología BSS consiste en tener un punto de acceso (AP) conectado a la infraestructura de una red LAN y un número de estaciones inalámbricas. Este tipo de topologías están apoyadas

por un punto de acceso que actúa como el servidor para una célula WLAN. La comunicación entre un nodo A y nodo B fluye del nodo A hacia el punto de acceso y del punto de acceso al nodo B. Ver figura 2.8.

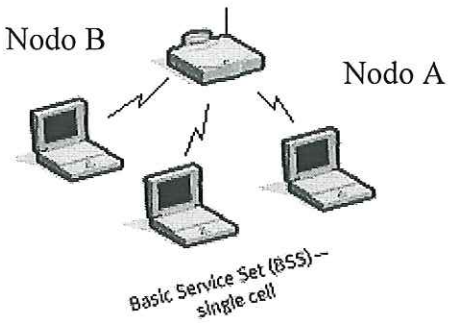


Figura 2.8: Conjunto de Servicios Básicos (BSS)

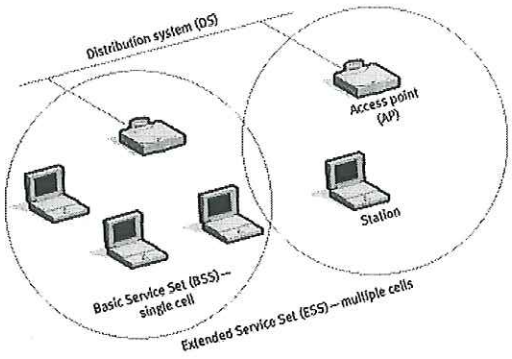


Figura 2.9: Conjunto de Servicios Extendido múltiples celdas (ESS)

2.1.3.3 Topología ESS

La topología ESS consiste en una serie de traslapes de la topología BSS (cada una contiene un punto de acceso AP) conectadas en conjunto por un sistema distribuido (DS), aunque el sistema distribuido podría ser cualquier tipo de red, es casi invariable a una red Ethernet. Los nodos pueden comunicarse con los puntos de acceso y así es como se le puede dar cobertura a un Campus-LAN [14]. Ver figura 2.9.

2.1.3.4 Topología de malla (Mesh Wireless Networks)

La evolución de las WLAN aun continua en sus diferentes variantes del estandar 802.11. El grupo de trabajo conocido como Wi-Mesh Alliance (WiMA), está conformado por compañías como Nortel, Thomson, Philips e InterDigital, entre otras. Este grupo trabaja en una nueva especificación conocida como IEEE 802.11s, que aún se encuentra en desarrollo. Las Wi-Fi en malla o también conocidas como redes Mesh son diseñadas para poder ser usadas tanto por usuarios independientes y pequeñas empresas como por municipios e incluso para aplicaciones militares.

La topología de las redes Mesh cada nodo puede estar conectado a uno o más nodos, a través de este mecanismo es posible llevar un mensaje de un nodo a otro por diferentes caminos. Según la normativa 802.11 actual, una infraestructura Wi-Fi compleja es interconectada usando LANs fijas de tipo Ethernet usando un cable UTP. El estándar 802.11s en cambio utiliza un protocolo de auto-configuración de rutas entre puntos de acceso mediante topologías multisalto, con el objeto de que los puntos de acceso se puedan comunicar entre ellos, ver figura 2.10. Dicha topología constituirá un WDS (Wireless Distribution System) que deberá soportar tráfico unicast, multicast y broadcast. Para ello se realizarán modificaciones en las capas física y MAC del 802.11 y se sustituirá la especificación BSS (Basic Service Set) actual por una más compleja conocida como ESS (Extended Service Set).

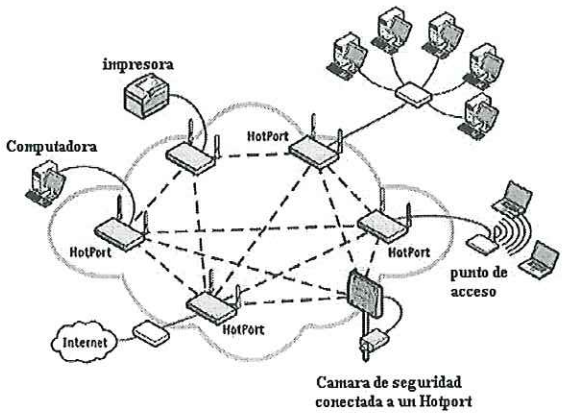


Figura 2.10: Red de Malla para redes WLAN

En noviembre de 2006 aparecieron los primeros borradores que serían aprobados en enero de 2007. Aún así, se prevé que la publicación del estándar se demore, como mínimo, hasta octubre de 2008, aunque los detalles técnicos podrán estar acabados a mediados de ese año [15].

2.1.4 Aplicaciones de las WLAN

Las aplicaciones de las redes de área local inalámbricas que podemos encontrar actualmente son muy variadas:

1. Entornos difíciles de cablear. Implementación de redes de área local en edificios históricos, de difícil acceso y en general en entornos donde la solución cableada no es viable.

2. Posibilidad de reconfiguración de la topología de la red sin añadir costos adicionales. Esta solución es muy típica en entornos dinámicos que necesitan una estructura de red flexible que se adapte a estos cambios.
3. Redes locales para situaciones de emergencia o congestión de la red cableada.
4. Entornos en los que se debe permitir el acceso a la información mientras el usuario se encuentra en movimiento y en tiempo real. Por ejemplo en hospitales, fábricas, almacenes, etc.
5. Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo (exposiciones, acontecimientos deportivos, zonas catastróficas, entre otros).
6. En ambientes industriales con severas condiciones ambientales, este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
7. Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes cableadas de área local situadas en dos edificios distintos.
8. Actualmente las que más se están explotando son las denominadas Zonas Wi-Fi, que son lugares públicos donde las WLAN ofrecen conexión a Internet: aeropuertos, estaciones de ferrocarril, auditorios de congresos, hoteles y otros lugares públicos.
9. Gobiernos y municipios locales, al igual que las instituciones educativas como universidades también ven esto como una gran oportunidad para proporcionar un servicio de valor a agregado.

2.1.5 Otras tecnologías inalámbricas.

Existen otras tecnologías para WLAN como HiperLAN tipos 1 y 2 y HomeRF. HiperLAN es un estándar ratificado por la ETSI (European Telecommunications Standards Institute), organización que se encarga de estandarizar las telecomunicaciones en todo el continente Europeo [16], además, HiperLAN es un estándar similar al 802.11 utilizado en Estados Unidos de América (EUA).

HiperLAN tipo 1 - Soporta la movilidad de los usuarios dentro de un espacio limitado alrededor de 50 metros y el flujo de datos que permite alcanza los 20 Mbps en un espectro de frecuencia en los 5 GHz.

HiperLAN tipo 2 es una variante de HiperLAN 1. Ofreciendo accesos a alta velocidad de 54 Mbps, trabajando en la banda de los 5 GHz.

HomeRF es una especificación realizada por el Grupo de Trabajo HomeRF (HRFGW), quien está compuesto por líderes de la industria en redes inalámbricas. Esta especificación está orientada para uso en el hogar y pequeñas oficinas, operando a 10 Mbps y en el espectro de frecuencia de 2.4 GHz [17].

2.2 Familia de estándares 802.11

2.2.1 Estándar 802.11

Banda de Frecuencia

El estándar original 802.11 trabaja a velocidades de 1 Mbps y 2 Mbps por medio de ondas de radio utilizando espectro disperso por salto de frecuencia (FHSS por sus siglas en ingles) o espectro disperso de secuencia directa (DSSS por sus siglas en ingles). Es importante mencionar que FHSS y DSSS son fundamentalmente mecanismos de transmisión diferentes incompatibles entre sí.

Modulación

Utilizando FHSS el 802.11 trabaja en la banda de los 2.4 GHz la cual se divide en 75 subcanales de 1 MHz. La técnica FHSS está limitada en velocidad a 2 Mbps. Estas limitaciones son manejadas primordialmente por las regulaciones de la FCC que restringen subcanales de ancho de banda a 1 MHz. En contraste, las técnicas de señalización de secuencia directa divide la banda de 2.4 GHz en 14 canales de 22 MHz de los cuales solo podemos utilizar tres canales libres de ruido para la transmisión.

Rango y Velocidades de Transmisión

El estándar 802.11 alcanza velocidades 1 Mbps y 2 Mbps en un rango de 2.412 GHz a 2.462 GHz (definido por la FCC) y para México es 2.4 GHz a 2.5 GHz [18].

Control de Acceso al medio (MAC)

El control de acceso al medio de 802.11 es muy parecido en concepto al 802.3 (Ethernet), que es diseñado para soportar múltiples usuarios sobre un medio compartido, censando el medio antes de accesarlo. El estándar 802.11 hace uso del protocolo de acceso múltiple con sensado de portadora con evasión de colisión (CSMA/CA) para el control de acceso al medio. CSMA/CA intenta evitar la colisión de paquetes mediante la autorización de tiempo y la prioridad para transmisión de información.

2.2.2 Estándar 802.11a

El estándar de 802.11a trabaja con velocidades de hasta 54 Mbps. La banda de frecuencia en la cual trabaja este estándar es 5 GHz. El tipo de modulación que implementa hacen posible que este estándar transmita a mayor velocidad y con menos interferencia en el envió de los datos.

El estándar 802.11a es rápido, robusto y flexible. Algunas ventajas con respecto al IEEE 802.11b, son [19]:

- Cinco veces mas rápido su velocidad.
- Hasta treinta veces más de capacidad.
- Habilidad de conectarse al mundo inalámbrico.
- Posibilidad de trabajar con instalaciones 802.11b (utilizando AP's dual).
- Mejor velocidades de transmisión a menores distancias.

Banda de Frecuencia

El estándar 802.11a para WLAN's trabaja en los 5 GHz del espectro de frecuencias desde 5.15-5.825 GHz, con velocidades hasta 54 Mbps. Utiliza un ancho de banda de 300 MHz en la U-NII (Unlicensed National Information Infrastructure), en México se utilizan las frecuencias 5.725-5.850 GHz [20].

Modulación

El estándar 802.11a utiliza multicanalización por división de frecuencia ortogonal (OFDM, Orthogonal Frecuency División Multiplexing – por sus siglas en ingles), para transmitir datos en la banda de frecuencia de 5 GHz, este tipo de modulación no solo provee una velocidad de transmisión alta, si no que también, mejora el eco de la transmisión y la distorsión que resulta de las multitrayectorias de propagación y la interferencia de la frecuencia de radio.

Los dispositivos utilizados en el 802.11a son requeridos para soportar velocidades de 6, 9, 12, 18, 24, 36, 48, o 54 Mbps. El 802.11a automáticamente decrementa la escala desde 54 Mbps dependiendo de la distancia y la carga de la red. Estas diferencias son el resultado de la implementación de las diferentes técnicas de modulación y los niveles del FEC (Forward Error Code). Un mecanismo llamado 64QAM (64-level Quadrature Amplitude modulation) es usado para empaquetar la información que viaja por el canal. En la figura 2.11, podemos observar el desempeño de la red a diferentes distancias.

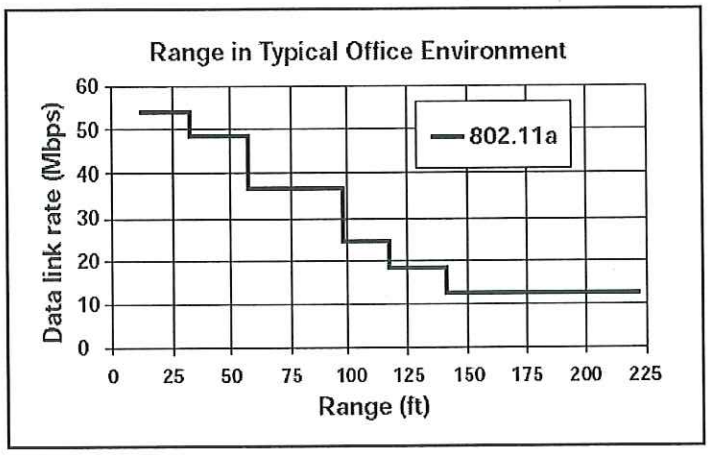


Figura 2.11: Cobertura del estándar 802.11a - Fuente [Intel]

Control de Acceso al Medio (MAC)

El 802.11a utiliza para el control de acceso al medio CSMA/CA. Este protocolo es usado para eliminar colisiones que se generen durante la transmisión del mensaje, éste trabaja mediante una autorización para poder trasmitir en un tiempo específico y con una prioridad [21].

2.2.3 Estándar 802.11b

Este estándar fue considerado en sus inicios como el estándar para la transmisión de datos a altas velocidades en WLAN's, donde los usuarios pudieran alcanzar niveles de desempeño, transmisión, y disponibilidad comparable con los usuarios de una LAN.

Uno de los puntos más críticos que ha detenido la demanda de WLAN's hasta el momento es la limitante de transmisión de datos. La arquitectura básica, características y servicios de 802.11b son definidos por el estándar 802.11 original con la diferencia de que 802.11b agrega velocidades más altas y una conectividad más robusta.

Banda de Frecuencia

El 802.11b se comunica utilizando ondas de radio debido a que estas ondas tienen una reflección alrededor de los obstáculos. El 802.11b trabaja en los 2.4 GHz del espectro de frecuencias, con una velocidad de hasta 11 Mbps. Este puede ser afectado por el medio en el

que se este utilizando y puede disminuir hasta velocidades de 5.5 Mbps o trabajar en las velocidades de 802.11 (2 Mbps – 1 Mbps).

Modulación

El estándar 802.11b utiliza DSSS esto nos permite trabajar en la banda de los 2.4 GHz dividiéndola en 14 canales de 22 MHz de los cuales solo tres pueden trasmitir libre de ruido.

Rango y Velocidades de Transmisión

802.11b soporta velocidades de hasta 11 Mbps, sin embargo, dependiendo de la distancia y carga que se trasmite en el medio se puede ver afectado de maneara en que sus velocidades se decrementan de 5.5, 2, hasta 1 Mbps. Para incrementar la velocidad de transmisión se emplean técnicas de codificación avanzadas como CCK (Complementary Code Keying) que consiste de grupos de 64 con palabras de código de 8bits. En la gráfica 2.12 podremos ver el desempeño de la red a diferentes distancias.

Control de Acceso al Medio (MAC)

El estándar 802.11b hace uso del protocolo CSMA/CA para el control de acceso al medio. El cual nos permite evitar colisiones generadas durante la transmisión. Su modo de operación es por medio de autorización de tiempo y la prioridad para transmisión de información.

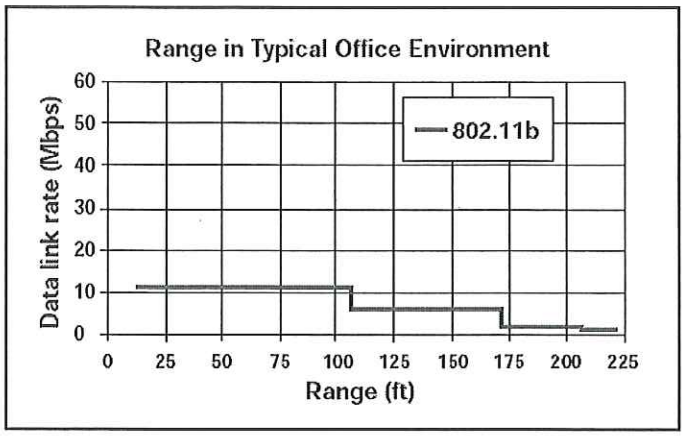


Figura 2.12: Cobertura del estándar 802.11b - Fuente [Intel]

2.2.4 Estándar 802.11g

El Grupo de Trabajo G de la IEEE se dedicó a explorar la nueva generación del estándar Ethernet inalámbrico 802.11g. Este estándar no estuvo finalizado sino hasta junio del 2003. El 802.11g llegó relativamente tarde al mercado inalámbrico. A pesar de esto, hoy por hoy es el estándar de facto en las redes inalámbricas existentes.

La interoperabilidad 802.11g con 802.11b es una de las razones principales de su masiva aceptación. Sin embargo, sufre el mismo problema en 802.11b con respecto a interferencia (demasiados puntos de acceso urbanos) debido a que funcionan en la misma banda de frecuencia.

El estándar 802.11g supera al estándar 802.11b en cuanto a la velocidad de transmisión, este estándar al igual que 802.11b tiene la desventaja de interferencia de señal, de tal forma que presenta los mismos problemas de interferencia con otros dispositivos, tales como, Bluetooth,

teléfonos inalámbricos, Walkie-Talkies para bebes, horno de microondas entre otros, pero tiene un alcance en velocidad arriba de los 20 Mbps.

Banda de Frecuencia

El estándar 802.11g toma lo mejor de los estándares 802.11a y 802.11b para crear productos intermedios. 802.11g opera en la banda de los 2.4 GHz que está sujeto a todas las regulaciones del 802.11b con tres canales de operación. Sin embargo, utiliza el esquema de modulación OFDM permitiendo así un desempeño en ancho de banda como 802.11a operando hasta 54 Mbps.

Modulación

802.11g usa la misma técnica de modulación que el 802.11a (ODFM) por lo tanto funciona con una tasa máxima de transferencia de datos de 54 Mbps. Para asegurar la interoperabilidad con el 802.11b, en las tasas de datos de los 5.5 y los 11 Mbps se revierte a CCK+DSSS (como 802.11b) y usa DBPSK/DQPSK + DSSS para tasas de transferencias de 1 y 2 Mbps.

Rango y Velocidades de Transmisión

802.11g ofrece un rango de operación de aproximadamente 33 metros o cerca de 100 pies, un rango menor que el 802.11b. Es importante señalar que la distancia puede variar dependiendo si se presentan algunos factores que obstruyan la señal como son algunos dispositivos que trabajan en la misma frecuencia.

Control de Acceso al medio (MAC)

802.11g utiliza el mismo tipo de MAC, CSMA/CA que 802.11a/b similar al MAC de Ethernet cableado. Algo muy importante es que 802.11g permite compatibilidad hacia atrás con los productos 802.11b.

2.2.5 Estándar 802.11c

Este estándar especifica métodos de conmutación inalámbrica, o lo que es lo mismo, métodos para conectar diferentes tipos de redes mediante redes inalámbricas.

2.2.6 Estándar 802.11d

Se le conoce como también como "método mundial" y se refiere a las diferencias regionales en tecnologías como a cuantos o cuales son los canales disponibles para usarse en las distintas regiones del mundo. Como usuario solo necesitamos especificar el país en el que queremos usar la tarjeta WLAN y el controlador se ocupa del resto.

2.2.7 Estándar 802.11e

De acuerdo a los problemas que presentaba el estándar IEEE 802.11 para el soporte de calidad de servicio, la IEEE puso en marcha un grupo de trabajo para revisar más profundamente esta problemática con el fin de hacerle algunas modificaciones y lograr así mejorar la calidad del servicio durante la transmisión de lo datos de una estación a otra.

El grupo de trabajo obtuvo como resultado una serie de modificaciones al estándar original de la IEEE 802.11 de 1999, en el cual incorpora nuevos términos como el de (QSTA – QoS Enhanced Station) que es el nombre que se les da a las estaciones que cuenta con soporte de calidad de servicio, y (STA) para aquellas que no lo soportan, así como, QAP para los puntos de acceso con soporte de calidad de servicio y AP para aquellos que no cuentan con el servicio.

La incorporación más novedosa del grupo de trabajo fue una nueva función de coordinación HCF – (Hybrid Coordination Function) función de coordinación hibrida, la cual se emplea para el conjunto de servicios básicos con soporte de QoS (QBSS).

La función HCF define dos modos de operación:

1. (EDCA – *Enhanced Distributed Channel Access*), Acceso a canal distribuido mejorado el cual consiste en un método de acceso basado en contienda, soporta priorizacion de tráfico.

2. (HCCA - *HCF Controlled Channel Access*), Acceso a canal controlado HCF el cual se encarga del rastreo mediante un coordinador híbrido (HC –*Hybrid Coordinator*). Éste está en el lado del QAP, soporta parametrizado de trafico.

Con estos nuevos mecanismos se mejoran las formas originales de acceso que se tenían con el (DCF y PCF) en el estándar original. Con estas modificaciones en la capa de acceso al medio se permitirá priorizar unas estaciones respecto a otras. Este estándar es considerado de vital importancia para el soporte de aplicaciones sensibles al retardo, como puede ser la videoconferencia. Diferentes estudios muestran el aumento de rendimiento que se puede alcanzar con este nuevo estándar [22].

Capítulo III

3. MODELOS DE PROPAGACIÓN

3.1 Introducción

En este capítulo se pretende dar una visión general sobre los diferentes modelos de propagación de señales de radiofrecuencia; en un entorno exterior (outdoor) e interior a un edificio (indoor).

La señal emitida por una antena (emisor) que viaja a lo largo de su trayectoria para llegar al receptor, sufre complicaciones con obstáculos naturales o artificiales, éstas hacen que la señal llegué deteriorada con menos potencia que la señal original emitida por el emisor. Estos obstáculos hacen muy difícil predecir la señal recibida en un determinado punto o analizar el canal de radio.

Los modelos de propagación se han enfocado tradicionalmente en predecir la potencia promedio de la señal recibida; así como la variación de la potencia en la proximidad espacial de un lugar en particular. En la actualidad el modelado de la señal es de gran interés en el campo de las comunicaciones inalámbricas.

Un modelo de propagación es un conjunto de expresiones matemáticas, diagramas y algoritmos utilizados para representar las características de radio de un determinado entorno [23]. Los modelos de propagación resultan de una serie de cálculos que describen las pérdidas de señal en un determinado punto, estas perdidas son dadas en decibeles (dB). Generalmente estos modelos se conjugan con datos reales y estadísticos para poder predecir el comportamiento o la propagación de las ondas de radio. La utilidad de estos modelos se basa en predecir la potencia de la señal que el emisor y el receptor realizan a una determinada distancia.

3.2 Mecanismos básicos de la propagación

A continuación se describen algunos fenómenos que aceptan la propagación de la señal (ondas electromagnéticas)

3.2.1 Reflexión

La reflexión ocurre cuando una onda electromagnética que se propaga por el aire incide contra un objeto de grandes dimensiones en comparación con la longitud de onda de la señal. El resultado puede ser que la señal sea absorbida, reflejada o una combinación de ambas. Esta reacción depende principalmente de:

- Propiedades físicas del obstáculo, como pueden ser su geometría, textura y composición.
- Propiedades de la señal, como el ángulo de incidencia, orientación y longitud de onda.

Los conductores perfectos reflejarán la totalidad de la señal. Otros materiales reflejarán solo una parte de la energía incidente y transmitirán el resto. La cantidad exacta de transmisión y reflexión depende igualmente del ángulo de incidencia así como del grosor y propiedades dieléctricas del material, como se muestra en la figura 3.1.

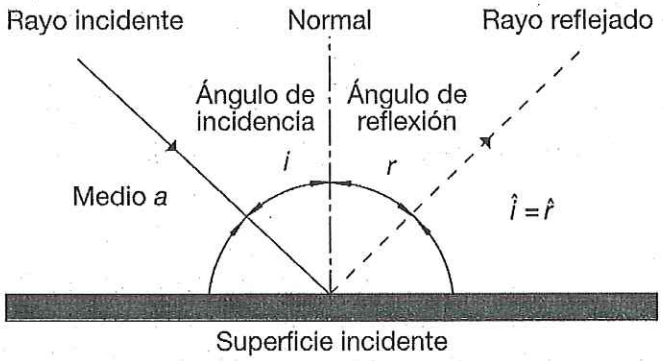


Figura 3.1: Represtación de la reflexión.

3.2.2 Difracción

En óptica se entiende por difracción la desviación del rayo luminoso al rozar el borde de un cuerpo opaco. Las ondas difractadas se forman cuando el camino de propagación de la onda de radio es obstruido por una superficie que tiene irregularidades o bordes puntiagudos o

angulados. La difracción ocurre cuando los obstáculos son impenetrables por las ondas de radio. Basándose en el principio de Huygen, el resultado son ondas secundarias alrededor y detrás del obstáculo, incluso en zonas sin visibilidad directa entre transmisor y receptor.

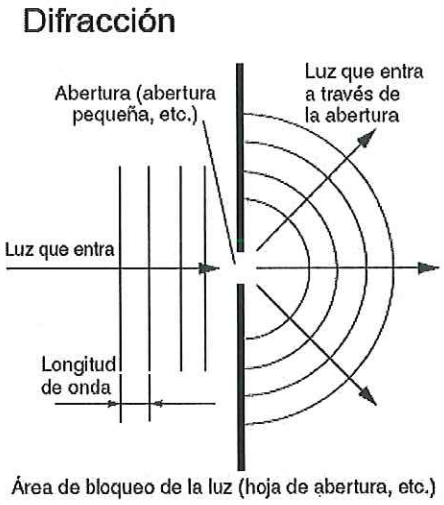


Figura 3.2: Representación de la Difracción.

Los escenarios cerrados contienen muchos tipos de objetos con estas características orientados tanto en el plano vertical como horizontal. La señal difractada depende de la geometría del objeto así como la amplitud, fase y polarización de la onda incidente en el punto de difracción, como se muestra en la figura 3.2.

3.2.3 Dispersión

La dispersión ocurre cuando en el camino la señal se encuentra con objetos cuyas dimensiones son pequeñas con relación a la longitud de onda. El resultado es que el frente de onda se rompe o dispersa en múltiples direcciones.

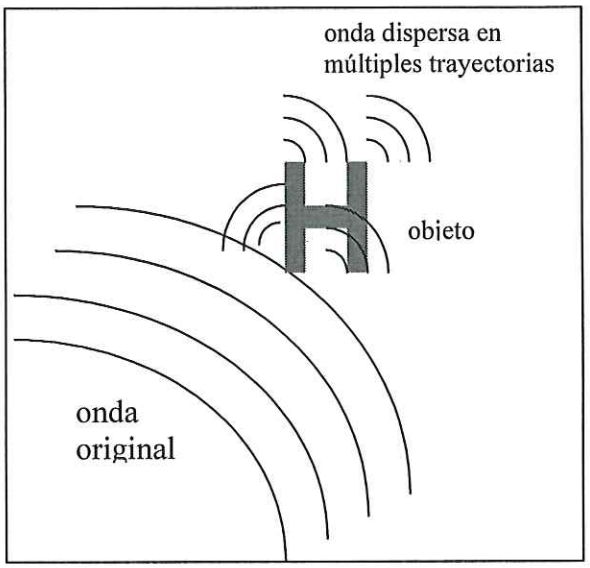


Figura 3.3: Represtación de la Difracción.

Las ondas dispersas son producidas por superficies desiguales, pequeños objetos y otras irregularidades presentes en el canal. La mayoría de las construcciones modernas contienen vigas de hierro forjado en su estructura además de conductos para los servicios eléctricos y de tuberías. En la práctica, el follaje, señales de tráfico o farolas pueden provocar dispersión en sistemas de comunicaciones inalámbricos. Ver figura 3.3.

Los modelos de propagación de radio se pueden clasificar en dos tipos principales: modelos para exteriores (outdoor) y modelos para interiores (Indoor). Además, de acuerdo al tamaño de la zona de cobertura, los modelos outdoor se pueden dividir en modelos de propagación en zonas grandes (macroceldas) y de zonas pequeñas (microceldas).

3.3 Modelos de propagación para exteriores (outdoor)

3.3.1 Modelos de propagación de RF en ambientes urbanos

Este tipo de modelos se especializan en ambientes en donde se presentan diferentes obstáculos, por lo cual el número de parámetros a considerar para estos modelos es mayor a los de espacios abiertos. Este tipo de modelos en la actualidad son muy utilizados en el campo de la telefonía móvil, donde es necesario observar el comportamiento de la señal en ambientes urbanos.

El crecimiento de las comunicaciones inalámbricas hoy en día y el gran auge de la telefonía móvil han hecho que estos modelos marquen la diferencia durante los diseños de cobertura en zonas urbanas, además que son considerados confiables para poder predecir la propagación de la señal.

Las primeras investigaciones fueron hechas por el investigador japonés Okumura. El método que utilizó Okumura requirió de un gran esfuerzo para su tiempo, ya que requería de interpretación de gráficas creadas a partir de mediciones hechas en su país [24].

Durante los siguientes años el investigador Masaharu Hata logro modelar las gráficas tomadas por Okumura y con esto logro realizar las ecuaciones que hoy en día se conocen con los apellidos de estos personajes [24].

Existen varios modelos para ambientes urbanos con parámetros y condiciones diferentes, dentro de los cuales se encuentran los siguientes modelos.

3.3.1.1 Modelo de Okumura

El modelo de Okumura es utilizado para predecir la potencia en el receptor para comunicaciones móviles y es uno de los más utilizados para la predicción de ambientes urbanos. Este modelo es aplicable para el rango de frecuencias en 150 a 1920 MHz, pero puede ser extrapolado sobre los 3000 MHz. Según el modelo, la distancia máxima de separación que puede existir entre el emisor y el receptor es de hasta 100 km. Las pérdidas existentes en el enlace pueden ser obtenidas con la ecuación (NUM):

Ecuación (1), Okumnura

$$L_{50}(dB) = L_F + A_{mu}(f,d) - G(h_{te}) - G(h_{re}) - G_{AREA}$$

Donde:

$L_{50}(dB)$	Es la atenuación mediana por trayectoria en decibeles
L_F	Es la atenuación por espacio libre
$A_{mu}(f,d)$	Es la atenuación relativa promedio (curvas)
$G(h_{te})$	Ganancia de la altura de la antena Tx
$G(h_{re})$	Ganancia de la altura de la antena Rx
G_{AREA}	Es la ganancia debida al tipo de ambiente

Okumura encontró que $G(h_{te})$ tiene una variación de pérdida de 20 dB/década y que $G(h_{re})$ tiene un variación de 10 dB/década para alturas menores de 20 mts.

3.3.1.2 Modelo de Hata

El modelo de Masaharu Hata es un modelo empírico donde muestra de manera gráfica las pérdidas por propagación previstas por Okumura. Este modelo es válido solo para las frecuencias de VHF y UHF pero dentro de los límites de los 150 MHz hasta los 1500 MHz. Las pérdidas existentes en el enlace pueden ser obtenidas por medio de la ecuación 2, en el que se ha incluido el factor de correlación suburbano [25].

Ecuación (2), Hata

$$L_{50}(dB)_{Hata} = 69.12 + 26.16 * \log(f_c) - 13.82 * \log(h_{te}) + (-3.2(\log 11.75_{re})^2 +$$

$$-32(\log 11.75 h_{re})^2 + (44.9 - 6.55 * \log(h_{te})) * \log(d) - 2\left(\log\left(\frac{f_c}{28}\right)\right)^2$$

Donde:

$L_{50}(dB)$	Es la atenuación mediana por trayectoria en decibeles
f_c	Frecuencia portadora en MHz
h_{te}	Altura efectiva de la antena trasmisora
h_{re}	Altura efectiva de la antena receptora
d	Distancia entre el transmisor y el receptor en km

3.3.1.3 Modelo PCS extensión para el modelo de Hata

El modelo de Hata-Extendido o también llamado COST-231 es una extensión del modelo Hata y puede ser utilizado para un rango de frecuencias entre los 1.500 y 2.000 GHz pero puede ser extrapolado y ser aplicado a los 2.45 GHz. La altura efectiva del transmisor va desde 30 a 200 m, la altura efectiva del receptor desde 1 a 10 m y la distancia máxima entre el emisor y receptor es hasta 20 km. Las pérdidas de enlace pueden ser obtenidas mediante la ecuación 3.

Ecuación (3), Hata extendido

$$L_{50}(dB)_{Hata-Ext} = 51.27 + 33.9 * \log(f_c) - 13.82 * \log(h_{te}) - 3.2(\log 11.75_{re})^2 + \\ + (44.9 - 6.55 * \log(h_{te})) * \log(d)$$

Donde:

$L_{50}(dB)$	Es la atenuación mediana por trayectoria en decibeles
f_c	Frecuencia portadora en MHz
h_{te}	Altura efectiva de la antena trasmisora
h_{re}	Altura efectiva de la antena receptora
d	Distancia entre el transmisor y el receptor en km

3.4 Modelos de propagación para interiores - indoor

En estos últimos años con la revolución de las telefonía celular y las redes inalámbricas WLAN, han hecho que varias compañías del ramo estén realizando investigación sobre la propagación de la señal en interiores, en las frecuencias que van desde la 500 MHz a los 5 GHz. Precisamente es en este campo donde las grandes compañías han logrado desarrollar sus modelos para la predicción de la señal en interiores lo cual ha traído consigo un gran beneficio para ellas durante la planeación de redes en interiores.

Los modelos de propagación para interiores se dividen en cinco clases:

Los modelos estadísticos: estos tipos de modelos requieren de una descripción del tipo construcción para determinar el comportamiento de la señal, estos modelos resultan muy adecuados para predecir el comportamiento de la señal en hoteles, aeropuertos, oficinas, hospitales, casas.

Los modelos empíricos de trayectoria directa: este tipo de modelos son los más estudiados en la actualidad y se basa en la trayectoria entre el emisor y receptor de un sistema de comunicación móvil.

Los modelos empíricos de multi-trayectorias: estos modelos son utilizados por medio de cómputo numérico mediante programas de computadora. Los datos son almacenados y calculados para predecir nuevas trayectorias.

Existen dos grupos: El modelo de rayos ópticos y el modelo electromagnético, que son más utilizados para casos y frecuencias muy particulares. Cada uno de estos modelos tienen sus ventajas y desventajas pero se comportan de manera uniforme entre los modelos del mismo grupo con variaciones mínimas entre ellos.

3.4.1 Modelo de particiones en el mismo piso

Este modelo requiere de datos como el tipo de construcción en donde se pretende saber el comportamiento de la señal. Estos modelos son utilizados en ambientes donde se tienen los mismos tipos de construcción previamente tomadas. Este modelo solo le resta la pérdida de la señal de acuerdo al tipo de material con el que se esta trabajando.

Para este modelo es necesario generar una base de datos con el tipo de material en que fue realizado el experimento y la pérdida que hubo, en la tabla III, se muestran algunas mediciones experimentales de las pérdidas en edificios y diversos materiales de mayor uso en ambientes de interior.

Tabla III: Mediciones experimentales para cierto tipo de edificios [de WIRELESS COMUNICATION, RAPPAPORT]

Tipo de Material	Pérdida en dB	Frecuencia
Metal	26	815Mhz
Aluminio	20.4	815Mhz
Aislamiento de hoja	3.9	815Mhz
Bloques de concreto	13	1300Mhz
Pérdidas por un piso	20-30	1300Mhz
Pérdidas por un piso y una pared	40-50	1300Mhz
Atenuación observada cuando el transmisor toma un ángulo recto en la esquina del corredor	10-15	1300Mhz
Cubierta de metal-12ft^2	4-7	1300Mhz
Maquinaria ligera	1-4	1300Mhz
Maquinaria en General	5-10	1300Mhz
Maquinaria Pesada	10-12	1300Mhz
Escaleras de caracol	5	1300Mhz
Textil ligero	3-5	1300Mhz
Textil Pesado	8-11	1300Mhz
Area en donde los obreros inspeccionan el metal defectuoso	3-12	1300Mhz
Racks metálicos	4-9	1300Mhz
Cajas vacías de inventario	3-6	1300Mhz
Pared bloques de concreto	13-20	1300Mhz
Ducto del el techo	1-8	1300Mhz
Caja de metal de 4m	10-12	1300Mhz
Rack de almacenamiento con papeles	2-4	1300Mhz
Rack de 2.5m con partes metalicas	4-6	1300Mhz

Tipo de Material	Pérdidas en dB	Frecuencia
Aluminio (1/8 in)	47	9.6Ghz
Aluminio(1/8 in)	46	28.8Ghz
Aluminio(1/8 in)	53	57.6Ghz
Pared de Concreto	8-15	1300Mhz
Piso de concreto	10	1300Mhz
Zona Comercial	38	9.6Ghz
Zona Comercial	51	28.8Ghz
Zona Comercial	59	57.6Ghz
Placa de madera comprimida seca	1	9.6Ghz
Placa de madera comprimida seca	4	28.8Ghz
Placa de madera comprimida seca	8	57.6Ghz
Dos Placas de madera comprimida seca	4	9.6Ghz
Dos Placas de madera comprimida seca	6	28.8Ghz
Dos Placas de madera comprimida seca	14	57.6Ghz
Placa de madera comprimida mojada	19	9.6Ghz
Placa de madera comprimida mojada	46	28.8 Ghz
Placa de madera comprimida mojada	57	57.6 Ghz
Dos Placas de madera comprimida mojada	39	9.6 Ghz
Dos Placas de madera comprimida mojada	46	28.8 Ghz
Dos Placas de madera comprimida mojada	57	57.6Ghz

3.4.2 Modelo Multi-pared/COST-231

Este modelo fue especialmente diseñado para interiores, toma en cuenta las pérdidas de espacio libre y las pérdidas por los pisos penetrados por trayectoria directa que existe entre el transmisor y el receptor.

Este modelo es empírico para pérdidas en paredes [26], de modo que toma en conjunto el espacio libre con la pérdida de la señal en las paredes y pisos que existen entre el receptor y el transmisor. El modelo COST-231 presenta la siguiente ecuación:

Ecuación (4), COST-231

$$PL = PL_{FS} + L_C + \sum K_{WI} L_{WI} + L_F n^{n+2/n+1^{-.046}}$$

Donde

PL_{FS}	Es la pérdida en decibeles en el espacio libre entre el trasmisor y el receptor
L_C	Es la constante de pérdida en decibeles
K_{WI}	Es el número de paredes penetradas de un tipo
n	Es el número de pisos penetrados
L_{WI}	Son las pérdidas por el tipo de pared *i*
L_F	Son las pérdidas por pisos adyacentes
B	Es un número medido empíricamente

Estas mediciones son basadas en el tipo de construcción que se está analizando. Para este modelo se han hecho más mediciones en oficinas por lo que se toman un promedio y se utilizan en la ecuación para aplicarla al caso especifico de oficinas.

Para la ecuación n se toma en cuenta el valor n=4 para ambientes en oficinas para cálculos en ambientes moderadamente, de estar muy saturado por obstáculos el valor de n=3 pero normalmente n=4, es el promedio y si además de esto le damos valores de $L_C = 37dB, L_F = 18.3, b = 0.46$ este modelo puede reducirse de manera significativa

$$PL(d) = 37 + 30Log(d) + 18.3n^{n+2/n+1^{-.046}}$$

y la ecuación anterior se puede simplificar más si no existen penetración por paredes por lo que el tercer término de la ecuación puede ser eliminado quedando lo siguiente:

$$PL(d) = 37 + 30Log(d)$$

De manera que, como se puede observar esta ecuación es muy simple, de tal forma que esta ecuación es la misma para un modelo de pérdidas básico. Para obtener mejores resultados es necesario con datos experimentales de las pérdidas entre los diferentes pisos y paredes

3.4.3 Modelo de pérdidas por particiones entre pisos.

Este modelo es muy similar al modelo de pérdidas en el mismo piso se basa en bases de datos recopiladas de mediciones experimentales tomadas en varios edificios. Las pérdidas entre piso de un edificio está determinada por los materiales de construcción externas al edificio. Es importante para este modelo constar con información del tipo de material con el que está construido el edificio. Como se muestra en el tabla IV.

Tabla IV: Parámetros de pérdidas por FAF

Edificio	*1900 Mhz FAF(dB)*	*s(dB)*	*Número de Lugares*
Primer Edificio			
Un Piso	31.3	4.6	110
Dos Pisos	38.5	4.0	29
Segundo Edificio			
Un Piso	26.2	10.5	21
Dos Piso	33.4	9.9	21
Tres Pisos	35.2	5.9	20
Cuatro Pisos	38.4	3.4	20
Cinco Pisos	46.4	3.9	17
Tercer Edificio			
Un piso	35.4	6.4	74
Dos pisos	35.6	5.9	41
Tres pisos	35.2	3.9	27

3.3.4 Modelo de atenuación lineal por trayectoria

Este modelo es muy sencillo en su aplicación, contempla una parte real de mediciones por pérdidas por trayectoria tiene un gran peso en este modelo. Andelman (2004) lo propuso como un modelo a utilizarse cuando el emisor y el receptor se encuentran en el mismo piso, este modelo toma en cuenta trayectorias para interiores en dB a partir de la potencia radiada, estas pérdidas están dadas por el modelo de espacio libre que es la parte teórica de este modelo, mas el factor lineal con cierto rango, este factor se obtiene experimentalmente.

La ecuación que describe este modelo es:

Ecuación (5), Pérdidas por trayectoria

$$PL(d) = PL_{FS} + (a)(d)$$

Donde:

PL_{FS} : Son las pérdidas por el espacio libre

a : Es el coeficiente de atenuación lineal

d : Es la distancia entre el transmisor y receptor

Para una mejor idea de este modelo podemos plantear el hecho de la existencia de un ambiente de oficina, el coeficiente de atenuación de pérdidas por trayectorias es, a=0.47 (dB/m). Este modelo no toma en cuenta los efectos propios de la atenuación a gran escala, como normalmente serían tomados en cuenta para un modelo de espacio abierto.

3.3.5 Modelo Keenan-Montley

Es conocido también como modelo multipared (MKM), añade las pérdidas introducidas por las paredes y los suelos que atraviesa la onda directa entre el transmisor y el receptor, su formulación más general se da en la siguiente expresión

Ecuación (6), Keenan-Montley

$$PL(d) = PL_M + 10nLog(d) + K_F PL_{FS}$$

Donde:

PL_M : Son las pérdidas por trayectoria reales medidas a 1m

PL_{FS} : Son las pérdidas en el espacio libre que también incluye las pérdidas por penetración en los pisos

K_F : Es el número de pisos penetrados

La parte real son las mediciones que se dan por pérdida por trayectoria, que son usados para ajustar el modelo.

Capítulo IV

4. MECANISMOS DE SEGURIDAD

4.1 Introducción

Recordemos que la comunicación en redes inalámbricas se efectúa por radio frecuencia, es decir, nuestra información viaja por el aire, lo cual hace que la transmisión de los datos y el acceso a nuestra red sea insegura.

Antes de introducirnos en el análisis de aspectos y métodos de seguridad para WLAN's es importante conocer que tipos de ataque o aspectos de inseguridad estamos expuestos. Todas las redes de área local están expuestas a varios tipos de ataque, de los cuales los más frecuentes son *Ataques Activos* y *Ataques Pasivos*. Del primero, son aquellos en los que los intrusos obtienen acceso a la red de manera ilegal y causan daños a la información. Mientras que los *Ataques Pasivos* se caracterizan por la forma en que el intruso se infiltra a la red sin

dañar la información, sin embargo, hace uso de los recursos (hardware, acceso a Internet, etc.), además de husmear la información [27].

Las redes inalámbricas son más susceptibles a estos ataques debido a que los intrusos no requieren conexión física para accesar a la red. Dada esta vulnerabilidad que de manera natural se expone, cualquiera que quisiera entrar de manera ilegal a la red lo podría hacer rastreando la señal que viaja por el aire, decodificar la información, y accesar a la red con datos de otro usuario. Esto significa que para proteger la WLAN se necesitan elementos internos o externos implementados para autorizar el acceso a la red. La protección a los recursos e información de la WLAN puede ser catalogado en diferentes niveles: básico, intermedio y avanzado [28].

4.2 Técnicas de seguridad para redes inalámbricas

4.2.1 SSID (Service Set Identifier)

SSID es un método de seguridad mínimo integrado por los fabricantes de los equipos que existen actualmente en el mercado, pero no el suficiente para que la WLAN sea segura. SSID permite a la WLAN ser segmentada en múltiples redes cada una con un diferente identificador [29], el identificador es de 32 caracteres que se encuentra en la cabecera del paquete que es enviado al AP. El SSID actúa como un simple identificador cuando un dispositivo móvil intenta conectarse a la WLAN.

El SSID diferencia una WLAN de otra, de tal manera que todos los AP's y los dispositivos móviles que intenten conectarse a una WLAN deben usar el mismo SSID. A un dispositivo no se le permitirá conectarse al BSS a menos de que pueda proporcionar el SSID [26]

Debido a que el SSID puede ser capturado en forma clara, no ofrece ningún tipo de seguridad a la WLAN, sin embargo, es conocido y compartido.

4.2.2 Filtrado de direcciones MAC (Media Access Control)

Una manera de incrementar la seguridad, es la configuración de un listado de direcciones MAC para cada uno de los puntos de acceso (AP) que conforma una red inalámbrica, cada uno de los clientes (estación inalámbrica) asociados a estos AP's deben aparecer dentro de

este listado, en el caso de que una dirección MAC del alguna estación no aparezca en ese listado del AP deniega el acceso a la red.

Otra manera de que los clientes puedan accesar a laWLAN por este método es que el listado de direcciones se encuentre almacenado en un servidor denominado RADIUS (lo mencionaremos más adelante), el cual tiene una interacción con el punto de acceso, el AP hace una petición al servidor RADIUS con la dirección MAC y el identificador del usuario para saber si se encuentra o no dentro del listado de direcciones MAC.

Ventajas

- AP-RADIUS elimina el tener que estar alimentado el listado de direcciones MAC en cada AP, puesto que se tiene solo un listado que se encuentra en el servidor RADIUS, el cual es consultado por cada AP.
- Solamente las direcciones MAC que estén registradas en el listado son las únicas que pueden tener acceso a los servicios y recursos de la WLAN.

Desventajas

- Debe haber una labor intensa en la retroalimentación del listado de direcciones MAC de los clientes en el AP.
- Este tipo de seguridad es implementado con un número pequeño de usuarios.
- Es importante utilizar este método en conjunto con otros que mencionáremos mas adelante, puesto que la utilización de este por sí sólo no es confiable.

4.2.3 WEP (Wire Equivalent Privacy)

El método de encriptación WEP pretende minimizar el riesgo de la intercepción de la señal de radio frecuencia (RF). El WEP tiene como función principal encriptar y autenticar los clientes con el punto de acceso de acuerdo al estándar 802.11, basado en el algoritmo de encriptación llamado RC4 de RSA Data Systems.

El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confiabilidad equivalente al de las redes LAN cableadas, mediante cifrado de los datos que son transportados por las señales de radio. Según el estándar, WEP debe proporcionar confidencialidad, autentificación y control de acceso en las redes WLAN. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de la red.

4.2.3.1 Funcionamiento.

WEP utiliza el algoritmo RC4 para la encriptación con llaves de 64 bits, aunque existe también la posibilidad de utilizar llaves de 128 bits. Veremos que en realidad son 40 y 104 bits, ya que los otros bits restantes van en el paquete como Vector de Inicialización (IV).

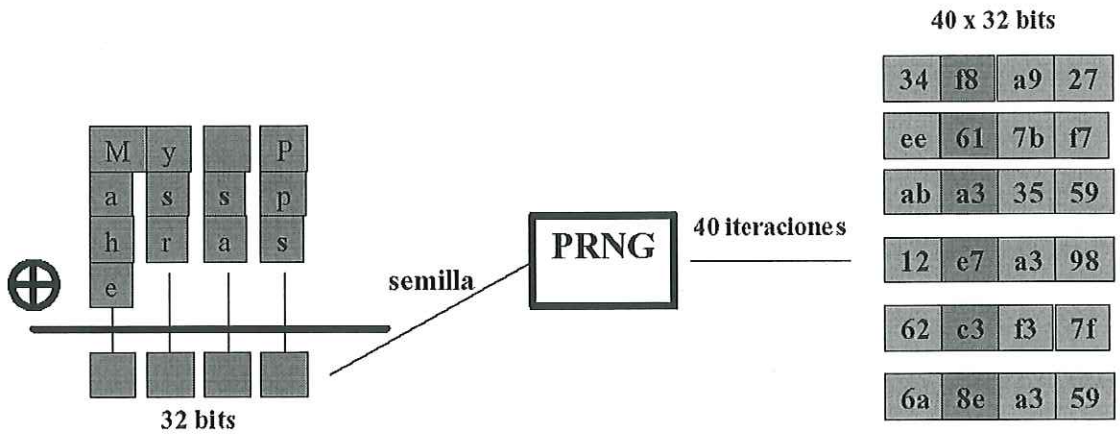


Figura 4.1: Generación de llaves del protocolo WEP

La llave de 40 ó 104 bits, se genera a partir de una clave (passphrase) estática de forma automática, aunque existe software que permite introducir esta llave manualmente. La clave o passphrase debe ser conocida por todos los clientes que quieran conectarse a la red wireless que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente.

A partir de la clave o passphrase se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP. Ver figura 4.1.

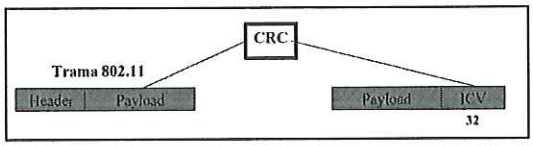
Se hace una operación XOR con la cadena ASCII (*My Passphrase*) que queda transformada en una semilla de 32 bits que utilizará el generador de números pseudo aleatorios (PRNG) para generar 40 cadenas de 32 bits cada una.

Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits. De estas 4 llaves sólo se utilizará una para realizar la encriptación WEP como veremos a continuación.

4.2.3.2 Encriptación

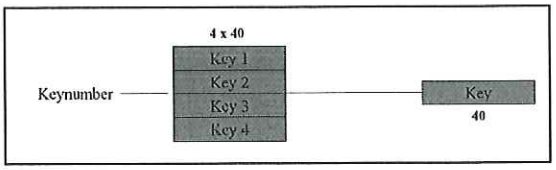
Para generar una trama encriptada con WEP se sigue el siguiente proceso:

Partimos de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (Header) y contiene los datos (Payload-carga útil). El primer paso es calcular el CRC de 32 bits del payload de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único del payload en concreto, que nos servirá para verificar que el payload recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como **valor de chequeo de integridad** (ICV: Integrity Check Value):



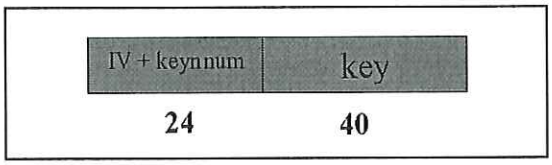
Paso 1.

Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles:



Paso 2.

Y añadimos el **Vector de Inicialización** (IV) de 24 bits al principio de la llave seleccionada:

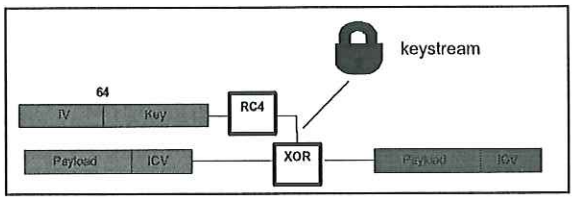


Paso 3.

El IV es simplemente un contador que suele ir cambiando de valor a medida que vamos generando tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para encriptar la trama. En el caso de utilizar encriptación de 128 bits tendríamos 24 bits de IV y 104 de llave.

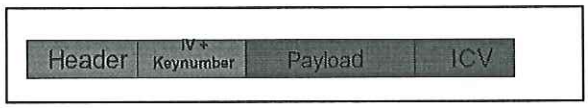
Llegado a este punto, aplicamos el algoritmo RC4 al conjunto IV+Key y conseguiremos el keystream o flujo de llave. Realizando una operación XOR con este keystream y el conjunto Payload+ICV obtendremos el Payload+ICV cifrado, este proceso puede verse en el siguiente gráfico.

Se utiliza el IV y la llave para encriptar el Payload + ICV:



Paso 4.

Después añadimos la cabecera y el IV+Keynumber sin cifrar. Así queda la trama definitiva lista para ser enviada:



Paso 5.

El proceso de encriptación en conjunto se ve resumido en la figura 4.2.

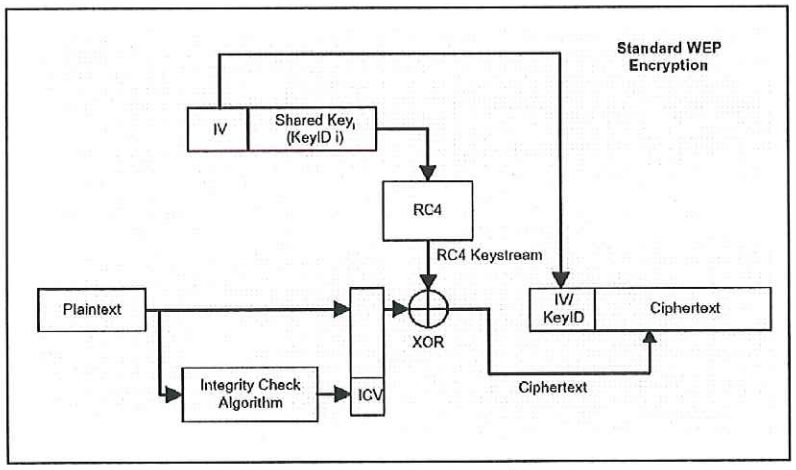
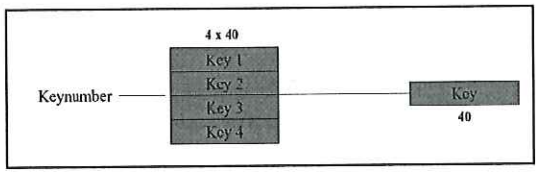


Figura 4.2: Esquema general de encriptación WEP

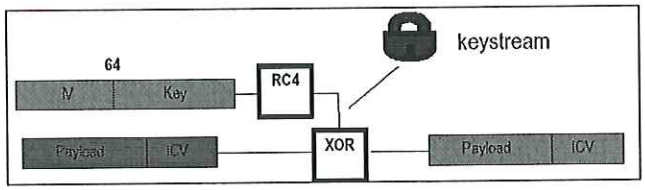
4.2.3.3 Desencriptación

Ahora vamos a ver el proceso que se realiza para desencriptar una trama encriptada con WEP: Se utiliza el número de llave que aparece en claro en la trama cifrada junto con el IV para seleccionar la llave que se ha utilizado para cifrar la trama:



Paso 1.

Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64 bits de llave. Aplicando RC4 a esta llave obtenemos el keystream válido para obtener la trama en claro (plaintext) realizando una XOR con el Payload+ICV cifrados y la llave completa como se describe a continuación.



Paso 2.

Una vez obtenido el texto plano (plaintext), se vuelve a calcular el ICV del payload obtenido y se compara con el original. El proceso completo puede verse en la figura 4.3.

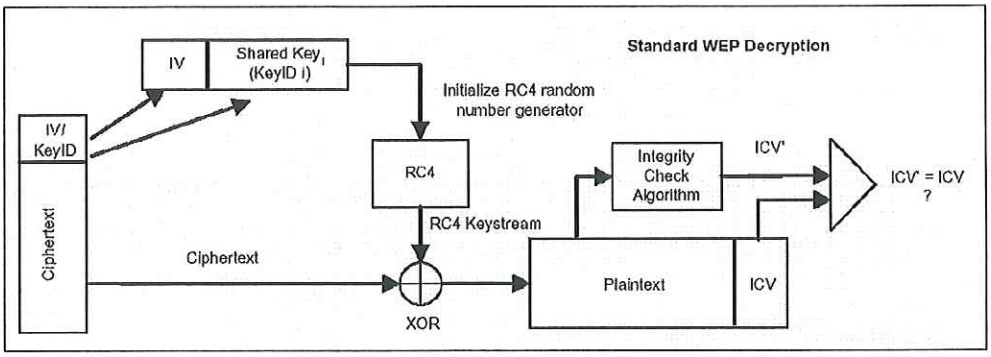


Figura 4.3: Desencriptación de tramas en WEP

4.2.3.4 Vulnerabilidad en el WEP

Es frecuente escuchar que el algoritmo de encriptación RC4 es vulnerable a ataques debido a que existe software en Internet que permiten que cualquier persona pueda infiltrar en la WLAN en un tiempo aproximado de 15 minutos [30]. La protección por WEP por sí sóla es inadecuada.

En la figura 4.4 podemos observar como un cliente de la WLAN se comunica con el AP utilizando WEP.

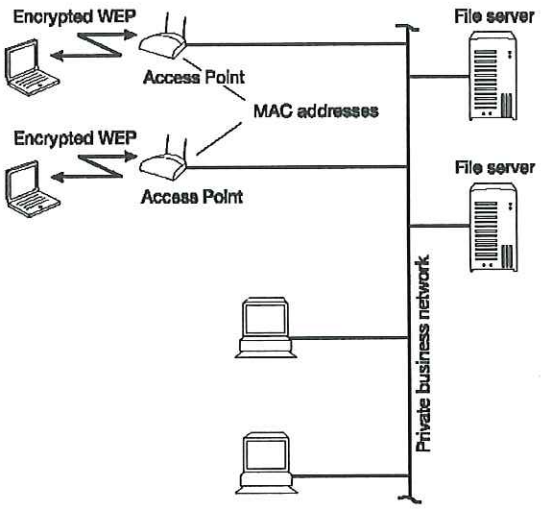


Figura 4.4: Fuente: Wireless Security and VPN - Intel

4.2.4 RADIUS

RADIUS es un servidor para la autenticación y manejo de cuentas para usuarios remotos. Es principalmente usado por los ISP (Internet Service Providers), aunque puede también ser utilizado en cualquier red que necesite un servicio centralizado de la autenticación y/o manejo de cuentas para sus estaciones de trabajo (STA).

RADIUS soporta una amplia variedad de esquemas de autenticación. Un usuario hace la petición para su autenticación con el servidor, ya sea contestando directamente en la consola su login/password o usando los protocolos CHAP o PAP.

El servidor obtiene la información personal del usuario de uno de los siguientes lugares [31]:

Base de datos del sistema. El login y password del usuario se encuentra en un subdirectorio dentro del servidor, p.ej. /etc/passwd para los sistemas UNIX.

Base de datos de RADIUS. El ID y el password del usuario se encuentran almacenados en la base de datos de RADIUS. El password del usuario está almacenado de forma encriptada utilizando los algoritmos de hash MD5 o DES, cualquiera de estas formas son apropiadas.

Autenticación SQL. Esto es cuando la información de los usuarios se encuentra en una base de datos SQL. La estructura de la base de datos es completamente definida por el administrador del sistema, RADIUS no restringe la definición de la base de datos de ninguna manera.

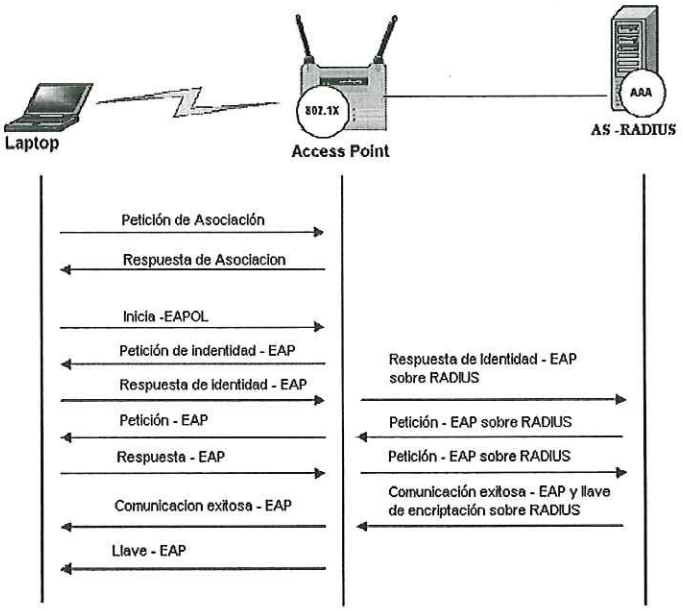


Figura 4.5: Diagrama que muestra los pasos que ocurren para asociar, autenticar y distribución de llaves.

4.2.4.1 EAP (Extensible Authentication Protocol)

EAP es un método para establecer una conversación de autenticación entre un usuario y un servidor de autenticación(AS). Dispositivos intermediarios tales como AP's y servidores Proxy no toman parte de esta conversación, su papel es retransmitir mensajes de EAP entre la STA y el AS.

4.2.4.2 EAPOL (Extensible Authentication Protocol Over LAN)

Es una técnica para encapsular los paquetes EAP en un ambiente LAN (Ethernet, Token Ring, FDDI), además de transportar los paquetes EAP, EAPOL también proporciona funciones de control, tales como, iniciar, terminar sesiones y la distribución de llaves.

4.2.5 WPA (Wi-Fi Protected Access)

Debido a los numerosos puntos débiles de las redes LAN inalámbricas, la Wi-Fi Alliance, trabajando en colaboración con la IEEE, dieron a conocer en octubre 2002 las especificaciones WPA, presentándolas como el software de seguridad que sustituiría al WEP. La WPA es una especificación de implementaciones de seguridad basadas en estándares, que deben ser empleadas para los sistemas LAN inalámbricos.

Esta medida tiene como objetivo suplir el déficit de seguridad del WEP. La mayoría de los WPA anteriores son compatibles con el estándar IEEE 802.11i, que se aprobó a finales del 2003. En la especificación WPA se trató que se pudiera seguir utilizando el hardware ya disponible. Mediante actualizaciones de Software/Firmware para los AP y los adaptadores de red inalámbricos se posibilita que estos puedan seguir utilizándose.

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

IEEE 802.1X. Estándar del IEEE ratificado en el 2001 es utilizado para proporcionar un control de acceso en redes basadas en puertos. El concepto de *puerto*, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service)* como se muestra en la figura 4.5. Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

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

MIC (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas.

4.2.5.1 Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2^48 combinaciones de claves diferentes, lo cual parece un número suficientemente como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*). Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de claves compartido de WEP, así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

4.2.5.2 Modos de funcionamiento de WPA

Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos

4.2.6 802.11i/WPA2

El estándar IEEE 802.11i reemplaza formalmente el WEP del estándar IEEE 802.11 original por un modo específico del estándar de cifrado avanzado (AES, Advanced Encryption Standard), conocido como Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) Protocol (CCMP). CCMP proporciona tanto confidencialidad (cifrado) como integridad a los datos. En la tabla V, se presentan las principales mejoras que se hicieron para el protocolo WAP2/802.11i con respecto al WEP.

Claves temporales de 802.11i/WPA2

A diferencia de WEP, que utiliza una única clave para el cifrado de datos de difusión única y generalmente una clave separada para el cifrado de datos de difusión y de multidifusión, 802.11i/WPA2 usa un conjunto de cuatro claves diferentes para cada par de clientes

inalámbricos-AP inalámbricos (conocidas como las claves temporales de par o "pairwise") y un conjunto de dos claves diferentes para el tráfico de difusión y de multidifusión.

Tabla V: Mejoras del protocolo WEP vs WPA2/802.11i

Punto débil de WEP	Cómo WPA2/802.11i aborda el punto débil
Vector de inicialización (IV) demasiado corto	En AES CCMP, se reemplazó el IV por un campo llamado número de paquete y se duplicó su tamaño a 48 bits.
Integridad débil de los datos	El cálculo de suma de comprobación cifrado con WEP se reemplazó por el algoritmo AES CBC-MAC, que está diseñado para proporcionar una sólida integridad de los datos. El algoritmo CBC-MAC calcula un valor de 128 bits y WPA2 utiliza los 64 bits de orden superior como un código de integridad de mensaje (MIC). WPA2 cifra el MIC con el cifrado de modo contador de AES.
Usa la clave principal en lugar de una clave derivada	Al igual que WPA y el Protocolo de integridad de claves temporales (TKIP, Temporal Key Integrity Protocolo), AES CCMP usa un conjunto de claves temporales derivadas de una clave principal y otros valores. La clave principal se origina en el proceso de autenticación 802.1X mediante Protocolo de autenticación extensible-Seguridad de la capa de transporte (EAP-TLS) o EAP protegido (PEAP).
No reasigna claves	AES CCMP reasigna claves automáticamente para crear nuevos conjuntos de claves temporales.
No ofrece protección contra la reproducción	AES CCMP usa el campo número de paquete como contador para ofrecer protección contra la reproducción.

4.2.7 VPN(Virtual Private Networks)

Esta tecnología hace posible que los usuarios de una red no confiable puedan conectarse a una red privada de una manera fácil y segura. Para redes de tipo empresarial y académico VPN es una buena solución para una acceso inalámbrico y es la mejor alternativa para eliminar el uso de WEP y filtrado de direcciones MAC.

Actualmente las VPN's son utilizados para intranets y accesos remotos, para esto se utilizan varios mecanismos de seguridad para proteger la información y asegurarse que solo un usuario autorizado pueda accesar a la red.

IPsec (Internet Protocol Security), como es definido por la IEEE, es el mecanismo comúnmente usado para asegurar el tráfico en una VPN. IPsec puede utilizar DES, 3DES y otros algoritmos para encriptar información, algoritmos de alto rendimiento (MD5, SHA) para la autenticación de paquetes y certificados digitales para validar llaves publicas. Las VPN's también soportan una variedad de métodos de autenticación de usuarios tales como RADIUS y certificados digitales, estos métodos permiten una fácil integración a la infraestructura de la red existente. Ver figura 4.6.

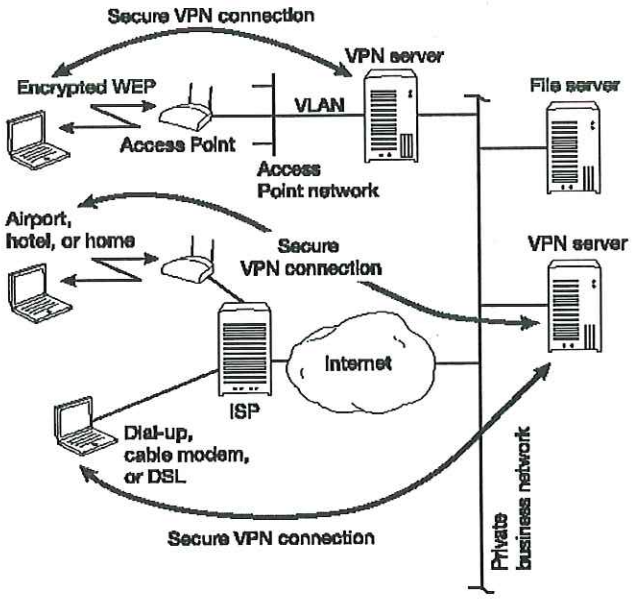


Figura 4.6: Esquema de seguridad VPN para WLAN 802.11

Capítulo V

5. PROPUESTA METODOLÓGICA

5.1 Introducción

En este capítulo describiremos a detalle una metodología que facilita el diseño de redes de área local inalámbricas WLAN para cualquier organización. Esta metodología establece seis componentes los cuales son suficientes para integrar todos los elementos que son necesarios para contar con una red WLAN óptima y segura. En la figura 5.1 se muestra el diagrama general de sus componentes, el centro representa el diseño de una WLAN que se quiere construir, es alimentado por cada una de sus componentes. Estás componentes establecen una configuración propia que será integrada al diseño y de esa manera se proporcione un diseño que cumpla con los requerimientos que se establecieron al inicio antes de empezar con el diseño de la WLAN.

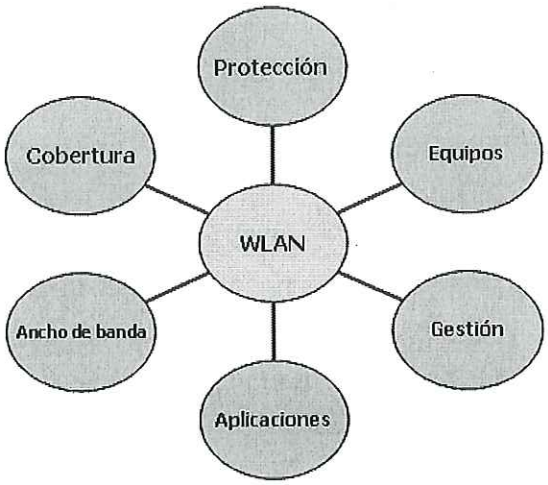


Figura 5.1: Diagrama General.

A través de éstos seis componentes cualquier organización será capaz de poder planear, diseñar y construir una red inalámbrica en cualquier parte de manera óptima y segura. La metodología integra cada elemento necesario para que la comunicación se de con un buen desempeño y confiabilidad durante la transmisión de los datos. También contempla la posibilidad de incorporar elementos acorde a las necesidades de la organización, mediante la cual se construye una red inalámbrica de manera dinámica adicionando solo aquellos elementos que satisfagan las necesidades establecidas.

La metodología establece una ruta crítica que marca lo mínimo requerido para lograr tener un diseño confiable y con éxito. En la figura 5.2 se muestra en color más obscuro los parámetros que necesariamente tienen que ser considerados durante la construcción del diseño, es por ello que cada componente incluye diferentes configuraciones que se podrían requerir durante la planeación y el diseño de una red WLAN.

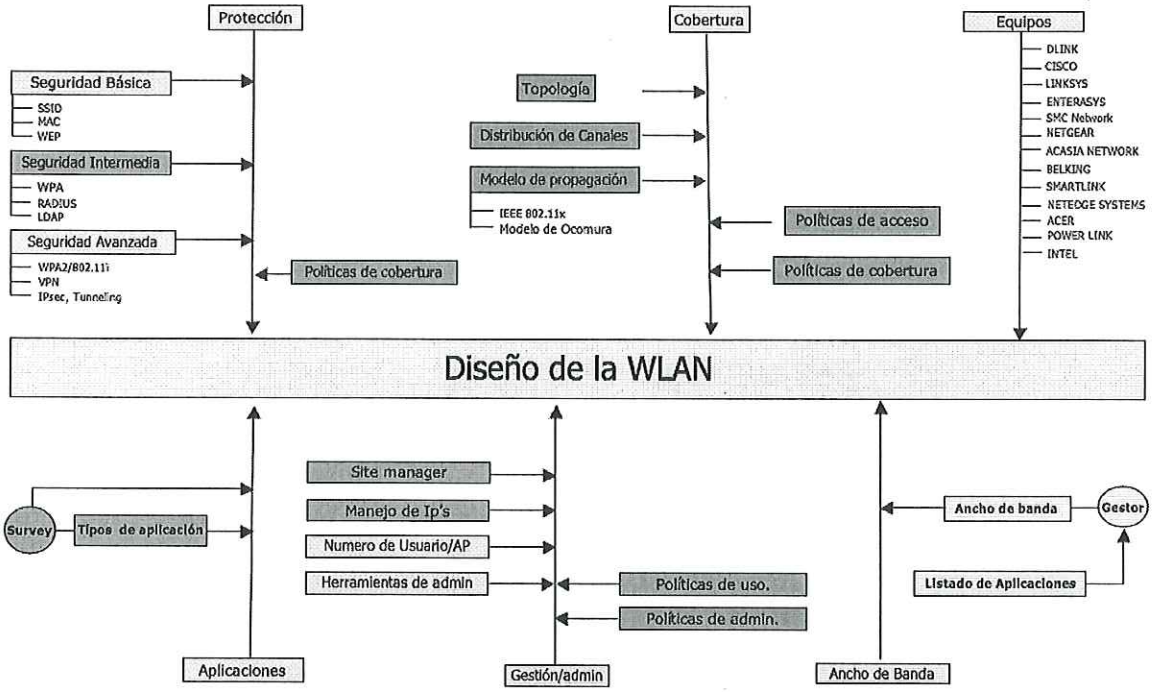


Figura 5.2: Ruta critica para diseñar redes WLAN

5.2 Protección/Seguridad

Debido a que este tipo de redes utilizan el aire para su comunicación, como ya se ha mencionado, están expuestas a cualquier espía que con los dispositivos necesarios pueden rastrear la señal y utilizar los recursos de la red para su beneficio. Instalar y configurar una WLAN puede ser proceso sencillo pero, precisamente esto, lo convierte en un blanco fácil de ataques externos e internos que pueden poner en riesgo a la organización.

Muchas de las organizaciones que incorporan este tipo de redes han sufrido de ataques en sus redes privadas, mucho se debe a la falta de planeación y un diseño pobre ante las amenazas

de los usuarios intrusos que siempre están en la espera de un error durante la implementación de la WLAN.

Recordemos que la comunicación en redes inalámbricas se efectúa por radio frecuencia (RF), es decir, nuestra información viaja por el aire, lo cual hace que la transmisión de los datos y el acceso a nuestra red sea insegura.

Las redes inalámbricas son mas susceptibles a estos ataques debido a que los intrusos no requieren conexión física para acceder a la red. Dada esta vulnerabilidad que de manera natural se expone, cualquiera que quisiera entrar de manera ilegal a la red lo podría hacer rastreando la señal que viaja por el aire, decodificar la información, y acceder a la red con datos de otro usuario.

Esto significa que, para proteger la WLAN se necesitan elementos internos o externos a la WLAN implementados para autorizar el acceso a la red. La protección a los recursos e información de la LAN puede ser catalogado en diferentes niveles: básico, intermedio y avanzado [29].

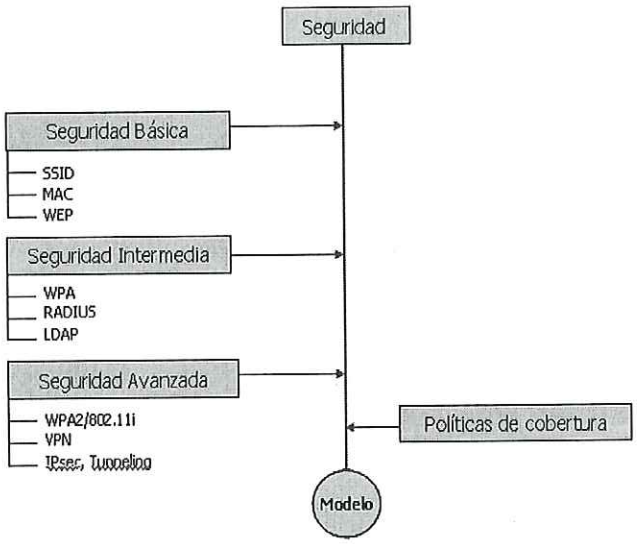


Figura 5.3: Diagrama de Seguridad

La metodología contempla la posibilidad de una configuración de protección básica, intermedia o avanzada, cada configuración integra mecanismos que ayudan a contrarrestar los problemas de seguridad de las redes WLAN. Ver figura 5.3.

5.2.1 Protección Básica

La protección básica presenta un nivel mínimo de seguridad el cual debe de ser implementado en cualquier WLAN. Siendo muy fácil de implementar, este nivel no es muy efectivo ya que no se reducen los riesgos de ataque. Ver figura 5.4.

Puntos mínimos para efectuar una protección básica:

1. Cambiar el Service Set Identifier (SSID) que viene asignado por defecto desde el fabricante.

2. Habilitar la encriptación WEP.

3. Manejar el control de acceso mediante direcciones MAC.

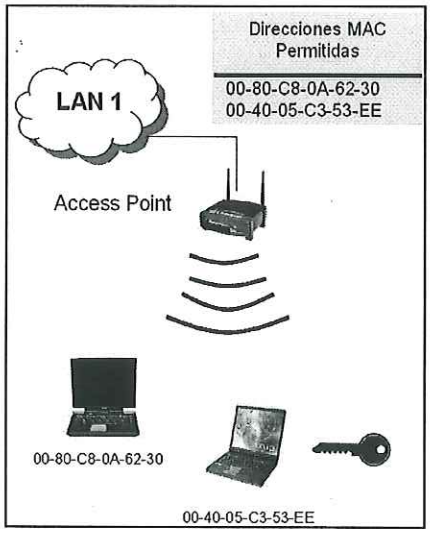


Figura 5.4: Esquema de seguridad básica

5.2.2 Protección Intermedia

La protección intermedia incluye los puntos de protección del modelo básico, además, incluye un sistema de autenticación de usuario RADIUS para acceder a la red, el cual consiste en un servidor para la autenticación y administración de cuentas para usuarios remotos. Es principalmente usado por los ISP (Internet Service Providers), aunque puede también ser utilizado en cualquier red que necesite un servicio centralizado de la autenticación y/o manejo de cuentas para sus estaciones de trabajo (STA). RADIUS soporta una amplia variedad de esquemas de autenticación.

Un usuario hace la petición para su autenticación con el servidor como se muestra en la figura 5.5, ya sea contestando directamente en la consola su login/password o usando los protocolos CHAP, PAP u otros.

Puntos para efectuar la protección intermedia:

1. Cambiar el Service Set Identifier (SSID) que viene asignado por defecto desde el fabricante.
2. Habilitar la encriptación WEP.
3. Manejar el control de acceso mediante direcciones MAC.
4. Incluir un sistema de autenticación como: LDAP, RADIUS

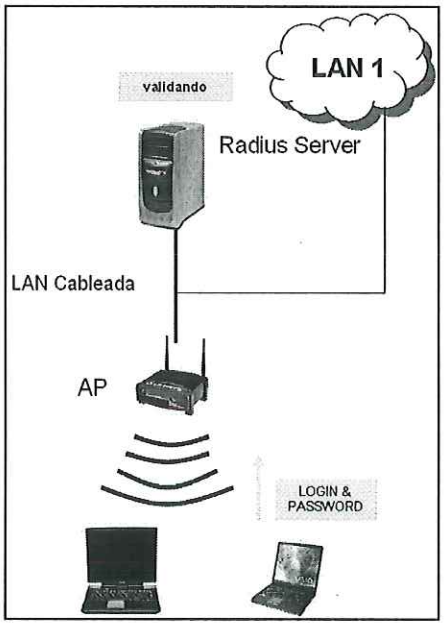


Figura 5.5: Esquema de seguridad intermedia

5.2.3 Protección Avanzada

La protección avanzada incluye los puntos de protección del modelo intermedio, además que incluye métodos de encriptación a nivel capa 3 del modelo OSI y crea túneles seguros por donde viaja la información. Ver figura 5.6.

Puntos para efectuar la protección avanzada:

1. Cambiar el Service Set Identifier (SSID) que viene asignado por defecto desde el fabricante.
2. Habilitar la encriptación WEP.
3. Manejar el control de acceso mediante direcciones MAC.
4. Incluir un sistema de autenticación como: LDAP, RADIUS.
5. Se incluye encriptación por terceras partes como IPsec, SSL o TLS utilizando un sistema de autenticación **VPN, IPSec**

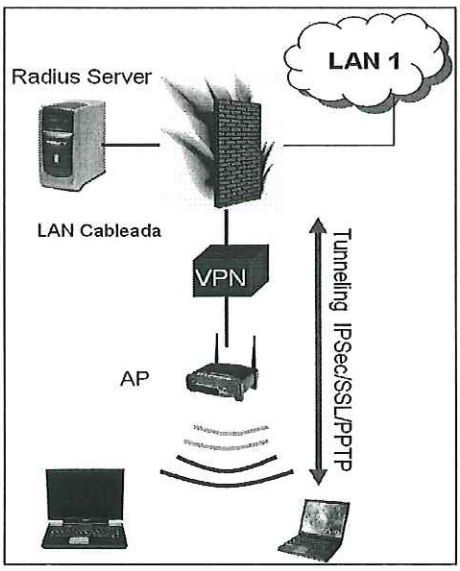


Figura 5.6: Esquema de seguridad avanzada

5.3 Cobertura

Haciendo un análisis de las tecnologías y estándares que existen hoy en día podemos obtener información sobre el alcance o cobertura en metros dentro de ambientes interiores o exteriores, las velocidades máximas de transmisión, numero de canales y la frecuencia de operación, sin embargo, hay que tomar en cuenta que las especificaciones dadas por los fabricantes a sus productos en cuanto a cobertura son ciertas solo en condiciones ideales, por lo que hay que corroborarlas mediante un análisis de propagación de la señal en donde se determine la calidad y potencia de la señal, así como el caudal eficaz en bits por segundo en los puntos más importantes del área a considerar. Ver figura 5.7.

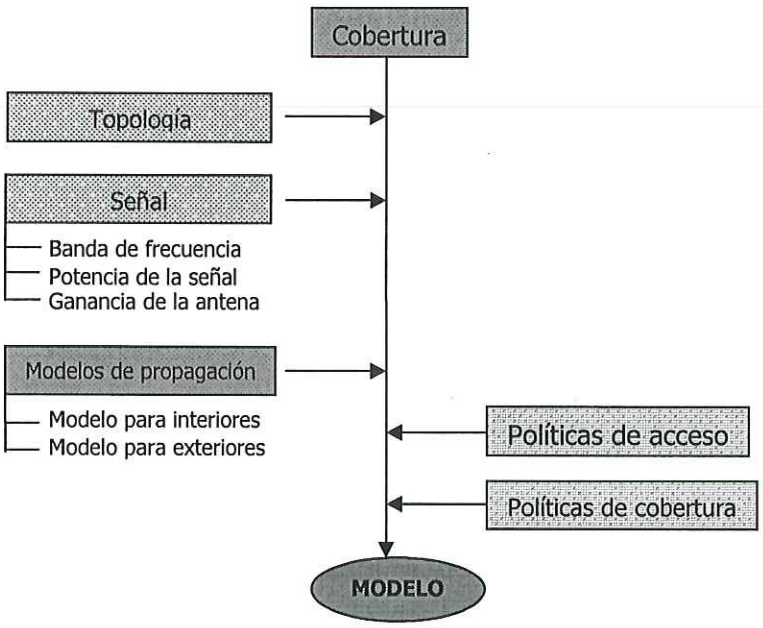


Figura 5.7: Diagrama de cobertura

En las redes inalámbricas la condición de no tener línea de vista provoca mayores problemas que la de tenerla, así como la determinación de los canales y la calidad de los enlaces. En el caso de un ambiente interior, ambas condiciones existen, independientemente de que las señales recorran distancias muy cortas, esto es debido a la gran cantidad de obstáculos presentes en el ambiente (materiales para las fabricación de las paredes, las alturas de cada piso, las divisiones entre pisos, cantidad de vidrio utilizado en las paredes exteriores, además del mobiliario y los equipos que están dentro del inmueble). El tamaño de los posibles lugares es diverso, desde pequeño hasta grande, y la densidad de los obstáculos varia desde baja hasta alta. Estas configuraciones de las áreas de trabajo se encuentran resumidas en la Tabla [VI]

Tabla VI. Tipos de zonas de cobertura [de WIRELESS COMUNICATION, RAPPAPORT]

Configuración	***Tamaño del Lugar***	***Densidad de los obstáculos***
1	Grande sin particiones	Baja
2	Grande con particiones suaves	Baja a media
3	Grande sin particiones	Alta
4	Pequeño	Baja
5	Pequeño	Alta

La configuración de las zonas de cobertura se divide en seis casos donde la división obedece al tipo de enlace de comunicación entre la terminal (usuario) y la estación base (Punto de Acceso), según sea la implementación. Esta es una lista con los seis posibles casos [30].

1. Zona Extragrande.
2. Zona Grande.
3. Zona Mediana.
4. Zona Pequeña.
5. Microzona.
6. Sistema Distribuido.

La radio propagación de interiores es afectada por los mismos mecanismos que la de exteriores, estos son reflexión, refracción, y dispersión. Sin embargo, las condiciones varían mucho más en función de diferentes factores físicos que involucran tanto el diseño de los edificios, como su altura y los materiales con los que están construidos.

Particularmente esta metodología propone en su componente de cobertura el uso de un modelo de propagación para interiores llamado modelo de particiones en el mismo piso.

5.3.1 Modelo de particiones en el mismo piso

Para este modelo se requiere de datos específicos del tipo de construcción de la que se requiera saber las pérdidas. Por lo que este modelo se aplica a construcciones en específico, el cual consta de una serie de mediciones realizadas a diferentes materiales para obtener el calculo de las pérdidas en la construcción. en la siguiente tabla [VII] se muestra una serie de mediciones hechas para diferentes materiales y ubicaciones, se pueden ver las pérdidas generadas por estos materiales, además se puede observar la frecuencia a la que fueron realizados las mediciones.

Tabla VII. Mediciones experimentales para ciertos tipos de edificios[de WIRELESS COMUNICATION, RAPPAPORT]

Tipo de Material	Pérdida en dB	Frecuencia
Metal	26	815Mhz
Aluminio	20.4	815Mhz
Aislamiento de hoja	3.9	815Mhz
Bloques de concreto	13	1300Mhz
Pérdidas por un piso	20-30	1300Mhz
Pérdidas por un piso y una pared	40-50	1300Mhz
Atenuación observada cuando el transmisor toma un ángulo recto en la esquina del corredor	10-15	1300Mhz
Cubierta de metal-12ft^2	4-7	1300Mhz
Maquinaria ligera	1-4	1300Mhz
Maquinaria en General	5-10	1300Mhz
Maquinaria Pesada	10-12	1300Mhz
Escaleras de caracol	5	1300Mhz
Textil ligero	3-5	1300Mhz
Textil Pesado	8-11	1300Mhz
Area en donde los obreros inspeccionan el metal defectuoso	3-12	1300Mhz
Racks metálicos	4-9	1300Mhz
Cajas vacías de inventario	3-6	1300Mhz
Pared bloques de concreto	13-20	1300Mhz
Ducto del el techo	1-8	1300Mhz
Caja de metal de 4m	10-12	1300Mhz
Rack de almacenamiento con papeles	2-4	1300Mhz
Rack de 2.5m con partes metalicas	4-6	1300Mhz

Para el objetivo de nuestro trabajo es necesario contar con listados de las mediciones experimentales para su uso y cálculo, para poder predecir una zona de cobertura con pérdidas más aproximado a lo real y proporcionar una distribución geográfica de los AP's con la mayor cobertura posible, en un inmueble determinado, y con información especifica que definen el tipo de construcción del inmueble en la organización que esta requiriendo el diseño de la WLAN.

5.4 Ancho de Banda

El ancho de banda y las velocidades de transmisión que nos brindan las WLAN permiten hoy hasta velocidades de hasta 54 Mbps con el estándar 802.11a/g mientras que el estándar 802.11b permite velocidades de transmisión de hasta 11 Mbps como se muestra en la Tabla 1. Este ancho de banda es mucho menor al de las redes cableadas, las cuales operan a 100 Mbps y hoy en día hasta 1000 Mbps. El ancho de banda especificado por los estándares 802.11a/b/g son teóricos y se cumple solo en condiciones ideales.

Por eso es necesario tener un mecanismo que nos permita optimizar el ancho de banda y poder asegurar anchos de banda a los usuarios de la WLAN, esta componente incorpora un gestor, el cual trabaja conjuntamente con las aplicaciones.

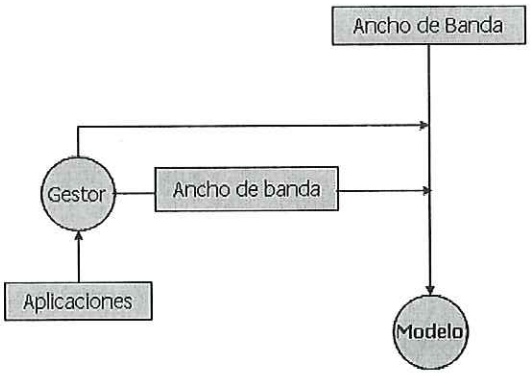


Figura 5.8: Diagrama del gestor de ancho de banda

En la figura 5.8, se muestra la manera en la que el gestor optimiza ancho de banda filtrando solo aquellos paquetes que fueron permitidos en la componente de aplicaciones y que se especificaron previamente.

Uno de los mecanismos que permiten hacer este filtrado es: CBQ (Clase Base Queueing) Encolado Basado en Clases, es el método que propone el modelo para realizar esta actividad, CBQ es un algoritmo basado en clases, el cual propone la división y compartición del ancho de banda en clases estructuradas jerárquicamente, como se muestra en la figura 5.9, cada clase tiene su propia cola y comparte una parte de acho de banda. Una clase hija puede tomar prestado ancho de banda de su padre si le sobra ancho de banda [32]. Existen varios métodos para optimizar el acho de banda tanto de hardware como de software, sin embargo para fines prácticos de este trabajo se plantea el uso de esta herramienta de uso libre que puede ser instalada en un ambiente LINUX y realizar las pruebas correspondientes.

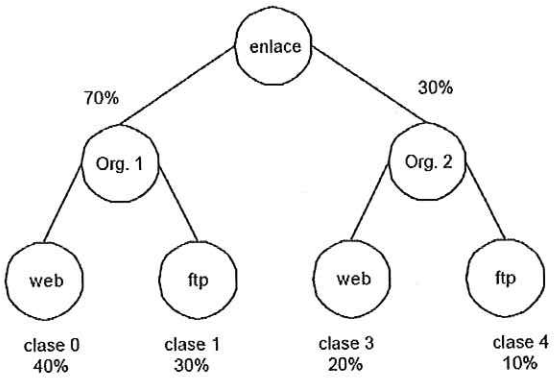


Figura 5.9. Ejemplo de Compartición de Ancho de Banda CQB

5.5 Aplicaciones

Un componente importantísimo para este modelo son las aplicaciones que los usuarios finalmente usan o ejecutan sobre estas redes por lo que es importante delimitar el tipo de

aplicaciones van a ser ejecutadas, tales como acceso a Internet, correo electrónico, consultas a bases de datos y transferencias de archivos. Dado el limitado ancho de banda, no sería recomendado que se utilizaran aplicaciones que consumen mucho ancho de banda, como pueden ser transferencia de video, imágenes, videoconferencia y el videostreaming. Sin embargo, la gestión que estamos haciendo con nuestra componente de manejo de ancho de banda nos permite poder utilizar esos servicios con gran ganancia durante la transmisión, esto solo si es necesario, por que si bien las WLAN no incorporan QoS. Esta herramienta nos permite otra alternativa de uso.

El proceso de planeación plantea la necesidad de tener identificadas las aplicaciones que la organización permitirá correr sobre su WLAN, por ello se realiza un "cuestionario" que trata de identificar las aplicaciones que comúnmente utilizan los usuarios sobre las redes inalámbricas y definir cuales de ellas serían de mayor o menor uso, con el objetivo de establecer jerarquías sobre el filtrado de los paquetes. Este cuestionario lo podemos observar en el [Anexo A] para ser aplicado a los empleados de la organización con el objetivo de contar con estos bancos de datos que contengan información de las aplicaciones asociadas a un cierto ancho de banda por aplicación. En la Figura 5.10, se muestra el proceso de identificación de las aplicaciones utilizando la encuesta (survey).

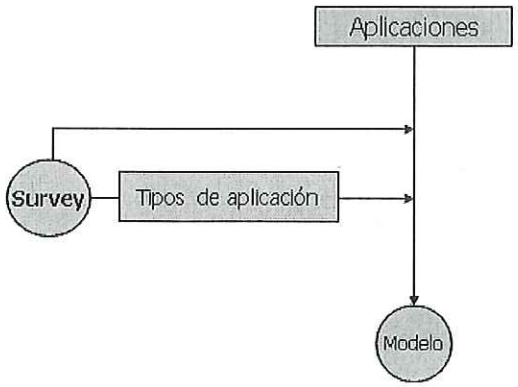


Figura 5.10: Diagrama de aplicaciones

5.6 Equipos/Infraestructura de red

Desde 1999 que fue cuando se ratifican los estándares 802.11a/b, las compañías que se dedican a la fabricación de equipo para redes inalámbricas empiezan a lanzar sus primeras versiones. Los equipos que han sido lanzados desde 1999 han trabajado en los respectivos espectros de frecuencia acorde con el estándar en fabricación como lo muestra en Tabla 1. En la actualidad la familia estándares que ha dominado el mercado de las redes inalámbricas es el IEEE 802.11.

¿Porqué 802.11b ha sido el dominante? La respuesta es sencilla, empresarios del área en redes inalámbricas empezaron a fabricar equipos con el estándar 802.11b certificándolos por el organismo conocido como *WECA* (Wi-Fi Alliance). Mientras que el estándar 802.11a se empezó a fabricar a principios del 2001.

Como los estándares 802.11a/b no son compatibles entre sí, los fabricantes lanzan al mercado equipos independientes para cubrir necesidades particulares. Ésto se realizó en las últimas dos décadas, tal es el caso, que para finales del 2002 compañías líderes del mercado en redes inalámbricas lanzan equipos duales, es decir, equipos con ambos estándares.

Con la aprobación del estándar 802.11g en el 2003, las equipos 802.11a/b/g ofrecen rendimientos adecuados a las conveniencias de los clientes, en la próximas generaciones de las aplicaciones requerirán mayor capacidad de procesamientos y los usuarios reclamarán mayor ancho de banda y mayores coberturas. En respuestas a estas necesidades los grupos líderes en productos trabajan conjuntamente para lanzar próximamente el IEEE 802.11n junto con la Wi-Fi Alliance.

Es importante mencionar que no serviría de nada proponer un diseño elaborado mediante esta metodología, si los equipos que van a ser adquiridos para la implementación de la WLAN no pueden soportar las diversas configuraciones que arroja esta componente, de modo que, si antes era sencillo adquirir un equipo, ahora será necesario observar cuidadosamente sus características que presentan tantos los AP's como los clientes inalámbricos.

Capítulo VI

6. CASO DE ESTUDIO: Universidad Autónoma de Baja California campus Ensenada

---

6.1 Introducción

Durante este capítulo haremos un análisis geográfico del campus Ensenada y daremos un repaso a la infraestructura de red con la que cuenta la UABC actualmente. La UABC fue fundada el 28 de febrero de 1957 debido a una fuerte demanda de la sociedad en construir una escuela de nivel superior en el estado de Baja California, es una institución de servicio público descentralizada de la administración del estado, fue creada con el fin de impartir educación para formar profesionistas, investigadores profesores universitarios, y técnicos útiles en la sociedad, fomentar la investigación científica y extender los beneficios de la cultura. En 1970 se inicio la unidad de Ensenada con la escuela de Ciencias Marinas.

La UABC está compuesta por autoridades universitarias como la junta de gobierno, rector, patronato universitario, directores de las facultades, escuelas e institutos y consejos técnicos y de investigación.

La UABC ha crecido y se ha desarrollado como máxima institución de educación superior en el estado. Cuenta con 33 unidades académicas, (4 escuelas, 22 facultades, 7 institutos de investigación), distribuidas en los cinco municipios de la entidad de Baja California. Cubriendo las principales localidades urbanas y la zona rural, donde atiende a más de 29,792 estudiantes en licenciaturas, y a 951 en 48 posgrados.

6.2 Análisis Geográfico del Campus Ensenada

El campus Ensenada actualmente denominada como la unidad de Ciencia y Tecnología cuenta con tres facultades, dos institutos de investigación, una biblioteca, un departamento de información académica, además del edificio administrativo y un área de deportes, todas estas serán motivo de análisis para el diseño de la red inalámbrica actual de la UABC campus Ensenada. Ver figura 6.1.

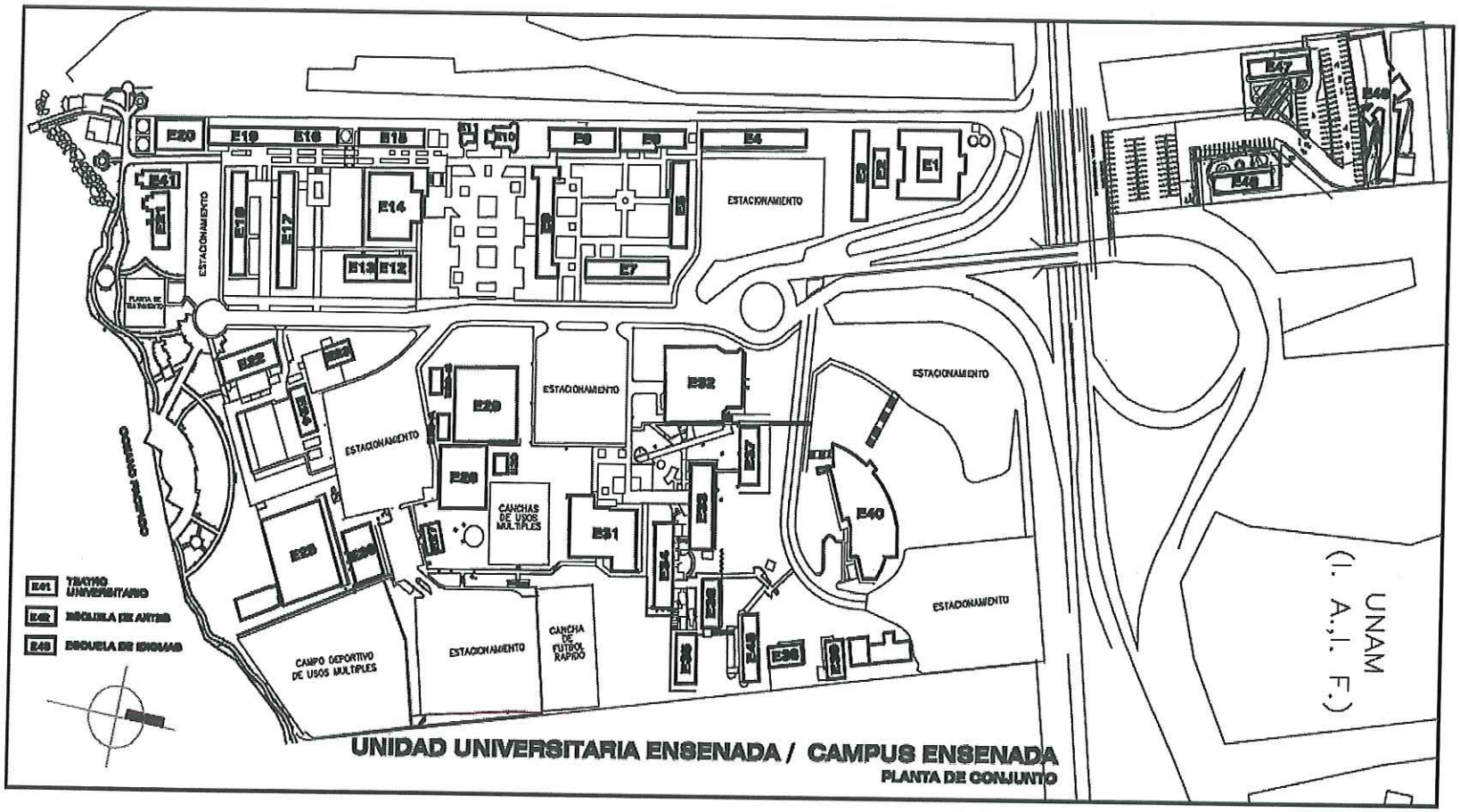


Figura 6.1: Universidad Autónoma de Baja California unidad Ensenada

6.2.1 Facultad de Ciencias

La Facultad de Ciencias inicia oficialmente sus actividades académicas en 1977 bajo el nombre de Escuela Superior de Ciencias Biológicas, con la *carrera de biología.* En 1979 se creo la *licenciatura en Física*, por iniciativa de investigadores del instituto de Astronomía de la UNAM en Ensenada y adopta el nuevo nombre de Escuela Superior de Ciencias, posteriormente en 1986 nacieron simultáneamente las *licenciaturas de Ciencias Computacionales y Matemáticas Aplicadas.*

En 1989 se aprobó la creación de la maestría en Manejo de Ecosistemas de Zonas Áridas, con lo que se le denomina Facultad de Ciencias, además actualmente oferta la *Maestría en Tecnologías de la Información y un Doctorado en Medio Ambiente y Desarrollo.*

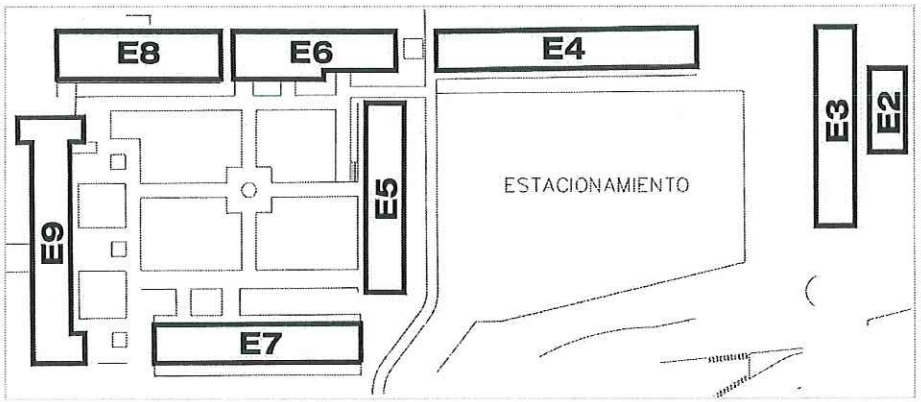


Figura 6.2: Facultad de Ciencias, UABC.

La Facultad de Ciencias esta compuesta por 8 edificios, 1 aula equipada, 5 aulas pequeñas de cómputo, 45 cubículos, 1 auditorio, 12 salones de clase [33]. para una población de 517

estudiantes de licenciatura y 33 estudiantes de posgrado [34], su mapa geográfico se muestra en la figura 6.2.

6.2.2 Facultad de Ingeniería

La Facultad de ingeniería inicio como ingeniería civil en obras portuarias el 15 de agosto de 1983 y se transforma a *Ingeniería Civil* en 1988. La carrera de *Ingeniería en Electrónica* inicia en 1989 y actualmente se encuentra acreditada a nivel nacional.

En 1994 nace la carrera de *Ingeniería en Computación* y actualmente se encuentra acreditada a nivel nacional teniendo un gran éxito, en áreas como Automatización, Redes de Computadoras e Ingeniería de Software. La carrera de *Ingeniería Industrial* inicio en enero de 2002. Ofreciendo las áreas de Manufactura, Control de Calidad y Desarrollo Empresarial.

En 1988 ofrece la *Maestría en Ingeniería* y en 2003, en forma conjunta con otras unidades académicas, ofrece la *Maestría y Doctorado en Ciencias e Ingeniería.* Actualmente la facultad posee la certificación ISO 9001-2000 en los laboratorios de : Civil, Electrónica Básica, Comunicaciones, Mecatrónica, Computación y el Centro de Desarrollo de Proyectos y Servicios de Ingeniería [35].

La Facultad de Ingeniería está compuesta por 7 edificios dentro de los cuales, existen 4 laboratorios de cómputo, 20 cubículos, 1 auditorio, 1 aula de usos múltiples, 30 salones de clase, 3 laboratorios de electrónica, 1 industrial, 1 sala de maestría, y cuenta con una población de 1288 alumnos inscritos en sus diferentes carreras de licenciatura y 35 estudiantes

de posgrado [34], recientemente la Facultad de Ingeniería cuenta con un edificio de tres niveles el edificio E1, en la figura 6.3 se muestra un mapa geográfico de la Facultad.

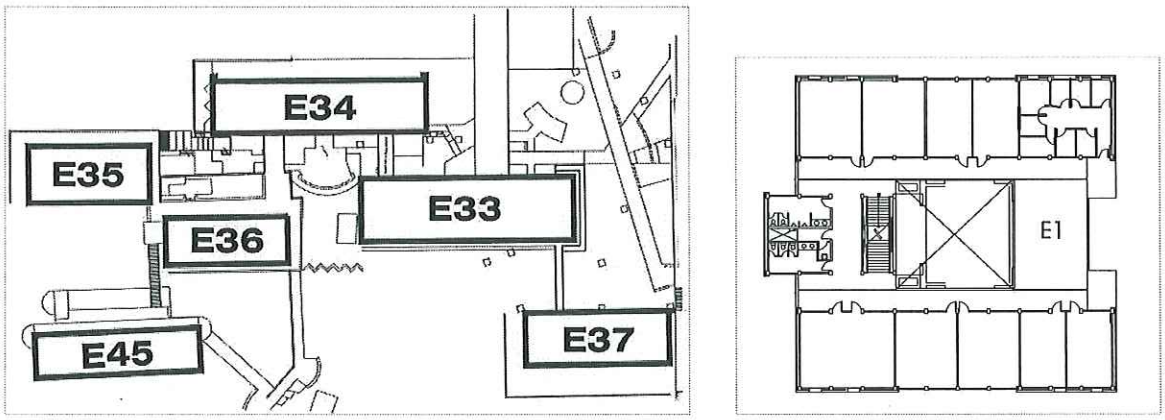


Figura 6.3: Facultad de Ingeniería, UABC.

6.2.3 Facultad de Ciencias Marinas.

La Facultad de Ciencias Marinas (FCM) se imparte la carrera de *oceanólogo,* fue creada el 15 de diciembre de 1960 como Escuela Superior de Ciencias Marinas y cambia a la Facultad en noviembre del 1987, en 1985 fue creado el posgrado en oceanografía Biológica, el cual es reformado y con la colaboración de Instituto de Investigaciones oceanológicas de la misma Universidad da lugar en 1990 a la maestría y doctorado en oceanografía Costera en 1987 se crea la especialidad en administración de recursos marinos [36]. Recientemente la Facultad incorporó dos nuevos programas de licenciatura en ciencias ambientales y biotecnólogo en acuacultura.

La Facultad de Ciencias Marinas actualmente tiene 10 edificios, 3 laboratorios de cómputo, cuenta con laboratorios de bio*logía,* Unidad de Biotecnología en Piscicultura, Edificio de Biología, Instalaciones de Geología y Física, Instalaciones de Biología y Química, Instalaciones de Aulas Magnas, Instalaciones de Acuicultura [37]. La FCM tiene una población de 210 estudiantes. De licenciatura y 101 estudiantes del posgrado [34]. En la figura 6.4 se presenta el mapa geográfico de esta Facultad.

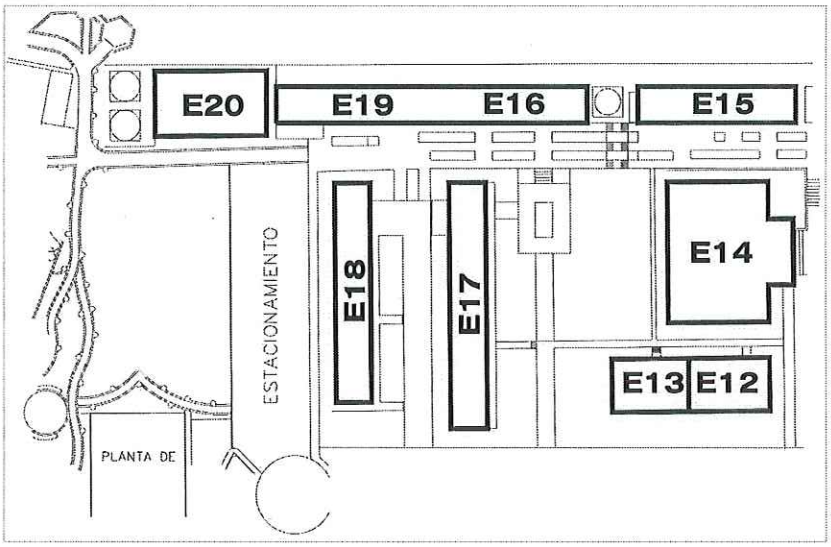


Figura 6.4: Facultad de Ciencias Marinas, UABC.

6.2.4 Biblioteca

La coordinación de Información Académica a través de los departamentos de información Académica dependientes de las vicerrectorias en cada campus, administran y coordinan el sistema bibliotecario de la UABC. Su finalidad es proporcionar servicios de información para satisfacer las necesidades generadas en los procesos de enseñaza-aprendizaje, investigación y difusión de la cultura.

Cuenta a con un catalogo único conocido como "Cimarrón", que permite localizar en el acervo bibliotecario el recurso o tema que se requiera, además de realizar operaciones por medio de Internet sin necesidad de acudir a la biblioteca.

La biblioteca está compuesta por 1 edificio con 10 cubículos, 1 sala de cómputo, 1 sala de hemeroteca, 1 sala de videoteca y la visitan alrededor de 400 usuarios por día. [38]. En la figura 6.5 se presenta un mapa del interior del edificio.

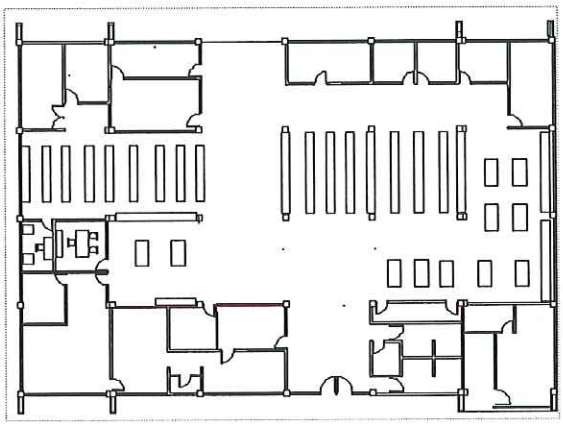


Figura 6.5: Biblioteca Central del Campus Ensenada

6.2.5 Instituto de Investigaciones Oceanológicas

El Instituto de Investigaciones Oceanológicas (IIO), con más de 40 años de experiencia en el estudio del mar y sus costas promueve la conservación, la protección y el manejo sustentable de los recursos marinos, la calidad del medio ambiente, los enlaces entre la ciencias del mar y el desarrollo de la comunidad regional y nacional, así como la formación de profesionistas de licenciatura y posgrado.

En el Instituto se desarrolla investigación en las áreas de Oceanografía biológica, Física, Química, y geoquímica Ambiental, en las disciplinas de: acuicultura, Biotecnología, Fisiología y Nutrición, Botánica, Contaminación y su prevención, Dinámica de Poblaciones, Ecología Molecular, Geociencias Ambientales, Instrumentación Electrónica, Aprovechamientos de Recursos Naturales, Oceanografía sinóptica, modelación, entre muchas otras.

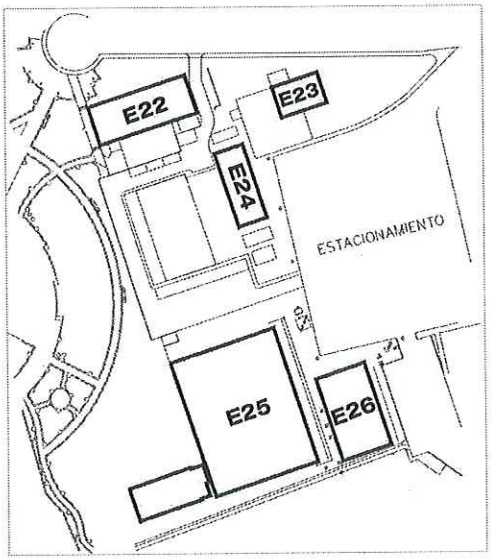


Figura 6.6: Instituto de Investigaciones Oceanológicas, UABC.

Instituto de Investigaciones Oceanológicas (IIO): El instituto de Investigaciones Oceanológicas cuenta con 6 edificios dentro de los cuales hay 50 cubículos, 15 laboratorios, 1 laboratorio de cómputo, 1 auditorio y cuenta con 300 usuarios [39]. En la figura 6.6 podemos observar su mapa geográfico dentro de la UABC;

6.2.6 Instituto de Investigación y Desarrollo Educativo (IIDE)

EL IIDE creado por acuerdo del Consejo Universitario en 1990 ha formado recursos humanos altamente calificados y una sólida infraestructura física y tecnológica para cumplir con sus objetivos de contribuir a modernizar la educación superior y lograr la excelencia académica, especialmente de la UABC, así como de realizar investigación, formar especialistas y desarrollar tecnología que inician en el quehacer educativo.

En 1996, el IIDE inicio su programa de maestría en Ciencias Educativas, y en 2004 inauguro el programa de doctorado en Educación en colaboración con la DES de Educación y Humanidades.

Actualmente el IIDE cuenta con una sala virtual (red edusat, sistema de videoconferencia), un laboratorio de cómputo además de taller de reparación y mantenimiento

El IIDE cuenta con 1 edificio dentro del cual hay 1 aula virtual, 1 laboratorio de cómputo, 12 cubículos, y cuenta con 30 usuarios. El IIDE actualmente tiene una población de 33 estudiantes de posgrado [40]. En la figura 6.7 se muestra la figura del edificio antiguo de IDE y en la figura 6.8 se muestran las nuevas instalaciones del IDE, los cuales se encuentran cruzando la carretera Tijuana-Ensenada que los divide.

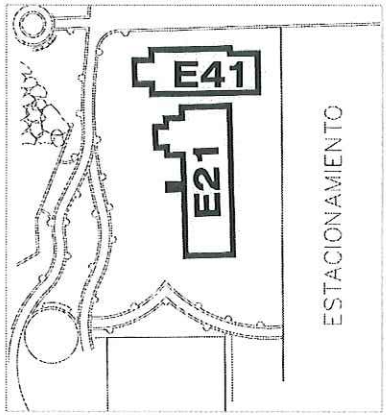


Figura 6.7: Instituto de Desarrollo Educativo, UABC. (Antiguos Edificios)

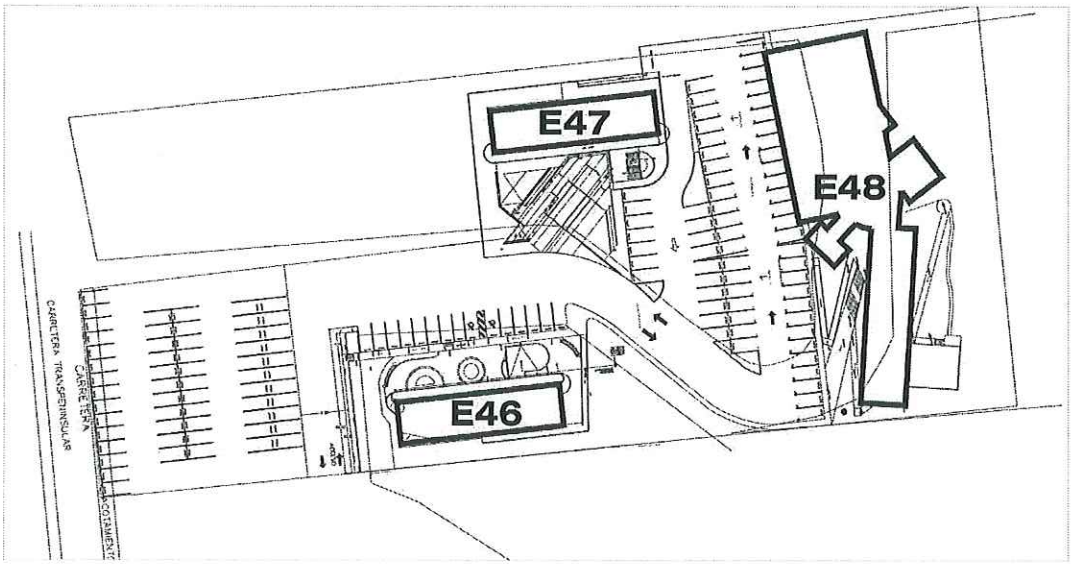


Figura 6.8. Instituto de Desarrollo Educativo, UABC. (Nuevos Edificios)

6.2.7 Departamento de Información Académica (DIA)

El Departamento de Información Académica antes (CECUUE), cuenta con 1 edificio el cual se divide en 4 niveles, dentro del nivel 1 se encuentran 5 salas de cómputo, 1 sala de vídeo conferencia y 1 auditorio. El nivel 2 cuenta con 1 sala de cómputo, 1 salón de conferencias, 1

área de redes y 5 cubículos, el nivel 3 cuenta con 1 sala de cómputo, 12 cubículos y 1 sala de y a salas de cómputo y el nivel. [41]. En la figura 6.9 se muestra el mapa geográfico de DIA dentro de las instalaciones de la UABC.

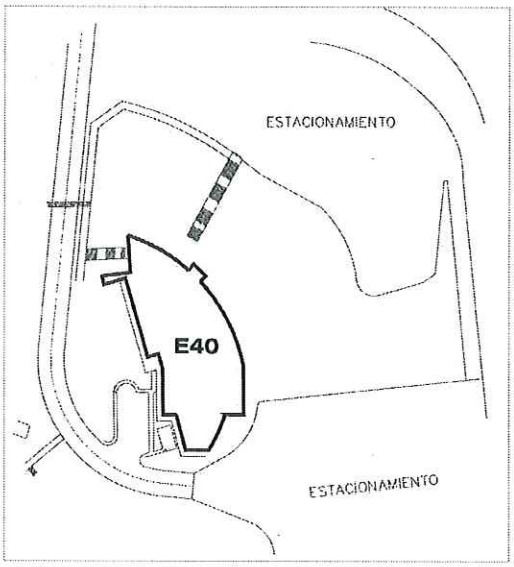


Figura 6.9: Departamentos de Información Académica, UABC.

6.2.8 Vicerrectoría.

En el edificio de rectoría o edificio administrativo se encuentra los diferentes departamentos que se encargan de la administración y servicios que ofrece la UABC a sus estudiantes, dentro de los cuales están: Bienestar Estudiantil, Obras e Instalaciones, Investigación y Postrado, Extensión Universitaria, Servicios Escolares, Departamento de Servicio Social y Becas, Finanzas etc. Dentro de los cuales se encuentran más 50 usuarios, 30 oficinas 4 aulas de uso general.

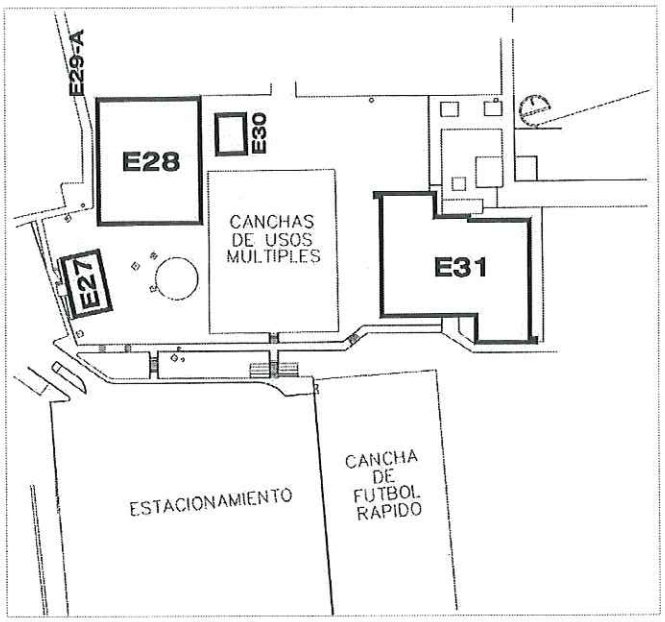


Figura 6.10: Rectoría y Deportes, UABC.

6.3 Análisis de infraestructura de la red actual

6.3.1 Infraestructura de red cableada del campus Ensenada

La UABC cuenta con cuatro enlaces principales: un enlace dedicado de 4 Mbps del tipo UNINET el cual se utiliza para la llegada de los paquetes, un enlace de 6 Mbps que se utiliza para las peticiones que se realizará dentro del campus Internet a través de Telnor (ISP) y otro enlace que se tiene con CICESE para INTENET-2, además de dos conexiones INFINITUM para accesos locales como es la red inalámbrica WLAN y las salas de DIA.

La UABC cuenta una dorsal a lo largo y ancho del campus de fibra óptica multimodo, la cual da servicio de red de datos, telefonía y vigilancia (cámaras de video), por medio de la cual se proveen velocidades de hasta 1000 Mbps a cada una de las áreas (Escuelas, Facultades,

Institutos, Centros de Investigación, etc.) a través de dispositivos que hacen la interconexión entre áreas. Ver figura 6.11.

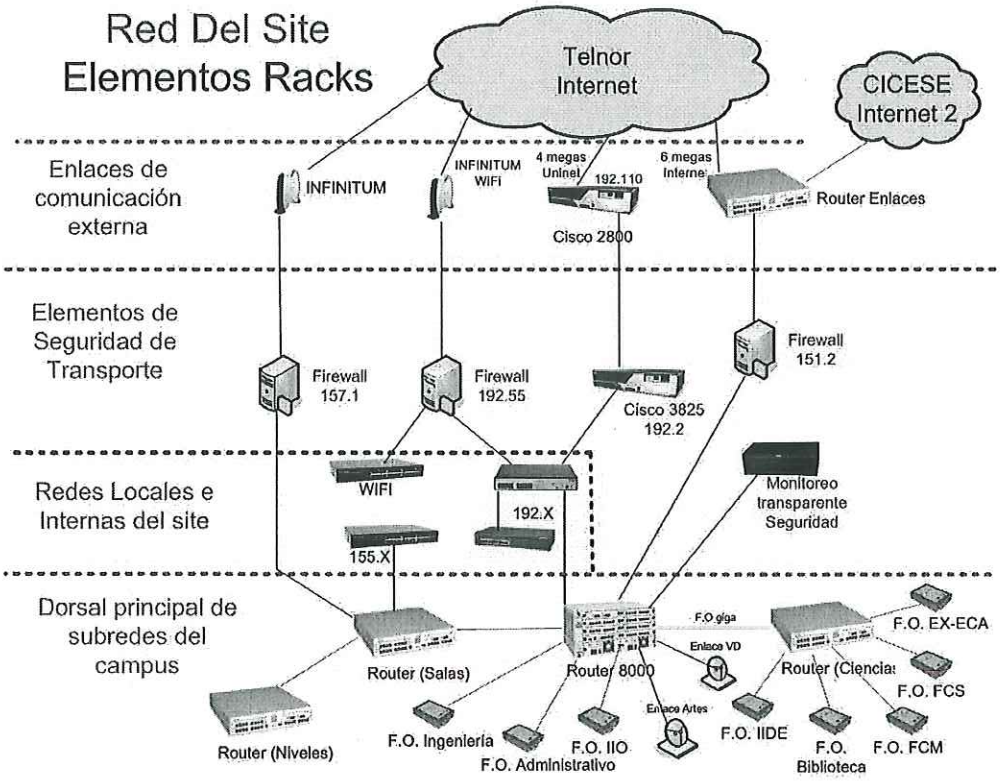


Figura 6.11: Infraestructura de Red de la UABC campus Ensenada.

6.3.2 Infraestructura de la Red Inalámbrica WLAN.

Desde junio del 2006 la UABC lanza un proyecto de Internet inalámbrico en la UABC [43], en la cual esta primera etapa contempla los principales espacios abiertos y jardines del campus. Se encuentran distribuidos por el campus siete puntos de acceso los cuales dan servicios a la facultad de ingeniería, facultad de ciencias, a la facultad de ciencias marinas, al

instituto de investigaciones oceanológicas, y biblioteca, además de algunos espacios como es la explanada y otros lugares como estacionamientos y áreas recreativas.

Tabla VIII; Relación de Puntos de acceso que cubren el campus Ensenada, UABC

SSID	Dirección MAC	Canal	Ubicación	Int/Ext
alumnos	00118808A0D1	6	E32 - biblioteca	Interior
alumnos	001188071B68	11	E32 - biblioteca	Interior
alumnos	001188081A78	11	E25 - IIO	Exterior
alumnos	00118805E0B8	11	E17 - FCM	Exterior
alumnos	001188061520	1	E8 - FC	Exterior
alumnos	00118805CAD8	11	E9 - FC	Exterior
alumnos	00118805E0A6	6	E2 - Ingeniería	Exterior
alumnos	00118804A1E5	11	E1 - Ingeniería	Exterior

Los puntos de acceso, de la marca Enterasys de la serie RoamAbout AP4102, están directamente conectados a la dorsal de fibra óptica de la UABC. Es importante mencionar que existe una dorsal a lo largo y ancho de la UABC de fibra óptica multimodo por medio de éstas se separa el tráfico de la red de datos, cámaras de seguridad y la red inalámbrica WLAN. De esta manera el tráfico de datos es independiente para cada una de ellas. En la tabla VIII se presenta una relación de los puntos de acceso que cubren las áreas de cobertura de la señal inalámbrica, se muestran su ubicación y los canales en los cuales trabajan.

6.3.2.1 Cobertura actual de la Red Inalámbrica

6.3.2.1.1 Instituto de Investigaciones Oceaonológicas (IIO)

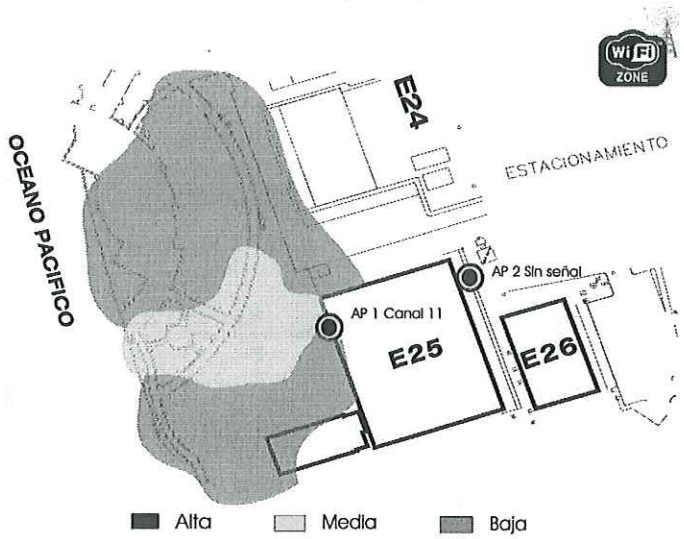


Figura 6.12: Cobertura de la Red Inalámbrica de alumnos en el IIO – exterior

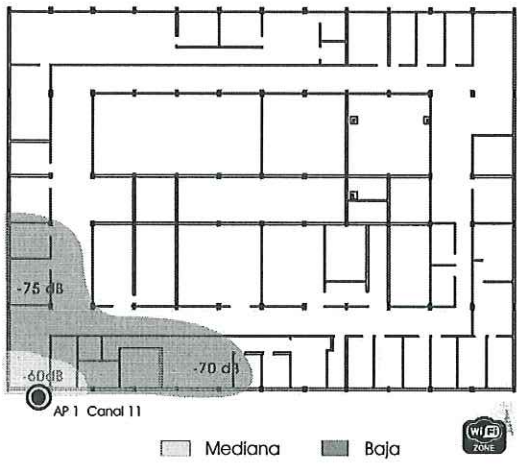


Figura 6.13: Planta alta IIO

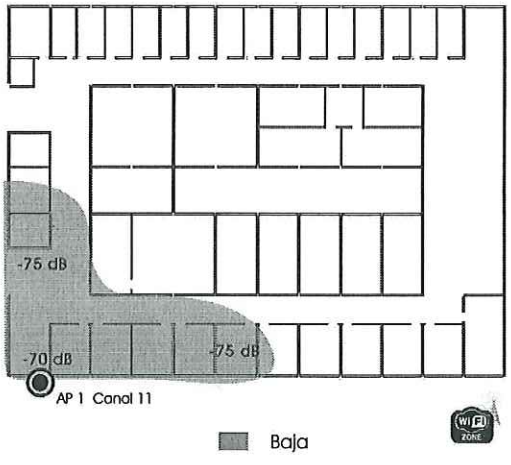


Figura 6.14: Planta baja IIO

6.3.2.1.2 Facultad de Ciencias Marinas (FCM)

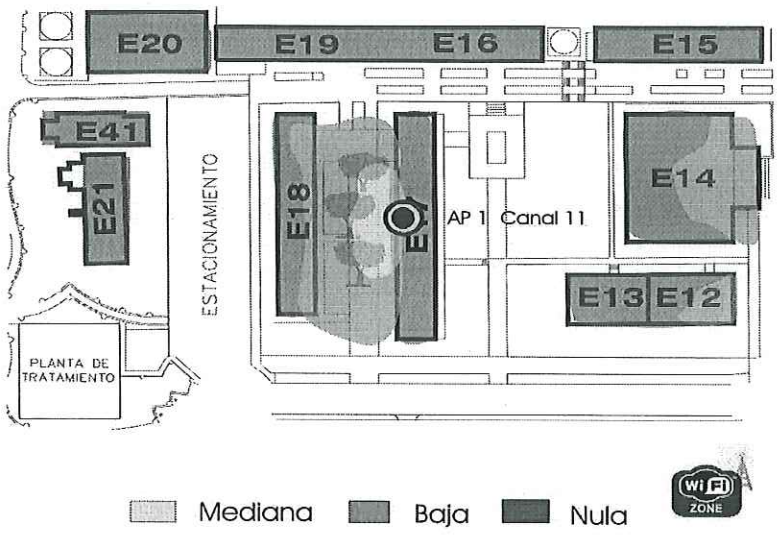


Figura 6.15: Cobertura de la Red Inalámbrica en la FCM – exterior

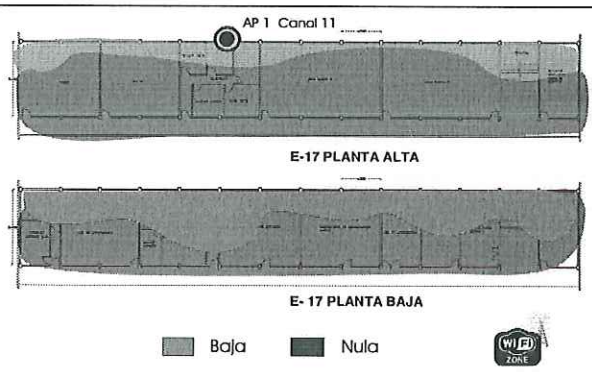


Figura 6.16: Cobertura del E17 - interior

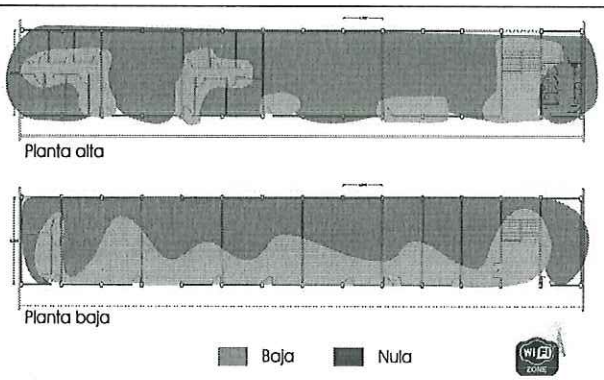


Figura 6.17: Cobertura del E18 - interior

6.3.2.1.3 Facultad de Ciencias (FC)

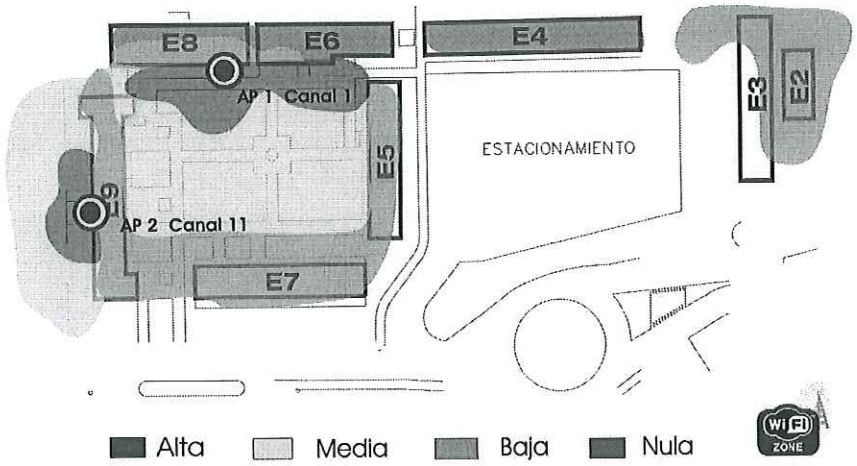


Figura 6.18: Cobertura de la red inalámbrica en la FC – exterior

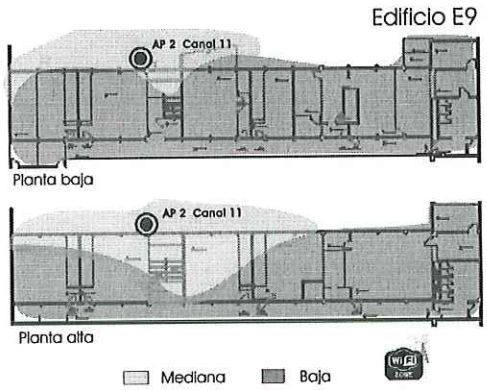


Figura 6.19: Cobertura del Edificio 9 - interior

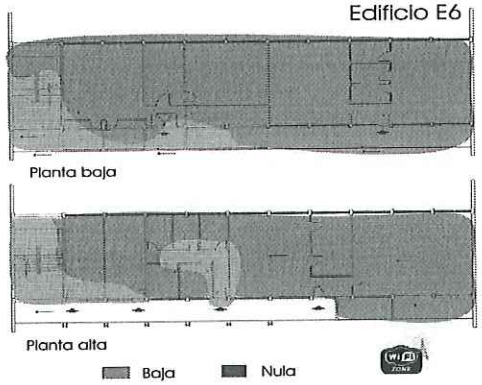


Figura 6.20: Cobertura del Edificio 6 - interior

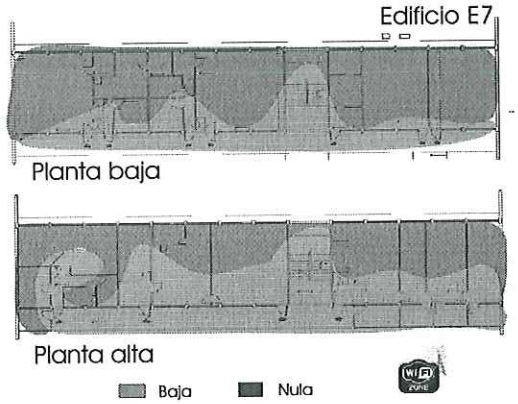


Figura 6.21: Cobertura del Edificio 7 - interior

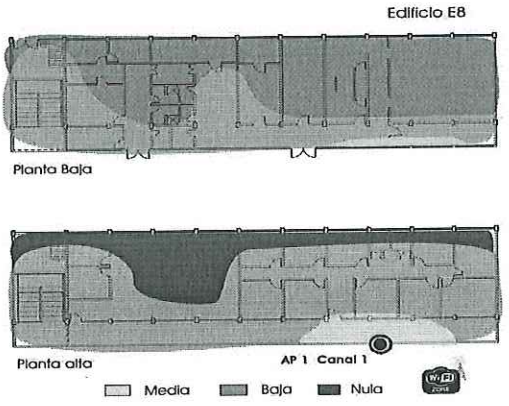


Figura 6.22: Cobertura del Edificio 9 - interior

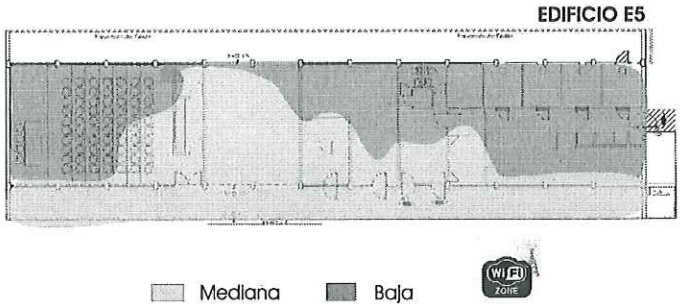


Figura 6.23: Cobertura del Edificio 9 - interior

6.3.2.1.4 Biblioteca

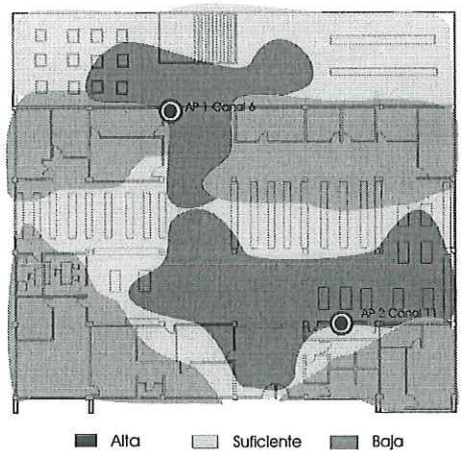


Figura 6.24: Cobertura de la biblioteca central del Campus Ensenada

6.3.2.1.5 Facultad de ingeniería

Primera Sección

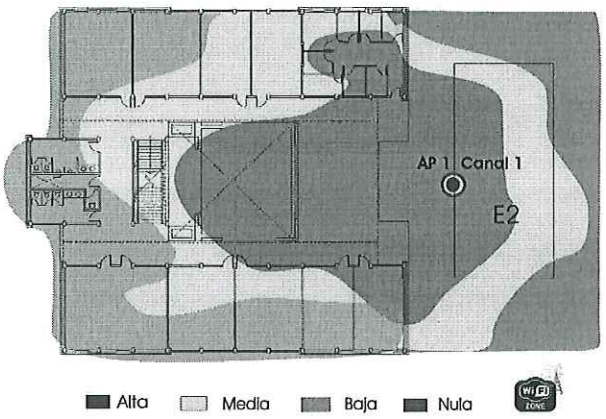


Figura 6.25: Cobertura del primer nivel del edificio E1

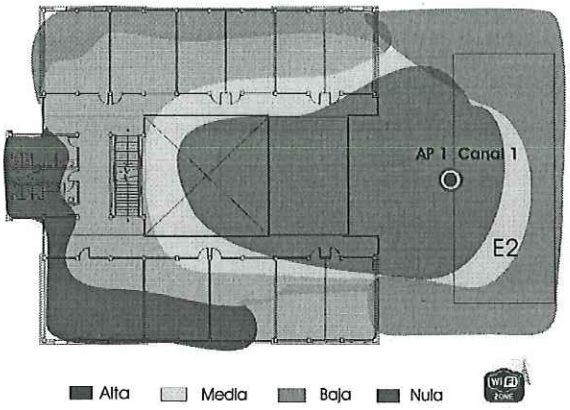


Figura 6.26: Cobertura del segundo nivel del edificio E1

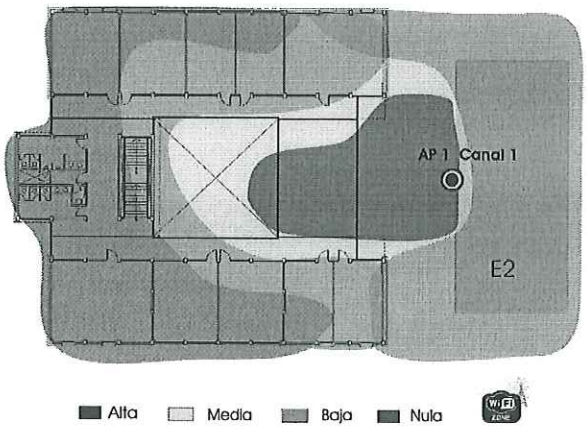


Figura 6.27: Cobertura del tercer nivel del edificio E1

Segunda sección

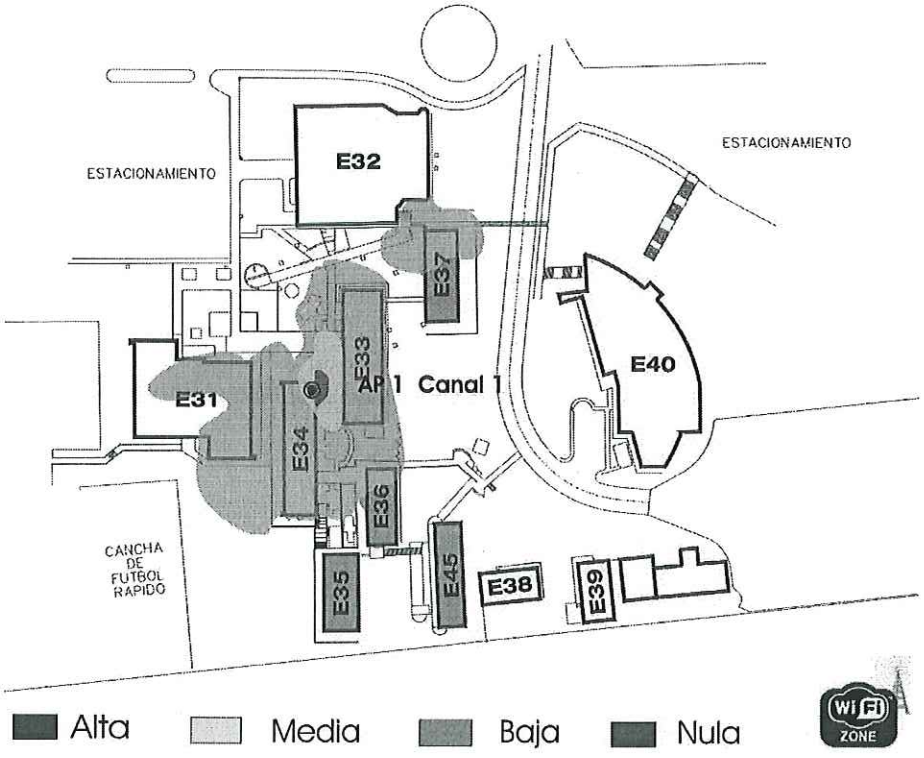


Figura 6.28: Cobertura de la res inalámbrica en la Facultad de Ingenierita

6.4 Análisis de Seguridad de la WLAN del Campus Ensenada

La Dirección de Informática de la Universidad Autónoma de Baja California (UABC) se encarga de la seguridad de los servicios de cómputo en el campus Universitario, existe hoy en día un tipo de seguridad intermedia para el acceso a la red inalámbrica, además de mecanismo adicionales no propios de la WLAN como firewall, Proxy servers y un RADIUS Server para autenticación de los usuarios inalámbricos, este mecanismo está ligado a la cuenta de correo electrónico institucional de cada universitario.

6.6 Análisis de los resultados de la encuesta

Una actividad que resulta interesante es aplicar un mecanismo que te permita conocer el sentimiento de las personas dentro de la organización. Este tipo de mecanismo como las encuestas nos van a permitir tener mayor conocimiento de las necesidades reales de los usuarios, además de saber que tanto conocen los usuarios en relación con la tecnología Wi-Fi, esto permitirá a los encargados de diseñar una WLAN establecer el punto de partida en cada una de las etapas durante la planeación y el diseño de la WLAN.

En nuestro caso de estudio se aplicó una encuesta para conocer el desempeño que ha tenido la WLAN del campus Ensenada desde su implementación, sin embargo no perdamos de vista que este tipo de encuestas se tienen que realizar durante el proceso de planeación y el diseño de la WLAN.

La encuesta tiene como objetivo evaluar el desempeño de la red WLAN actual de campus Universitario, particularmente está hecha para obtener información que ayude en la configuración de los componentes que propone esta metodología, como es la cobertura de la señal, dentro del campus, las aplicaciones que regularmente utilizan los usuarios, como podría crecer en un futuro el numero de usuarios de la red WLAN del campus Universitario, el nivel de satisfacción que ha tenido en los usuarios a partir de su implementación, que nivel de conocimiento tienen los usuarios sobre la tecnología Wi-Fi. A través de estas encuestas se podrá ajustar y configurar de manera adecuada cada componente, para obtener un buen funcionamiento de la WLAN en el campus.

La encuesta se realizó en las instalaciones de campus universitario de la ciudad de Ensenada durante el periodo 2006-1 y 2006-2. En total se aplicaron cien encuestas a universitarios, que fueron clasificados en cinco grupos: técnicos, administrativos, docentes, investigadores y estudiantes. El número de encuestados por grupo lo podemos observar en la grafica 6.29, en la cual podemos observar claramente que más de la mitad fueron estudiantes, con sesenta y cinco encuestados, los cuales realizan sus estudios en alguna de las unidades académicas que mencionamos anteriormente, el resto de los encuestados fueron los siguientes: diez investigadores, seis técnicos, catorce profesores de tiempo completo y cinco administrativos, es importante mencionar que todos los encuestados no pertenecen a una solo unidad académica si no que fueron encuestados de manera aleatoria en las diferentes unidades académicas del campus.

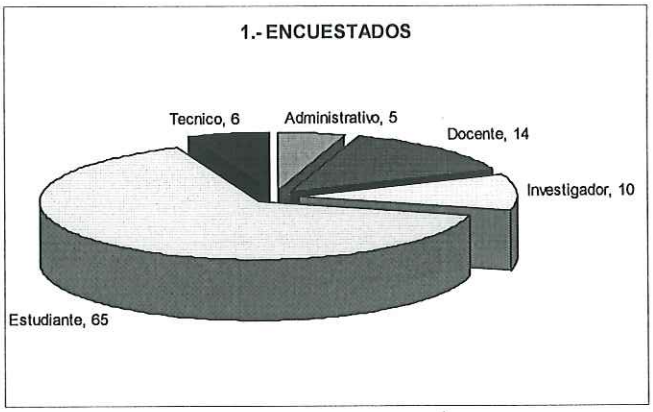


Figura 6.29 : Numero de personas encuestadas

Una de las intenciones de la encuesta era poder estimar el número de usuarios potenciales a utilizar la red inalámbrica y estimar el crecimiento que podría haber durante los próximos años, por lo que realizamos dos preguntas para ello. La primera pregunta fue sí ya contaba con un computadora portátil y segunda que sí en cuanto tiempo estaría dispuesto a comprar un equipo de cómputo portátil, como podemos observar los resultados de esta pregunta en la figura 6.30, más de la mitad de los encuestados cuentan ya con una computadora portátil (laptop) con el cincuenta y ocho por ciento de los encuestados, mientras que el resto de ellos están pensando en adquirir una, dentro de los próximos cinco años. Ver figura 6.31.

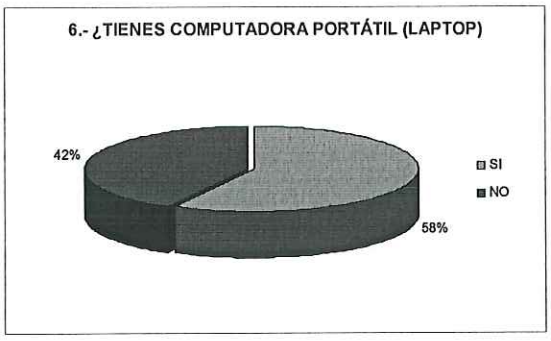


Figura 6.30 : Porcentaje de personas que cuenta con computadora portátil.

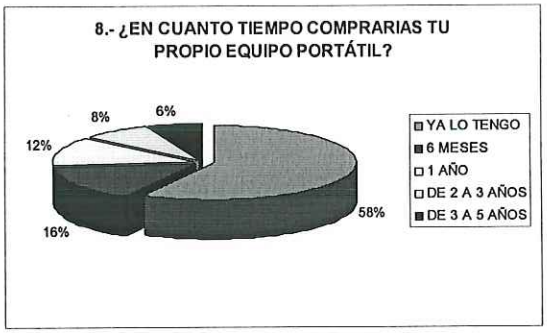


Figura 6.31 : Porcentaje de personas próximas en adquirir un equipo de cómputo.

Otra de las intenciones de la encuesta era conocer que tanto conocimiento y experiencia tienen los universitarios en el uso de esta tecnología Wi-Fi, por lo que para esto, preguntamos si sabían que era una red inalámbrica, que tan útil podría ser para ellos esta tecnología y si tienen conocimiento de cómo debe configurar su equipo para poder hacer uso de este servicio. Como podemos observar en la figura 6.32, solo el diez y seis por ciento de los encuestados no conocen de esta tecnología, el sesenta y seis por ciento considera que es mucho muy útil para ellos contar con una red inalámbrica, el resto la considera un poco útil o nada. Ver figura 6.33.

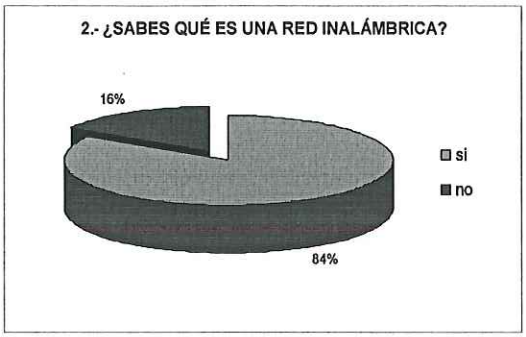


Figura 6.32 : Porcentaje de personas que saben o no que es una rede inalámbrica

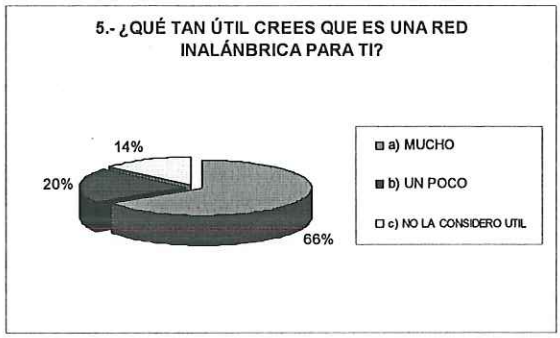


Figura 6.33 : Porcentaje de personas que piensan que tan útil puede ser una red inalámbrica

En relación a su experiencia sobre como debe configurar el equipo el treinta y ocho por ciento de los encuestaron dijeron que no tenían los conocimientos para poder configurar sus computadoras portátiles para poder acceder a la red inalámbrica, lo cual nos hace pensar que requieren de ayuda para poder establecer esta conexión, el resto no tiene problemas.

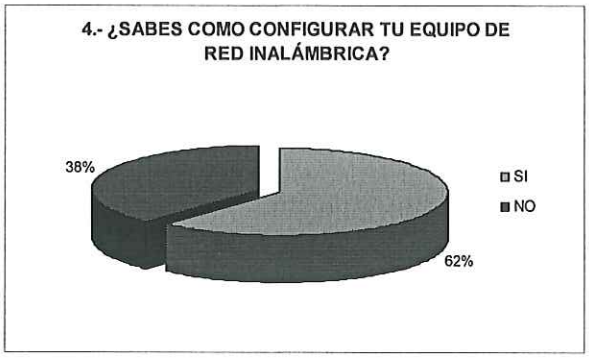


Figura 6.34 : Porcentaje de personas saben o no configurar sus equipos

Figura 6.35 : Porcentaje de personas que saben o no que equipo tendrían que comprar

También se les preguntó si sabría que tipo de computadora tendría que comprar para poder utilizar el servicio de red inalámbrica. El sesenta y dos por ciento dijo que sí sabía que características tenía que tener para comprar un equipo compatible con la red inalámbrica de la universidad, el resto dijo que no. Ver figura 6.35.

Otro de los objetivos de la encuesta era saber si los universitarios ya tienen conocimiento de que existen una red inalámbrica en el campus Universitario y si saben en que lugares pueden utilizarla. Ver figura 6.37. El setenta y cuatro por ciento de las personas que se encuestaron tienen conocimiento de que ya existe una red inalámbrica en la UABC, el resto de ellos desconoce si se cuenta con esta tecnología, y se les preguntó en que áreas de la universidad consideraban ellos que debería tener mayor cobertura para poder hacer uso de este servicio y la mayoría coincidió que en las aulas de clases con el sesenta y cuatro por ciento, mientras que el resto piensa que en las oficinas, biblioteca, cafetería y solo el cuatro por ciento en los jardines. Este último dato llamo mucho la atención, ya que como mencionábamos

anteriormente la universidad cubrió en esta primera etapa los jardines y áreas de estar para los estudiantes. Ver figura 6.36.

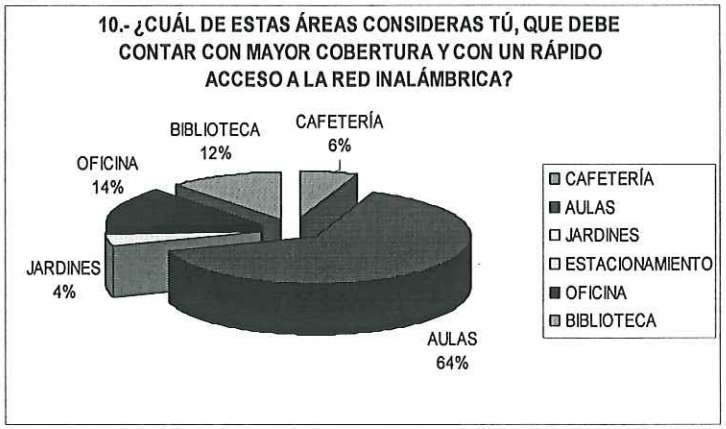


Figura 6.36 : Porcentaje de personas que consideran en que áreas debe haber mayor cobertura

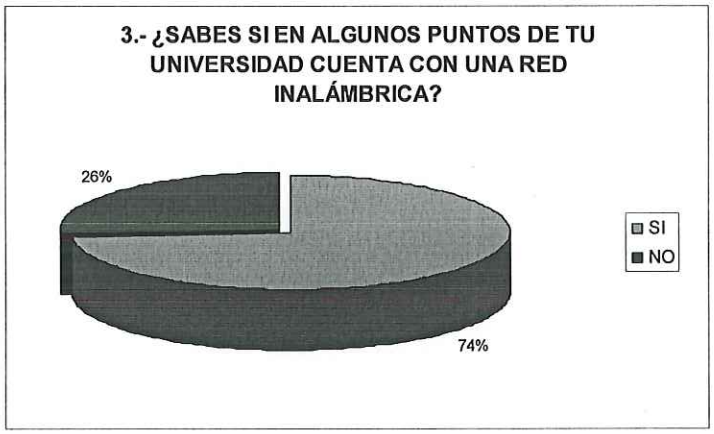


figura 6.37: Porcentaje de personas que saben o no que existe la red inalámbrica en la UABC

Identificar las horas de mayor uso para poder usar herramientas de administración que nos ayuden a resolver el congestionamiento de tráfico que se genera en las horas, las horas de mayor uso se muestran en la figura 6.38. Preguntamos que tan eficiente crees que sea la red

inalámbrica de la UABC, por lo que el sesenta y seis por ciento de los encuestados contestaron que no es muy eficiente, y el resto opinó que si era eficiente. Ver figura 6.39.

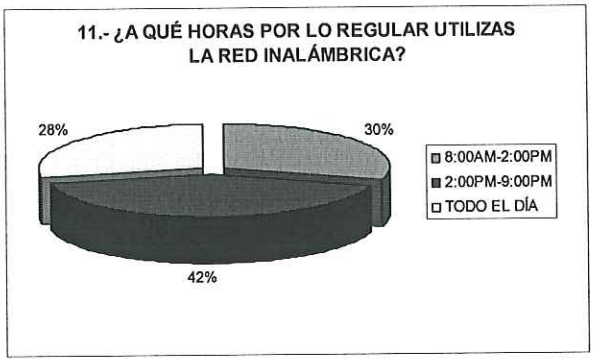


Figura 6.38 : Horario de mayor uso de la red inalámbrica de la UABC

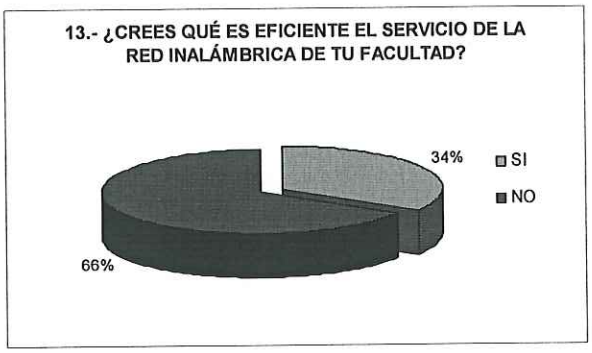


Figura 6.39 : Nivel de eficiencia de la red inalámbrica de la UABC.

Una de las razones por las que es necesario realizar esta encuesta durante el proceso de diseño es para identificar el tipo de aplicaciones que se estarán ejecutando sobre la red inalámbrica y de esta manera poder administrar los servicios adecuadamente y poder ofrecer los servicios que realmente estarán utilizándose por usuarios finales, también se les preguntó a los usuarios que tipo de aplicaciones son las que más utilizaban cuando trabajaban en la red inalámbrica, se les pidió que la contestaran en orden de prioridad, y bien se obtuvieron datos interesantes, algunos ya muy conocidos como el de navegar en Internet, la actividad numero uno que realizan los usuarios de la red inalámbrica. Sin embargo un dato interesante resulto que la actividad como segunda opción que tiene que ver con servicios internos que presta la universidad a través del WEB, como son el proceso de inscripción y llenado de formatos en general de los diferentes departamentos administrativos y académicos que tiene la Universidad para los estudiantes. Descargas por Internet y acceso a bases de datos de

información académica fueron las actividades que menos realizan los usuarios, esta información la podemos observar en la figura 6.40.

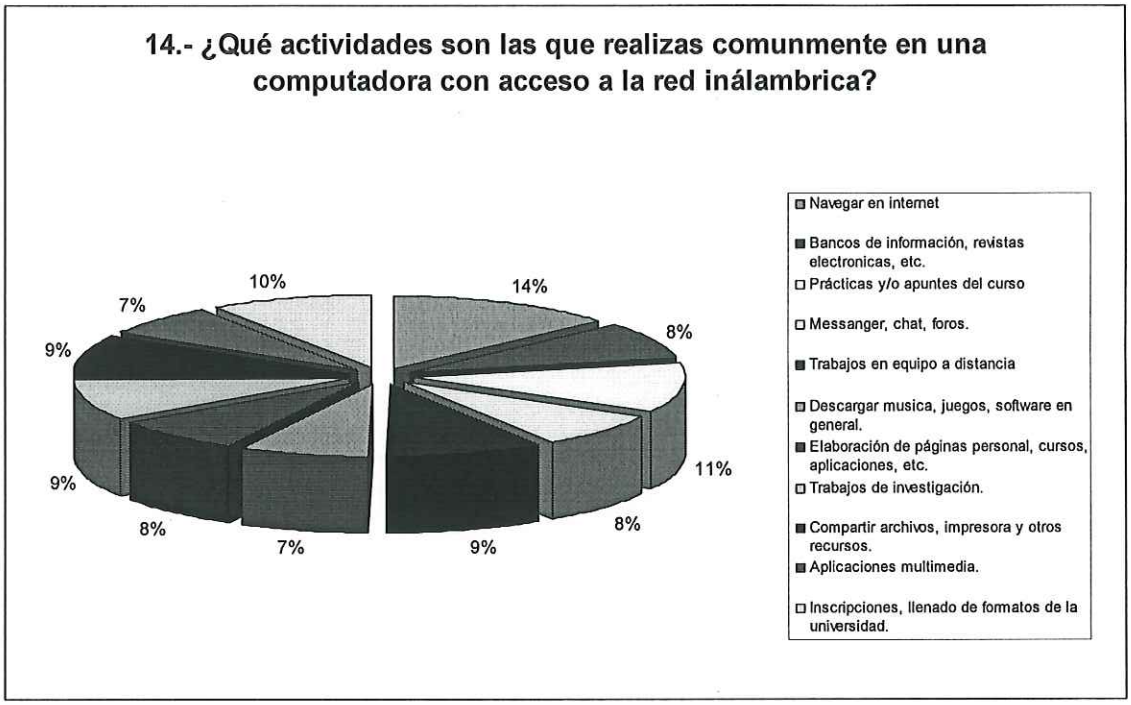


Figura 6.40 : Resultados de la encuesta en relación al tipo de actividades que realizan los usuarios mediante el uso de la red inalámbrica.

Capítulo VII

7. RESULTADOS Y DISCUSIÓN

7.1 Caso de Estudio

En la actualidad la red inalámbrica del campus Ensenada de la UABC, requiere de una revisión en varios de sus componentes. A continuación ubicáremos la red inalámbrica actual en la ruta crítica que se plantea, para poder establecer un juicio real de su efectividad y su desempeño.

La metodología especifica trece componentes a considerar durante el proceso de planeación y diseño de una WLAN. Sin embargo la red Universitaria cubre solo cinco de los trece que utiliza esta metodología. Esto de se debe a que durante la etapa de planeación no fueron considerados. Los componentes que la red Universitaria si cumple son: protección/seguridad al manejar una seguridad intermedia con la utilización de un servidor RADIUS con

mecanismo de autenticación de login y password. En la componente de cobertura si se considero que el manejo de los IPs fuera dinámico, y una página web sencilla para la autenticación y registro del certificado para los usuarios inalámbricos la cual forma parte de la componente gestión/administración. No obstante otra de ellas se dejó a un lado como la componente de cobertura la cual no se realizó adecuadamente con una buena distribución de los puntos de acceso.

Anteriormente presentamos gráficas de la potencia de la señal en cada uno de los edificios del campus, y pudimos observar que existen pérdidas de la señal en cada una de las áreas. Además existe una variedad de puntos de acceso alrededor del campus que no son parte de la red de alumnos y de los cuales no está regulado su funcionamiento. Estos puntos de acceso no regulados traen como consecuencia que sufran interferencias entre ellos. Las gráficas se muestran en el Anexo B. Ahí se muestran todos los puntos de acceso que fueron monitoreados con la herramienta Network Stumbler y que no forman parte de la red Universitaria.

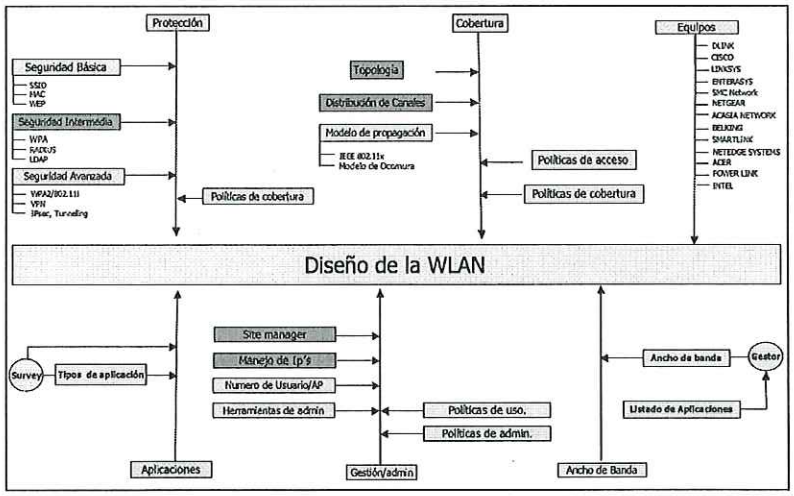


Figura 7.1: Ruta Critica que define la red WLAN de la UABC

El componente de gestión/administración contempla la posibilidad de contar con un sitio de Internet en apoyo a todas las actividades de gestión y manejo de usuarios. Además debe de contemplar la posibilidad de ver estadísticas y gráficas de tráfico para el monitoreo diario de la WLAN. El tipo de aplicaciones hoy en día que pueden ser ejecutadas está regido por un firewall que bloquea todo aquella información que no es permitida.

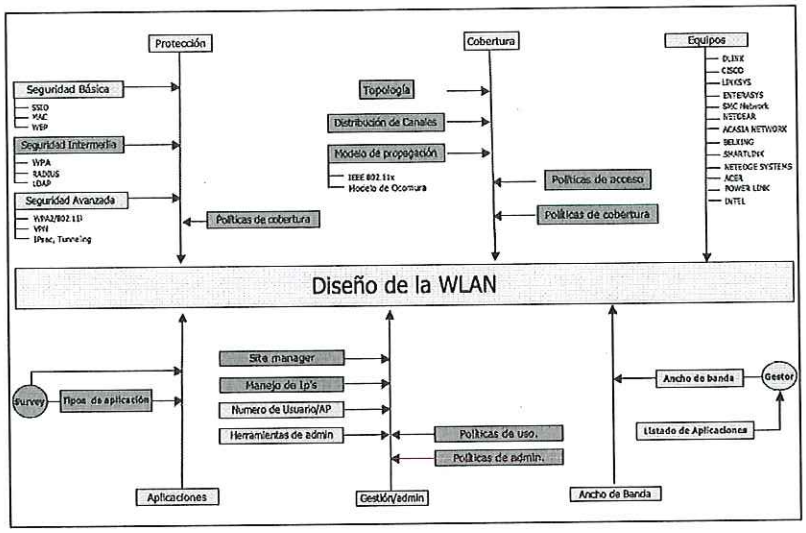


Figura 7.2: Ruta crítica que define lo mínimo a contemplar

7.2 Políticas de Seguridad

Desafortunadamente el departamento de información académica (DIA) no cuenta con un documento de políticas que regulen el buen funcionamiento de la red cableada y mucho menos la red inalámbrica de la Universidad. Este documento en la mayoría de los casos es elaborado al inicio antes de ser desplegada la red WLAN, y se construye en cada una de sus

fases de diseño. No existe hoy en día un documento de políticas que lleven al buen desempeño la red inalámbrica de la UABC.

La seguridad hoy en día es un punto que no hay que dejar pasar por alto, la información que viaja por el Internet es insegura y cualquier hacker que se proponga a robar información lo puede hacer fácilmente con las herramientas que actualmente existen. Muchos de los administradores de red no contemplan la seguridad como una de sus actividades principales e incluso no las programan en su ciclo de actividades.

La información, así como el recurso de cómputo, es de vital importancia brindarles la protección necesaria, ya sea en diferentes niveles: protección física, protección perimetral o protección en host.

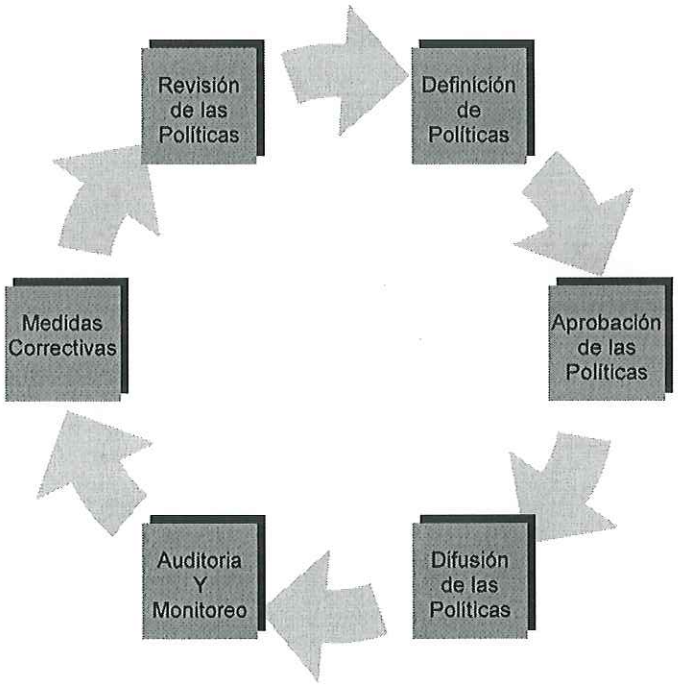


Figura 7.3: Proceso para definición de políticas de seguridad para WLANs

En la actualidad el proceso de desarrollo de las políticas es sumamente importante en cualquier organización o institución que cuente con una red, el desempeño y la operación de las acciones de trabajo deben ser aceptables, por lo que la realización de estas reglas se debe dar en un principio de manera clara y pensando siempre en el beneficio de la organización.

Es importante mencionar que la construcción de estas políticas es un proceso donde intervienen las personas responsables de las actividades que se realizan dentro de la organización, así como, los administradores encargados de la seguridad en la red.

Así como las redes cableadas, las redes WLAN requieren de políticas que estén diseñadas, implementadas y esforzadas al máximo en el desempeño para reducir al máximo una situación de inseguridad que se presente.

Las políticas para una WLAN, deben de cumplir con un proceso estándar que consta de seis pasos fundamentales: Ver figura 7.1.

1.- Definición y Documentación de las Políticas: Para establecer y documentar políticas para las redes inalámbricas WLAN, las organizaciones tienen que tomar en cuenta cuatro componentes clave para este proceso: Uso de las WLAN, configuración de red, seguridad, y el desempeño de la red. Aunque en cada organización será distinto el documento de políticas éstas son formuladas de acuerdo a estos cuatro grupos.

a) Políticas de Uso de las WLAN: Es importante determinar el tipo de aplicaciones que correrán sobre la red inalámbrica y las localidades donde debe tener o no

acceso. No es recomendable para aplicaciones con información muy sensible. Estas aplicaciones son determinadas por los usuarios y se obtiene a partir de una encuesta que se realiza a los empleados de la organización, en el Apéndice 2 presentamos un ejemplo de esta encuesta.

Tabla IX: Políticas de USO

Aplicaciones a través de la WLAN	Las aplicaciones que requieren de mucho ancho de banda y los datos extremadamente confidenciales de la empresa no son recomendadas para que corran sobre la WLAN
Network Roaming	Defina los puntos de acceso y las WLANs con las cuáles cada estación se permite conectar.
Ambientes descontrolados	La organización debe determinar dónde podrán conectarse descontroladamente las laptops con gíreles y definir las capacidades de acceso de las VPN conexiones de casa y otros lugares

b) Políticas de Configuración: Antes de que la WLAN sea desplegada, es importante que las políticas de configuración de la red sean establecidas, ya que a través de éstas la instalación y configuración de los equipos se realizarán, de lo contrario sí estas políticas fueran establecidas después de que la WLAN fuera instalada entonces se procederá a revisar la apropiada configuración de cada uno de los componentes de la misma.

Tabla X: Políticas de Configuración

Encriptación & autenticación para todo el tráfico de la WLAN	Como mínimo, las empresas deben emplear el cifrado WEP. Sin embargo, 802.1x, WPA y las tecnologías propietarias se recomiendan ampliamente para la empresa WLANs. El tráfico se debe supervisar para asegurarse de que el tráfico está cifrado y autenticado.
Autorización – Filtrado MAC o servidores RADIUS	El filtrado de direcciones MAC proporciona el control básico sobre el cual las estaciones pueden conectar a la WLAN. Una empresa más grande requerirá un servidor RADIUS para manejar centenares de estaciones y docenas de puntos de acceso. Supervise la WLAN para los usuarios no autorizados.
Nombre de la red – Cambio del SSID default	Los identificadores del servicio SSID debe ser cambiados de la configuración por defecto que traen los puntos de acceso AP, supervise la WLAN para los puntos de acceso por defecto o SSIDs incorrectos.
Configuración de los clientes XP	Las estaciones de Windows XP se deben configurar de nuevo con los ajustes necesarios que conectan la estación con el punto de acceso con la señal más fuerte - incluso si no es un punto de acceso autorizado. Supervise todas las estaciones para las estaciones inseguras y las asociaciones accidentales.

c) Políticas de Seguridad: Muchas aplicaciones de seguridad de las WLAN se pueden tratar con una red correctamente configurada. Sin embargo, las empresas deben también poner en ejecución políticas de seguridad adicionales para WLAN para la actividad desautorizada en la red, es importante que la organización junto con el jurídico pueden normar el tipo de sanción que pudiera generarse a partir de una

violación hacia alguna política, por lo que es conveniente que el abogado de la organización lleve a cabo los reglamentos necesarios para este proceso.

Tabla XI: Políticas de Seguridad

Prohibición de los puntos de acceso no autorizados	Todos los puntos de acceso se deben desplegar con seguridad. Las organizaciones deben supervisar toda la actividad para detectar los puntos de acceso no autorizados WLANs
Prohibición de las redes Ad-Hoc	Las estaciones se deben configurar para no permitir conexiones punto a punto de redes Ad-hoc. Supervise la WLAN para identificar redes Ad-hoc..
Limitar las horas de trabajo de los puntos de acceso	Los puntos de acceso se deben apagar en las horas de no uso se recomienda monitorear la señal inalámbrica durante esas horas de no uso.
Especificaciones de Hardware por los vendedores	Seleccionar el hardware adecuado para soportar todos los elementos de seguridad que serán implementados en la WLAN

d) Políticas de Desempeño: para maximizar el desempeño de la red WLAN, las organizaciones deben establecer políticas para medir el desempeño, una política de desempeño debe establecer:

- El máximo número de estaciones asociadas a un punto de acceso en un mismo tiempo, usualmente son de 5 a 15 clientes dependiendo del ancho de banda requerido por las estaciones.

- El tráfico permitido entre la WLAN y la red cableada de la organización, en cada uno de los puntos de acceso que están conectados a la red cableada.
- El tráfico permitido en el punto de acceso y una estación individual para que cada estación tenga asegurado su ancho de banda y un estación no afecta las otras.
- El uso de herramientas para verificar los patrones de comportamiento del tráfico para determinar los tiempos y lugares donde la señal se degrada.

2. Aprobación de las políticas: Una vez que las políticas ya están definidas y documentadas, el siguiente paso es enviarlas a los ejecutivos de la organización para su revisión y aprobación. La carencia de políticas internas de la organización pueden llevar a que el documento de políticas de la WLAN puedan fallar o no llevarse a cabo, la determinación de la gerencia es importante en la aplicación y la aprobación de estas políticas.

3. Difusión de las políticas: Después de recibir la aprobación, las políticas se deben dar a conocer a quienes se espera que la cumplan. En el caso de las WLAN esto puede incluir a empleados, contratistas independientes, vendedores en sitio o cualquier visitante frecuente. La educación eficaz de la política se puede lograr de muchas maneras, cada uno debe recibir una copia escrita de la política y después firmar una declaración de seguir terminantemente las políticas definidas, además de establecer sesiones de 30 minutos para dar a los empleados retroalimentación en pequeñas y varias sesiones para que todo quede claro. Así mismo debe poner atención en las áreas con problemas recurrentes y hacer más identificables las palabras clave.

4. Auditoria y monitoreo: Las políticas bien definidas para una WLAN son esenciales para que las organizaciones cosechen las ventajas previstas y eliminen los riesgos innecesarios asociados a las redes inalámbricas. Sin embargo, las políticas pueden llegar a ser inútiles si la organización no supervisa la conformidad de la política. Los encargados de la seguridad y de red tienen pocas opciones en la supervisión de la WLAN para hacer cumplir las políticas establecidas.

Algunas de las herramientas que se utilizan para monitorear la WLAN son:

Wired-Slide Network Scanners - (identifican algunos RAP's pero no se sugieren para empresas). Pueden analizar el tráfico entre la red y el punto de acceso. Pero no pueden monitorear encriptación y autentificar, SSID's, redes ad-hoc, etc.

Wireless Sniffers & Scanners - Se pueden utilizar periódicamente para vigilar que se cumplan las políticas. Están limitadas porque necesitan un administrador de la red que físicamente camine por el área con el dispositivo corriendo el sniffer o el scanner.

Policy Monitoring - Monitorear el cumplimiento de las políticas en toda la empresa se requiere combinar una administración centralizada de wire-side scanners y análisis de radio frecuencia de scanners inalámbricos.

5. Medidas correctivas: Después de supervisar para la conformidad de la política de una WLAN, las organizaciones deben tomar medidas correctivas para alterar las configuraciones de la red y eliminar las APs no autorizados y encargarse de las personas responsables de

violaciones. En gran medida se dan alteraciones a la WLAN esto trae como resultado una modificación al documento de políticas por lo que nuevamente se tiene que llevar al proceso completo desde documentar la política, ser aprobado por la gerencia, y este proceso se repite una y otra vez cando se presenta una medida correctiva o se crea alguna nueva.

6. Revisión de las políticas: Después de que se defina, se ponga en ejecución, y se haga cumplir una política WLAN, las organizaciones deben evaluar la eficacia y las limitaciones de la política. Los encargados de red que supervisan la puesta en práctica de la política deben solicitar la regeneración de los usuarios y de los que hacen cumplir la política. Conduciendo un proceso formal de la revisión, las política WLAN se deben revisar para verificar que estén especificadas las necesidades específicas de la organización. En muchos casos, la política de WLAN puede necesitar ser más rigurosa en la definición de la política de seguridad. Sin embargo, otras organizaciones pueden ser menos y tener en cuenta la mayor adopción, el uso, y la productividad de WLAN. Una vez que la política esté revisada, el proceso de la política se debe repetir para documentar todos los cambios, tiene que estar aprobado por la gerencia estas nuevas políticas, comunicar las políticas a todos los de la organización, supervisar para la conformidad de la política, hace cumplir la política, y finalmente revisar la política.

El documento de políticas para una WLAN es primordial en el funcionamiento máximo de seguridad y de la red misma de una organización, aunque cada organización deberá establecer sus políticas especificas todas ellas se basan en políticas generales que se muestran en el [Anexo C], las cuales son utilizadas por la metodología, para ser tomadas como base al realizar el documento general de políticas WLAN.

7.3 Gestor de ancho de banda CBQ

Uno de los mecanismos que permiten hacer este filtrado es: CBQ (Clase Base Queueing) Encolado Basado en Clases, es el método que propone el modelo para realizar esta actividad, CBQ es un algoritmo basado en clases, el cual propone la división y compartición del ancho de banda en clases estructuradas jerárquicamente, como se muestra en la figura 5.9, cada clase tiene su propia cola y comparte una parte de acho de banda. Una clase hija puede tomar prestado ancho de banda de su padre si le sobra ancho de banda [32].

Existen varios métodos para optimizar el acho de banda tanto de hardware como de software, sin embargo para fines prácticos de este trabajo se plantea el uso de esta herramienta de uso libre que puede ser instalada en un ambiente LINUX y realizar las pruebas correspondientes.

Capítulo VIII

8. CONCLISIONES

8.1 Del caso de estudio

El departamento de información académica de la UABC deberá contar con este documento que ayude a administrar su red inalámbrica, y al posible crecimiento que pudiera presentarse en un futuro o en una segunda etapa para cubrir mayor número de lugares en el campus. El documento también ayudará alcanzar un nivel óptimo en su funcionamiento. Es importante mencionar que la información que se genero aquí es la única que existen hoy en día en el campus, por lo que no está documentada la red actual. Este trabajo pretende aportar de manera inicial he ir incorporando cada elemento que no fue considerado durante su implementación.

En varias ocasiones hemos mencionado lo importante que es el proceso de planeación y diseño de una WLAN, con el seguimiento adecuado de la ruta critica, cualquier empresa,

institución educativa, hogar, hotel, restaurante, cualquier organización puede llevar a cabo el trabajo de diseño asegurando un éxito en su desempeño.

Esta metodologia integra todos los elementos que debe ser considerados para la implementación de una WLAN si bien es cierto que algunos de estos de estos elementos ya fueron tema de estudio de manera independiente, hoy en día no existe un procedimiento que ayude a construir una WLAN óptima y segura.

8.2 Del análisis de la cobertura

Todos los edificios de la Universidad Autónoma de Baja California campus Ensenada con excepción del DIA (Departamento de Información Académica) están construidos con la misma estructura y el mismo tipo de material solo varían en el número de pisos que constituyen el edificio.

Los edificios del campus Universitario de la ciudad de Ensenada tiene una estructura de trabes y columnas de concreto armado los cuales están unidos por muros envolventes (bloque + emplaste + pintura) y además de cancelaría de aluminio en puertas y ventanas esta estructura la podemos observar en la figura 8.1.

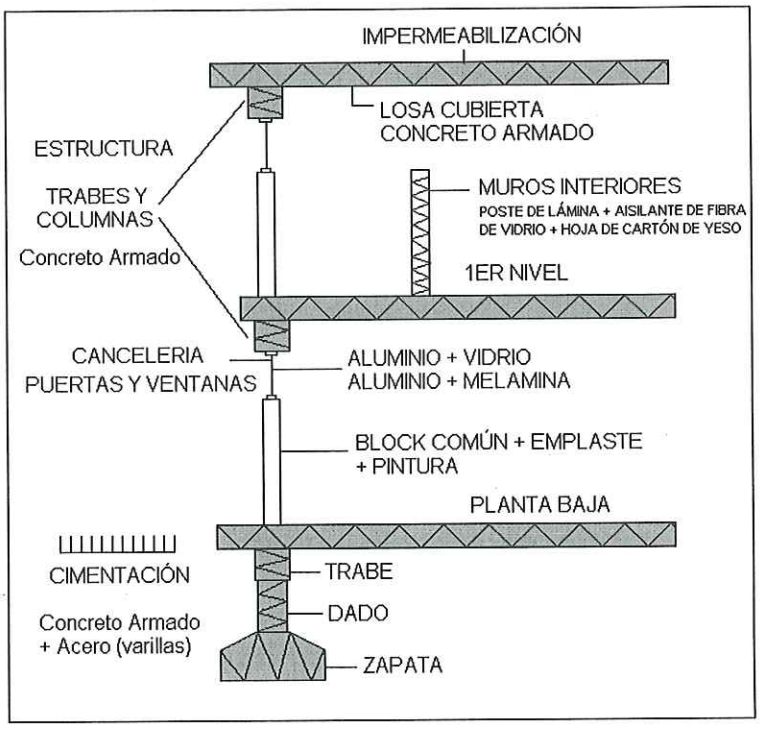


Figura 8.1: Estructura de construcción de un edificio de la UABC

En el campus Ensenada existen edificios de uno, dos y tres pisos de altura que están construidos en base a esta estructura. En el caso de que el edificio sea de un nivel (1 piso) la parte externa de la losa es cubierta de impermeabilizante, o si el edificio es de 2 niveles (2 pisos) la cubierta externa es una loseta que vendría ser el piso del segundo nivel y así mismo se repite la estructura para un edificio con 3 niveles (3 pisos), como es el caso del edificio de la Facultad de Ingeniería (E1).

Los muros que hacen las divisiones al interior del edificio se conocen como muros falsos (poste de lamina galvanizado + aislante de fibra de vidrio + hoja de cartón de yeso) como se muestra en la figura 8.1.

Como mencionamos en el capítulo cuatro, existen algunos modelos que requieren de conocer los materiales de construcción del inmueble, con base a esto, se realizó un análisis de predicción de la señal inalámbrica utilizando el modelo de propagación de pérdidas entre pisos, y como podemos observar en la figura 7.2 solo un porcentaje mínimo de señal viaja hacia dentro del edificio, en el caso de que el edificio tuviera un tercer nivel (3 pisos) el factor de atenuación seria de 35 dB para ese piso según el modelo de pérdidas entre pisos.

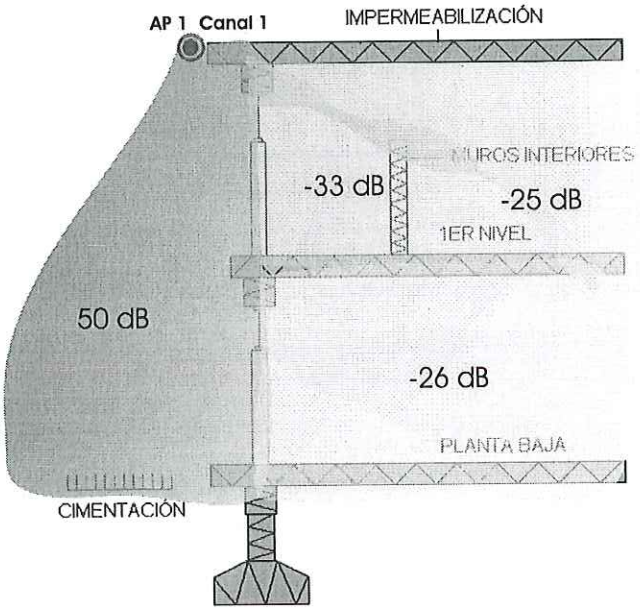


Figura 8.2: Cobertura de la señal en un edificio de dos niveles, de la UABC

8.3 Metodología vs Guías.

Regularmente existen en Internet guías, procedimientos o inclusive algunos artículos de algunas compañías que te ayudan a construir una red inalámbrica de manera muy sencilla, en estas guías se indica paso a paso las instrucciones que el usuarios tiene que seguir para lograr construir con éxito su WLAN, definitivamente este tipo de guías o tutoriales como regularmente los encontramos en Internet están enfocadas a usuarios principiantes que buscan saber como asociarse a un punto de acceso a través de su quipo portátil o cómo extender su conexión de Internet en sus hogares o en oficinas, sin embargo estas guías no son recomendadas para ser aplicadas en organizaciones con un mayor numero de usuarios y de equipos, con características muy diferentes.

Existen también de manera aislada infinidad de trabajos que hablan de cómo debes proteger tu computadora para trabajar en un ambiente inalámbrico, paso a paso indican como proteger la información que viaja por el aire utilizando algún mecanismo de protección para redes inalámbricas.

Hoy en día existen algunos trabajos que ya incorporan las componentes que son utilizados por esta metodología, un ejemplo de ello es el trabajode quien con exactitud cubre todos los elementos que deben ser considerados durante la creación de una WLAN [43]. Aunque esta metodología persigue el mismo fin, presenta las siguientes ventajas:

1. Puede ser utilizado para *evaluar* una red inalámbrica existente.
2. La *ruta crítica* es un elemento nuevo que aporta este trabajo para la construcción del diseño de una WLAN.
3. El ancho de banda en las redes inalámbricas es un elemento a considerar durante su diseño, para esto, esta metodología incorpora un *gestor de ancho de banda* que puede mejorar en gran medida el desempeño de una WLAN.
4. Si bien es cierto que las componentes que utiliza esta metodología son abordadas por algunos otros trabajos, ninguno de estos los describe a detalle, solo son nombradas como algo que debes considerar, pero nunca *"como lo debes realizar"*
5. Esta metodología contempla la posibilidad de generar las *políticas de seguridad* durante el proceso de diseño de la WLAN, y no después que ya esta implementada.

8.4 Recomendaciones

- El diseño de la red inalámbrica de la organización esta íntimamente ligada con el uso que se le quiere dar; o dicho de otra forma las áreas en las cuales se requiere de cobertura.

- En el caso de la UABC en su primera etapa fue pensado para áreas exteriores y jardines solo que las necesidades de los usuarios eran otras, bajo esta premisa es necesario replantear las áreas de cobertura según las necesidades de los usuarios o en su defecto pensar en una redistribución de los puntos de acceso existentes para obtener mayor beneficio. En la figura 8.3 se muestra una imagen de la Facultad de Ciencias en al cual se realizó un estudio para reacomodar los puntos de acceso para obtener mayor cobertura.

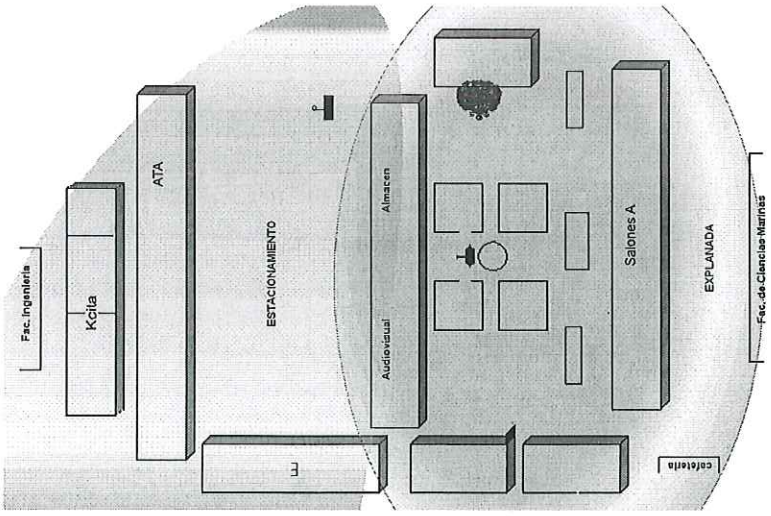
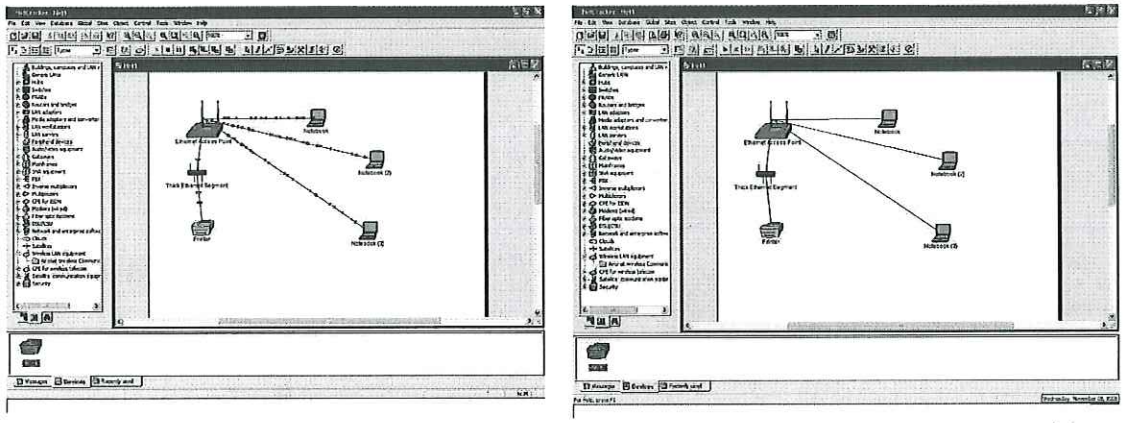


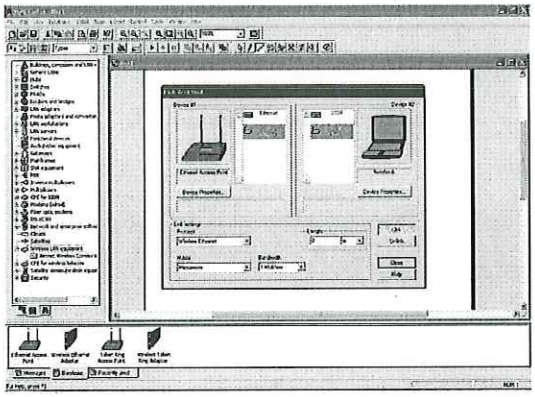
Figura 8.3: Reacomodo de puntos de acceso en la Facultad de Ciencias.

8.5 Trabajo Futuro.

- Desarrollo de un CAD (*Computer Aided Design*) diseño asistido por computadora, que permita realizar la planeación y el diseño de una WLAN utilizando una interfase grafica GUI en un ambiente de código abierto.



(a) (b)



(c)

Figura 8.4: (a) Transferencia de información en una WLAN, (b) Topología ESS, (c) Equipos y Dispositivos de interconexión

REFERENCIAS

[1] Definición de WLAN - WeboPedia
http://www.webopedia.com/TERM/WWLAN.html

[2] Dual Mode wireless: Beating 802.11g to the Punch - PC Magazine
http://www.pcmag.com/article2/0,4149,549930,00.asp

[3] Planeación y diseño de redes WLAN, Revista RED primera parte, julio del 2004,
http://eveliux.com

[4] The journal, Grant: Extricom 2007
http://www.thejournal.com/articles/20289/

[5] Grupo NAP, Colegio oficial de Ingenieros de Telecomunicaciones.
http://www.coit.es/

[6][3] Planeación y diseño de redes WLAN, Revista RED segunda parte, agosto del 2004,
http://eveliux.com

[7] Fundación Teleddes, diplomado en telecomunicaciones y redes de información.

[8][10] Wi-Fi Alliance
http://www.wi-fi.org

[9] WECA becomes Wi-Fi Alliance
http://siliconvalley.internet.com/news/article.php/1474361

[11] El alfabeto 802.11, Jörg Luther
https://www.linux-magazine.es/issue/04/80211.pdf

[12][14] IEEE 802.11b Wireless LANs - 3COM
http://www.3com.com/other/pdfs/infral/corpinfo/en_US/50307201.pdf

[13] Gast 2002, author de 802.11 Wireless Networks

[15] Definición topologías de malla para redes 802.11 - Wikipedia
http://es.wikipedia.org/wiki/Topología_en_malla

[16] Organización para la estandarización de protocolos Europeos - ETSI
http://www.etsi.org

[17] Sitio oficial de HomeRF
http://www.homerf.org

[18] Wireless Security and VPN - Intel
http://www.intel.com/ebusiness/pdf/prod/related/mobile/mobile/wp02300111.pdf

[19] The clear choice for Wireless LAN's - PROXIM
http://www.proxim.com/clearchoice/31O/form.html

[20] Definición topologías de malla para redes 802.11 - Wikipedia
http://es.wikipedia.org/wiki/Topología_en_malla

[21] 802.lla Scalable 5 GHz Wireless LAN
www.intel.com/network/connectivity/resources/doc_library/whitepapers/NP2040_1 1.01.pdf

[22] Grilo 2002, Performance evaluation of IEEE 802.11e
http://ieeexplore.ieee.org/

[23] Aleksandar Neskovic, Natascha Neskovic y George Paunovic, "Modem approaches in modelling of mobile radio systems propagation environment", IEEE Communications Surveys. Third Quarter 2000.

[24][25] Theodore S. Rappaport, Wireless Comunication,
Principles and practice, Segunda edición.

[26] Comisión Europea, 1999; Lott 2001

[27] Security of the WEP algorithm
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[28] Wireless Security: it's like securing your house - Intermec
http://epsfiles.intermec.com/eps_files/eps_wp/WirelessSecureWPWEB.pdf

[29] Definición de SSID - Webopedia
http://www.webopedia.com/TERM/S/SSID.html

[30] Wireless LAN Security
http://www.interlinknetworks.com/images/resource/
wireless_lan_security.pdf

[31] Radius - GNU Project - Free Software Foundation (FSF)
http://www.gnu.org/software/radius/radius.html

[32] CBQ, Referencias e información
http://www.icir.org/floyd/cbq.html

[33] Sitio oficial de la Facultad de Ciencias, UABC
http://webfc.ens.uabc

[34][41] Sitio oficial de la UABC.
http://www.uabc.mx

[35] Sitio oficial de la Facultad de Ingeniería, UABC.
http://www.uabc.mx

[36][37] Sitio oficial de la Facultad de Ciencias Marinas, UABC.
http://oceanologia.ens.uabc.mx

[38] Sitio oficial de la biblioteca central del campus Ensenada, UABC.
http://sia.mxl.uabc.mx

[39] Sitio oficial del Instituto de Investigaciones Oceanológicas, UABC.
http://iio.ens.uabc.mx

[40] Sitio oficial del Instituto de Investigación y Desarrollo Educativo, UABC. http://iide.ens.uabc.mx

[42] Gaceta universitaria, volumen #170. http://www.uabc.mx/gaceta/

[43] Yuval Shavit, Six steps to create a wireless LAN, 2008

GLOSARIO

802.11	Estándar ratificado por la IEEE en 1997, trabaja en la banda de frecuencia de 2.4GHz con velocidades hasta de 2Mbps.
802.11b	Estándar ratificado por la IEEE en 1999, trabaja en la banda de frecuencia de 2.4GHz con velocidades hasta de 11Mbps, conocido como Wi-Fi.
802.11g	Estándar en que será ratificado por la IEEE en marzo de 2003, trabaja en la banda de frecuencia de 2.4GHz con velocidades hasta de 54Mbps.
802.11a	Estándar ratificado por la IEEE en 1999, trabaja en la banda de frecuencia de 5GHz con velocidades hasta de 54Mbps, conocido como Wi-Fi5.
AP	Access Point, puente de comunicación entre una WLAN y una la LAN.
AS	Authentication Server, servidor de autenticación para dar acceso a usuarios de la WLAN.
Bit	Representa la mínima unidad de almacenamiento.
BPSK	Binary Phase Shift Keying, tipo de modulación para comunicaciones digitales.
BSS	Basic Service Set, tipo de interconexión de WLAN, modo infraestructura.
CAN	Campus Área Network, interconexión de varias LAN's en un espacio limitado.
CCK	Complementary Code Keying, técnica para codificar información en comunicaciones digitales.
CHAP	Challenge Handshake Authentication Protocol, tipo de autenticación para establecer comunicación en una arquitectura tipo cliente-servidor.
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance, protocolo para acceso al medio.
DSSS	Direct Sequence Spread Spectrum, tipo de modulación para comunicaciones digitales inalámbricas.
EAP	Extensible Authentication Protocol, protocolo para autenticar usuarios de la WLAN.
EAPOL	Extensible Authentication Protocol Over LAN, técnica para encapsular paquetes EAP en un ambiente LAN.
ESS	Extended Service Set, tipo de interconexión de WLAN, modo infraestructura.
Ethernet	Arquitectura para Redes de área local desarrollada por Xerox Corporation en 1976. Ethernet permite establecer la comunicación entre dos nodos (computadoras) de red.
ETSI	European Telecommunications Standards Institute, organización que se encarga de estandarizar las telecomunicaciones en todo el continente Europeo.

FCC	Federal Communications Comission, organización que regula las comunicaciones en USA.
FHSS	Frequency Hopping Spread Spectrum, Tipo de modulación para comunicaciones digitales inalámbricas.
GHz	Abreviación de GigaHertz. Un GHz representa un mil millones de ciclos por segundo.
HiperLAN	High Performance Radio Local Área Network, es un conjunto de estándares de comunicación WLAN utilizado en el continente Europeo.
HomeRF	Home Radio Frequency, tecnología inalámbrica diseñada para uso en el hogar. Trabaja hasta los 10Mbps.
Host	Computadora personal o servidor de aplicaciones.
Hub	Punto común de interconexión para dispositivos en red.
IBSS	Independent Basic Service Set, tipo de interconexión de WLAN, modo infraestructura.
IEEE	Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos), es una organización no-lucrativa compuesta por profesionales del área de ingeniería en electrónica y eléctrica para generar las especificaciones de estándares.
IP	Internet Protocol (Protocolo de Internet).
IPsec	Internet Protocol Security (Protocolo de Internet Seguro). Soporta intercambio seguro de paquetes en la capa 3 del modelo OSI.
ISA	Industry Standar Architecture, tipo de bus utilizado en computadoras IBM PC/XT y PC/AT.
ISO	International Organization for Standardization, organización que se encarga de definir estándares internacionales.
ISP	Internet Service Provider, Proveedor de servicos de Internet.
LAN	Local Área Network, red de área local.
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol, sistema para autenticar usuarios para conectarlos a la red o con un ISP.
MAC	Media Access Control, control de acceso al medio.
Mbps	Abreviación de Megabits por segundo. Mbps es una medida utilizada para la transferencia de datos.
MD5	Algoritmo para generar firmas digitales.
MHz	Abreviación de MegaHertz. Un MHz representa un millón de ciclos por segundo.
NIC	Network Interface Card, se refiere a interfase de red de computadora.
Novell	Sistema operativo para redes.
OFDM	Orthogonal Frequency Division Multiplexing, tipo de modulación para comunicaciones digitales inalámbricas.

OSI	Open System Interconnection, estándar ratificado por la ISO para comunicar redes de datos.
PAP	Password Authentication Protocol, tipo de autenticación para usuarios de red.
PPP	Point-to-Point Protocol, método para conectar computadoras al Internet a través de un MODEM.
QAM	Quadrature Amplitude Modulation, tipo de modulación para comunicaciones digitales.
QPSK	Quadrature Phase Shift Keying, tipo de modulación para comunicaciones digitales.
RADIUS	Remote Authentication Dial-In User Service, sistema para autenticar usuarios para conectarlos a la red o con un ISP.
RC4	Ron's Code o Rivest's Cipher, algoritmos para encriptación.
RF	Radio Frecuencia.
RSA	Rivest, Shamir y Adelman. Compañía que se dedica a ofrecer tecnologías de encriptación, en especial la encriptación de la llave publica.
SQL	Structured Query Language, lenguage de programación que nos permite establecer peticiones a una Base de Datos.
SSID	Service Set Identifier, Identificador del Conjunto de Servicios de una WLAN.
SSL	Secure Socket Layer, ofrece encriptación a la información enviada a través de Internet, trabaja en la capa 7 del modelo OSI.
STA	Station, abreviación de estación de trabajo.
TCP	Transmission Control Protocol, protocolo de control de transmisión de datos.
Throughput	Cantidad de información transferida de un nodo a otro.
TLS	Transport Layer Security, protocolo que garantiza la integridad y privacidad de los datos en aplicaciones cliente-servidor a través de Internet.
U-NII	Unlicensed National Information Infrastructure, infraestructura diseñada para proporcionar a las WLAN's comunicación en rangos cortos y altas velocidades.
UNIX	Sistema operativo para redes orientado a multiprocesos.
VPN	Virtual Private Network, red privada virtual.
WECA	Wireless Ethernet Compatibility Alliance, Alianza para la compatibilidad de redes inalámbricas Ethernet.
WEP	Wired Equivalent Privacy, técnica de seguridad implementada en redes inalámbricas.
Wi-Fi Alliance	Wi-FI (Wireless Fidelity Allience) es la alianza de empresas para certifica la interoperabilidad entre equipos con el estándar 802.11a/b.
Wi-Fi	Wireless Fidelity, nombre con el que se le conoce al estándar 802.11b.

Wi-Fi5	Wireless Fidelity 5, nombre con el que se el conoce al estándar 802.11a.
WLAN	Wireless Local Área Network, red de área local inalámbrica.

Anexo A

ENCUESTA APLICADA

Cuestionario aplicado a las personas que fueron objeto de estudio durante la elaboración de este trabajo, se aplicaron cien encuestas entre docentes, investigadores, técnicos, estudiantes, y administrativos.

Definición de la Encuesta:

Esta encuesta consiste en recabar información que nos permita evaluar el desempeño de la Red Inalámbrica actual de la Universidad Autónoma de Baja California campus Ensenada, con el fin de realizar un documento de recomendaciones para mejorar el servicio. Este trabajo es para el curso de Redes Inalámbricas que se imparte en la Facultad de Ciencias. La información que aquí se maneja es solo para obtener estadísticas e información que apoye durante el proceso de la elaboración de la propuesta.

Actividad que realiza:

☐ Docente ☐ Investigador ☐ Estudiante ☐ Tecnico

¿Sabes que es una red inalámbrica?:
Si_____

No____

¿Sabes si en algunos puntos de tu universidad cuenta con una red inalámbrica?:
Si_____ donde_____

No____

Si la respuesta anterior fue si:
¿Tienes idea como debes configurar tu equipo para poder entrar a la red inalámbrica?.
Si_____ ¿como te informaste? _____

No____

¿Qué tan útil crees que es la red inalámbrica para ti?
a) Mucho b) Un poco c) No la considero útil

¿Tienes computadora portátil (laptop)?:
Si_____

No_____

Si la respuesta anterior fue si:

¿Si la universidad te brindara el servicio de red inalámbrica desde cualquier punto de la unidad utilizarías tu equipo?:
Si_____

No_____

¿Comprarías tu propio equipo portátil?
No_____
Si_____ en cuanto tiempo:
6 meses_____ 1 año_____ de 2 a 3 años_____ de 3 a 5 años_____

¿Si tu universidad ya cuenta con una red inalámbrica sabes que equipo tendrías que comprar para poder conectarte?
Si_____

No_____

¿Si la universidad ya cuenta con una red inalámbrica de que lugares te conectarías? Ubícalos del 1 al 6.

___Cafetería ____Aulas ____Jardines ____Estacionamiento ____Oficina ___Biblioteca

¿A que horas por lo regular utilizas la red inalámbrica?
Hora:_____

¿Consideras que el área de estacionamientos debe tener cobertura por la red inalámbrica?
SI_____ NO_____

¿Crees que es eficiente el servicio de la red inalámbrica de tu Facultad?
SI_____ NO_____
POR QUE:_____
_____

¿En cuáles de estas áreas consideras tú, que debe contar con mayor cobertura y con un rápido el acceso a la red inalámbrica?
Ubícalos del 1 al 6.

___Cafetería ____Aulas ____Jardines ____Estacionamiento ____Oficina ___Biblioteca

¿Que consideras que la velocidad es adecuada en este momento?
SI_____ NO_____
POR QUE:_____
_____

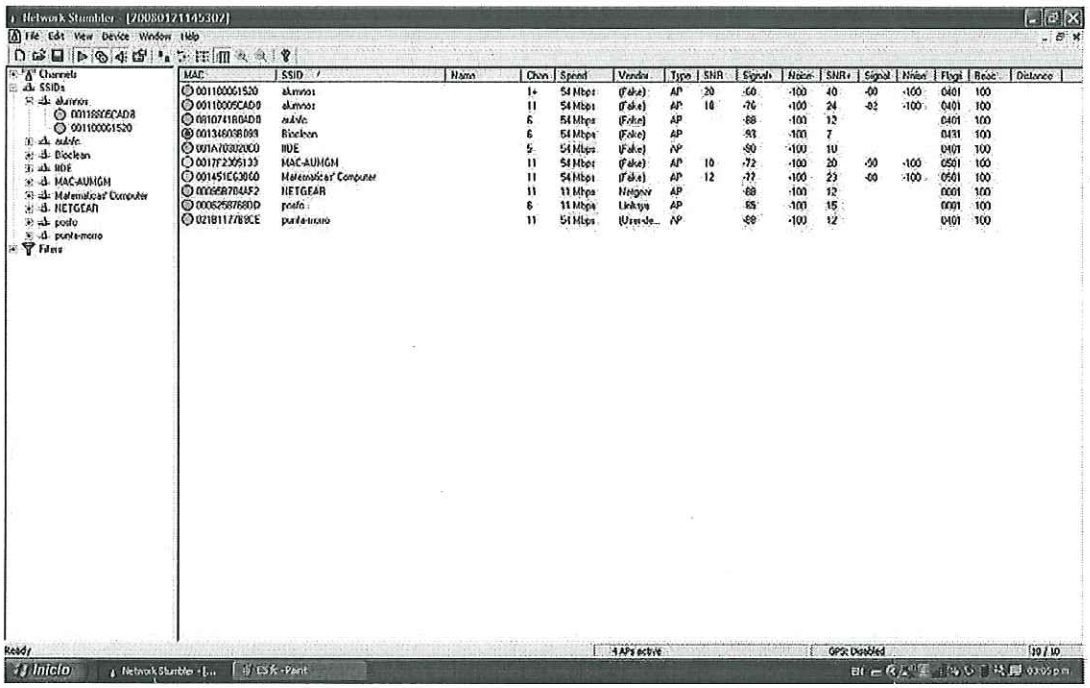
¿Que actividades son las que realizas comúnmente en una computara que tiene acceso a la red inalámbrica?
Ubícalos en orden del más al menos utilizado (1 al 10).

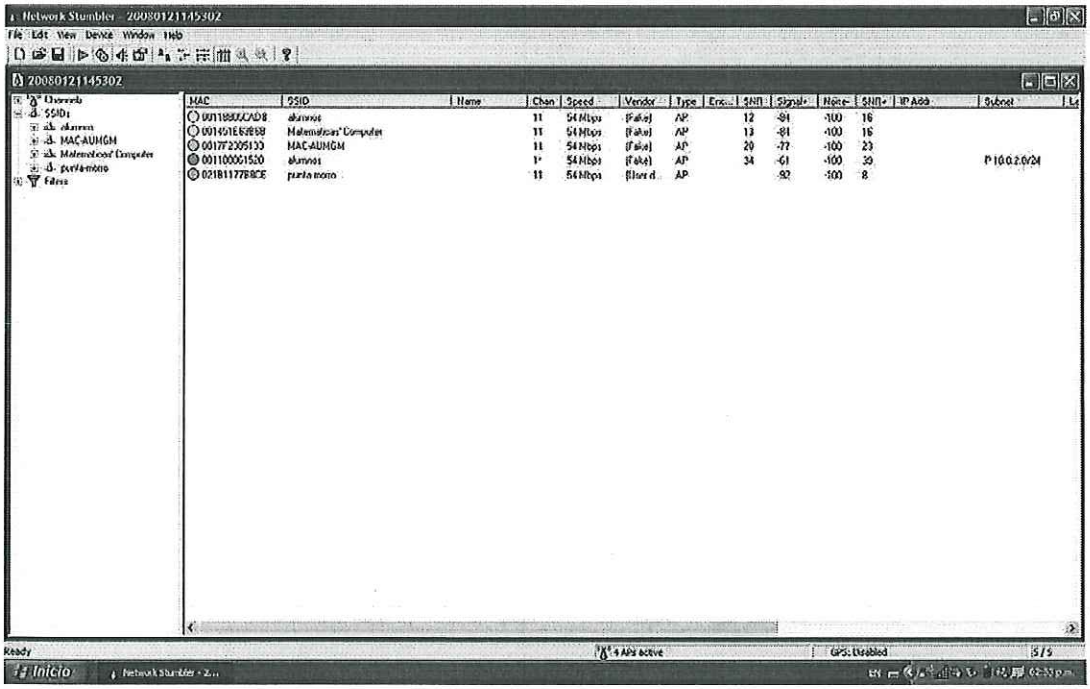
☐ Navegar en Internet	☐ Trabajo en Equipo a Distancia	☐ Compartir archivos, impresora y otros recursos.
☐ Bancos de Información, Revistas Electronicas, etc	☐ Descargar musica, juegos, software en general	☐ Aplicaciones multimedia
☐ Practicas y/o Aputes del Curso	☐ Elaboración de pagina personal, cursos, aplicaciones, etc	☐ Inscripciones, llenado de formatos de la universidad
☐ Messanger, Chat, Foros	☐ Trabajo de Investigación	Otros:_____

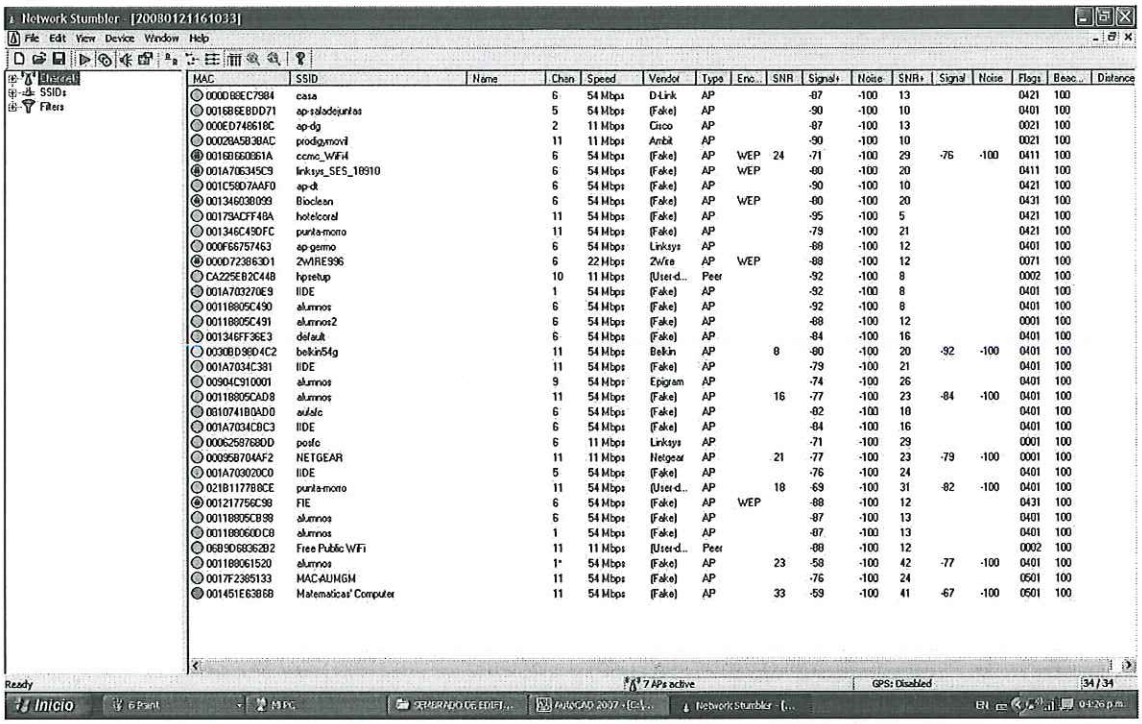
Anexo B

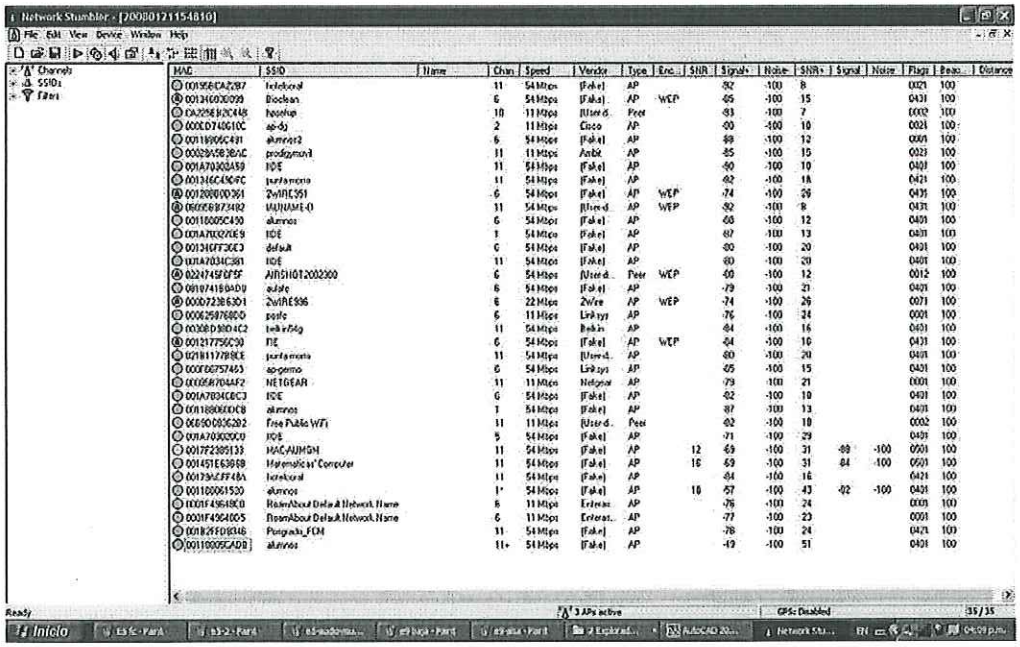
PUNTOS DE ACCESO NO AUTORIZADOS

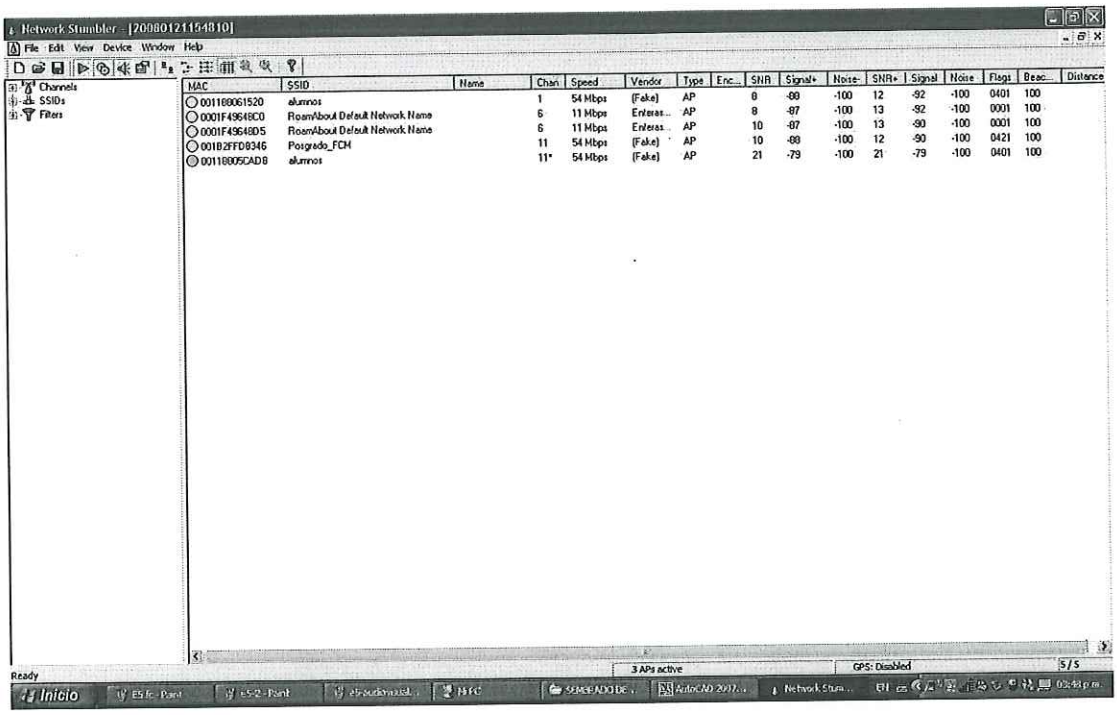
Durante el estudio y el análisis de propagación de la red inalámbrica del campus Universitario, pudimos observar mas de una docena de puntos de acceso activos que se encuentran funcionando sin autorización, aquí se presentan estas gráficas.

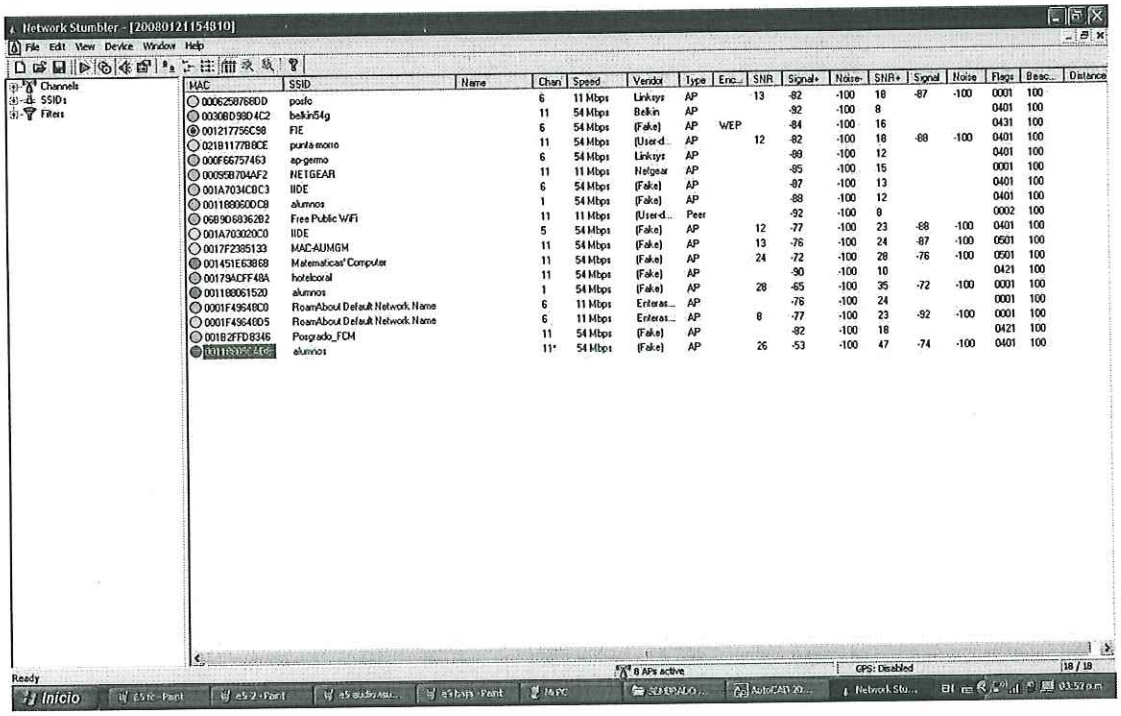

Network Stumbler - [20080121145302]
File Edit View Device Window Help
Channels
SSIDs
alumnos
001188006CAD8
001100061520
subfe
Bioclean
IIDE
MAC-AUMGM
Matematicas' Computer
NETGEAR
posfo
punta-morro
Filters
MAC SSID Name Chan Speed Vendor Type SNR Signal Noise SNR+ Signal Noise Flags Beac... Distance
001100061520 alumnos 1+ 54 Mbps (Fake) AP 20 -60 -100 40 -80 -100 0401 100
00110009CAD9 alumnos 11 54 Mbps (Fake) AP 18 -76 -100 24 -82 -100 0401 100
0810741B0AD8 subfe 6 54 Mbps (Fake) AP -88 -100 12 0401 100
0013460368B8 Bioclean 6 54 Mbps (Fake) AP -93 -100 7 0401 100
00IA70302000 IIDE 5 54 Mbps (Fake) AP -90 -100 10 0401 100
0017F2305133 MAC-AUMGM 11 54 Mbps (Fake) AP 10 -72 -100 20 -50 -100 0501 100
001451E63060 Matematicas' Computer 11 54 Mbps (Fake) AP 12 -77 -100 23 -80 -100 0501 100
00095B7D4AF2 NETGEAR 11 11 Mbps Netgear AP -88 -100 12 0001 100
0006258768DD posfo 6 11 Mbps Linksys AP -85 -100 15 0001 100
021B1177B8CE punta-morro 11 54 Mbps (Unknown... AP -88 -100 12 0401 100
Ready
4 APs active
GPS: Disabled
10 / 10
Inicio
Network Stumbler - [...
ES - Paint
03:09 p.m.

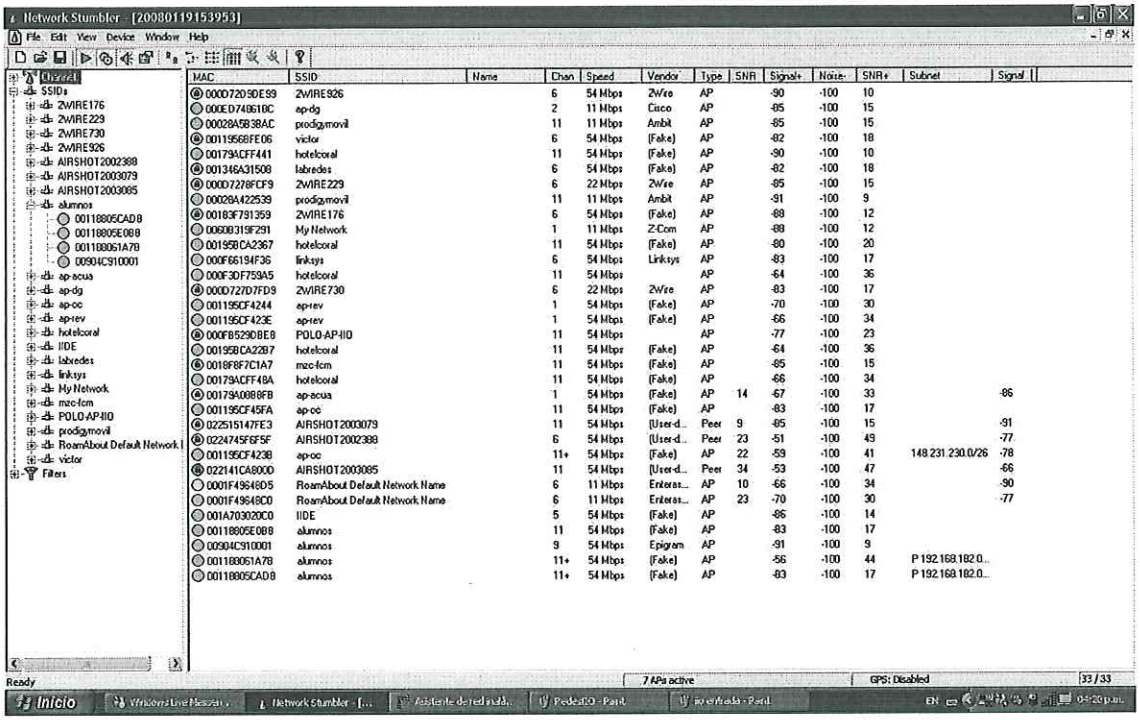

Network Stumbler - 20080121145302
File Edit View Device Window Help
20080121145302
Channels
SSIDs
alumnos
MAC-AUMGM
Matematicas' Computer
punta-morro
Filters
MAC SSID Name Chan Speed Vendor Type Enc... SNR Signal+ Noise- SNR+ IP Addr Subnet
001188006CAD8 alumnos 11 54 Mbps (Fake) AP 12 -84 -100 16
001451E63B68 Matematicas' Computer 11 54 Mbps (Fake) AP 13 -81 -100 19
0017F2305133 MAC-AUMGM 11 54 Mbps (Fake) AP 20 -77 -100 23
001100061520 alumnos 1* 54 Mbps (Fake) AP 34 -61 -100 39 P 10.0.2.0/24
021B1177B8CE punta-morro 11 54 Mbps (Unknown... AP -92 -100 8
Ready
4 APs active
GPS: Disabled
5 / 5
Inicio
Network Stumbler - 2...
02:32 p.m.

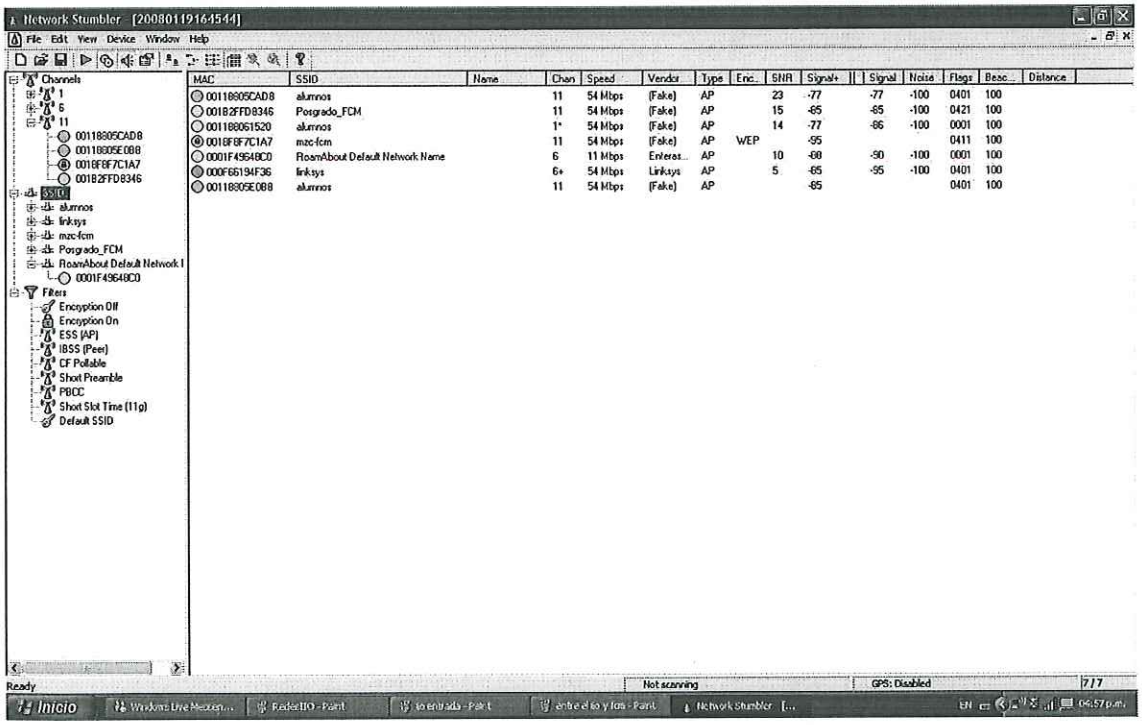

Network Stumbler - [20080121161033]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC SSID Name Chan Speed Vendor Type Enc... SNR Signal+ Noise- SNR+ Signal Noise Flags Beac... Distance
000D88EC7984 casa 6 54 Mbps D-Link AP -87 -100 13 0421 100
0016B8EBDD71 ap-saladejuntas 5 54 Mbps (Fake) AP -90 -100 10 0401 100
000ED746618C ap-dg 2 11 Mbps Cisco AP -87 -100 13 0021 100
00029A5B38AC prodigymovil 11 11 Mbps Ambit AP -90 -100 10 0021 100
0016B660861A ccmc_WiFi4 6 54 Mbps (Fake) AP WEP 24 -71 -100 29 -76 -100 0411 100
001A706345C9 linksys_SES_18910 6 54 Mbps (Fake) AP WEP -80 -100 20 0411 100
001C58D7AAF0 ap-dt 6 54 Mbps (Fake) AP -90 -100 10 0421 100
001346038099 Bioclean 6 54 Mbps (Fake) AP WEP -80 -100 20 0431 100
00179ACFF4BA hotelcoral 11 54 Mbps (Fake) AP -95 -100 5 0421 100
001346C49DFC punta-morro 11 54 Mbps (Fake) AP -79 -100 21 0421 100
000F66757463 ap-gerno 6 54 Mbps Linksys AP -88 -100 12 0401 100
000D723863D1 2WIRE996 6 22 Mbps 2Wire AP WEP -88 -100 12 0071 100
CA225EB2C448 hpsetup 10 11 Mbps (User-d... Peer -92 -100 8 0002 100
001A703270E9 IIDE 1 54 Mbps (Fake) AP -92 -100 8 0401 100
00118805C490 alumnos 6 54 Mbps (Fake) AP -92 -100 8 0401 100
00118805C491 alumnos2 6 54 Mbps (Fake) AP -88 -100 12 0001 100
001346FF36E3 default 6 54 Mbps (Fake) AP -84 -100 16 0401 100
0030BD98D4C2 belkin54g 11 54 Mbps Belkin AP 8 -80 -100 20 -92 -100 0401 100
001A7034C381 IIDE 11 54 Mbps (Fake) AP -79 -100 21 0401 100
00904C910001 alumnos 9 54 Mbps Epigram AP -74 -100 26 0401 100
00118805CAD8 alumnos 11 54 Mbps (Fake) AP 16 -77 -100 23 -84 -100 0401 100
0810741B0AD0 autofc 6 54 Mbps (Fake) AP -82 -100 18 0401 100
001A7034CBC3 IIDE 6 54 Mbps (Fake) AP -84 -100 16 0401 100
0006258768DD posfc 6 11 Mbps Linksys AP -71 -100 29 0001 100
000958704AF2 NETGEAR 11 11 Mbps Netgear AP 21 -77 -100 23 -79 -100 0001 100
001A7030020C0 IIDE 5 54 Mbps (Fake) AP -76 -100 24 0401 100
021B117788CE punta-morro 11 54 Mbps (User-d... AP 18 -69 -100 31 -82 -100 0401 100
001217756C98 FIE 6 54 Mbps (Fake) AP WEP -88 -100 12 0431 100
00118805CB98 alumnos 6 54 Mbps (Fake) AP -87 -100 13 0401 100
001188060DC8 alumnos 1 54 Mbps (Fake) AP -87 -100 13 0401 100
06B9D68362B2 Free Public WiFi 11 11 Mbps (User-d... Peer -88 -100 12 0002 100
001189061520 alumnos 1* 54 Mbps (Fake) AP 23 -58 -100 42 -77 -100 0401 100
0017F2385133 MAC-AUMGM 11 54 Mbps (Fake) AP -76 -100 24 0501 100
001451E63B6B Matematicas' Computer 11 54 Mbps (Fake) AP 33 -59 -100 41 -67 -100 0501 100
Ready
7 APs active
GPS: Disabled
34 / 34
Inicio
Network Stumbler - [...
04:26 p.m.


Network Stumbler - [20080121154810]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC SSID Name Chan Speed Vendor Type Enc... SNR Signal+ Noise- SNR+ Signal Noise Flags Beac... Distance
00179ACFF4BA hotelcoral 11 54 Mbps (Fake) AP -92 -100 8 0021 100
001346030099 Bioclean 6 54 Mbps (Fake) AP WEP -65 -100 15 0431 100
CA225EB2C448 hpsetup 10 11 Mbps (User-d... Peer -93 -100 7 0002 100
000ED746610C ap-dg 2 11 Mbps Cisco AP -90 -100 10 0021 100
00118805C491 alumnos2 6 54 Mbps (Fake) AP -88 -100 12 0001 100
00029A5B3BAC prodigymovil 11 11 Mbps Ambit AP -85 -100 15 0021 100
001A703020A9 IIDE 11 54 Mbps (Fake) AP -90 -100 10 0401 100
001346C49DFC punta-morro 11 54 Mbps (Fake) AP -82 -100 18 0421 100
001200000361 2WIRE351 6 54 Mbps (Fake) AP WEP -74 -100 26 0435 100
000958B73482 MAINAME-0 11 54 Mbps (User-d... AP WEP -82 -100 18 0431 100
00118805C490 alumnos 6 54 Mbps (Fake) AP -88 -100 12 0401 100
001A7032D0E9 IIDE 1 54 Mbps (Fake) AP -87 -100 13 0401 100
001346FF36E3 default 6 54 Mbps (Fake) AP -80 -100 20 0401 100
001A7034C381 IIDE 11 54 Mbps (Fake) AP -80 -100 20 0401 100
022474F0F5F AIRSHOT2002300 6 54 Mbps (User-d... Peer WEP -88 -100 12 0012 100
00187418AAD9 autofc 6 54 Mbps (Fake) AP -79 -100 21 0401 100
000D723863D1 2WIRE996 6 22 Mbps 2Wire AP WEP -74 -100 26 0071 100
0006258768DD posfc 6 11 Mbps Linksys AP -76 -100 24 0001 100
0030BD98D4C2 belkin54g 11 54 Mbps Belkin AP -84 -100 16 0401 100
001217756C98 FIE 6 54 Mbps (Fake) AP WEP -84 -100 10 0431 100
021B117788CE punta-morro 11 54 Mbps (User-d... AP -80 -100 20 0401 100
000F66757463 ap-gerno 6 54 Mbps Linksys AP -65 -100 15 0401 100
000958704AF2 NETGEAR 11 11 Mbps Netgear AP -79 -100 21 0001 100
001A7034CBC3 IIDE 6 54 Mbps (Fake) AP -82 -100 10 0401 100
001188060DC8 alumnos 1 54 Mbps (Fake) AP -87 -100 13 0401 100
06B9D68362B2 Free Public WiFi 11 11 Mbps (User-d... Peer -82 -100 10 0002 100
001A7030020C0 IIDE 5 54 Mbps (Fake) AP -71 -100 29 0401 100
0017F2385133 MAC-AUMGM 11 54 Mbps (Fake) AP 12 -69 -100 31 -88 -100 0501 100
001451E63B6B Matematicas' Computer 11 54 Mbps (Fake) AP 16 -69 -100 31 -84 -100 0501 100
00179ACFF4BA hotelcoral 11 54 Mbps (Fake) AP -84 -100 16 0421 100
001189061520 alumnos 1* 54 Mbps (Fake) AP 18 -57 -100 43 -82 -100 0401 100
0001F49648C0 RoamAbout Default Network Name 6 11 Mbps Enteras... AP -76 -100 24 0001 100
0001F4964005 RoamAbout Default Network Name 6 11 Mbps Enteras... AP -77 -100 23 0001 100
0018F8FD8346 Pinguelo_FCM 11 54 Mbps (Fake) AP -78 -100 24 0421 100
00118805CAD8 alumnos 11+ 54 Mbps (Fake) AP -49 -100 51 0401 100
Ready
3 APs active
GPS: Disabled
35 / 35
Inicio
04:09 p.m.


Network Stumbler - [20080121154810]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC SSID Name Chan Speed Vendor Type Enc... SNR Signal+ Noise- SNR+ Signal Noise Flags Beac... Distance
00118061520 alumnos 1 54 Mbps (Fake) AP 0 -88 -100 12 -92 -100 0401 100
0001F49648C0 RoamAbout Default Network Name 6 11 Mbps Enteras... AP 8 -87 -100 13 -92 -100 0001 100
0001F49648D5 RoamAbout Default Network Name 6 11 Mbps Enteras... AP 10 -87 -100 13 -90 -100 0001 100
001B2FFD8346 Posgrado_FCM 11 54 Mbps (Fake) AP 10 -88 -100 12 -90 -100 0421 100
00118005CAD8 alumnos 11* 54 Mbps (Fake) AP 21 -79 -100 21 -79 -100 0401 100
Ready
3 APs active
GPS: Disabled
5 / 5
Inicio


Network Stumbler - [20080121154810]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC SSID Name Chan Speed Vendor Type Enc... SNR Signal+ Noise- SNR+ Signal Noise Flags Beac... Distance
000625B768DD posfc 6 11 Mbps Linksys AP 13 -82 -100 18 -87 -100 0001 100
00308D98D4C2 belkin54g 11 54 Mbps Belkin AP -92 -100 8 0401 100
001217756C98 FIE 6 54 Mbps (Fake) AP WEP -84 -100 16 0431 100
021B1177B8CE punta morro 11 54 Mbps (User-d... AP 12 -82 -100 18 -88 -100 0401 100
000F66757463 ap-germo 6 54 Mbps Linksys AP -88 -100 12 0401 100
00095B704AF2 NETGEAR 11 11 Mbps Netgear AP -85 -100 15 0001 100
001A7034C0C3 IIDE 6 54 Mbps (Fake) AP -87 -100 13 0401 100
00118060DCB alumnos 1 54 Mbps (Fake) AP -88 -100 12 0401 100
06B90B836202 Free Public WiFi 11 11 Mbps (User-d... Peer -92 -100 8 0002 100
001A703020C0 IIDE 5 54 Mbps (Fake) AP 12 -77 -100 23 -88 -100 0401 100
0017F2385133 MAC-AUMGM 11 54 Mbps (Fake) AP 13 -76 -100 24 -87 -100 0501 100
001451E63B6B Matematicas' Computer 11 54 Mbps (Fake) AP 24 -72 -100 28 -76 -100 0501 100
00179ACFF48A hotelcoral 11 54 Mbps (Fake) AP -90 -100 10 0421 100
00118061520 alumnos 1 54 Mbps (Fake) AP 28 -65 -100 35 -72 -100 0001 100
0001F49648C0 RoamAbout Default Network Name 6 11 Mbps Enteras... AP -76 -100 24 0001 100
0001F49648D5 RoamAbout Default Network Name 6 11 Mbps Enteras... AP 8 -77 -100 23 -92 -100 0001 100
001B2FFD8346 Posgrado_FCM 11 54 Mbps (Fake) AP -82 -100 18 0421 100
00118005CAD8 alumnos 11* 54 Mbps (Fake) AP 26 -53 -100 47 -74 -100 0401 100
Ready
8 APs active
GPS: Disabled
18 / 18
Inicio


Network Stumbler - [20080119153953]
File Edit View Device Window Help
Channels
SSIDs
ZWIRE176
ZWIRE229
ZWIRE730
ZWIRE926
AIRSHOT2002388
AIRSHOT2003079
AIRSHOT2003085
alumnos
00118805CAD8
00118805E0B8
001180061A78
00904C910001
ap-acua
ap-dg
ap-oc
ap-rev
hotelcoral
IIDE
labredes
linksys
My Network
mzc-fcm
POLO-AP-IIO
prodigymovil
RoamAbout Default Network
victor
Filters
MAC SSID Name Chan Speed Vendor Type SNR Signal+ Noise- SNR+ Subnet Signal
000D7205DE99 ZWIRE926 6 54 Mbps ZWire AP -90 -100 10
000ED749616C ap-dg 2 11 Mbps Cisco AP -65 -100 15
00028A5B38AC prodigymovil 11 11 Mbps Ambit AP -65 -100 15
00119568FE06 victor 6 54 Mbps (Fake) AP -82 -100 18
00179ACFF441 hotelcoral 11 54 Mbps (Fake) AP -90 -100 10
001346A31508 labredes 6 54 Mbps (Fake) AP -82 -100 18
000D7278FCF9 ZWIRE229 6 22 Mbps ZWire AP -65 -100 15
00028A422539 prodigymovil 11 11 Mbps Ambit AP -91 -100 9
00183F791359 ZWIRE176 6 54 Mbps (Fake) AP -88 -100 12
00600315F291 My Network 1 11 Mbps Z-Com AP -88 -100 12
00195BCA2367 hotelcoral 11 54 Mbps (Fake) AP -80 -100 20
000F66194F36 linksys 6 54 Mbps Linksys AP -83 -100 17
000F3DF759A5 hotelcoral 11 54 Mbps AP -64 -100 36
000D727D7FD9 ZWIRE730 6 22 Mbps ZWire AP -83 -100 17
001195CF4244 ap-rev 1 54 Mbps (Fake) AP -70 -100 30
001195CF423E ap-rev 1 54 Mbps (Fake) AP -66 -100 34
000FB529DBE8 POLO-AP-IIO 11 54 Mbps AP -77 -100 23
00195BCA22B7 hotelcoral 11 54 Mbps (Fake) AP -64 -100 36
0018F8F7C1A7 mzc-fcm 11 54 Mbps (Fake) AP -85 -100 15
00179ACFF4BA hotelcoral 11 54 Mbps (Fake) AP -66 -100 34
00179A0088FB ap-acua 1 54 Mbps (Fake) AP 14 -67 -100 33 -86
001195CF45FA ap-oc 11 54 Mbps (Fake) AP -83 -100 17
0225151477E3 AIRSHOT2000079 11 54 Mbps (User-d... Peer 9 -65 -100 15 -91
0224745F6F5F AIRSHOT2002388 6 54 Mbps (User-d... Peer 23 -51 -100 49 -77
001195CF4238 ap-oc 11+ 54 Mbps (Fake) AP 22 -59 -100 41 148.231.230.0/26 -78
022141CA8000 AIRSHOT2003085 11 54 Mbps (User-d... Peer 34 -53 -100 47 -66
0001F49648D5 RoamAbout Default Network Name 6 11 Mbps Enteras... AP 10 -66 -100 34 -90
0001F49648C0 RoamAbout Default Network Name 6 11 Mbps Enteras... AP 23 -70 -100 30 -77
001A703020C0 IIDE 5 54 Mbps (Fake) AP -86 -100 14
00118805E0B8 alumnos 11 54 Mbps (Fake) AP -83 -100 17
00904C910001 alumnos 9 54 Mbps Epigram AP -91 -100 9
001180061A78 alumnos 11+ 54 Mbps (Fake) AP -56 -100 44 P 192.168.182.0...
00118805CAD8 alumnos 11+ 54 Mbps (Fake) AP -83 -100 17 P 192.168.182.0...
Ready
7 APs active
GPS: Disabled
33 / 33
Inicio
Windows Live Messen...
Network Stumbler - [...
Asistente de red instala...
RedesIIO - Paint
Bienvenida - Paint
EN
04:20 p.m.


Network Stumbler - [20080119164544]
File Edit View Device Window Help
Channels
1
6
11
00118805CAD8
00118805E0B8
0018F8F7C1A7
001B2FFD8346
SSIDs
alumnos
linksys
mzc-fcm
Posgrado_FCM
RoamAbout Default Network
0001F49648C0
Filters
Encryption Off
Encryption On
ESS (AP)
IBSS (Peer)
CF Pollable
Short Preamble
PBCC
Short Slot Time (11g)
Default SSID
MAC SSID Name Chan Speed Vendor Type Enc... SNR Signal+ Signal Noise Flags Beac... Distance
00118805CAD8 alumnos 11 54 Mbps (Fake) AP 23 -77 -77 -100 0401 100
001B2FFD8346 Posgrado_FCM 11 54 Mbps (Fake) AP 15 -65 -65 -100 0421 100
001180061520 alumnos 1* 54 Mbps (Fake) AP 14 -77 -86 -100 0001 100
0018F8F7C1A7 mzc-fcm 11 54 Mbps (Fake) AP WEP -95 0411 100
0001F49648C0 RoamAbout Default Network Name 6 11 Mbps Enteras... AP 10 -88 -90 -100 0001 100
000F66194F36 linksys 6+ 54 Mbps Linksys AP 5 -65 -95 -100 0401 100
00118805E0B8 alumnos 11 54 Mbps (Fake) AP -65 0401 100
Ready
Not scanning
GPS: Disabled
7 / 7
Inicio
Windows Live Messen...
RedesIIO - Paint
Bienvenida - Paint
entre ellos y los - Paint
Network Stumbler [...
EN
04:57 p.m.

Anexo C

POLITICAS DE SEGURIDAD

Aquí se presenta un documento que contiene las políticas generales base que pueden ser utilizados por cualquier organización para elaborar su documento técnico de políticas de seguridad para la red inalámbrica.

AirDefense

Wireless LAN Policy Checklist

Usage Policies

- ☐ **Applications Across the WLAN –** Bandwidth-intensive applications and extremely confidential enterprise data may not be best suited to run on the wireless LAN.
- ☐ **Network Roaming –** Define the access points and WLANs that each station is allowed to connect to.
- ☐ **Uncontrolled Environments –** Define where organization-owned, wireless-enabled laptops are allowed to connect to uncontrolled wireless LANs. Establish VPN capabilities for remotely connection to the enterprise network from home WLAN or hotspot.

Configuration Policies

- ☐ **Encryption & Authentication for All Wireless LAN Traffic –** At a minimum, enterprises should employ the built-in WEP encryption. However, 802.1x, WPA and proprietary technologies (LEAP) are highly recommended for enterprise WLANs. Traffic should be monitored to ensure that traffic is encrypted and authenticated.
- ☐ **Authorization – MAC Filtering or RADIUS Server –** MAC address filtering provides basic control over which stations can connect to an enterprise WLAN. Larger enterprises will require a RADIUS server to manage hundreds of stations and dozens of access points. Monitor the WLAN for unauthorized users.
- ☐ **Naming the Network – Changing Default SSIDs –** Service Set Identifiers should be changed from default settings and renamed as to not draw attention from outsiders. (e.g. Avoid SSIDs of *CEO Office* or *Cash Register*) Monitor the WLAN for access points with default or improper SSIDs.
- ☐ **Reconfigure Default Windows XP Settings –** Windows XP stations should be reconfigured from default settings that connect the station to the access point with the strongest signal – even if it's not an authorized access point. Monitor all stations for insecure stations and accidental associations.

Security Policies

- ☐ **Prohibit Unauthorized "Rogue" Access Points –** All access points should be securely deployed through the IT organization. Organizations should monitor all WLAN activity to detect rogue WLANs attached to the wired network.
- ☐ **Prohibit Ad Hoc Networks –** Stations should be configured to not allow peer-to-peer, ad hoc networks between stations. Monitor the WLAN to identify ad hoc networks and recognize stations that are configured to allow ad hoc networks even if no peer-to-peer network exists at that time.
- ☐ **Limit Off-Hours Traffic –** Turn off the access point during non-use hours and monitor the airwaves for off-hours traffic.
- ☐ **Vendor-Specific Hardware –** Limit WLAN hardware to select vendors which support the deployed security measures and monitor for unauthorized vendors.

Performance Policies

- ☐ **Maximum No. of Stations Connected to an Access Point –** Network performance decreases dramatically when too many stations connect to the same access point. Network administrators should be alerted to when more than 15 or 20 stations are on the same access point.
- ☐ **Maximum Bytes allowed between an Access Point and the Wired Network –** Make sure your WLAN does not overly drain bandwidth from the wired network by establishing a maximum number of bytes for traffic between the access point and wired network.
- ☐ **Maximum Bytes allowed between an Access Point and a Single Station –** Establish a performance threshold for the maximum number of bytes allowed between an access point and individual stations to guard against one station utilizing excessive bandwidth degrading the performance of others connected to the access point.

Anexo D

TRABAJOS PRESENTADOS

1. Planeación y diseño de redes WLAN, revista la RED, julio y agosto del 2004. Autores Evelio Martínez Martínez y Adrián Enciso Almanza, profesores de la Universidad Autónoma de Baja California.

2. Construcción de un modelo para el diseño de redes de área local inalámbricas, IEEE 802.11a/b/g, CiComp 2006. Autores Adrián Enciso Almanza y Evelio Martínez Martínez, profesores de la Universidad Autónoma de Baja California.

SEGURIDAD PROFUNDA: FIREWALLS SIN PUERTAS ABIERTAS

4.3.2-01

RED

LA COMUNIDAD DE EXPERTOS EN REDES

Año XIV • Julio 2004

Los soportes de e-México

www.red.com.mx

ISSN • 1405 • 6280

AÑO XIV • Julio 2004 • $50.00

00162

7 52435 76600 3

Por Evelio Martínez y Adrián Enciso

Planeación y diseño de redes WLAN

Primera de dos partes

Las redes inalámbricas de área local (WLAN) son hoy una realidad y están teniendo éxito gracias, en gran medida, a que su costo ha disminuido considerablemente. Es posible conseguir un punto de acceso (AP, access point) o una tarjeta de red inalámbrica por menos de 100 dólares.

La tecnología Wi-Fi (como se conoce comúnmente a las WLANs), utiliza frecuencias de radio (RF) para transmitir información en vez de utilizar los tradicionales cables para comunicación. Es claro que una de las principales ventajas de las redes sin alambres es la movilidad y la fácil integración con las redes cableadas existentes. Pero quizá su mayor ventaja, con respecto a otras tecnologías inalámbricas, es que las frecuencias que utiliza son de uso libre.

Las WLAN han tenido alta aceptación en oficinas, universidades y hogares, así como en áreas públicas: hoteles, aeropuertos y restaurantes. Todos ven a la tecnología inalámbrica como una estrategia para atraer clientes al ofrecer Internet dentro de sus negocios.

Planear y diseñar

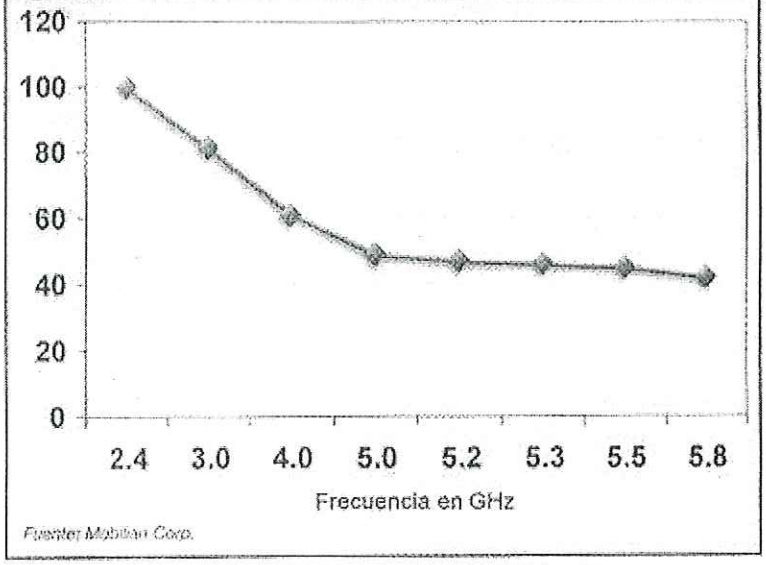
En este tipo de redes es común que los usuarios finales, entusiasmados por el boom que han alcanzado las WLANS, compren e instalen equipo sin una previa planeación y diseño, lo que trae como resultado un deficiente desempeño y, en casos extremos, el robo de la información.

Instalar y configurar una WLAN puede ser un proceso sencillo pero, precisamente esto, la convierte en un blanco fácil de ataques externos e internos que pueden poner en riesgo a la organización. Recordemos que el medio por el cual se comunican dispositivos inalámbricos es el aire, y que cualquier espía con los dispositivos necesarios puede rastrear las señales y utilizar los recursos de la red en su beneficio. En este artículo describiremos cómo planear y diseñar una red WLAN, con la intención de optimizar su desempeño y, al mismo tiempo, reducir el nivel de inseguridad que presenta este tipo de redes.

Factores a considerar en el diseño y planeación de una red WLAN

1. Ancho de banda / Velocidad de transmisión.
2. La frecuencia de operación.
3. Aplicaciones que van a correr en la WLAN.
4. Máximo número de usuarios.
5. Área de cobertura.
6. Material con el que están construidos los edificios.
7. Conexión de la WLAN con la red cableada.
8. Disponibilidad de productos en el mercado.

Figura 1. Comparación en cobertura entre 2.4 GHz y 5.8 GHz



Fuente: Meraki Corp.

9. Planeación y administración de las direcciones IP.
10. Los identificadores de la red (SSID).
11. Seguridad.

Ancho de banda / Velocidad de transmisión: Debemos tomar en cuenta el ancho de banda y la velocidad de transmisión que nos brindan las WLAN. Los estándares IEEE 802.11a y IEEE 802.11g, permiten velocidades de hasta 54 Mbps; por otro lado, el estándar IEEE 802.11b permite velocidades de transmisión de hasta 11 Mbps. Este ancho de banda es mucho menor al de las redes cableadas, las cuales operan a 100 Mbps. El ancho de banda especificado por los estándares 802.11a/b/g es teórico y se cumple sólo en condiciones ideales. En la vida real, el máximo desempeño depende de muchos otros factores.

Tabla 1. Comparación entre los estándares 802.11a, b y g

Parámetro	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Frecuencia/Ancho de banda	5 GHz (300 MHz)	2.4 GHz (83.5 MHz)	2.4 GHz (83.5 MHz)
Modulación	OFDM	DSSS	OFDM
Ancho de banda por canal	20 MHz (6 canales utilizables)	22 MHz (3 canales)	22 MHz (3 canales)
Tasa de transmisión	54 Mbps	11 Mbps	54 Mbps
Cobertura interior/exterior	30/50 metros	50/150 metros	30/50 metros
Potencia máxima*	200 mW, 1 W, 4 W	1 mW/MHz	200 mW, 1 W, 4 W
Usuarios simultáneos	64	32	50

*varía según la potencia y posición de la antena

La frecuencia de operación: Cuando se diseña una WLAN, seleccionar la frecuencia de operación que define el estándar que se va utilizar puede ser causa de confusión. Universalmente, las WLAN utilizan las frecuencias de 2.4 GHz (802.11b) y 5 GHz (802.11a/g). El hecho de utilizar alguna de ellas tiene muchas implicaciones. Se han realizado diversos estudios sobre la propagación de las señales en estas dos frecuencias, dando como resultado que la frecuencia más baja (2.4 GHz) ofrece mejor propagación, logrando más del doble de cobertura que la frecuencia de 5 GHz (ver figura 1).

Tipos de aplicaciones: Es importante delimitar el tipo de aplicaciones que se van a correr en la red inalámbrica, tales como acceso a Internet, correo electrónico, consultas a base de datos y transferencia de archivos. Dado el limitado ancho de banda, no es recomendable que se utilicen las WLAN para aplicaciones que consumen mucho ancho de banda, como pueden ser la transferencia de video e imágenes, la videoconferencia o el audio/video streaming.

Número máximo de usuarios: Uno de los factores más importantes a considerar cuando se diseña una WLAN es delimitar el número de usuarios que utilizará la red. Como se ve en la tabla 1, los estándares definen diferente número de ellos conectados simultáneamente a un punto de acceso (AP). Es obvio que, a mayor número de usuarios conectados a una WLAN, menor será el desempeño de la misma. Hay que tener en cuenta el número máximo de usuarios que soporta cada estándar (ver tabla 1).

Área de cobertura: Mientras la frecuencia aumenta, el rango de cobertura de la señal disminuye, de modo que, usualmente, la periodicidad de operación de 5 GHz tiene menor rango de cobertura que la de 2.4 GHz. De acuerdo con esto, si se utiliza el estándar 802.11a se requiere un número mayor de AP's para extender la cobertura, lo que implica un mayor presupuesto.

Por otro lado, el estándar 802.11b tiene una mayor cobertura aunque con un menor ancho de banda. También hay que tener en cuenta si el punto de acceso se va a instalar en exteriores o interiores, pues de ello dependerá el rango de cobertura. En cubículos cerrados ésta es de 20 metros, mientras que en los abiertos alcanza los 30 metros. En pasillos y corredores es de hasta 45 metros y, en exteriores, de hasta 150 metros. El uso de antenas con mayor ganancia aumentará considerablemente la cobertura.

Conexión de la WLAN con la red cableada: Los puntos de acceso necesitan electricidad para poder operar, así como estar conectados a la red cableada. Se recomienda instalar los puntos de acceso en lugares estratégicos, sin olvidarse de estas dos conexiones. Existen puntos de acceso que proveen la electricidad al AP a través del cable de par trenzado. A esta característica se le conoce como PoE (Power over Ethernet).

Disponibilidad de productos en el mercado: Hay que estar conscientes del mercado de puntos de acceso. Si compramos uno de ellos debemos de tomar en cuenta factores como el costo y el soporte técnico disponible. A veces lo barato puede salir caro.

En la siguiente edición hablaremos acerca de la administración de las direcciones IP, así como de identificadores de red y, algo esencial, la seguridad.

s autores son docentes
a Facultad de Ciencias
la Universidad Autóno-
ma de Baja California
(UABC). Se les puede
ontactar respectivamente
en evelio@uabc.mx y
acerios@uabc.mx

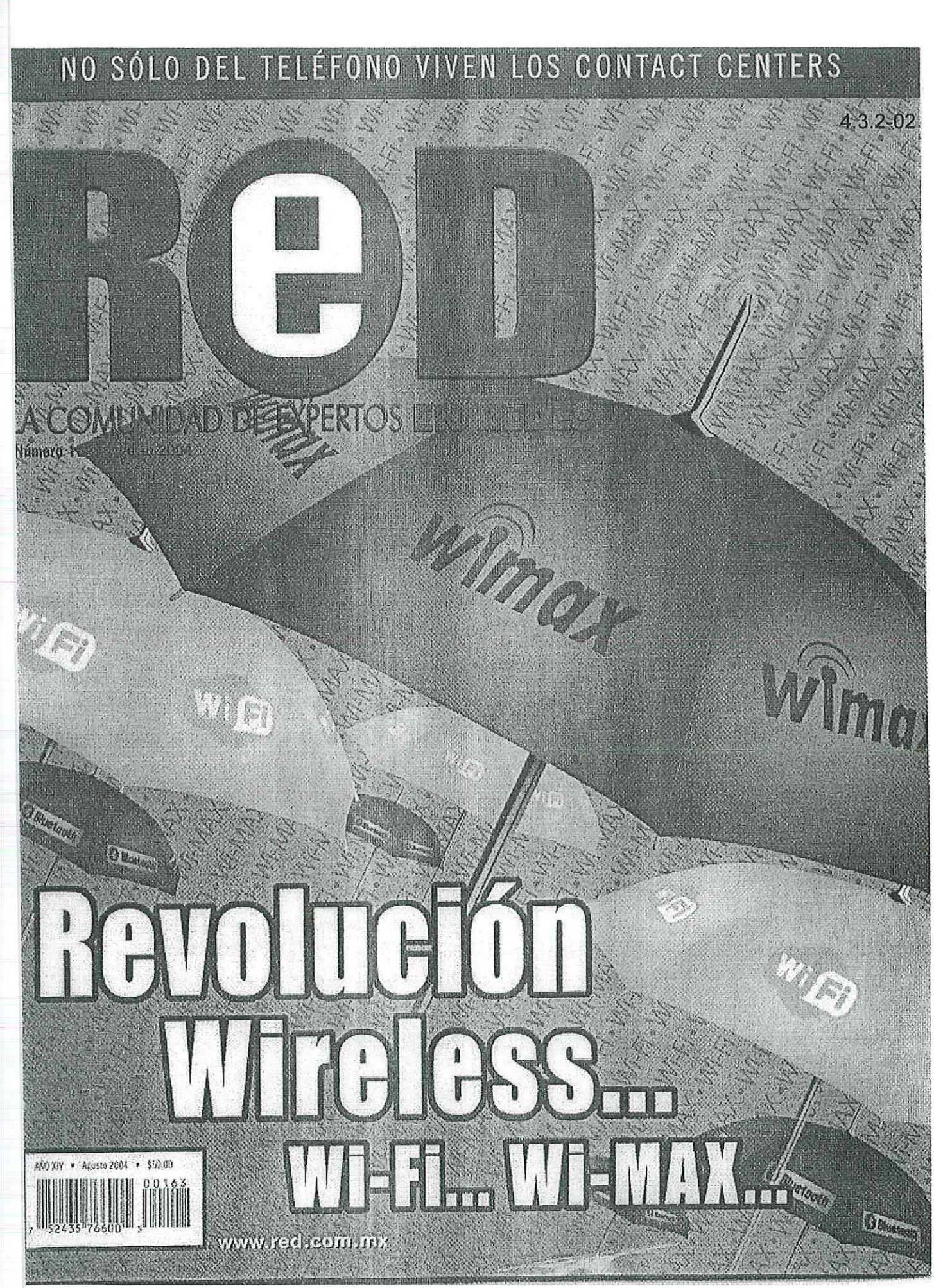
NO SÓLO DEL TELÉFONO VIVEN LOS CONTACT CENTERS

4.3.2-02

RED

LA COMUNIDAD DE EXPERTOS LEADERS

Número [illegible]



Revolución Wireless...

Wi-Fi... Wi-MAX...

AÑO XIV • Agosto 2004 • $42.00
00163
7 52435 76600 3

www.red.com.mx

Por Evelio Martínez y Adrián Enciso

Planeación y diseño de redes WLAN

Segunda y última parte

Las redes inalámbricas son cada vez más accesibles, pero no hay que dejar de lado los factores seguridad y soporte.

En la edición anterior hablamos de que la tecnología Wi-Fi (cómo se conoce comúnmente a las WLANs) utiliza frecuencias de radio en lugar de los tradicionales cables para la comunicación, de la importancia de planear y diseñar un WLAN antes de instalarla, así como de los factores que se deben considerar para ello.

En esta segunda parte complementamos la información, esperando que todo, en su conjunto, le guíe en dicho proceso.

Otros de los factores a considerar en el diseño y planeación de una red de este tipo:

Planeación y administración de las direcciones IP (Internet protocol): Los dispositivos inalámbricos necesitan de una dirección IP para poder identificarse, por lo que será necesario reservar direcciones IPs para los dispositivos inalámbricos que se quieran conectar a la red. En caso de que no existan las suficientes, será necesario emplear ruteadores inalámbricos que puedan proporcionar direcciones IP privadas. También hay que considerar el uso de servidores de DHCP para asignar direcciones dinámicamente, lo cual puede ser contraproducente. El administrador de la red deberá decidir si se utiliza ésta opción o si es mejor asignar direcciones manualmente.

Los identificadores de la red (SSID): Los SSIDs son los identificadores de los puntos de acceso. Se deben poner SSIDs adecuados y no muy obvios. La razón: estos identificadores son fácilmente rastreables por aplicaciones o por otros APs (Access points). Es muy común que al instalar un AP no se cambie el nombre del SSID (identificadores de la red) que trae de fábrica. Esta mala práctica ocasiona que los usuarios maliciosos identifiquen claramente el nombre del fabricante del AP y puedan conocer la contraseña, para después entrar al panel de administración de la configuración del AP y tomar el control total de la red.

La Seguridad: Éste es, quizás, el factor menos tomado en cuenta al instalar una WLAN y resulta ser de lo más crítico. Las WLAN son más susceptibles a ataques debido a que los intrusos no requieren conexión física para accesar a la red. En este punto hay que tener en cuenta cuál será el nivel de seguridad que queremos para proteger nuestra red. Existen tres niveles de seguridad: básico, intermedio y avanzado.

En el *nivel básico* existe, por omisión, un mecanismo de seguridad en el estándar 802.11x, conocido como WEP, que utiliza una llave o contraseña de 64 o 128 bits para acceder al AP. También existe en este nivel el filtrado de direcciones MAC. Con este mecanismo se logra filtrar aquellas direcciones MAC que no pertenezcan a nuestra red.

En el *nivel intermedio* de seguridad se encuentran los servidores de autentificación, tales como el RADIUS y el kerberos. Para ellos se requiere la instalación y configuración de un servidor de autentificación, el cual implica un gasto extra por la contratación de una persona calificada que lo instale, configure y administre. El acceso al AP se hace mediante un *login* y *password* más personalizado para cada usuario. El servidor de autentificación validará ésta información antes de darle acceso al AP. Una de las desventajas de los servidores de autentificación es que pueden ser accesados maliciosamente por los hackers y obtener la lista completa de contraseñas y usuarios.

En el *nivel avanzado* de seguridad ya se hace uso de servidores de autentificación más sofisticados. En este nivel se pueden emplear protocolos de encriptación tales como IPSec, SSL o TLS. También pueden comprarse equipos VPN para crear túneles seguros entre los usuarios y los servidores de autentificación.

Glosario de términos

802.11	•Estándar ratificado por la IEEE en 1997, trabaja en la banda de frecuencia de 2.4GHz con velocidades hasta de 2Mbps.
802.11b	•Estándar ratificado por la IEEE en 1999, trabaja en la banda de frecuencia de 2.4GHz con velocidades hasta de 11Mbps, conocido como Wi-Fi.
802.11g	•Estándar ratificado por la IEEE en el 2003, trabaja en la banda de frecuencia de 2.4GHz con velocidades hasta de 54Mbps.
802.11a	•Estándar ratificado por la IEEE en 1999, trabaja en la banda de frecuencia de 5GHz con velocidades hasta de 54Mbps, conocido como Wi-Fi5.
AP	•Access Point, punto de acceso inalámbrico.
DSSS	•Direct Sequence Spread Spectrum, espectro disperso de secuencia directa.
DHCP	•Dinamic Host Control Protocol, protocolo de asignación dinámica de direcciones IP.
FHSS	•Frequency Hopping Spread Spectrum. Espectro disperso con salto en frecuencia.
GHz	•Abreviación de GigaHertz. Un GHz representa un mil millones de ciclos por segundo.
IEEE	•Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos.
IP	•Internet Protocol, protocolo de Internet.
LAN	•Local Area Network, red de área local.
LDAP	•Lightweight Directory Access Protocol, sistema para autenticar usuarios para conectarlos a la red o con un ISP.
MAC	•Media Access Control, control de acceso al medio.
Mbps	•Abreviación de Megabits por segundo. Mbps es una medida utilizada para la transferencia de datos.
MHz	•Abreviación de MegaHertz. Un MHz representa un millón de ciclos por segundo.
NIC	•Network Interface Card, se refiere a interfase de red de computadora.
OFDM	•Orthogonal Frequency Division Multiplexing, tipo de modulación para comunicaciones digitales inalámbricas.
RADIUS	•Remote Authentication Dial-In User Service, sistema para autenticar remotamente usuarios.
RF	•Radio Frecuencia.
SSID	•Service Set Identifier, Identificador del Conjunto de Servicios de una WLAN.
SSL	•Secure Sockets Layer, protocolo de encriptación seguro a nivel de sockets.
TLS	•Transport Layer Security, protocolo de encriptación seguro en la capa de transporte.
VPN	•Virtual Private Network, redes privadas virtuales.
WEP	•Wired Equivalent Privacy, técnica de seguridad implementada en redes inalámbricas.
Wi-Fi	•Wireless Fidelity, nombre con el que se le conoce al estándar 802.11b.
WLAN	•Wireless Local Area Network, red de área local inalámbrica.

Los autores son docentes de la Facultad de Ciencias de la Universidad Autónoma de Baja California (UABC). Se les puede contactar respectivamente en evelio@uabc.mx y aonciso@uabc.mx

Beneficios

Los beneficios identificados, al instalar una WLAN son múltiples:

• Ahorro de costos en el despliegue de redes: las redes wireless son más económicas.

• Movilidad e itinerancia: no sólo es sencillo el desplazamiento del puesto de trabajo, sino que en algunos casos (PDAs, Tablet PCs) el puesto de trabajo está virtual e indisolublemente ligado a la persona .

• Mayor comunicación interna y flujo de información: el canal de comunicación está siempre abierto.

• Reuniones más optimizadas, con menos logística externa e, incluso, sin desplazamientos (reuniones on-line mediante la combinación de tecnología wireless y aplicaciones de teletrabajo y videoconferencia).

• Preferido por usuarios: han mostrado reiteradamente su predisposición al uso de la tecnología, no presentando el rechazo habitual al cambio que se da en otros entornos.

• Facilita la introducción y uso de servicios avanzados y futuros: VoIP, mensajería instantánea.

• Mayor facilidad para el desarrollo de productos: el mejor conocimiento de esta tecnología y sus posibilidades permite generar ideas novedosas de uso, y

• Mayor rendimiento laboral por sensación de confort en el puesto de trabajo

¿Son seguras?

La seguridad hoy en día es un punto que no hay que dejar por alto. Muchas de las organizaciones que instalan WLANs no contemplan la seguridad como una de sus prioridades.

Es importante tener conciencia de que la red inalámbrica tiene los mismos problemas básicos de cualquier red cableada: se pueden tomar todos los resguardos en el lado inalámbrico, pero no sirve de nada si la red no tiene reglas de seguridad mínimas, tales como acceso controlado a los recursos, políticas de autentificación y securitización de la información sensible, etcétera.

La carencia de políticas de seguridad es el principal riesgo de pérdida de información. En el caso de las redes inalámbricas, la inexistencia de políticas o las malas prácticas hacen que sea tan fácil obtener un SSID o acceso de administrador a un AP, sólo leyendo el manual del mismo ya que las cuentas de administrador y el SSID tienen su valor por default.

En lo que respecta a los dispositivos WLAN, debemos de tomar en cuenta que las especificaciones definidas por los estándares son probadas en condiciones ideales; por lo tanto, son sólo teóricas. En la práctica estos parámetros pueden variar, dependiendo de dónde y cómo sean instalados y configurados tales equipos.

La planeación y el diseño en una red, por más pequeña que sea, nos permitirá sacarle más provecho, logrando un mejor desempeño en términos de velocidad de transmisión al correr nuestras aplicaciones y una mayor seguridad de nuestra información.

No sólo hay que considerar factores como el precio, hay que estar seguros de que contaremos con el soporte técnico adecuado y la seguridad de que nuestra WLAN funcionará perfectamente. Una vez que esté seguro de ello, proceda a su instalación. ◘

Construcción de un Modelo para el Diseño de Redes de Área Local Inalámbricas, IEEE 802.11

Adrián Enciso Almanza[1], Evelio Martínez Martínez[2],

1. Universidad Autónoma de Baja California, Facultad de Ciencias, aenciso@uabc.mx
2. .Universidad Autónoma de Baja California, Facultad de Ciencias, evelio@uabc.mx

Resumen— En este artículo presentaremos un modelo para el diseño de redes de área local inalámbricas - IEEE 802.11a/b/g, el cual nos permita implementar una WLAN en cualquier lugar de una manera optima y segura, analizaremos cada uno de componentes que integran el modelo, como son la protección, cobertura, equipamiento, gestión, aplicaciones, y ancho de banda, con estos componentes el modelo podrá adaptarse a las necesidades de cualquier organización que requiera de un diseño. Presentaremos los resultados obtenidos hasta lo que va de este trabajo, análisis de coberturas, proceso para la definición de políticas y análisis de seguridad.

Palabras clave— WLAN, Wi-Fi, IEEE 802.11, Redes de Área Local Inalámbrica.

I. INTRODUCCION

Las Redes inalámbricas en los últimos años han ganado mucha popularidad en el mercado, particularmente, las redes locales de datos inalámbricas (WLAN), tecnología que ha tenido mucha aceptación en oficinas, universidades, hogares, así como en áreas públicas como hoteles, aeropuertos, restaurantes. Estos últimos ven esto como una estrategia para atraer clientes y ofrecer Internet gratis dentro de sus negocios [1].

La tecnología Wi-Fi, cómo se le conoce comúnmente a las WLAN's, usan tecnología de radio frecuencias (RF) para trasmitir y recibir datos a través del aire, proveen los mismos beneficios y recursos que ofrece una red LAN tradicional pero sin la limitación de estar conectado a través de un cable. Una WLAN es un sistema de comunicación de datos flexible implementada como una extensión o una alternativa de una red de área local cableada permitiendo además incrementar la productividad y eficiencia de las actividades diarias de la empresa.

Una WLAN puede ser montada fácilmente por cualquier usuario en cualquier parte, siempre y cuando tenga los permisos para hacerlo. Sin embargo, una WLAN necesita de administración así como una LAN o quizá aun más. Esta es una de las principales características por la que las WLAN se identifican su fácil implementación y precisamente esto las hace que de alguna forma sean un blanco fácil para ataques externos e incluso internos. Recordemos que el medio por el cual se comunican los dispositivos inalámbricos es el aire, y que cualquier espía con los dispositivos necesarios puede rastrear las señales y utilizar la WLAN para actos no benéficos

La industria de dispositivos móviles se beneficiará de una rápida adopción de redes de área local inalámbricas (WLANs), al crecer el número de usuarios frecuentes de redes WLAN en América del Norte de 4.2 millones en el 2003 a más de 31 millones en el 2007.

– Gartner –

Hasta el 2006, el 70 por ciento de los ataques exitosos a redes inalámbricas de área local WLAN se deberán a una configuración errónea de los puntos de acceso-AP y a la paquetería de los clientes.

– Gartner –

Las WLAN no vienen a sustituir las LAN cableadas, sino más bien, vienen a expandir y complementar la red de área local. Las conexiones inalámbricas nos pueden ayudar a proyar aquellas zonas en las que es difícil tirar cableado o incluso esté prohibido romper paredes. De este modo, el tener una extensión inalámbrica de una LAN podría ser de mucha importancia para alcanzar las posibilidades de conexión que nos brindan las WLAN.

Sin embargo, aun presentando esa vulnerabilidad que se da en forma automática, el estándar que ha dominado el mercado de las WLAN es el 802.11 y sus diferentes variantes, como lo son: 802.11a, 802.11b, 802.11g, y muy pronto 802.11n.

Tabla 1. Comparación entre los estándares 802.11a, b y g			
Parámetro	**IEEE 802.11a**	**IEEE 802.11b**	**IEEE 802.11g**
Frecuencia/Ancho de banda	5 GHz (300 MHz)	2.4 GHz (83.5 MHz)	2.4 GHz (83.5 MHz)
Modulación	OFDM	DSSS	OFDM
Ancho de banda por canal	20 MHz (6 canales utilizables)	22 MHz (3 canales)	22 MHz (3 canales)
Tasa de transmisión	54 Mbps	11 Mbps	54 Mbps
Cobertura interior/exterior	30/50 metros	50/150 metros	30/50 metros
Potencia máxima*	200 mW, 1 W, 4 W	1 mW/MHz	200 mW, 1 W, 4 W
Usuarios simultáneos	64	32	50

II. PLANEACION Y DISEÑO

Una WLAN es un sistema de comunicación de datos flexible implementada como una extensión o una alternativa de una red de área local cableada permitiendo además incrementar la productividad y eficiencia de las actividades diarias de la empresa. Hoy las WLAN's trabajan en los 2.4 GHz y 5GHz bandas de frecuencias como se muestra en la tabla 1. Los elementos básicos para formar una red inalámbrica son:

- Tarjeta de Red (NIC)
  En una red LAN inalámbrica, el NIC es la interfase entre los clientes del sistema y el punto de acceso (AP), para crear una conexión transparente a la Red.

- Punto de Acceso (AP)
  El punto de acceso es un equipo inalámbrico similar al Hub, un AP es típicamente conectado la LAN cableada, a través de un cable estándar Ethernet, y se comunica con los dispositivos inalámbricos por medio de una antena. El punto de acceso se encarga de mantener las conexiones de los clientes que se encuentran a través de su área de cobertura permitiendo o negando el tráfico hacia el interior de la red.

En este tipo de redes es común que los usuarios finales, entusiasmados por el boom que han alcanzado las WLAN compren e instalen los equipos sin previo planeación y diseño, lo que trae como resultado un deficiente desempeño y, en algunas ocasiones, el robo de información.

A pesar de que las redes inalámbricas ofrecen muchos beneficios, las organizaciones necesitan tomar en cuenta varios puntos antes su implementación, como son:

Seguridad. Estudios realizados al protocolo WEP por parte del grupo de investigación del Departamento de Ciencias Computacionales de la Universidad de California, Berkeley, muestran vulnerabilidades importantes [2], que hacen insegura la WLAN. Lo cual implica que si una organización esta pensando es adoptar esta tecnología inalámbrica deben implementar mecanismos adicionales de seguridad para proteger información importante.

Desempeño. El uso de una red inalámbrica requiere de ancho de banda, por ejemplo, podríamos tener a 50 usuarios queriendo acceder a los recursos de la red. Esto podría fácilmente tumbar nuestro punto de acceso (AP), debido a esto debemos considerar mecanismo que nos ayuden a optimizar el ancho de banda.

Infraestructura. Las tarjetas NIC's consumen bastante energía de las computadoras personales de tal manera deberán cargar su baterías mas seguido a consecuencia de esto las organizaciones necesitan asegurarse de proveer las suficientes conexiones eléctricas dentro de sus instalaciones y de fácil acceso. Añadiendo que los usuarios deben estar conscientes de este problema y posiblemente utilizar el modo de ahorro de energía en su computadora personal.

III. MODELO

Instalar y configurar una WLAN puede ser proceso sencillo pero, precisamente esto, lo convierte en un blanco fácil de ataques externos e internos que pueden poner en riesgo a la organización.

Debido a que este tipo de redes utilizan el aire para su comunicación como ya se ha mencionado, están expuestas a cualquier espía que con los dispositivos necesarios pueden rastrear la señal y utilizar los recursos de la red para su beneficio.

Muchas de las organizaciones que incorporan este tipo de redes han sufrido de ataques en sus redes privadas, mucho se debe a la falta de planeación y un diseño pobre ante las amenazas de los usuarios intrusos que siempre están en la espera de un error durante la implementación de la WLAN.

En un estudio realizado en la Facultad de Ciencias de la Universidad Autónoma de Baja California en el periodo 2003-2 al 2004-2 [3], que trabajó sobre los factores que tendrían que considerarse en el diseño y planeación de una red WLAN, tuvieron como resultado:

1. Ancho de banda, Velocidad de transmisión.
2. La frecuencia de operación.
3. Aplicaciones que correrán sobre la WLAN.
4. Máximo numero de usuarios.
5. Área de cobertura.
6. Material con el que están construidos los edificios.
7. Conexión de la WLAN can la red cableada.
8. Disponibilidad de productos en el mercado.

Estos factores fueron la base para establecer los seis componentes que en este articulo se propone para construir un modelo que nos permita poder diseñar redes de área local inalámbricas para cualquier organización, estos factores nos ayudaron a definir cada componente que integrara el modelo.

En la Figura 1, se presenta el diagrama general del modelo, que parte del centro que representa el diseño de una WLAN que se quiere diseñar y que se alimenta con cada uno de los componentes los cuales establecen una configuración propia que será integrada al diseño y de esa manera arrojen un diseño que cumpla con cada una de las necesidades que se establecieron en un inicio para su diseño.

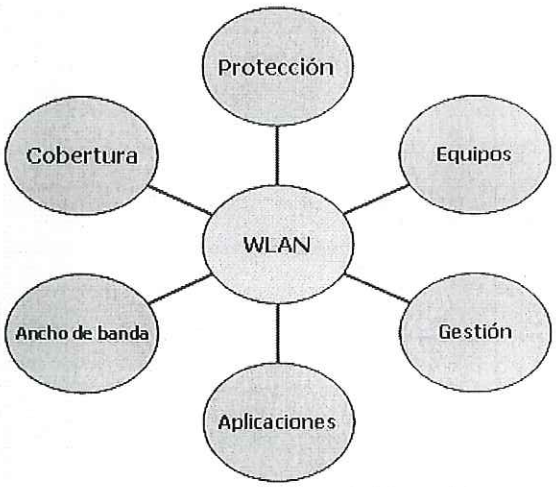


Fig. 1. Diagrama General del Modelo

A continuación se describe en este articulo los seis componentes que serán suficientes para poder planear, diseñar y construir una red inalámbrica en cualquier organización de manera optima y segura, integra cada elementos necesario para que la comunicación se de con un buen desempeño y confiabilidad durante la transmisión de los datos, el modelo que se propone contempla la posibilidad de incorporar elementos acorde a las necesidades de la organización, y con el cual se construye una red inalámbrica de manera dinámica adicionando solo aquellos elementos que satisfagan las necesidades establecidas. El modelo establece una ruta critica que marca lo mínimo requerido para lograr con éxito y tener un diseño confiable, es por ello que cada componente incluye diferentes configuraciones que se podrían requerir durante la planeación y el diseño de una red WLAN.

IV. COMPONENTES DEL MODELO

Protección

Recordemos que la comunicación en redes inalámbricas se efectúa por Radio Frecuencia, es decir, nuestra información viaja por el aire, lo cual hace que la transmisión de los datos y el acceso a nuestra red sea insegura.

Antes de introducirnos en el análisis de aspectos y métodos de seguridad para WLAN's es importante conocer que tipos de ataque o aspectos de inseguridad estamos expuestos. Todas las redes de área local están expuestas a varios tipos de ataque, estos se dividen en *Ataques Activos* y *Ataques* Pasivos, del primero, son aquellos en los que los intrusos obtienen acceso a la red de manera ilegal y causan daños a la información, mientras que los *Ataque Pasivos* se caracterizan por la forma en que el intruso se infiltra a la red sin dañar la información, sin embargo, hace uso de los recursos (hardware, acceso a Internet, etc.), además de husmear la información [2].

Las redes inalámbricas son mas susceptibles a estos ataques debido a que los intrusos no requieren conexión física para acceder a la red. Dada esta vulnerabilidad que de manera natural se expone, cualquiera que quisiera entrar de manera ilegal a la red lo podría hacer rastreando la señal que viaja por el aire, decodificar la información, y acceder a la red con datos de otro usuario.

Esto significa que, para proteger la WLAN se necesitan elementos internos o externos a la WLAN implementados para autorizar el acceso a la red. La protección a los recursos e información de la LAN puede ser catalogado en diferentes niveles: básico, intermedio y avanzado [4].

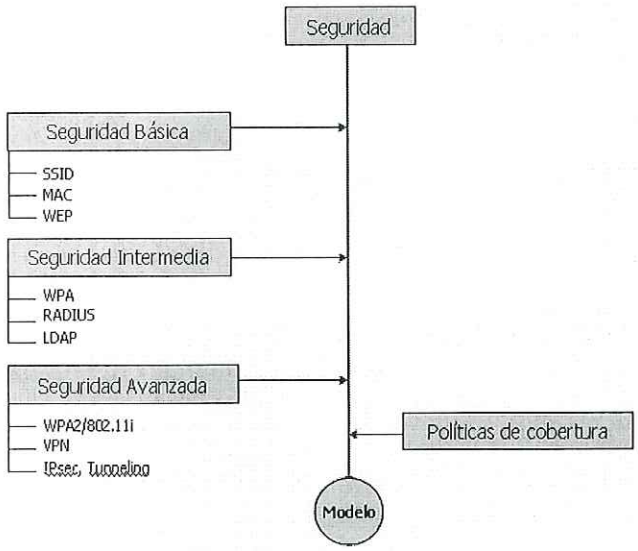


Fig. 2. Diagrama de Seguridad

Protección Básica

La protección básica presenta un nivel mínimo de seguridad el cual debe de ser implementado en cualquier WLAN. Siendo muy fácil de implementar, este nivel no es muy efectivo ya que no se reducen los riesgos de ataque, ver Figura 3.

Puntos mínimos para efectuar una protección básica:

1. Configurar el Service Set Identifier (SSID) que viene programado por defecto desde el fabricante.
2. Habilitar la encriptación de WEP.
3. Manejar el control de acceso mediante direcciones MAC.

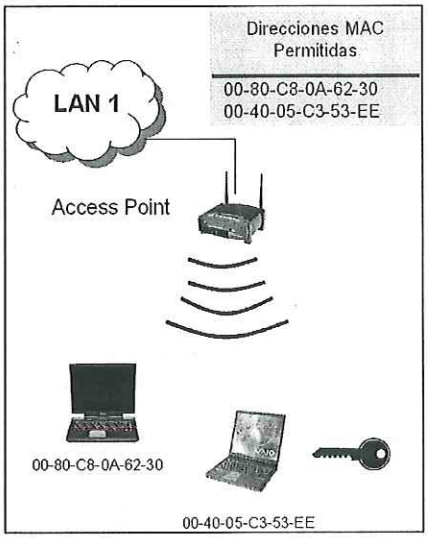


Fig. 3. Esquema de seguridad básica

Protección Intermedia

La protección intermedia incluye los puntos de protección del modelo básico, además, incluye un sistema de autenticación de usuario RADIUS para acceder a la red, el cual consiste en un servidor para la autenticación y manejo de cuentas para usuarios remotos. Es principalmente usado por los ISP (Internet Service Providers), aunque puede también ser utilizado en cualquier red que necesite un servicio centralizado de la autenticación y/o manejo de cuentas para sus estaciones de trabajo (STA). RADIUS soporta una amplia variedad de esquemas de autenticación.

Un usuario hace la petición para su autenticación con el servidor como se muestra en la Figura 4, ya sea contestando directamente en la consola su login/password o usando los protocolos CHAP, PAP u otros.

Puntos para efectuar la protección intermedia:

1. Configurar el Service Set Identifier(SSID) que viene programado por defecto desde el fabricante.
2. Habilitar la encriptación de WEP.
3. Manejar el control de acceso mediante direcciones MAC.
4. Incluir un sistema de autenticación como: LDAP, RADIUS

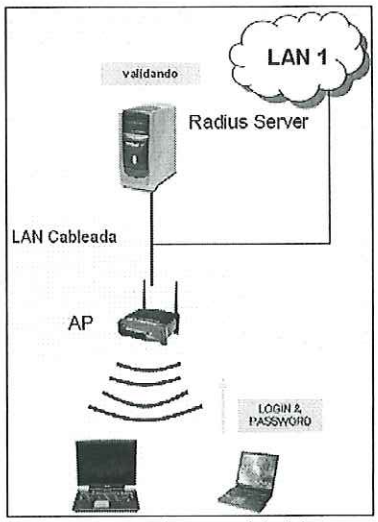


Fig. 4. Esquema de seguridad intermedia

Protección Avanzada

La protección avanzada incluye los puntos de protección del modelo intermedio, además que incluye métodos de encriptación a nivel capa 3 del modelo OSI y crea túneles seguros por donde viaja la información como se muestra en la Figura 5.

Puntos para efectuar la protección avanzada:

1. Configurar el Service Set Identifier(SSID) que viene programado por defecto desde el fabricante.
2. Habilitar la encriptación de WEP.
3. Manejar el control de acceso mediante direcciones MAC.
4. Incluir un sistema de autenticación como: LDAP, RADIUS.
5. Se incluye encriptación por terceras partes como IPsec, SSL o TLS utilizando un sistema de autenticación**VPN, IPSec**

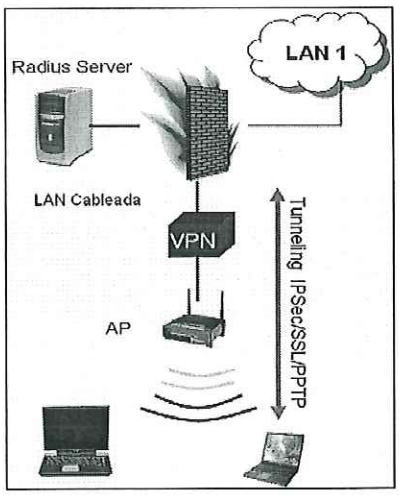


Fig. 5. Esquema de seguridad avanzada

Cobertura

Haciendo un análisis de las tecnologías y estándares que existen hoy en día podemos obtener información sobre el alcance o cobertura en metros dentro de ambientes interiores o exteriores, las velocidades máximas de transmisión, numero de canales y la frecuencia de operación, ver Tabla 1, sin embargo, hay que tomar en cuenta que las especificaciones dadas por los fabricantes a sus productos en cuanto a cobertura son ciertas solo en condiciones ideales, por lo que hay que corroborarlas mediante un análisis de propagación de la señal en donde se determine la calidad y potencia de la señal, así como el caudal eficaz en bits por segundo en los puntos más importantes del área a considerar.

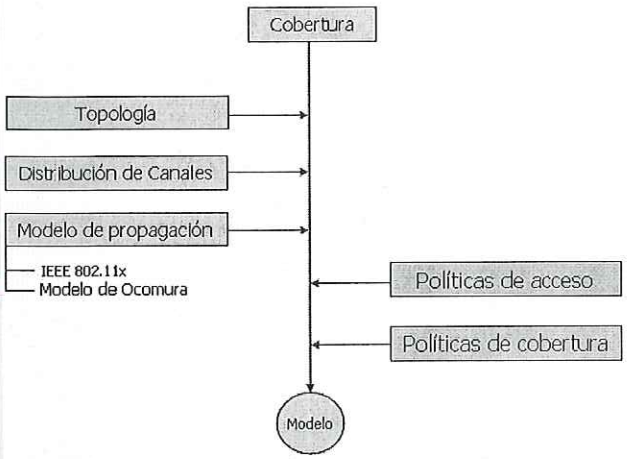


Fig. 6. Diagrama de cobertura

En las redes inalámbricas la condición de no tener línea de vista provoca mayores problemas que la de tenerla, así como la determinación de los canales y la calidad de los enlaces. En el caso de un ambiente interior, ambas condiciones existen, independientemente de que las señales recorran distancias muy cortas, esto es debido a la gran cantidad de obstáculos presentes en el ambiente (materiales para las fabricación de las paredes, las alturas de cada piso, las divisiones entre pisos, cantidad de vidrio utilizado en las paredes exteriores, además del mobiliario y los equipos que están dentro del inmueble). El tamaño de los posibles lugares es diverso, desde pequeño hasta grande, y la densidad de los obstáculos varia desde baja hasta alta. Estas configuraciones de las áreas de trabajo se encuentran resumidas en la Tabla [2]

Tabla 2. Tipos de zonas de cobertura[de WIRELESS COMUNICATION, RAPPAPORT]

Configuración	*Tamaño del Lugar*	*Densidad de los obstáculos*
1	Grande sin particiones	Baja
2	Grande con particiones suaves	Baja a media
3	Grande sin particiones	Alta
4	Pequeño	Baja
5	Pequeño	Alta

La configuración de las zonas de cobertura se divide en seis casos donde la división obedece al tipo de enlace de comunicación entre la Terminal (usuario) y la estación base (Punto de Acceso), según sea la implementación. Esta es una lista con los seis posibles casos [6].

1. Zona Extragrande.
2. Zona Grande.
3. Zona Mediana.
4. Zona Pequeña.
5. Microzona.
6. Sistema Distribuido.

La radio propagación de interiores es denominada por los mismos mecanismos que la de exteriores, estos son reflexión, refracción, y dispersión, Sin embargo, las condiciones varían mucho mas en función de diferentes factores físicos que involucran tanto el diseño de los edificios, como su altura y los materiales con los que están construidos.

Particularmente este modelo en su componente de cobertura se propone el uso un modelo de propagación para interiores llamado:

Modelo de particiones en el mismo piso

Para este modelo se requiere de datos específicos del tipo de construcción de la que se requiera saber las perdidas. Por lo que este modelo se aplica a construcciones en especifico, el cual consta de una serie de mediciones realizaras a diferentes materiales para obtener el calculo de las perdidas en la construcción, en la siguiente tabla se muestra una seria de mediciones hechas para diferentes materiales y ubicaciones, se pueden ver las perdidas generadas por estos materiales, además se puede observar la frecuencia a la que fueron realizados las mediciones.

Tabla 1. Mediciones experimentales para ciertos tipos de edificios[de WIRELESS COMUNICATION, RAPPAPORT]

Tipo de Material	Pérdida en dB	Frecuencia
Metal	26	815Mhz
Aluminio	20.4	815Mhz
Aislamiento de hoja	3.9	815Mhz
Bloques de concreto	13	1300Mhz
Pérdidas por un piso	20-30	1300Mhz
Pérdidas por un piso y una pared	40-50	1300Mhz
Atenuación observada cuando el transmitor toma un ángulo recto en la esquina del corredor	10-15	1300Mhz
Cubierta de metal-12ft^2	4-7	1300Mhz
Maquinaria ligera	1-4	1300Mhz
Maquinaria en General	5-10	1300Mhz
Maquinaria Pesada	10-12	1300Mhz
Escaleras de caracol	5	1300Mhz
Textil ligero	3-5	1300Mhz
Textil Pesado	8-11	1300Mhz
Area en donde los obreros inspeccionan el metal defectuoso	3-12	1300Mhz
Racks metálicos	4-9	1300Mhz
Cajas vacías de inventario	3-6	1300Mhz
Pared bloques de concreto	13-20	1300Mhz
Ducto del el techo	1-8	1300Mhz
Caja de metal de 4m	10-12	1300Mhz
Rack de almacenamiento con papeles	2-4	1300Mhz
Rack de 2.5m con partes metalicas	4-6	1300Mhz

Para el objetivo de nuestro trabajo es necesario contar con listados de las mediciones experimentales para su uso y calculo, para poder predecir una zona de cobertura con perdidas mas aproximado a lo real y proporcionar una distribución geográfica de los AP's con la mayor cobertura posible, en un inmueble determinado, y con datos necesarios que definen el tipo de construcción del inmueble en la organización que esta requiriendo el diseño de la WLAN.

Ancho de Banda

El ancho de banda y las velocidades de transmisión que nos brindan las WLAN permiten hoy hasta velocidades de 54Mbps con el estándar 802.11a/g mientras que el estándar 802.11b permite velocidades de transmisión de 11Mbps como se muestra en la Tabla 1. Este ancho de banda es mucho menor al de las redes cableadas, las cuales operan a 100Mbps y hoy en día hasta 1000Mbps. El ancho de banda especificado por los estándares 802.11a/b/g son teóricos y se cumple solo en condiciones ideales.

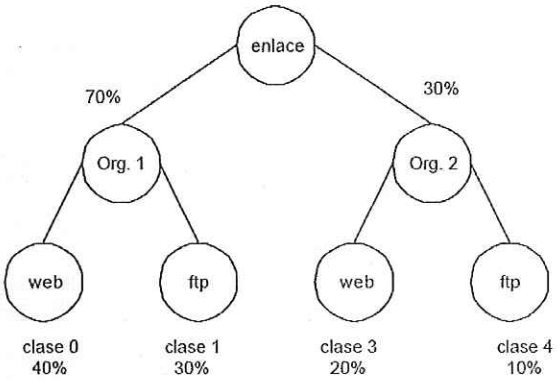


Fig. 7. Ejemplo de Compartición de Ancho de Banda CQB

Por eso es necesario tener un mecanismo que nos permita optimizar el ancho de banda y poder asegurar anchos de banda a los usuarios de la WLAN, esta componente incorpora un gestor, el cual trabaja conjuntamente con las aplicaciones y tipos (niveles) de usuarios que están definidos en otras componentes del modelo (aplicación y protección), CBQ (Clase Base Queueing) Encolado Basado en Clases es el método que propone el modelo para realizar esta actividad, CBQ es un algoritmo basado en clases, el cual propone la división y compartición del ancho de banda en clases estructuradas jerárquicamente, como se muestra en la Figura 7, cada clase tiene su propia cola y comparte una parte de acho de banda. Una clase hija puede tomar prestado ancho de banda de su padre si le sobra ancho de banda [7]. Existen varios métodos para optimar el acho de banda tanto de hardware como software de uso libre, sin embargo para fines prácticos de este trabajo se plantea el uso de esta herramienta que puede ser instalada en un ambiente LINUX y realizar las pruebas correspondientes.

En la figura 8, se muestra la manera en la que el gestor optimiza ancho de banda filtrando solo aquellos paquetes que fueron permitidos en la componente de aplicaciones y que se especificaron previamente.

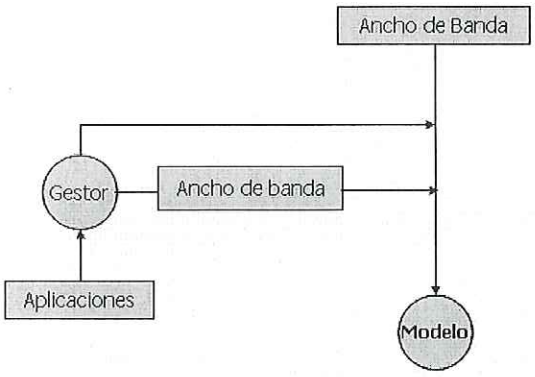


Fig. 8. Diagrama de manejo de Ancho de Banda

Aplicaciones

Un componente importantísimo para este modelo son las aplicaciones que los usuarios finalmente usaran o estar corriendo sobre estas redes por lo que es importante delimitar el tipo de aplicaciones van a ser ejecutadas, tales como acceso a Internet, correo electrónico, consultas a bases de datos y transferencias de archivos. Dado el limitado ancho de banda, no sería recomendado que se utilizaran aplicaciones que consumen mucho ancho de banda, como pueden ser transferencia de video, imágenes, videoconferencia y el videostreaming, sin embargo, la gestión que estamos haciendo con nuestra componente de manejo de ancho de banda nos permite pode utilizar esos servicios con gran ganancia durante la transmisión, esto solo si es necesario, por que si bien las WLAN no incorporan calidad en sus servicios (QoS). Esta herramienta nos permite otra alternativa de uso.

El proceso de planeación plantea la necesidad de tener indetificadas las aplicaciones que la organización permitirá correr sobre su WLAN por ello se realiza un "survey" que trata de identificar las aplicaciones que comúnmente utilizan los usuarios de las redes inalámbricas y aplicaciones que serian de mayor y menor uso con el objetivo de establecer jerarquías sobre el filtrado de los paquetes. Este survey lo podemos obtener de la pagina http://lcc.ens.uabc.mx/~wifi/survey.pdf para ser aplicado a los empleados de la organización con el objetivo de contar con estos bancos de datos que contengan información de las aplicaciones asociadas a un cierto ancho de banda por aplicación. En la Figura 9, se muestra el proceso de identificación de las aplicaciones utilizando el survey.

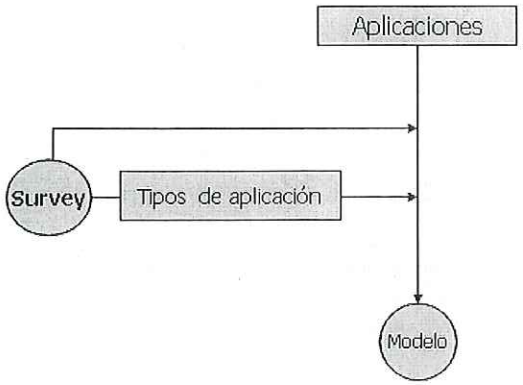


Fig. 9. Diagrama de aplicaciones

Equipos

Desde 1999 que fue cuando se ratifican los estándares 802.11a/b, las compañías que se dedican a la fabricación de equipo para redes inalámbricas empiezan a lanzar sus primeras versiones. Los equipos que han sido lanzados desde 1999 han trabajado en los respectivos espectros de frecuencia acorde con el estándar en fabricación como lo muestra en Tabla 1. En la actualidad la familia estándares que ha dominado el mercado de las redes inalámbricas es el IEE 802.11.

¿Por que 802.11b ha sido el dominante? La respuesta es sencilla, empresarios del área en redes inalámbricas empezaron a fabricar equipos con el estándar 802.11b certificándolos por el organismo conocido como *WECA* (Wi-Fi Alliance). Mientras que el estándar 802.11a se empezó a fabricar a principios del 2001.

Como los estándares 802.11a/b no son compatibles entre si, los fabricantes lanzan al mercado equipos independientes para cubrir necesidades particulares. Esto se realizo en las ultima dos décadas, tal es el caso, que para finales del 2002 compañías lideres del mercado en redes inalámbricas lanzan equipos duales, es decir, equipos con ambos estándares.

Con la aprobación del estándar 802.11g en el 2003, las equipos 802.11a/b/g ofrecen rendimientos adecuados a las convenciencias de los clientes, en la próximas generaciones de las aplicaciones requerirán mayor capacidad de procesamientos y los usuarios reclamaran mayor ancho de banda y mayores coberturas, en respuestas a estas necesidades los grupos lideres en productos trabajan conjuntamente para lanzar próximamente el IEEE 802.11n junto con la WI-FI Alliance.

Es importante mencionar que no serviría de nada proponer un diseño elaborado mediante este modelo, si los equipos que van a ser adquiridos para la implementación de la LAN no pueden soportar las diversas configuraciones que arroja este modelo, de modo que, si antes era sencillo adquirir un equipo ahora será necesario observar cuidadosamente sus características que presentan tantos los AP's como los clientes inalámbricos.

V. RESULTADOS

Este trabajo solo presenta hasta este momento algunos resultados preliminares los cuales vienen a soportar o apoyar cada una de las propuestas que aquí se propone. Es importante que este modelo tenga fundamento solido en cada uno de sus componentes ya que depende de ello se logrará crear diseños confiables, en una siguiente fase se espera poder probar el modelo con un diseño real ya implementado para comparar los resultados y poder establecer un criterio sobre el diseño que arroja el modelo.

Los resultados obtenidos son:

- Análisis de seguridad configuración e implementación de la seguridad básica e intermedia con servidores LDAP y RADIUS para la autenticación de los usuarios, así como la evaluación de los protocolos para una protección avanzada

- Análisis de la propagación de la señal en un edificio interior para determinar la zona de cobertura, observando las variaciones que existen al usar un dispositivo inalámbrico con menor potencia (computadoras portátiles) y otro dispositivo con mayor potencia (PCI y USB Wireless Card) para posteriormente comparar los datos obtenidos con las listas de perdida de señal con materiales específicos que nos proporciona el modelo de particiones en el mismo piso, la comparación se muestra en las Figuras 9 y 10.

- Proceso para la definición de las políticas, en la actualidad proceso de desarrollo de las políticas es sumamente importante en cualquier organización que cuente con una LAN.

En la actualidad el proceso de desarrollo de las políticas es sumamente importante en cualquier Organización o Institución que cuente con una Red, el desempeño y la operación de las acciones de trabajo deben ser aceptables, por lo que la realización de estas reglas se debe dar en un principio de manera clara y pensando siempre en el beneficio de la organización.

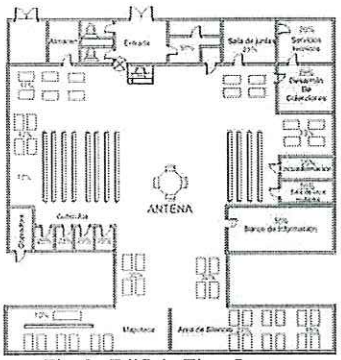


Fig. 9. Edificio Tipo, Laptop

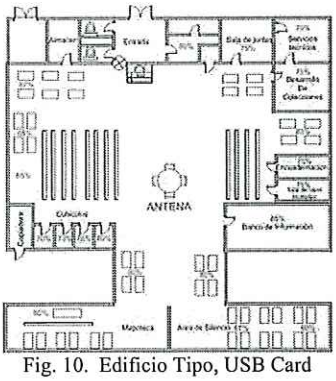


Fig. 10. Edificio Tipo, USB Card

El desempeño y la operación de las acciones de trabajo deben ser aceptables, por lo que la realización de estas reglas se debe dar en un principio de manera clara y pensando siempre en el beneficio de la organización.

Es importante mencionar que la construcción de estas políticas es un proceso donde intervienen las personas responsables de las actividades que se realizan dentro de la organización, así como, los administradores encargados de la seguridad en la red. Así como las redes cableadas, las WLAN requieren de políticas que estén diseñadas, implementadas y esforzadas al máximo desempeño para reducir al máximo una situaciones de inseguridad que se presente [8].

> *Los administradores deben establecer por escrito reglas, dictando que las ondas aéreas (u ondas de radio) dentro de la empresa sean un recurso manejado, no diferente a un recurso alambrado*
>
> **Gartner, September 20002**

Para tratar de definir las políticas para una WLAN las cuales deben convertirse en parte del documento que integra las políticas generales de la red de la empresa y debe estar reflejado dentro de los seis pasos del proceso de definición de políticas los cuales son.

) Las políticas primero se definen y se documentan. *(para cada uno de los componentes del modelo existe un proceso de definición de políticas)*
) Aprobación de las políticas (ejecutivos o altos mandos de la organización).
.) Difusión y educación del personal
.) Auditoria y Monitoreo.
.) Aplicación de acciones correctivas.
.) Revisión de efectividad y limitaciones de las políticas

EFERENCIAS

] IEEE 802.11b Wireless LANs – 3COM
tp://www.3com.com/other/pdfs/infra/corpinfo/en_US/503 7201.pdf

] Security of the WEP algorithm
tp://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

] Planeación y diseño de redes WLAN, Evelio Martínez, drián Enciso.
p://www.eveliux.com

] Wireless Security: it's like securing your house - termec
p://epsfiles.intermec.com/eps_files/eps_wp/WirelessSecu WPWEB.pdf

[5] Defining Best Practices for Designing and Implementing 802.11 Wireless Security
http://www.vigilar.com/wp802.pdf

[6] Cardana Angel, "ANTENAS", alfaomega, Edición 2000

[7] S. Floyd, V. Jacobson, "Link Sharing and Resource Management Modelsfor Packet Networks". IEEE/ACM Transaction on Networking, Vol. 3, No. 4, pp. 365-386, Agosto 1995.

[8] Wireless LAN Policies for Security & Management, AirDefense 2003, www.airdefense.net.