UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

PROYECTO DE INVESTIGACIÓN PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA

DISEÑO DE UN PROYECTO PARA UNA ORGANIZACIÓN
QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA :
HÉCTOR HIROSHI SAISHIO JIMÉNEZ

ASESOR :
ACT. FRANCISCO DAVID MEJÍA RODRÍGUEZ

MÉXICO, D.F. 2005

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.

NOMBRE: Sasha Jiménez Hevia Hucsh

FECHA: 24/Febrero/05

FIRMA:

A Dios, por ser mi compañero incondicional y haberme brindado el regalo de la vida.

A la Facultad de Contaduría y Administración y a la Universidad Nacional Autónoma de México por mi formación profesional.

A ti mamá, mi agradecimiento para toda la vida, por tu inquebrantable amor, tu firme dedicación y tu constante compromiso.

A ti papá, por ser un ejemplo de disciplina y por tu apoyo en mi formación como profesionista.

A ti Midori y a ti Hiromi, por ser mi fuente de alegría, por su sutil dulzura y ser la luz que me procura.

Mi más grande gratitud a la familia Salazar por su incondicional amor y formidable cariño.

A ti tía Mary por ser un ejemplo de fortaleza, ternura y comprensión.

A Naomi, Osamu y Asami, por su enorme afecto y gentileza.

Con especial consideración al Actuario David Mejía por su asesoría y apoyo incondicional de maestro y amigo.

A la Mtra Graciela Bribiesca con respeto y cariño que siempre le he profesado, gracias por su apoyo invariable a lo largo de la carrera y el impulso en este proyecto.

A Carlos Navarro de 3COM por tu increíble paciencia, pero sobre todo por tu amistad y tus enseñanzas.

Al profesor Salvador Meza por su colaboración informativa en este trabajo.

A Alejandra, Alejandro, Brissa, Cristian, Diana, Erika, Gris, Iris, Jaime, Lulú, Luis, Manuel, Marco, Melissa, Mireya, Roberto, sin advertir el lugar en el que se encuentre su nombre ya que carece de importancia, los amo y para ustedes mi infinita gratitud.

Con todo cariño y amor, para ti este Proyecto, que es el resultado de un esfuerzo. Jamás podré olvidar lo que tú vales para mí.

"Agradezco a mi familia que son mis mejores amigos y a mis mejores amigos que son mi familia. Gracias a todos, los nuevos, los de siempre, los de tiempo atrás, los de momentitos, los que hacen hábito conmigo, los que me abrazan, los que me regañan, los que me quieren como soy, pero sobre todo los que me han tocado el corazón y los que han llegado a mí, a mi casa y a mi vida."

ÍNDICE

I. INTRODUCCIÓN

I. 1. Presentación

En la actualidad las telecomunicaciones impulsan uno de los procesos de cambio más importantes que haya vivido la humanidad: la Era de la información. Con ella, se transforma cotidianamente la forma en que millones de personas en México y en todo el mundo se educan, trabajan, se comunican y se informan. La incorporación de tecnologías a las actividades diarias, permiten potenciar con un gran nivel de aplicabilidad distintos escenarios.

La capacidad que la tecnología ha demostrado y su efectividad en aspectos como la transmisión de la información y del conocimiento, ha dado pie a la idea de incorporar estos recursos, un ejemplo de esto son las comunicaciones inalámbricas en el mundo, que han tenido un gran avance y uso, estimuladas por la ratificación del estándar 802.11 del IEEE.

En las condiciones tecnológicas actuales, es posible el diseño y desarrollo de una red inalámbrica o wireless network, como una forma de implementar tecnología de vanguardia en la Facultad de Contaduría y Administración, ésta sería una decisión estratégica que tendría que ser tomada por el Consejo Técnico de la Facultad en conjunto con la Academia de Informática, ya que proporcionaría soporte a los procesos educativos y a procedimientos del Sistema de Administración Escolar, pero implica un diseño de los mismos para posteriormente definir como se utilizará.

La popularización de las redes inalámbricas y su posible interconexión ha dado pie a que potencialmente se puedan crear redes móviles, con un amplio ancho de banda en extensas zonas urbanas, dando lugar a redes metropolitanas. Una red inalámbrica implica un concepto inmediato: hacer cómputo "sin cables", sin que el equipo personal esté visiblemente conectado a algo. Involucra dos avances tecnológicos fundamentales: la comunicación inalámbrica para transmisión de datos (conocidas genéricamente como wireless) y la miniaturización de los componentes de un equipo de cómputo, al grado de portarlos como un accesorio más del vestir. De manera secundaria, pero no por ello menos importante, tiene que ver con el continuo desarrollo de aplicaciones y sistemas operativos (software) más sofisticados y especializados.

El diseño y desarrollo de una red wireless para un recinto académico, como lo es la Facultad de Contaduría y Administración, implica e involucra la realización de un conjunto de actividades propias del área de telecomunicaciones, de disciplinas administrativas y por supuesto de la informática. El presente proyecto, es una síntesis de la labor de investigación, en torno a toda la propuesta de diseño y desarrollo de una red inalámbrica, desde las causas que motivaron la integración del proyecto hasta la conclusión a la que se logró, una vez desarrollada la investigación. Del mismo modo comprende un conjunto de actividades para la gestión y control del proyecto, como son la determinación de la complejidad y los recursos a emplearse.

I. 2. Selección del Proyecto

La elección de este proyecto como opción de titulación emerge a partir de diversos factores entre los cuales destaca, la trascendencia y el éxito en los últimos años de las redes inalámbricas por lo que me abocaré a puntualizar la importancia de este tipo de redes y las tecnologías subyacentes, los problemas que plantean, sus posibilidades y expectativas.

El proyecto de una red wireless, surge como una inquietud debido a que el mundo está en constante movimiento y la tecnología cada día está presente de manera natural en nuestras vidas. Las universidades no están al margen de estos cambios y deben aprovechar las oportunidades que el ambiente actual ofrece. La fuerza que a la fecha han cobrado las tecnologías inalámbricas se debe, en gran medida, a las ventajas de movilidad para los usuarios y a los precios competitivos que tienen en relación con las redes alámbricas convencionales. Es elemental precisar, que más que tratar de reemplazar, las redes inalámbricas complementan a la tecnología alámbrica, estableciendo nuevas aplicaciones y añadiendo flexibilidad a la red.

La implementación de esta tecnología en la Facultad, tendría una oportunidad en la educación distribuida, la cual permite que el alumno tenga la libertad de estudiar en el momento y lugar que elija. La independencia en el aprendizaje y la oportunidad de trabajar de manera colaborativa, con los compañeros universitarios que pueden estar ubicados en lugares geográficos distintos, apoyados en todo momento por la guía de los profesores usando diferentes tecnologías como Internet, donde y cuando se necesite, sin la necesidad de desplazarse a lugares específicos en un tiempo determinado.

En la actualidad, es preciso contar con las tecnologías necesarias en los institutos, en los centros de investigación, pero sobre todo en las universidades, porque es aquí donde se constituye, se integra y totaliza el conocimiento para formar a los futuros profesionistas, docentes e investigadores de nuestro país; por ello, es indispensable tener instalaciones y equipos que faciliten cada vez más la integración a las vanguardias tecnológicas. Existen diversas aplicaciones que se obtendrían con la implementación de una red wireless como:

- Formación disponible 7 x 24 horas a cualquier hora y en cualquier lugar. Ampliando la cobertura, eliminando las barreras de lugar y tiempo.
- Movilidad de Servicios de Comunicación
- Soluciones de formación inmediatas.
- Gestión del conocimiento.
- Formación constante: creación y actualización de contenidos.
- Formación online guiada por el asesor. Cada usuario avanza de acuerdo a su tiempo
- Aprendizaje autónomo con prácticas interactivas.
- Mejora del desempeño del docente, por cuanto parte del tiempo que antes se dedicaba a la clase, se invertirá en un mejor diseño curricular y en investigación.

I. 3. Metodología

Las fuentes de información empleadas para la realización de este proyecto fueron diversas, ya que se involucró una amplia gama de referencias de investigación como son: la búsqueda y consulta bibliográfica principalmente, páginas en Internet, observación directa y práctica profesional.

Se partió con la consulta bibliográfica, basada en libros, revistas especializadas acerca de redes inalámbricas, páginas de Internet y proyectos para una organización. La observación directa se dió en el terreno profesional.

La experiencia en clases fue otro punto importante dentro de la metodología, debido a que se realizaron consultas de apuntes, temas en clase y trabajos en materia de telecomunicaciones. Todas estas fuentes de información permitieron que sustentara la propuesta del proyecto y que finalmente se viera aterrizada en este trabajo de investigación.

Descripción del tema

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. Esta tecnología nació como consecuencia de las necesidades de movilidad y que por sus numerosas aplicaciones y ventajas cada día está creciendo más su demanda en el mercado.

Esta nueva alternativa tiene muchas aplicaciones, así como ventajas. ¿A quién no le gustaría poder conectarse a una red en cualquier lugar y momento? Las redes inalámbricas son sencillas de instalar, usar, y manejar y por tanto, vale la pena la inversión inicial en el equipo. El costo de instalación y mantenimiento de una W LAN generalmente es más bajo que el coste de instalación y mantenimiento de una red cableada tradicional y resulta beneficiosa a largo plazo.

Las WLAN ofrecen la posibilidad de compartir información en tiempo real, sin la necesidad de buscar conexión física, lo que permiten portabilidad y movilidad. Aunque esta tecnología puede ser una alternativa para redes fijas de área local (LAN), no pretende reemplazar al sistema tradicional con cable, sólo lo complementa en situaciones en que es difícil hacer una conexión.

En este proyecto abordaré el tema de las redes inalámbricas, haciendo un análisis de la situación actual, considerando la infraestructura con la que se debe contar, los servicios que se pueden ofrecer; esto implica aspectos como: los equipos o dispositivos inalámbricos, su funcionamiento, estándares, organismos, costos, etc., todo con el fin de plantear una actualización tecnológica, lo que permitirá que la red actual brinde una diversa gama de servicios a la comunidad y complementar su desempeño académico.

I. 4. Objetivos

El presente proyecto de titulación, es una memoria del proceso de investigación realizada, siendo su objetivo dar una visión preliminar del trabajo efectuado, al sumar el conjunto de productos resultados de este proceso.

Este enfoque comparte mis experiencias con respecto al proyecto, haciendo hincapié en el aprendizaje teórico-práctico obtenido, a partir de mi formación académica y profesional. Esto aportará al lector los posibles resultados a obtener en proyectos, así también se identificarán puntos susceptibles a optimizarse, lo que mejorará los resultados de proyectos futuros.

Cabe mencionar que este documento no tiene como propósito ser una referencia técnica de las herramientas, metodologías y /o estrategias utilizadas durante el transcurso del proyecto. Para este fin, se han abordado dos capítulos titulados: Marco Teórico y Marco Conceptual, en donde el lector podrá encontrar información más detallada.

Contenido

El desarrollo del primer capítulo tiene como objetivo dar al lector un enfoque del presente documento, al explicar aspectos preliminares del inicio del mismo, como son: la presentación, la selección del proyecto, los objetivos a alcanzar, la metodología utilizada para su elaboración, así como la definición del contenido y la pauta para desarrollar los siguientes capítulos.

Las principales fuentes de información se presentan en el capítulo II titulado Marco Teórico, las cuales corresponden con el tema del proyecto, así como los conocimientos adquiridos de las mismas, tales como libros, diseño de sistemas o proyectos para organizaciones, manuales, revistas, periódicos, páginas de Internet o URL´s, utilizados en esta investigación. De esta forma, se hace un breve resumen de los capítulos consultados con su correspondiente referencia bibliográfica.

El contar con una visión preliminar del contexto, mediante la definición de términos y conceptos elementales, proporciona las bases para comprender y fundamentar el proyecto de investigación, debido a esto, el tercer capítulo es el Marco Conceptual. El asentar debidamente este capítulo, permite contar con una percepción clara de los alcances y posibles proyecciones, así como la identificación de oportunidades. De igual forma se hace hincapié en la disposición a probar la tecnología cuando hay aplicaciones que se advierten como efectivas, sin embargo dada la extensión de cada uno de los temas que se exponen no se profundizará en todos los conceptos de cada tecnología.

El capítulo IV es el de Análisis, dedicado a llevar a cabo el por qué de este proyecto, y su planteamiento para poder llevar a cabo un buen desarrollo, pues es necesario tener claro la importancia de los elementos que interactuarán con el mismo.

El capítulo V denominado Propuesta Tecnológica, presenta diversos planteamientos y alternativas detalladas, acerca del diseño de la red inalámbrica, apoyándome en la investigación realizada así como en los criterios necesarios para poder determinar la solución mas apropiada para el entorno de la facultad.

En el capítulo VI de Resultados Obtenidos, se especifican los beneficios de implementar de manera apropiada una red inalámbrica, del mismo modo se vislumbran las limitaciones y restricciones del proyecto.

En el capítulo VII Costo del Proyecto, se indican los costos de inversión en equipos, contemplando los criterios o factores de factibilidad del fabricante de equipos en telecomunicaciones.

El capítulo VIII llamado Normatividad, aborda la trascendencia de políticas, procedimientos y reglas en seguridad, para prevenir vulnerabilidades, amenazas y cerciorase de un óptimo funcionamiento de una red inalámbrica.

En las Conclusiones, se presentan de manera general los resultados obtenidos y las deducciones teóricas derivadas del proyecto de investigación y se proponen alternativas de continuidad.

Finalmente se presenta una serie de Anexos con información documental, relativa a la configuración de los dispositivos empleados; lugares públicos e Instituciones educativas en México en los que actualmente se brindan servicios con tecnología inalámbrica; así como un Glosario en donde se abordan términos conceptuales y complementan los aspectos técnicos.

II. MARCO TEÓRICO

II. 1. Acopio Bibliográfico

En el Marco Teórico se reúnen los documentos de apoyo, la documentación y todos los conocimientos adquiridos de diversas referencias consultadas tanto bibliográficas como electrónicas. De este modo el lector podrá encontrar información mas detallada de las mismas.

II. 1. 1. Libros de Consulta

Nombre del Libro	Tecnología móvil : GSM, GPRS, UMTS y WI-FI
Autor	Luis Arroyo Galán
Editorial	Madrid : Anaya Multimedia
Edición	1ª Edición
ISBN	84-415-1582-4
Colocación Biblioteca	TK6570.M6 A77 Biblioteca D.G.S.C.A
Capítulo VI Redes LAN Inalámbricas	Este capítulo trata nociones conceptuales de redes inalámbricas, del porque son atractivas para quienes trabajan en el área de redes, los clientes objetivo, del sí la conectividad de esta tecnología está o no lo suficientemente madura y los costos promedios de su implementación.

Nombre del Libro	The Communications Handbook
Autor	Jerry D. Gibson
Editorial	Boca Ratón, Florida : CRC, c2002
Edición	2ª Edición.
ISBN	0-8493-0967-0
Colocación Biblioteca	TK5101 C66 2002 Biblioteca D.G.S.C.A
Capítulo I Wireless Personal Communications: A Perspective	Se brinda una perspectiva sobre como operan las redes inalámbricas en la actualidad, los servicios que se ofrecen con la adopción de esta tecnología y como, mediante la evolución de los dispositivos inalámbricos, se ha logrado un vertiginoso despliegue de soluciones innovadoras. De igual manera se habla de cuestiones de seguridad pero de manera muy general.

Nombre del Libro	Wireless Data Networking
Autor	Nathan Muller J.
Editorial	Boston: Artech House, 1995
Edición	1ª. Edición
ISBN	0890067538
Colocación Biblioteca	TK 5105 M85 Biblioteca D.G.S.C.A
Capítulo I **Introduction to Wireless Network**	En este capítulo se aborda el tema del porque hacer uso de una conectividad inalámbrica, sustentando como punto principal la movilidad de los usuarios, los avances recientes en la estandarización y el crecimiento de Internet. Se menciona la importancia decisiva del espectro, la forma en como se encuentra dividida la banda ISM y los rangos de frecuencia utilizados para el funcionamiento de esta tecnología. También se señalan las limitaciones y los desafíos en el establecimiento de una red inalámbrica.

Nombre del Libro	Wireless Technology Protocols, Standars and Techniques.
Autor	Yacoub Michel Daoud
Editorial	Boca Ratón : CRC
Edición	2ª Edición.
ISBN	0849309697
Colocación Biblioteca	TK6570-M6-Y34 Biblioteca D.G.S.C.A
Capítulo I **Wireless Network**	En este capítulo se abordan conceptos básicos de una red inalámbrica, se detallan las generaciones que la constituyen, los estándares vigentes y especificaciones sobre los cuales están desarrollados (mostrando sus características y requisitos técnicos), así como la manera en que esta tecnología ha ganado aceptación universal con el número de suscripciones inalámbricas.

II. 1. 2. Libros de Lectura Rápida

L. Harte, "Introduction to 802.11 Wireless LAN (Wlan), Technology, Market, Operation, and Services", April 2004.

R. Flickenger, "Building Wireless Community Networks", 2nd Edition.

II. 2. Diseño de un Proyecto para una Organización

Nombre del Proyecto	Actualización Tecnológica de la Red de Cómputo de la FCA
Autor	Karla Arias Mondragón
Fecha	2004
Carrera	Licenciatura en informática
Universidad	UNAM Facultad de Contaduría y Administración

El tema central que se presenta en este proyecto es muy interesante, ya que se plantea una actualización tecnológica de la red (en este caso, el modelo propuesto está basado en Fast Ethernet y Gigabit Ethernet), de la Facultad de Contaduría y Administración, para satisfacer las necesidades de comunicación de la red de cómputo y proveer un servicio óptimo. Para la realización de este trabajo se despliega toda una investigación detallada de la integración y distribución de la red con la que se cuenta, así como los servicios que ésta provee para el acceso e intercambio de información de datos.

Nombre del Proyecto	Investigación en Telefonía Celular Aplicada a Ambientes de Aprendizaje en Comunidades Amplias.
Autor	Enríquez Dentón, C
Fecha	2003
Carrera	Ingeniería en Sistemas Computacionales
Universidad	Escuela de ingeniería, Universidad de las Américas -Puebla
Capítulo IV Acceso a Internet Inalámbrico	Los temas que se abordan específicamente en este capítulo son: los inicios de la Era Inalámbrica, los beneficios y oportunidades por el uso de la tecnología en la educación, uso y limitaciones de los dispositivos inalámbricos, los beneficios loables para la UDLA-P con el uso de la tecnología para el campus wireless.
Capítulo V Servicios Inalámbricos Orientados al Aprendizaje en la UDLA-P	Los tópicos que se plantean son la necesidad de una Universidad Inalámbrica en la UDLA-P, un Campus Wireless en la UDLA-P que apoye el aprendizaje de estudiantes especiales, los lineamientos en el desarrollo de servicios inalámbricos orientados al aprendizaje en la UDLA-P.

II. 3. Revistas

Nombre del Periódico	PC WORLD
Fecha de Publicación	26 de Febrero del 2004
Nombre del Artículo	Guía de redes inalámbricas

En esta publicación se consultó un artículo acerca del como las redes inalámbricas definitivamente están pasando por su mejor momento: actualmente tienen precios razonables, son confiables y relativamente fáciles de instalar.

II. 4. Periódicos

Nombre del Periódico	El Universal
Fecha de Publicación	22 de Mayo del 2004
Nombre del Artículo	El uso de WIFI crece en México

En este artículo se refiere al estándar WiFi (o acceso a Internet inalámbrico a través de equipos móviles) considerado como la promesa de la tecnología y las telecomunicaciones a nivel mundial y como ha cobrado auge en México pese a las grandes barreras económicas, legales y geográficas a las que se enfrenta.

Nombre del Periódico	Reforma
Fecha de Publicación	6 de Junio del 2004
Nombre del Artículo	Afecta a inalámbricos la vulnerabilidad

En esta edición se aborda el tema de la seguridad, la falta de medidas de seguridad apropiadas en las redes inalámbricas (WiFi) y en las conexiones de alta velocidad en Internet. Analistas y firmas en seguridad tecnológica advierten de un ataque masivo de virus cibernéticos

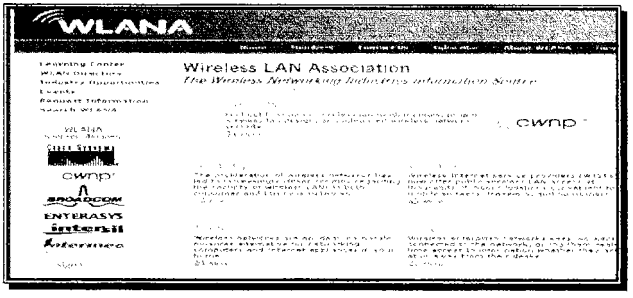
Nombre del Periódico	Reforma
Fecha de Publicación	10 de Noviembre del 2004
Nombre del Artículo	A encontrar Hotspots

La publicación proporciona datos relevantes, tales que ciudades como Filadelfia planean ofrecer acceso inalámbrico en toda su área urbana en el 2005. Otras pequeñas ciudades como Grand Haven (Michigan) ya lo ofrecen, y en otros continentes, ciudades como Amsterdam (Holanda) también piensan en crear redes WiFi.

II. 5. URL´s

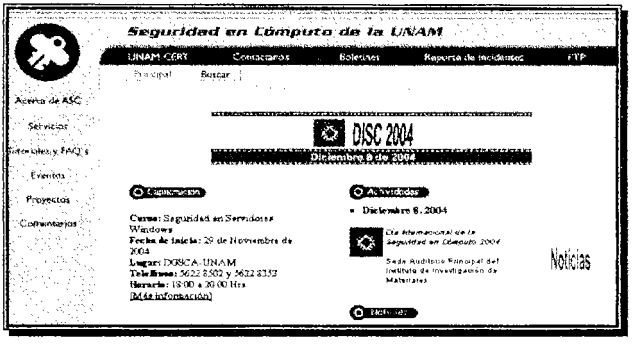
http://www.wlana.org/direct/direct.htm

Este sitio contiene información relevante en cuanto a innovaciones de la tecnología inalámbrica, patrocinadores y afiliados de la industria, ediciones que sirven para dar un panorama a los clientes, así como una perspectivas detallada de productos wireless, boletines de noticias y opinión de analistas líderes de la industria.



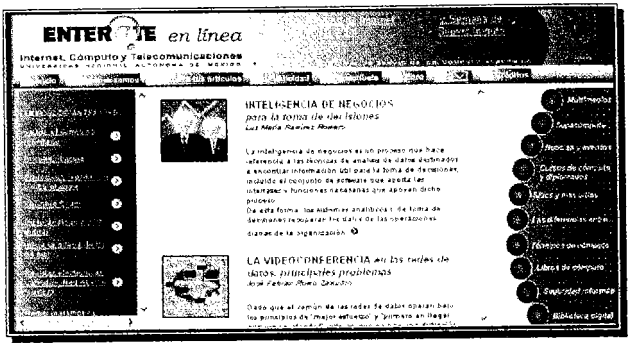
http://www.seguridad.unam.mx

Esta página está dedicada a proporcionar esquemas de seguridad computacional para la universidad. A través de la misma, realiza las siguientes tareas: respuesta a incidentes, elaboración de boletines de seguridad en cómputo, diseño de esquemas en seguridad computacional, diseño de políticas de seguridad en cómputo, organizar y coordinar los eventos GASU, DISC y la semana de seguridad en cómputo, investigación y desarrollo de herramientas de seguridad para sistemas Unix y NT.



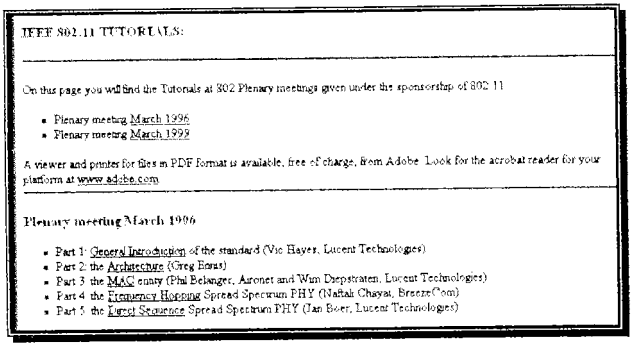
http://www.enterate.unam.mx/

Entérate es un suplemento de divulgación sobre Cómputo, Internet y Telecomunicaciones que se publica en versión electrónica. En este sitio se ofrece a la comunidad universitaria y a la sociedad en general, una publicación periódica que aborda de manera muy sencilla, temas altamente especializados, de igual forma analiza las tendencias y perspectivas de las nuevas tecnologías de la información, particularmente de Internet, difunde conocimiento sobre tecnologías emergentes y sus aplicaciones, además orienta sobre los usos educativos del cómputo.



http://grouper.ieee.org/groups/802/11/Tutorial/

Este sitio, perteneciente a la IEEE contiene documentación relativa al estándar 802.11.



- http://www.ciberhabitat.gob.mx/universidad/

Esta página maneja diversos temas con respecto a la Tecnología de la Información y las Comunicaciones (TIC), es publicada por el Instituto Nacional de Estadística, Geografía e Informática (INEGI) y pone a disposición de la sociedad hispano parlante, un sitio educativo en Internet llamado Ciberhábitat, el cual aborda el tema de la TIC desde diferentes ámbitos: uso de TIC en diferentes sectores, impacto en la sociedad, explicaciones de aspectos técnicos y tutoriales. Todo esto en forma didáctica.

II. 6. Otras fuentes

Tutoriales en formato PDF

Nombre	Wireless How To

Este documento explica algunos aspectos sobre Redes Inalámbricas, como configurarlas, y posibles problemas que puedan surgir. Se comenta de igual forma, que a diferencia de la red de cable, la red inalámbrica requiere algunos trucos para que funcione correctamente.

III. MARCO CONCEPTUAL

III. 1. Antecedentes

Originalmente los sistemas de redes inalámbricas se idearon y comercializaron como un medio de reducción de costes en la instalación de redes en empresas y oficinas. Al no requerir ningún tipo de cableado permitían disponer de una red local LAN (Local Area Network) en poco tiempo y con menor inversión de infraestructura.

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Procedimientos de la IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología. Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread spectrum"(frecuencias altas), siempre a nivel de laboratorio.

En mayo de 1985, tras cuatro años de estudios, la FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 Ghz, 5,725-5,850 Ghz a las redes inalámbricas basadas en "Spread Spectrum"(ISM es una banda para uso comercial sin licencia).

Las ventajas de las redes en estos rangos de frecuencias son claras: no requieren licencias, permisos ni necesidad de comunicación para su despliegue y pueden ser implantadas en cualquier ubicación. Pero como contrapartida surgen una serie de importantes inconvenientes: interferencias impredecibles con redes próximas por selección de frecuencias iguales o parcialmente solapadas, espectro empleado por otras aplicaciones (Redes Bluetooth, usos domésticos como teléfonos inalámbricos, emisores de vídeo, mandos de control remoto...), potencia de emisión muy limitada que restringe mucho la cobertura y una banda de uso muy estrecha que permite delimitar muy pocos canales no interferentes. La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por la IEEE 802 para que la red sea considerada realmente una LAN.
Finalmente, se define un estándar, la norma IEEE 802.11 para redes WLAN en Junio de 1997. Sin embargo, las tasas de datos proporcionadas por este estándar son demasiados lentas para sostener los requerimientos generales de los negocios afectando a la demanda de las WLAN.

Reconociendo la necesidad crítica de mantener tasas de transmisión de datos mayores, la IEEE ratificó el estándar 802.11b (también conocido como 802.11 de tasa alta) para transmisiones de hasta 11 Mbps en Septiembre de 1999. Con este estándar, el 802.11b, las WLAN son capaces de alcanzar funcionamiento inalámbrico y throughput comparable a Ethernet. Inmediatamente, la asociación de ingenieros electrónicos, IEEE, designa una comisión de trabajo para desarrollar una tecnología de red en dichas bandas: la 802.11. A partir de ese momento se liberan una serie de estándares, en el SITI/LAN 2003, Salón

Internacional de Redes, Internet y Comunicaciones que tuvo lugar en Madrid el 6 de febrero, fue el escenario elegido para la presentación de la nueva generación Wireless-G (norma 802.11g) con velocidades de hasta 54 Mbps.

Normalización

En 1990, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN. Pero no es hasta 1994 cuando aparece el primer borrador, y en junio de 1997 que se da por finalizada la norma. En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Personal Communications Systems). En ese mismo año, la ETSI (European Telecommunications Standards Institute), a través del comité ETSI-RES 10, inicia actuaciones para crear una norma a la que denomina HiperLAN (HIgh Performance LAN) para, en 1993, asignar las bandas de 5,2 y 17,1 GHz. En 1993 también se constituye la IRDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos. En 1996, finalmente, un grupo de empresas del sector de informática móvil y de servicios, forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Entre los miembros fundadores de WLI Forum se encuentran empresas como ALPS Electronic, AMP, Data General, Contron, Seiko, Epson y Zenith Data Systems.

En un futuro no lejano, el previsible aumento del ancho de banda asociado a las redes inalámbricas y, consecuentemente, la posibilidad de tecnología multimedia móvil, permitirá atraer a mercados.

Generaciones de Redes Inalámbricas

La primera generación (1G) de redes inalámbricas fue constituida a finales de los años 70's con intentos primarios de proporcionar servicios de telefonía de voz a los suscriptores móviles. Los sistemas inalámbricos de la 1G, están básicamente caracterizados por el uso de frecuencias moduladas (FM) para la transmisión de voz y por el acceso múltiple de división de frecuencia (FDMA). Diversas redes de la 1G fueron desarrolladas de manera independiente en varias regiones del mundo, con sistemas representados por las principales tecnologías que a continuación se señalan: el Servicio telefónico móvil avanzado (AMPS) en Norteamérica; el Sistema de comunicación de acceso total (TACS), el TACS europeo (ETACS), y el sistema de teléfono móvil nórdico (NMT) en Europa; TACS de Japón (JTACS) y Nipón TACS (NTACS) en Japón.

En la segunda generación (2G) las redes inalámbricas emergieron a principios de los años 90´s y estaban totalmente basadas en técnicas de transmisión digital. Los sistemas 2G tuvieron como objetivo el proporcionar una mejor eficiencia del espectro, una comunicación más robusta, voz y servicios de datos a baja velocidad, aislamiento de voz, así como la capacidad de autentificación. Tres tecnologías elementales se basan en los principios de 2G: El Sistema global para comunicaciones móviles (GSM), TIA/EIA/IS-136 (IS-136) o el Servicio Digital Telefónico Móvil Avanzado AMPS (D-AMPS), y TIA/EIA/IS-95A (IS-95A). GSM e IS-136 emplea el Acceso múltiple de división de tiempo (TDMA), mientras que IS-95A utiliza el acceso múltiple de división de código (CDMA) como arquitecturas de acceso múltiple. Aunque los sistemas 2G se basan totalmente en tecnologías digitales, su capacidad de transmisión de datos es algo sencilla.

El arribo de Internet y el incremento en la demanda de servicios de acceso móvil para aplicaciones en Internet, engrandecieron el desarrollo de tecnologías inalámbricas que, como evolución de los sistemas 2G existentes, soportó la transmisión de datos. Dentro de este marco, el Servicio General de Paquetes de Radio (GPRS), IS-95B, y los Datos a Alta Velocidad (HDR) emergieron como tecnologías inalámbricas de datos. GPRS agrupado con GSM o con IS-136, IS-95B son una evolución de IS-95A -, y HDR satisfizo las expectativas con la incorporación de capacidades de transmisión de datos en sistemas inalámbricos. HDR, en particular, prevé velocidad de datos según los requerimientos de los sistemas de tercera-generación (3G).
El concepto de redes inalámbricas 3G es incorporado por el organismo Internacional de Telecomunicaciones Móviles (IMT-2000). Los estándares y las especificaciones del IMT-2000 han sido desarrollados por varias organizaciones de estándares alrededor de todo el mundo bajo el auspicio de la Unión Internacional de Telecomunicaciones (ITU).

Una amplia gama del sector usuario, de tecnología de radio, de cobertura de radio, y de equipo de usuario, están resguardadas por el IMT-2000. Básicamente, un sistema 3G debe proveer servicios multimedia, en modo de circuito así como operaciones en modo de paquetes, para el sector de usuarios, tales como el privado, el público, el de negocios, los residenciales, loops locales, otros servicios basados en redes terrestres y redes satelitales. Dos tecnologías de gran importancia en la transmisión de radio que satisfacen los requisitos 3G son: el Acceso Universal de radio terrestre (UTRA) y la interfaz de radio CDMA Multi-Portador (cdma2000).

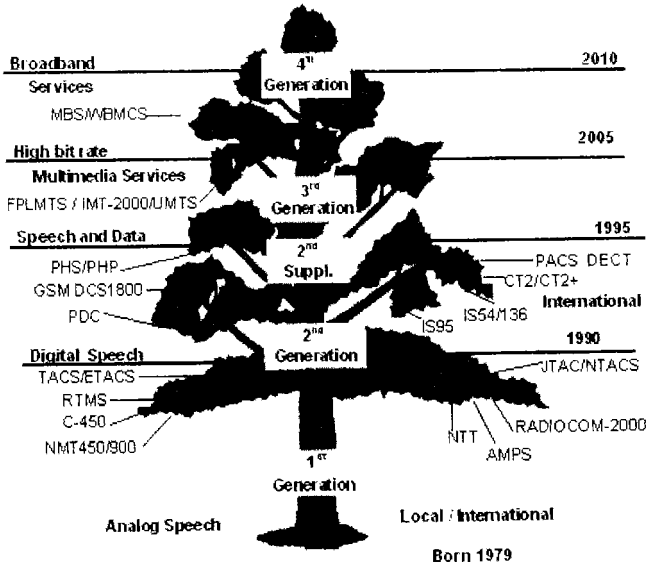


Figura III – 1

Generaciones de Redes Inalámbricas

III. 2. Definición de Redes Inalámbricas ó Wireless Local Área Network

WLAN son las siglas en inglés de Wireless Local Area Network. Es un sistema de comunicación de datos flexible muy utilizado como alternativa a las redes LAN cableada o como una extensión de ésta. El término de red inalámbrica *[wireless networking]* se refiere a la tecnología que permite a dos o más computadoras comunicarse a través de protocolos de red estándar, llámese TCP/IP (Transmission Control Protocol and the Internet Protocol), FTP (File Transfer Protocol), pero sin el uso de un cable [Bluetooth, 2002]. Cualquier red que no utilice un cable para comunicarse, podría ser considerada una red inalámbrica; las redes celulares también son redes inalámbricas, aunque por el momento se clasifican como medios de comunicación de voz más que de datos, mientras que la transmisión vía satélite entra dentro de las llamadas redes WAN.

Una red inalámbrica se define en términos de estándares y de especificaciones las cuales son desarrolladas por diversas organizaciones de estandardización o asociaciones de la industria. Por lo tanto, los estándares y las especificaciones varían para diversas tecnologías. Por otra parte, existe un marco común que caracteriza los sistemas inalámbricos.

Los estándares 802 de la IEEE especifican la capa física del modelo de red OSI. Al TCP/IP no le concierne sobre que medios de red subyacente opera; entre ambos es posible construir una red que opere sobre cualquier medio- cable coaxial, alambre de par trenzado sin blindaje, fibra óptica y por supuesto ondas de radio.

Las redes inalámbricas tienen formas versátiles de transferir datos, ya que pueden operar sobre una variedad de ondas de radio, desde el espectro infrarrojo hasta las bandas de teléfono celular.
Este tipo de redes utiliza radio frecuencias para trasmitir información entre dichos equipos y funciona igual que si estuviera conectado a una red cableada. Los usuarios pueden acceder a archivos, aplicaciones, correo electrónico, impresoras y compartir el acceso a Internet de la misma manera como si estuviera accediendo físicamente a una red LAN.

Esta tecnología ha dado lugar al nacimiento de posibilidades de comunicación impensables gracias a las redes ciudadanas, que en un futuro no muy lejano pueden cambiar nuestro concepto de las telecomunicaciones e Internet abriendo un mundo de servicios y aplicaciones. Cada día se reconocen más este tipo de redes en un amplio sector, tanto en las empresas de comunicaciones como en las industrias, que desean estar en comunicación constante, con todas sus oficinas y departamentos alrededor del mundo. Las instituciones educativas no son la excepción en esta área, se tienen universidades de prestigio mundial, en las que es una realidad el poder acceder al aprendizaje educativo por medio de algún dispositivo móvil, que este enlazado a una red inalámbrica. Las aplicaciones de las redes inalámbricas son infinitas. De momento van a crear una nueva forma de usar la información, pues estará al alcance de todos a través de Internet en cualquier lugar (en el que haya cobertura).

III. 3. Clasificación de Redes Inalambricas: WPAN, WLAN, WWAN

Como se ha comentado anteriormente, conceptualmente la única diferencia existente entre las redes locales convencionales y las inalámbricas es la inexistencia de cableado entre los equipos. Por ello, para poner énfasis en esta característica, se presenta una clasificación de redes locales donde se añade la inicial W (del inglés, wireless, inalámbrico). Se puede distinguir entre:

- **WPAN.** Tradicionalmente este tipo de redes se basa en infrarrojos que permiten la comunicación entre dos elementos a baja velocidad y a una distancia cercana a los 30 metros. Hoy en día como alternativa de comunicación está tomando auge el estándar Bluetooth. Estas redes están pensadas para cubrir un área del tamaño de una habitación y su finalidad es la conexión de dispositivos diversos, por ejemplo: un teléfono móvil o un ordenador portátil con una agenda electrónica (PDA), etc.
- **WLAN.** La norma más usada en este tipo de redes es la 802.11b, promovida por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), y que la asociación Wi-Fi está ayudando a consolidar. En segundo lugar, aunque menos utilizado, se sitúa HomeRF. La distancia que abarca llega desde varios metros hasta decenas de metros Son las redes que cubren el ámbito de una casa, una oficina, un campus o el edificio de una empresa. Para la finalidad de este proyecto son las que se van a abordar en este proyecto.
- **WWAN.** Por su gran tamaño, estas redes son explotadas por las empresas de telefonía móvil. Hasta la llegada de la telefonía móvil de tercera generación, el UMTS, la alternativa actual es el uso del GPRS, aunque su velocidad es bastante reducida. La distancia abarca desde decenas a miles de Km. Son las redes cuyo ámbito cubre áreas más amplias como por ejemplo: una ciudad.

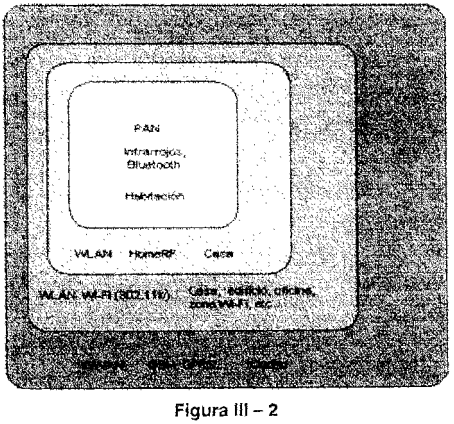


Figura III – 2

Clasificación de redes inalámbricas

III. 4. Elementos de una Red Inalámbrica

Se enumeran a continuación los principales tipos de equipos empleados para la construcción de infraestructuras de redes inalámbricas y que serán empleados por los equipos terminales de cliente para la apropiada interconexión. Aunque se clasificarán de una manera formal, en la realidad los equipos de los fabricantes suelen integrar modos híbridos de funcionamiento que diluyen dicha estructuración. Por ejemplo es ya normal encontrar gateways que operan además como puntos de acceso y bridges, o bridges como AP's y repeaters. Además de esta clasificación, en casi todos los casos existen modelos de interior, pensados para operar en recintos cerrados y protegidos, y de exteriores, más robustos y con mayor margen de temperaturas de funcionamiento.

- **Punto de acceso ("*Access Point*", AP)**

Es un nodo especial en una red inalámbrica que actúa como punto centralizador y gestor del tráfico del resto de equipos (terminales de cliente) subscritos a él y dentro de la celda de cobertura. Dispone comunmente de una interfaz Ethernet que le permite estar interconectado a una red cableada (LAN), además de la interfaz inalámbrica por la cual se conectan los equipos de dicha naturaleza. Permite la comunicación entre ambas interfaces y entre los propios equipos inalámbricos a nivel 2 (modelo OSI). En general en una misma localización puede coexistir más de un punto de acceso siempre que no interfieran fuertemente sus frecuencias de funcionamiento. Los equipos presentes estarán subscritos sólo a uno. El punto de acceso cumple con la función de capturar la información transmitida por las terminales y dispositivos de red equipados con tarjetas de red inalámbrica y adaptarla para que pueda ser transmitida por la red de cable.

El punto de acceso es el encargado de gestionar las comunicaciones inalámbricas de su área de cobertura. Entre las funciones que realiza es la de identificar nuevos usuarios, manejo de comunicaciones de usuarios en movimiento, registro de frecuencias asignadas, etc.

Este dispositivo también tiene funciones de control de acceso y seguridad, de forma que garantiza que los usuarios que accedan a la red sean únicamente los estipulados y además que las comunicaciones que realiza, trata de que sean seguras.

La configuración de estos equipos es muy sencilla, apenas necesitando la introducción de su dirección IP (en la mayoría de ellos se puede activar el cliente DHCP que poseen y de esta forma la capturan automáticamente), la del gateway por defecto, los parámetros de la parte inalámbrica y su securización.

Dependiendo del modelo que se utilice, este dispositivo implementa diferentes funciones, pero su misión elemental es adaptar la información transmitida en un medio inalámbrico a otro cableado, garantizando la calidad y seguridad de la transmisión.

- **Bridges**

Son elementos que interconectan dos o más redes locales (a nivel 2 OSI). En el mundo wireless el concepto se matiza: deben interconectar redes locales fijas. Esta definición expone su principal uso, la

interconexión de redes fijas separadas por una distancia física la cual se ha cubierto mediante un segmento inalámbrico. Poseen dos interfaces, uno Ethernet y otro inalámbrico. Los parámetros inalámbricos (canal de frecuencia, bitrate, identificador de servicio-SSID, etc.) de ambos extremos deben ser idénticos para posibilitar la comunicación. Virtualmente se pueden encadenar un número ilimitado de parejas de bridges para enlazar infraestructuras muy distantes o con obstáculos entre sí. La configuración de estos dispositivos suele ser también bastante simple, requiriendo adicionalmente a los parámetros indicados para un AP poco más que la introducción de la dirección IP del bridge del otro extremo.

Los bridges que se encuentran comerclalmente disponibles suelen agregar otras funcionalidades como son el disponer de otros modos de operación: como AP, repeater e incluso como adaptador de red para equipos de cliente.

- **Repetidores ("*Repeaters*")**

Permiten extender la cobertura de AP's mediante la regeneración y re-envío de información a zonas anteriormente sin suficiente señal. Teóricamente poseen una única interfaz inalámbrica, que les permite conectarse por un lado al punto de acceso para el cual operan, y por otro lado a los equipos inalámbricos que se le subscriben. Operan con los mismos parámetros que el AP para el cual trabajan (frecuencia, bitrate, etc.).

La ventaja de extender de esta forma la cobertura de las redes tiene su precio: dado que toda la información que un equipo le transmite la tiene que remitir al AP, la eficiencia de la solución es inferior al 50%.

También es factible encadenar numerosos repeaters para ampliar todavía más el alcance, pero numerosos problemas que aparecen por colisiones, retardos de señal y penalización en el uso del espectro, no se aconseja emplear más de uno. En el mercado apenas existen como tal estos equipos. Dependiendo del fabricante, muchos gateways como AP's y bridges pueden configurarse en modo de funcionamiento repeater, siendo la solución empleada.

- **Routers y Gateways**

Poseen capacidad de enrutamiento (niveles 3 y 4 OSI) de los paquetes de información que los atraviesan, una de sus interfaces es inalámbrica, existiendo al menos otra fija Ethernet a la cual se suele denominar puerto WAN. La mayoría de modelos existentes en el mercado no posee funcionalidades puras de router, sino que están especialmente diseñados para actuar como pasarela entre la red inalámbrica directamente gestionada por el equipo y las redes externas (red local de empresa, red de acceso a Internet u otras). Por ello con frecuencia se les denomina gateway.

Su complejidad interna es superior al resto de los otros equipos. No sólo realizan labores de mayor procesamiento de la información como el enrutamiento, sino que además han sido enriquecidos con funcionalidades avanzadas en networking (traducción de direcciones por NAT y PAT o servidor DHCP de direccionamiento propio) y seguridad (firewall interno avanzado, listas de acceso por dirección MAC Ethernet, bloqueo de acceso a Url's para control paterno, restricción de uso por franja horaria). Además de lo anterior, suelen proporcionar en la parte LAN, además del interfaz wireless, un conmutador Ethernet integrado de varios puertos. Ya menos frecuente, también algunos modelos poseen un servidor interno de impresión junto

a un puerto serie, paralelo o USB para conectar una impresora. Igualmente existen modelos que poseen una interfaz para interconectarse directamente con redes ADSL.

Actualmente, algunos ruteadores cuentan funcionalidades de gestión de redes privadas virtuales (VPN's) e incluso proporcionan voz sobre IP (VoIP). De forma análoga al resto de los equipos, los gateways pueden proporcionar modos de configuración que les permiten operar como puntos de acceso, repeaters e incluso bridges.

Con toda esta riqueza de funciones, los gateways reúnen en un único equipo las prestaciones que hasta el momento necesitaban varios (un router, un AP wireless, un módem ADSL, un firewall) y a un precio muy competitivo.

- **Antenas**

Los equipos anteriores poseen habitualmente uno o dos conectores mediante los cuales se pueden acoplar antenas externas para la emisión de la señal inalámbrica. También se encuentran otros modelos con antenas internas o no reemplazables, lo que limita su uso en muchas instalaciones.

Las clasificaciones de las antenas pueden atender a numerosos criterios, siendo los principales por su ubicación y por la forma del lóbulo de emisión de la radiación. Atendiendo a la ubicación, las antenas pueden ser de interiores o de exteriores. En las primeras, el volumen es pequeño, la estética y no suelen ser de gran potencia. En las segundas es su robustez frente al medio. Por la forma de su patrón de emisión son:

a. **Omnidireccionales** (cobertura circular), envían la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.
b. **Direccionales o sectoriales** (cubren un determinado ángulo), envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.
c. **Muy directivas** (ángulos por debajo de los 12 grados).

Además de todo lo anterior, hay que tener en cuenta la ganancia que presenta cada modelo de antena para realizar correctamente un diseño, encontrando modelos comerciales desde 2 a 24 decibelios (dB). Otras clasificaciones atienden a la tecnología de diseño (parabólicas, yagi, helicoidales, de panel, etc.) y a la polarización de la señal (lineal -horizontal o vertical- y circular -izquierda o derecha).

Pese a ser un elemento al cual se le presta escasa atención a la hora de realizar una instalación, es sin embargo uno de los pilares fundamentales de todo diseño. Una inadecuada selección de antenas puede suponer una deficiente cobertura en la zona de operación, con áreas de sombra con imposibilidad de recepción y otras con escasa señal, degradando las prestaciones de todo el conjunto. Por contra, uno de los principales defectos de los diseñadores un exceso de potencia de señal conlleva la cobertura de zonas más alejadas de lo deseado, pudiendo interferir con otras celdas (con lo que de nuevo baja el rendimiento del sistema por múltiples conexiones), además de permitir que equipos alejados puedan recibir las emisiones, facilitando notablemente la tarea de hackers. También a la hora de realizar la selección y ubicación física de

las antenas (techos, paredes, esquinas, azoteas, etc.) pueden primar factores como la estética, precio o simple desconocimiento, agravando el error de diseño.

No se debe olvidar el importante papel que juega el cable coaxial de antena. A las frecuencias de trabajo de los equipos Wi-Fi, 2,4 y 5 giga hercios, la atenuación es elevada y unos pocos metros de distancia pueden representar un grave deterioro de la señal. Se debe emplear cableado especial de baja atenuación y diseñar con distancias entre punto de acceso y antena no superiores a 10 metros.

- **Otros componentes**

Aunque no son propiamente equipos inalámbricos, existen una serie de dispositivos que complementan o enriquecen las prestaciones y funcionalidades de dicho tipo de redes. En instalaciones en las cuales existan numerosos puntos de acceso, la gestión de la configuración y estado de los mismos puede llegar a ser una tarea que requiera numerosos recursos. Los sistemas de gestión específicos para estos dispositivos permiten una cómoda visualización de su estado, detección de anomalías y actualización de configuraciones.

La totalidad de los equipos actuales poseen mecanismos internos de securización para reducir al máximo los intentos de intrusión y la protección de las comunicaciones por un medio abierto como es el aéreo. De nuevo la gestión de los terminales habilitados, las claves de acceso y la consulta de incidencias puede ser inviable en grandes instalaciones si se realiza individualmente. Adicionalmente se pueden demandar medidas de seguridad más avanzadas y un preciso control de los usuarios del sistema. Para ello se pueden implantar sistemas de securización avanzados que proporcionan mecanismos de tunelado de la información (VPN), cifrado (IPSEC), registro de usuarios (Radius) o gestión de claves, por ejemplo.

Recientemente han aparecido en los mercados soluciones denominadas "hot spot in a box". Bajo ese término se proporciona una solución combinada simplificada de gestión centralizada de equipos, de seguridad y de acceso de usuarios. Está dirigido a negocios que deseen implantar un servicio comercial de acceso a Internet mediante redes inalámbricas de pequeño tamaño, en donde el registro y contabilización del uso son los parámetros prioritarios.

Por último, aunque no propiamente componentes de la infraestructura de una red wireless, sí se deben citar equipos destinados a la instalación, conservación y seguridad. Dentro de los cuales se encuentran analizadores de espectros, scanners, sniffers, analizadores de protocolos, por ejemplo.

Infraestructura para Terminales del Cliente

Con el fin de interconectarse a las redes inalámbricas, los equipos de cliente necesitan adaptadores específicos que se describirán a continuación. En algunos casos el adaptador y el equipo forman un conjunto indisoluble orientado a cumplir una función muy específica (adaptadores multimedia, servidores de impresión, etc.)

- **Tarjetas de Red**

Cualquier dispositivo, para poderse conectar a cualquier tipo de red, necesita un elemento que adapte la información que genera a las característica físicas y requisitos de la red a la que se conecta. Este elemento se llama tarjeta de red o en inglés NIC (Network Interface Card). Por lo tanto todos los elementos que se conectan a la red deben de disponer de este tipo de elemento.

Las tarjetas de red deben cumplir con los protocolos que la red demanda. En el caso de la red cableada, pueden ser el IEEE 802.3, 802.4, 802.5. Para las redes inalámbricas el más usual es el 802.11. A su vez, las tarjetas de red, deben de adaptarse a la forma de trabajo del dispositivo a conectar a la red, teniendo en cuenta aspectos tales como velocidad de proceso, forma de direccionamiento, etc.

- **PC-Cards**

Hasta el momento, son los adaptadores fundamentales para permitir la conexión de portátiles, tablet PC's y otros dispositivos móviles, aunque cada vez más se comercializan con soluciones internas ya integradas. A su ventaja de pequeño tamaño y universalidad, hay que restarle la peor prestación de sus pequeñas antenas internas. Pese a ser infrecuente, en algunos modelos puede sustituirse la antena interna por una externa mediante la utilización de un pequeño conector que poseen. Recientemente han aparecido tarjetas en otros formatos, como SD (Secure Digital).

El objetivo prioritario es cubrir emergentemente el área de los asistentes personales (PDA). Esta tendencia se incrementará con la reciente aparición de chipsets de muy bajo consumo, uno de los puntos débiles actuales de la tecnología.

- **PCI**

Aunque parezca contradictorio, el mercado de equipos de sobremesa está demandando fuertemente adaptadores wireless en formato de tarjeta PCI. PC's que deban cambiar su ubicación con frecuencia, salas inalámbricas y soluciones especiales son las aplicaciones más comunes. Lo que parece un inconveniente, la necesidad de abrir el equipo para insertar la tarjeta, puede convertirse en una ventaja por la dificultad frente a robo. Generalmente poseen una pequeña antena externa la cual se puede sustituir fácilmente por otras de mayores prestaciones.

- **USB**

Los adaptadores wireless externos USB aportan notables ventajas. Primeramente no necesitan alimentación externa. Son además de muy pequeño tamaño y pueden orientarse muy fácilmente para recibir mejor la señal.

Su universalidad y facilidad de activación es otro punto fuerte. En contra, se encuentra su rara posibilidad de uso de antenas externas y su exposición ante robo. Muy recientemente han aparecido adaptadores con la especificación USB 2.0. La razón de ello es que el potencialmente elevado bitrate que se puede obtener mediante los estándares 802.11g y 11a (54 Mbps teóricos, por debajo de 25 Mbps en la práctica), superaba con creces las capacidades de la antigua especificación del bus USB 1.1 (7 Mbps útiles) lo que representaba un cuello de botella ya solucionado en la nueva versión.

- **Equipos dedicados**

La extensión del uso de las redes inalámbricas está alcanzando a segmentos hasta hace poco impensables. El sector del hogar está viviendo una extraordinaria actividad, que se refleja en la aparición de adaptadores para consolas de juegos, equipos de sonido, televisiones y pantallas, cámaras fotográficas, cámaras de vigilancia, adaptadores para la interconexión a cualquier elemento multimedia, etc. con interfaces Wi-Fi. Para la oficina ya se disponen, además de los anteriores, de adaptadores para impresoras remotas, sistemas de proyección de PC, PDA y terminales para usos de logística, etc.

Adicionalmente a la mejora en las prestaciones de los adaptadores de clientes (menos consumo, más seguros, mayor velocidad), lo que se observará es una creciente penetración en equipos tanto del hogar (vídeos, sistemas de control y vigilancia) como fundamentalmente en empresa (sistemas de gobierno de maquinaria, sensores, equipos para aplicaciones móviles). Pero quizá la clave esté destinada a otro uso: la telefonía y transmisión de voz por IP sobre redes wireless.

El mercado objetivo son las redes de telefonía dentro de la empresa y los hotspots públicos, pues dentro de su cobertura se podrían realizar las llamadas mediante la red inalámbrica (WLAN), mucho más económicas y con capacidades de datos (navegación Internet, correo) a alta velocidad, mientras que en el resto de localizaciones se emplearía la telefonía celular habitual.

El extraordinario esfuerzo que las mayores empresas del sector y las visiones de los más reconocidos gurús nos sitúan pronto en un mundo rodeados por equipos inalámbricos con servicios inimaginables, surgidos de la convergencia de voz / datos / vídeo / audio que parece haber encontrado en esta tecnología su aglutinador ideal.

A continuación se muestra en el siguiente esquema la conformación de la red inalámbrica con los dispositivos integrados para su funcionamiento.

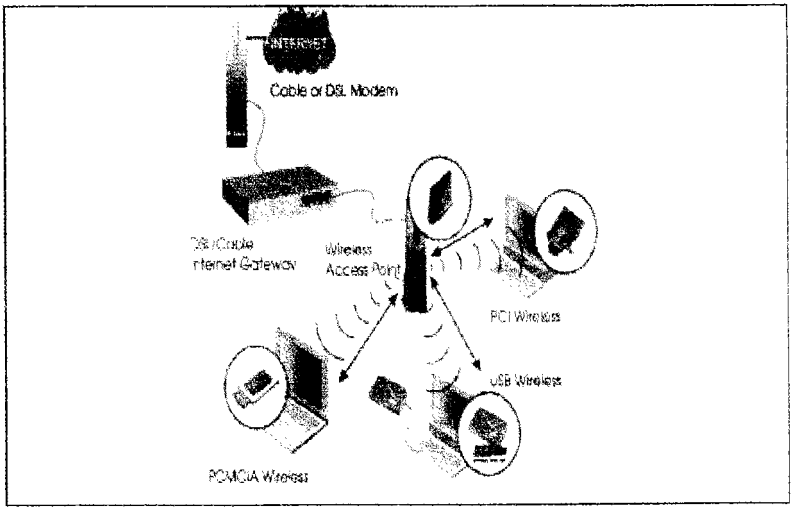


Figura III – 3
Esquema de una Red Wireless

III. 5. Relación con el Modelo OSI

III. 5. 1. Capa Física

Considerando el modelo OSI para la estructura en capas de una red inalámbrica, la capa física es la de nivel inferior. Nos proporciona los mecanismos para transmitir la información por un determinado medio físico, en este caso el medio aéreo. Esto comprende la modulación específica para el canal de transmisión, los mecanismos de protección de la información frente a ruido e interferencias y la estructuración en canales de uso. La filosofía de los miembros del comité de la IEEE al permitir la elección entre dos capas ha sido la de posibilitar que los usuarios exploten las ventajas / características de cada una en determinados aspectos. Esto añade un factor más de complicación al tema general de interoperatividad de productos, al mismo tiempo que impone la necesidad de evaluar cuidadosamente cada tecnología, dado que se plantea la necesidad de escoger la tecnología.

Técnicas de Comunicación

El estándar 802.11 define tres mecanismos de comunicación para el nivel físico:

- Infrarrojo (IR) Luz infrarroja en banda base, es decir sin modular,
- Espectro expandido por salto de frecuencias o Frequency Hopping Spread Spectrum (FHSS) y
- Espectro expandido por secuencia directa o Direct Sequence Spread Spectrum (DSSS), ambas en la banda de frecuencia 2.4 GHz ISM.

Actualmente, no existen dispositivos que implementen el estándar 802.11 con infrarrojo, puesto que obliga a contar con visión directa entre los puntos de comunicación. En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización.

Modo	Frecuencia	Velocidad	Modulación
DSSS	2.4GHz (ISM)	1 Mbps 2 Mbps	DBPSK DQPSK
FHSS	2.4GHz (ISM)	1 Mbps 2 Mbps (opc).	2-GFSK 4-GFSK
DFIR	Infrarrojos (850-950 NM)	1 Mbps 2 Mbps (opc).	PPM

Tecnología de Radiofrecuencia.

Las redes inalámbricas que utilizan radio frecuencia pueden clasificarse atendiendo a su capa física, en sistemas de banda estrecha (narrow band) o de frecuencia dedicada, que nos es un apartado de la IEEE 802.11, y en sistemas basados en espectro disperso o extendido (spread spectrum), elegido por IEEE 802.11.

1) Frecuencia dedicada

Esta técnica trabaja de modo similar a la forma en que se difunden las ondas desde una estación de radio. Hay que sintonizar en una frecuencia muy precisa tanto el emisor como el receptor. La señal puede atravesar paredes y se expande sobre un área muy amplia, así que no se hace necesario enfocarla. Sin embargo, estas transmisiones tienen problemas debido a las reflexiones que experimentan las ondas de radio (fantasmas); para evitarlas en lo posible, estas transmisiones están reguladas, en Estados Unidos por la FCC.

Hay que sintonizar muy precisamente para prevenir las posibles interferencias. Los productos comerciales que utilizan infrarrojo o frecuencias dedicadas, aportan únicamente un tercio del mercado de las WLAN's.

2) Spread Spectrum o Espectro Expandido

Esquema de modulación que consiste en lo siguiente: la señal se expande (su espectro) a través de un ancho de banda mayor que el mínimo requerido para transmitir con éxito. Mediante un sistema de codificación se desplaza la frecuencia o la fase de la señal de forma que ésta quede expandida. Posteriormente, en el receptor la señal se recompone para obtener la información inicial que se deseaba transmitir. En definitiva, se esparce la señal a lo largo de un amplio margen del espectro evitando concentrar la potencia sobre una única y estrecha banda de frecuencia como ocurre con las técnicas convencionales de este modo puede usar un rango de frecuencias que este ocupado ya por otras señales. Todos los elementos de cada red local inalámbrica basadas en espectro expandido utilizan el mismo código de expansión, lo cual permite la diferenciación y que esa red coexista con otras redes o con otros sistemas en la misma banda de frecuencias.

La técnica del espectro disperso (Spread Spectrum) emplea un ancho de banda mayor del necesario para la transmisión de la información, con el fin de aminorar los efectos de las interferencias y hace uso de la encriptación. Por sus características, es casi imposible interceptar una comunicación que utilice esta técnica sin conocer los detalles de su implementación.

Otras alternativas que han sido globalmente aceptadas por la industria y adoptadas por IEEE 802.11 se refieren a los esquemas DSSS (Direct Sequence Spread Spectrum) y FHSS (Frecuency Hopping Spread Spectrum), ambos dentro de la órbita de la tecnología conocida como "spread spectrum" o "espectro expandido". Esta tecnología se ha impuesto frente a las tecnologías tradicionales, por su excelencia y por sus mejoras en cuanto a complejidad y costes.

- **Técnica de Espectro Expandido por Salto de Frecuencia o FHSS (Frequency Hopping Spread Spectrum.)** Esta técnica utiliza una señal de banda estrecha con una frecuencia de modulación que se va cambiando cada cierto intervalo de tiempo. Es decir, la expansión de la señal se produce transmitiendo una ráfaga en una frecuencia, saltando luego a otra frecuencia para transmitir otra ráfaga, y así sucesivamente. El emisor y el receptor deben conocer la secuencia de cambio para una correcta sincronización.

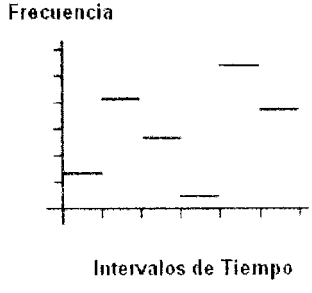


Figura III – 4

Técnica de Espectro Expandido por Salto de Frecuencia o FHSS

- **Técnica de Espectro Expandido por Secuencia Directa o DSSS (Direct Sequence Spread Spectrum.)** En este caso, un grupo de bits de información se mezcla con una secuencia de bits redundantes muy rápidos, denominados "chips", diseñados de forma que aparezcan aproximadamente el mismo número de ceros que de unos. Esta secuencia, un código Barker también llamado código de dispersión o PseudoNoise, se introduce sustituyendo a cada bit de datos; puede ser de dos tipos, según sustituya al cero o al uno lógico. Tanto emisor como receptor deben conocer los valores de los chips para poder comunicarse; se emplean secuencias con unas propiedades matemáticas determinadas que las hacen más optimas para la modulación.

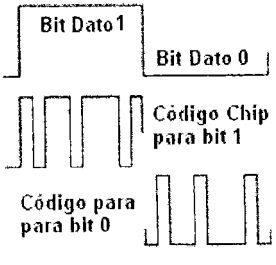


Figura III – 5

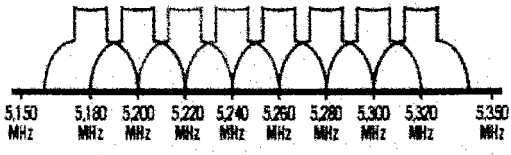
Técnica de Espectro Expandido por Secuencia Directa o DSSS

Ambas técnicas no son compatibles, por lo que dos dispositivos deben emplear la misma tecnología para poder comunicarse. FHSS consume menor potencia que DSSS, sus dispositivos son menos complicados (menor coste de fabricación) y es más robusto a las interferencias y al problema del multitrayecto en espacios cerrados; sin embargo, con DSSS se obtiene una velocidad de transmisión mayor, y dado el abaratamiento de las técnicas de fabricación, se está imponiendo en el mercado de dispositivos wireless.

3) OFDM (Wideband Orthogonal Frequency Division Multiplexing)

Esta es la técnica utilizada por el estándar 802.11ª en la que se codifica la información en múltiples radio frecuencias simultáneamente, es decir, parte una señal (portadora) de alta velocidad en decenas o centenas de señales de menor velocidad que son transmitidas en paralelo (subportadoras). Cada portadora tiene un ancho de banda de 200 MHz y es dividido en 52 subcanales siendo cada uno de 300 KHz aproximadamente de ancho (ver Figura III – 6). De estos canales, el COFDM (código OFDM) usa 48 para datos y los 4 restantes se usan para la corrección de errores. OFDM es tolerante al ruido y la señal que se transmite es difícil de descifrar.

Los equipos con tecnología OFDM son una buena solución en distancias moderadas para redes de información punto a punto, multipunto, acceso de alta velocidad a Internet, videoconferencia, telefonía.



There are eight independent channels in the lower 200 MHz of the 5-GHz spectrum.

Figura III – 6
Técnica OFDM

Canales Definidos para Redes Inalámbricas

En el estándar 802.11, en lo referente a la banda ISM (de instrumentación, científicas o médicas) de los 2,4 GHz, define trece canales para la comunicación inalámbrica, definidos según su frecuencia central, con una separación de 5 MHz entre ellos. Sin embargo, la disponibilidad de dichos canales se somete a las regulaciones de cada país. Así, en EEUU y Canadá sólo se disponen de los canales 1 a 11, mientras que en Europa y Australia se pueden manejar los trece primeros canales. En el siguiente cuadro se muestra los 11 canales con su respectiva frecuencia y el ancho de banda que les corresponde.

Canal	Frecuencia central	Ancho de banda
1	2412 MHz	2401 - 2423 MHz
2	2417 MHz	2406 - 2428 MHz
3	2422 MHz	2411 - 2433 MHz
4	2427 MHz	2416 - 2438 MHz
5	2432 MHz	2421 - 2443 MHz
6	2437 MHz	2426 - 2448 MHz
7	2442 MHz	2431 - 2453 MHz
8	2447 MHz	2436 - 2458 MHz
9	2452 MHz	2441 - 2463 MHz
10	2457 MHz	2446 - 2468 MHz
11	2462 MHz	2451 - 2473 MHz

Figura III – 7
Frecuencias de Banda Comunes

Sin embargo, debido a la técnica de comunicación en espectro disperso empleada, el ancho de banda se expande más allá de la separación entre canales contiguos. Como aproximación, se estima un ancho de banda de unos 22 MHz (más allá, la potencia emitida se sitúa en 30 dB por debajo de la frecuencia central) , por lo que cada canal emplea frecuencias de hasta 11 MHz por encima y por debajo de la frecuencia central, solapándose unos a otros.

Como resultado, dos dispositivos que empleen canales contiguos, o sin la debida separación, se crearán interferencias mutuamente, repercutiendo en las prestaciones de la red inalámbrica.

Por lo tanto, es conveniente, en el caso de que existan varias redes inalámbricas en el mismo lugar, que se utilicen canales con la suficiente separación.

Para evitar totalmente el solapamiento de los canales usados, se deben dejar cinco canales de separación entre los usados (ver Figura III-8).

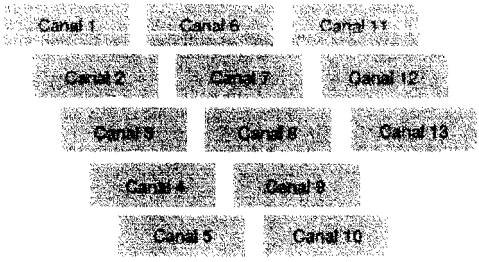


Figura III – 8

Solapamiento de los Canales

Por lo tanto, esto nos lleva a que únicamente disponemos de tres canales (por ejemplo, el 1, el 6 y el 11) para una coexistencia sin interferencias de distintas redes wireless en el mismo area. Sin embargo, un análisis más profundo de la señal en redes wireless nos indica que la potencia se va reduciendo a medida que se separa de la frecuencia central, así que se recomienda utilizar hasta cuatro canales con un solapamiento mínimo, y así las interferencias creadas apenas afectan a las prestaciones de la red.

Una vez obtenida la secuencia de canal, se introduce en un sistema de modulación de alta eficiencia y robustez. Dependiendo de la velocidad deseada, el nivel de protección frente a ruidos y el protocolo empleado (b, g, a), se disponen de diversos sistemas: Baker, CCK, PBCC (para 11b) y OFDM (adicional en 11g y a).

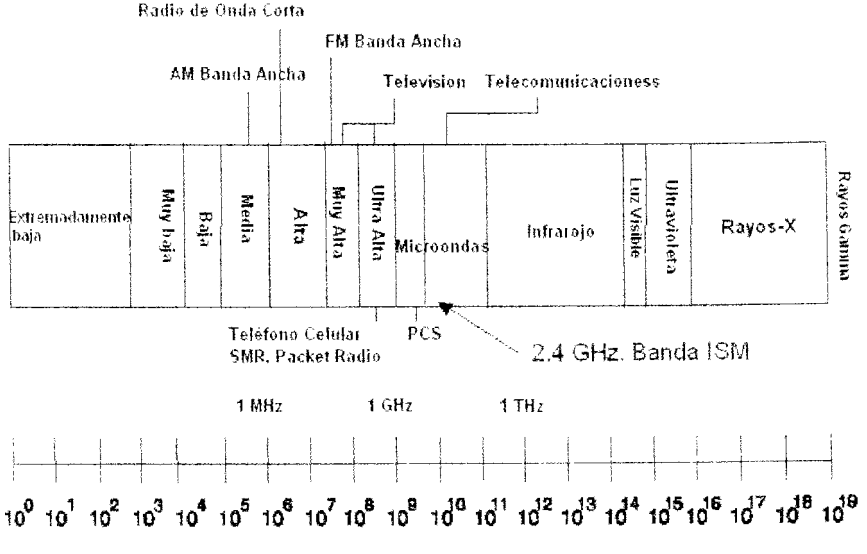


Figura III – 9 Espectro Electromagnético

III. 5. 2. Capa de Enlace o Capa MAC.

Una vez resuelto el problema del empaquetamiento y modulación de la información, es necesario determinar cómo los dispositivos tienen acceso al medio de transmisión para enviarla y recibirla. La norma IEEE 802.11 define una única capa MAC (dividida en dos subcapas) para todas las capas físicas, a fin de conseguir importantes volúmenes de producción de chips con la consiguiente reducción en precios. Es fundamental considerar que el medio es abierto, en el sentido que pueden coexistir múltiples emisores y receptores en el mismo espacio físico, por lo que es vital el implantar un mecanismo robusto y eficiente de diálogo.

Mecanismos de Acceso para WLAN's

Existen dos categorías:

- Protocolos con arbitraje (FDMA, TDMA)
- y protocolos por contención ó por detección de portadora (CDMA/CD, CDMA/CA, usado por 802.11), aunque también se han diseñado protocolos que son una combinación de estas dos categorías.

La Multiplexación en Frecuencia (FDM), divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, llamado multiplexación en el tiempo (TDM), requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos. El protocolo de acceso múltiple por división de código (CDMA), es el mecanismo de acceso por excelencia para que puedan coexistir diferentes redes basadas en espectro disperso. Las WLAN's que emplean mecanismos de contención como acceso al medio, están basadas en el modelo de detección de "portadora" utilizado por la tecnología de red local más difundida en la actualidad, Ethernet / IEEE 802.3. Varias de las primeras redes utilizaban exactamente el mismo algoritmo de acceso al medio, (CSMA/CA) detección de portadora con detección de colisiones: Cuando una estación desea transmitir, primero verifica que el medio de comunicación esté libre (es decir, detecta la portadora). Si éste está libre, transmite su información y si no, espera a que se libere el medio y transmite. Como existe la posibilidad de que dos estaciones transmitan información simultáneamente, este mecanismo exige que al transmitir se siga evaluando el canal, y si se detecta alguna perturbación en la transmisión (detección de colisión), se supone que ha ocurrido un conflicto, por lo que la transmisión se suspende y las estaciones involucradas en el conflicto esperan un tiempo aleatorio antes de repetir nuevamente el algoritmo.

El modelo de acceso por contención (una ligera variante del usado en redes Ethernet con cable) que más se utiliza en la actualidad, y que ha sido incorporado al estándar 802.11 como 1ª subcapa MAC es el

llamado de detección de portadora con detección de colisión CSMA/CA, introduce una variante en el algoritmo anterior: La mayor probabilidad de tener una colisión en CSMA/CA se da precisamente al terminar una transmisión pues puede haber más de una estación esperando que la transmisión termine, tras lo cual estas estaciones comenzarán a enviar información provocando una colisión en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión, espera un tiempo aleatorio antes de transmitir, disminuyendo así la probabilidad de colisión.

En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debido al problema conocido como la terminal oculta (o nodo escondido): Un dispositivo inalámbrico puede transmitir con la potencia suficiente para que sea escuchado por un nodo receptor, pero no por otra estación que también desea transmitir y que por tanto no detecta la transmisión. Para resolver este problema, la norma 802.11 ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo, al que denomina Reservation-Based Protocol, que es la 2ª subcapa MAC. Cuando una estación está lista para transmitir, primero envía una solicitud al punto de acceso (RTS) quien difunde el NAV (Network Allocation Vector) -un tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS de solicitud- a todos los demás nodos para que queden informados de que se va a transmitir (y que por lo tanto no transmitan) y cuál va a ser la duración de la transmisión. Estos nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra de backoff (tiempo de retroceso) aleatorio. Si no encuentra problemas, responde con una autorización (CTS) que permite al solicitante enviar su trama (datos). Cuando el punto de acceso ha recibido correctamente la información, envía una trama de reconocimiento (ACK) notificando al transmisor.

Dificultades en el Método de Acceso

IEEE 8022.11 no puede basarse en CSMA/CD ya que hay:

1) Estaciones ocultas
   - Dos estaciones asociadas al mismo Access Point, pueden estar a tal distancia entre sí como para que una no detecte las trasmisiones de la otra
   - Esto dificulta el "Carrier Sensing" de Ethernet
2) Imposibilidad de detección de colisiones propias.
   - Las estaciones wireless no pueden trasmitir y recibir al mismo tiempo, por lo que no se pueden detectar las colisiones propias.

IEEE 802.11 brinda la posibilidad de implementar distintos métodos de acceso:

1) **PCF: Point Coordination Function.** Su objetivo es el de evitar colisiones (contention free access method), el método que emplea es el Polling, en el que una estación central o Point Coordinator, idealmente el Access Point, actúa como administrador del medio, otorgando a cada estación su turno de trasmisión, sin embargo aún no se encuentra en los dispositivos actuales

2) DCF: Distributed Coordination Function (Opción Corta y Opción Larga). Su objetivo es el de administrar el medio por medio de un método de contención, el método que emplea es el CSMA/CA, los nombres de opción corta y opción larga son utilizados sólo con fines de aprendizaje, en rigor, se trata de dos configuraciones de la misma función.

- **El Proceso (Versión Larga)**

La estación que tiene un frame listo para trasmitir, hace un Carrier Sensing, si no detecta portadora (el medio está libre) envía un frame de control: RTS (request to send) y el destinatario responde con otro: CTS (clear to send). Si el CTS es recibido exitosamente, el medio queda reservado y la estación puede ahora enviar su frame de datos. La operación termina cuando el destinatario responde al frame de datos con un frame de control: ACK (acknowledge o reconocimiento).

- **El Proceso (Versión Corta)**

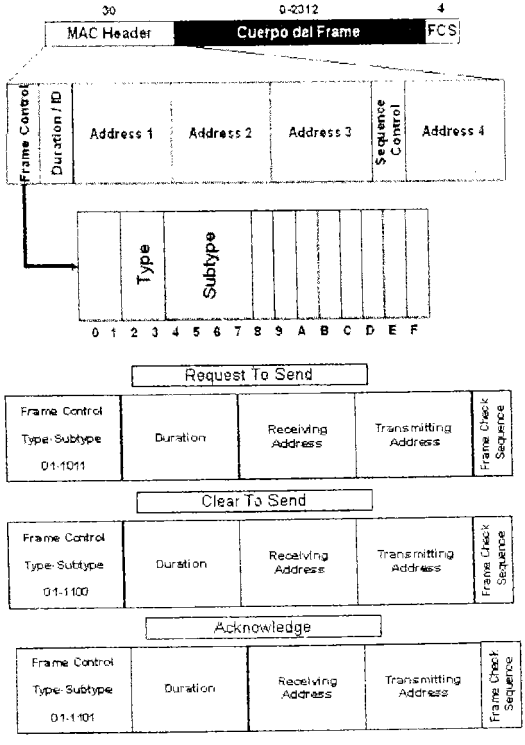
Si el frame de datos es corto, la operación anterior es muy ineficiente, en ese caso es preferible enviar directamente el frame de datos y utilizar el ACK como comprobación de éxito, esta opción es la más utilizada y en general es la que viene configurada de fábrica.

Muchos Access Points ofrecen la opción de configurar un umbral en el tamaño del frame, en ese caso:

a) si el frame es menor que el umbral, se utiliza la versión corta

b) si el frame es mayor que el umbral, se utiliza la versión larga

Formato del Frame y Frames de Control: RTS / CTS / ACK



III. 6. Componentes de la Arquitectura de IEEE 802.11

La arquitectura consiste en varios componentes que interactúan para proveer una LAN inalámbrica que soporta movilidad transparente para las capas superiores.

1) Infraestructura ó Basic Service Set (BSS).

En el modo de infraestructura se utiliza puntos de acceso (AP), estos dispositivos realizan una importante labor para el mantenimiento de la red simplificándolo en gran medida. Los puntos de acceso deberán proveer soporte de asociación y autentificación para que los dispositivos puedan conectarse con él, permitir roaming para dispositivos procedentes de otros AP's de la misma red. Además deberán aportar mecanismos de sincronización, control de energía y funciones de calidad de servicio.

Un punto de acceso permite cubrir una célula y dar cobertura a toda una zona, esta zona se le conoce como BSS o conjunto de servicios básicos. Además los AP's podrían estar interconectados, o conectados a una red cableada, esto permite extender el alcance de la red, ya que donde no llegue el alcance de un AP llegará otro, para ello se hace necesario funciones de roaming entre celdas. Estando conectado a una red fija, o una LAN, permitirá a los dispositivos móviles acceder a servicios de los LAN's tradicionales, como intranets o recursos fijos.

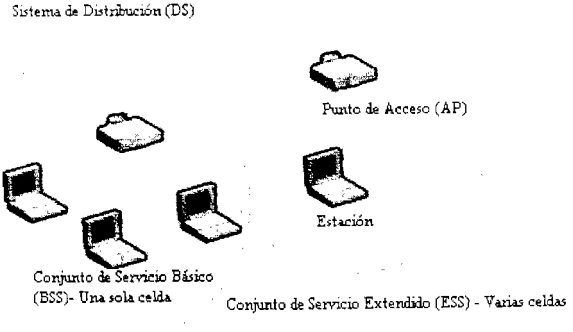


Figura III – 10

Ejemplo de una Red Wireless en Modo Infraestructura.

Varios AP's conectados forman un ESS o conjunto de servicios extendidos. Y la red que los conecta se le conoce como sistema de distribución. Este sistema de distribución podría estar montado sobre cualquier sistema, no siendo limitado a variantes de IEEE802.3. Muchas redes WLAN's requieren el acceso a una LAN para los diferentes servicios (impresoras, servidores de archivos, etc.) es recomendable que trabajen en el modo infraestructura.

Todos los dispositivos, independientemente de que sean Tarjetas de Red o Access Points tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo:

a. **Modo Managed**, es el modo en el que el TR se conecta al AP para que éste último le sirva de "concentrador". El TR sólo se comunica con el AP.
b. **Modo Master**. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TR's si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

2) Ad Hoc (ó modo peer-to-peer o Independent Basic Service Set IBSS)

Este modo utiliza mecanismos para crear redes "al vuelo", sin ningún tipo de infraestructura. Esto puede ser muy interesante de cara a redes de área personal, o para redes domésticas destinadas para usuarios con pocos conocimientos de comunicaciones. En este tipo de redes la comunicación es directa máquina a máquina y el alcance esta dado por el alcance individual de cada máquina. También se dice que forma un IBSS o Independent Basic Service Set. No existen Puntos de Acceso ni ningún tipo de equipo que dé soporte a la red en sí. En este modo de operación, la información viaja directamente entre el emisor y receptor sin pasar por ningún otro equipo. Este es el modo más fácil, rápido y barato de establecer una red inalámbrica, pero presenta la enorme desventaja de que los equipos deben estar dentro del área de cobertura de los demás para comunicarse con ellos, por lo que sólo es aconsejable para redes con pocos equipos y próximos entre sí. Además, no existe un punto de interconexión con la red cableada.

Este modo es útil para una rápida y fácil puesta en marcha de una red inalámbrica en cualquier lugar donde no exista infraestructura wireless como en un cuarto de hotel, un centro de convenciones, un aeropuerto, o donde el acceso a la red alámbrica esta restringida.

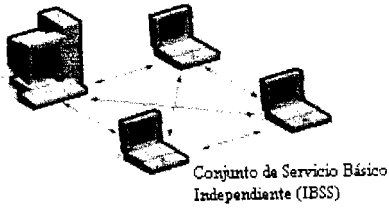


Figura III – 11
Ejemplo de una Red Wireless en Modo Ad-Hoc.

En este tipo de redes, todos los nodos funcionan como enrutadores (routers) y se ven involucrados tanto en el descubrimiento como en el mantenimiento de rutas. Los algoritmos de enrutamiento usados en las redes Ad-Hoc se pueden clasificar en dos grupos:

a. Basados en tablas de enrutamiento:

Estos algoritmos tratan de mantener la información necesaria para el enrutamiento continuamente actualizada. Cada nodo mantiene una o más tablas con los datos para encaminar hacia cualquier otro nodo de

la red. Los cambios en la topología de la red propician el envío masivo de paquetes para mantener las tablas actualizadas. Los siguientes algoritmos se encuadran dentro de esta categoría: DSDV (The Destination-Sequenced Distance-Vector Routing Protocol), CGSR(Clusterhead Gateway Switch Routing) y WRP (The Wireless Routing Protocol). Los protocolos anteriores difieren en el número de tablas utilizadas y en la política de envío de paquetes para mantener las tablas actualizadas.

b. Basados en enrutamiento de baja demanda:

En contraste con los algoritmos basados en tablas, las rutas son creadas sólo cuando se requieren. Cuando un nodo requiere una ruta hacia un destino concreto se inicia un proceso de descubrimiento de ruta. Este proceso termina cuando se encuentra un camino hacia el destino o cuando se examinan todas las alternativas y ninguna lleva al destino final. Cuando la ruta es descubierta, es necesario mantenerla (mantenimiento de ruta) hasta que el destino se vuelva inalcanzable o la ruta deje de ser necesaria. Algunos ejemplos de este tipo de protocolos son: AODV (Ad Hoc On-Demand Distance Vector Routing), DSR (Dynamic Source Routing), LMR (Lightweight Mobile Routing), TORA (Temporary Ordered Routing Algorithm), ABR (Associative-Based Routing) y SSR (Signal Stability Routing). AODV, reúne características y es una variación de protocolos de enrutamiento anteriormente desarrollados como el WRP y DSDV.

3) Mesh Networks

Los inicios de las redes acopladas son militares. Inicialmente se usaron para comunicarse con aquellas unidades de militares que aún estando lejos de las zonas de cobertura de sus mandos estaban lo suficientemente cerca entre si como para formar una cadena a través de la cual se pudiese ir pasando los mensajes hasta llegar a su destino (los mandos). Las redes Mesh, o redes acopladas, para definirlas de una forma sencilla, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los PA están dentro del rango de cobertura de algún TR que directamente o indirectamente está dentro del rango de cobertura del PA.

También permiten que los TR's se comuniquen independientemente del PA entre sí. Esto quiere decir que los dispositivos que actúan como TR pueden no mandar directamente sus paquetes al PA sino que pueden pasárselos a otros TR's para que lleguen a su destino.
Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos (Hops en inglés) o con un número que aún no siendo el mínimo sea suficientemente bueno. Es tolerante a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

Hoy por hoy uno de los principales fabricantes de software y hardware para redes acopladas es LocustWorld el cual pretende popularizarlas de tal manera que cualquiera pueda acceder a Internet desde cualquier lugar. Actualmente se llevan vendidas unas 270 unidades y la empresa pretende a largo plazo permitir la construcción de redes gigantescas.

Servicios de la Arquitectura

Los servicios se dividen en dos grupos: los servicios que son parte de cada estación, y los servicios que son parte de un Sistema de distribución (DS) . Los servicios que tienen que ofrecer las estaciones son los siguientes:

1) **Servicios de estación.** Lo conforman los siguientes servicios

- **Autenticación.** Define la identidad del dispositivo inalámbrico. Este distintivo permite acceder al dispositivo a la WLAN. La autentificación se realiza mediante una lista de direcciones físicas (MAC address) definidas en un PA o en una base de datos.
- **Des-autenticación.** Servicio usado para eliminar la identidad, de un dispositivo inalámbrico, previamente conocida. Una vez llevada a cabo el dispositivo no cuenta mas con acceso a la WLAN.
- **Privacidad.** Usado para proteger los datos mientras viajan de un dispositivo a otro a través de la red.
- **Entrega de Datos.** Asegura que los datos sean transmitidos de manera confiable de un dispositivo a otro.

2) **Los servicios de distribución**, son un conjunto de servicios encargados de tomar las decisiones de cómo los marcos de datos deben ser enviados por la red. Existen diferentes tipos de servicios que conforman este conjunto. A continuación será descrito el papel que desempeña cada uno dentro del servicio de distribución.

- **Asociación.** Este servicio es iniciado en cuanto el dispositivo movil se conecta a un PA. Establece una conexión lógica entre dispositivos y determina la ruta que el sistema de distribución necesita para la entrega de datos.
- **Reasociación.** Similar al servicio de asociación que incluye además la información actual del servicio. Así, en el caso de roaming, esta información le dice al PA actual cual fue el ultimo PA. Con esto, el nuevo contacta al anterior para recuperar cualquier dato que se encuentre en espera de ser enviado a su destino.
- **Disociación.** Este servicio es el encargado de deshacer la asociación hecha entre el PA y el dispositivo inalámbrico.
- **Distribución.** Usado por el PA actual para determinar si los datos se envían a otro PA, aun dispositivo inalámbrico o a la red alámbrica.
- **Integración.** Servicio encargado de traducir los daros del formato 802.11 l formato de red alámbrica y viceversa.

III. 7. Clasificación de las Redes Inalámbricas

Lo primero que tenemos que hacer antes que nada es situarnos dentro del mundo inalámbrico. Para ello vamos a hacer una primera clasificación que nos centre ante las diferentes variantes que podemos encontrarnos:

1) **Redes Inalámbricas Personales**

Dentro del ámbito de estas redes podemos integrar a dos principales actores:

a) **Infrarrojos**. Estas redes se usan actualmente mediante el intercambio de información pero son muy limitadas dado su corto alcance, necesidad de "visión sin obstáculos" entre los dispositivos que se comunican y su baja velocidad (hasta 115 kbps). Se encuentran principalmente en ordenadores portátiles, PDAs (Agendas electrónicas personales), teléfonos móviles y algunas impresoras.

b) **Bluetooth.** Estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles de nueva generación y algún que otro ordenador portátil. Su principal desventaja es que su puesta en marcha se ha ido retrasando desde hace años y la aparición del mismo ha ido plagada de diferencias e incompatibilidades entre los dispositivos de comunicación de los distintos fabricantes que ha imposibilitado su rápida adopción. Opera dentro de la banda de los 2.4 Ghz.

2) **Redes Inalámbricas de Consumo**

a) **Redes CDMA** (estándar de telefonía móvil estadounidense) **y GSM** (estándar de telefonía móvil europeo y asiático). Son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes.

b) **802.16.** Son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas (**MAN**) en la banda de entre los 2 y los 11 Ghz.

3) **Redes Inalámbricas 802.11**

a) **Redes inalámbricas o WN** básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del IEEE (Organismo de estandarización internacional). Como suele pasar siempre que un estándar aparece y los grandes fabricantes se interesan por él, aparecen diferentes aproximaciones al mismo lo que genera una incipiente confusión. En el siguiente tema se abordara el tema de las series y los estándares inalámbricos 802.11.

III. 8. Estándares Inalámbricos

Las redes de área local inalámbricas WLAN se utilizan ondas de radio para transmitir los datos, esta tecnología se llama comunicación de datos por radiofrecuencias (RF). Este tipo de transmisión es empleado por una gran variedad de sistemas, teniendo cada uno sus características especiales.

Las ventajas de los sistemas de comunicación por RF son muchas. Para comenzar con el simple hecho de no tener cable, éste no se tiene que desplegar por toda la instalación. El cable es caro, menos flexible que la cobertura de RF y tiende a estropearse. Implementar una infraestructura sin cable puede ser más efectivo desde el punto de vista del coste, que instalar cable a través de un entorno industrial, especialmente si la configuración puede cambiar. La mayor parte de países ponen sus propias normas para regularizar el uso de las frecuencias en RF. Mientras los estándares para algunas tecnologías inalámbricas, sobre todo teléfonos celulares, varían ampliamente dependiendo de la región geográfica, las redes inalámbricas son casi homogéneas gracias a la coordinación entre los órganos que establecen los estándares y los fabricantes de tecnología inalámbrica. Antes de centrarme en el estándar 802.11, indicaré brevemente las diferentes características de las versiones de este protocolo.

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11c	Estándar que define las características que necesitan los AP's para actuar como puentes (bridges). Ya está aprobado y se implementa en algunos productos.
802.11d	Estándar que permite el uso de la comunicación mediante el protocolo
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.

802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).
802.11m	Estándar propuesto para el mantenimiento de las redes inalámbricas.
802.1X	Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores

Figura III – 12
Estándares Inalámbricos

III. 8. 1. Series 802.11

Los estándares IEEE 802.11 para LAN's inalámbricas fueron desarrollados por el Instituto de Ingenieros Eléctrico y Electrónicos (Institute of Electrical and Electronics Engineers, IEEE) y son reconocidos en la mayor parte del mundo. IEEE 802.11 define tres formas diferentes en que las redes inalámbricas puede transferir los datos: radiando infrarrojos (IR), distribución del espectro en secuencia directa (DSSS Direct Sequence Spread Spectrum) del espectro radioeléctrico, y distribución de salto en frecuencia del espectro radioeléctrico (FHSS Frequency Hopping Spread Spectrum). El estándar de RF basado en 802.11 domina prácticamente las redes inalámbricas actuales. Los estándares de IEEE802.11 son de libre distribución y cualquier persona puede ir a la página Web del IEEE y descargarlos (http://www.ieee.org). Estos estándares sólo definen especificaciones para las capas físicas y de acceso al medio y no tratan modos o tecnologías a usar para la implementación final.

Esto debe permitir y facilitar la interoperabilidad entre fabricantes de dispositivos IEEE802.11, los puntos de accesos de un vendedor puede inter operar con dispositivos, o más precisamente, tarjetas de red inalámbricas de otro vendedor, ya que todos los dispositivos son DSSS o FHSS y para asegurarse de ello se ha creado una alianza denominada WECA, para crear y definir procedimientos para conseguir certificados de interoperabilidad y de cumplimiento de especificaciones, todo dentro de un estándar llamado Wifi o también llamado "Wireless Fidelity".

El nombre además es un indicativo del enfoque doméstico y muy orientado hacia el usuario final. En la situación actual no hay un único estándar de redes inalámbricas, sino que conviven diversos estándares promovidos por diferentes organismos y asociaciones. No se pretende realizar una descripción exhaustiva de estas normas, sólo comentar, cuál es el estándar que tiene mayor presencia en el mercado.

II. 8. 2. 802.11b (Wi-Fi)

802.11b es el estándar que más ampliamente se suele emplear. Utiliza la banda de frecuencias de 2.4GHz y proporciona generalmente 11Mb por segundo de velocidad de transmisión. Esta velocidad es suficiente para la mayoría de las aplicaciones. Los sistemas 802.11b se pueden emplear en todo el mundo. Presenta varios de los inconvenientes que tiene el 802.11a como son la falta de QoS, además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues en los 2.4Ghz funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos Bluetooth, lo cual puede provocar interferencias.

En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo. Está estandarizado por la IEEE. Wi-Fi se suele emplear cuando se habla de cualquier tipo de red 802.11, ya sea 802.11b, 802.11g, banda dual, etc. Sin embargo, cualquier producto que trate llamarse Wi-Fi, deben ser certificados por la Alianza Wi-Fi. Se espera que el crecimiento venga impulsado por la tecnología Wi-Fi, así como por la mayor presencia de las tarjetas multiprotocolo, capaces de operar en estándares diversos como el 802.11b y g.

Estándar 802.11b (Wi-Fi)	
Frecuencia longitud de onda	2.4GHz (2.400-2.4835 in North America)
Ancho de banda de datos	11Mbps, 5Mbps, 2Mpbs, 1Mbps
Medidas de seguridad	WEP Wireless Equivalency Protocol en combinación con espectro de dispersión directa
Rango de Operación óptima	50 metros dentro, 100 metros fuera
Adaptado para un propósito específico o para un tipo de dispositivo	Ordenadores portátiles, ordenadores de sobremesa donde cablear entraña dificultades, PDAs

Figura III – 13

Cuadro del Estándar de Comunicación 802.11b

III. 8. 3. 802.11a

802.11a es un estándar que funciona sobre una banda más amplia del espectro de frecuencia, entre 5.15 Ghz y 5.35 Ghz. En el 802.11a los productos pueden transmitir a 54, 48, 36, 24, 18, 12 o 6 Mbps, por lo tanto pueden ser considerablemente más rápidos que las redes 802.11b. La velocidad de 54 Mbps es necesaria para transferencias de archivo grandes como vídeo streaming. Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y g, la no incorporación a la misma de QoS (posibilidades de aseguro de Calidad de Servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos multimedia online), la no disponibilidad de esta frecuencia en Europa dado que esta frecuencia está reservada a la **HyperLAN2** (Ver http://www.hiperlan2.com).

Estándar 802.11a	
Frecuencia longitud de onda	5GHz
Ancho de banda de datos	54Mbps, 48Mbps, 36Mbps, 24Mbps, 12Mbps, 6Mbps
Medidas de seguridad	WEP, OFDM
Rango de Operación óptima	50 metros dentro, 100 metros fuera
Adaptado para un propósito específico o para un tipo de dispositivo	Ordenadores portátiles móviles en entornos privados o empresariales, ordenadores de sobremesa allí donde cablear sea inconveniente

Figura III – 14
Cuadro del Estándar de Comunicación 802.11a

III. 8. 4. 802.11g

802.11g es un estándar nuevo que también ofrece una velocidad de transmisión de datos de hasta 54Mbps. Sin embargo, utiliza la banda de 2.4 Ghz y por definición es compatible hacia atrás con los sistemas 802.11b. Esto significa que los sistemas 802.11b pueden funcionar sobre redes 802.11g; sin embargo, el rendimiento de un dispositivo 802.11b sobre una red 802.11g no mejorará. Ya que el 802.11g es compatible con 802.11b pero considerablemente más rápido, el 802.11g podría terminar remplazando al 802.11b.

Dispone de los mismos inconvenientes que el 802.11b. Las ventajas de las que dispone son las mismas que las del 802.11b además de su mayor velocidad.

Estándar 802.11g	
Frecuencia longitud de onda	2.4GHz
Ancho de banda de datos	54 Mbps
Medidas de seguridad	WEP, OFDM
Rango de Operación óptima	50 metros dentro, 100 metros fuera
Adaptado para un propósito específico o para un tipo de dispositivo	Ordenadores portátiles, ordenadores de sobremesa donde cablear entraña dificultades, PDAs. Compatible hacia atrás con las redes 802.11b

Figura III – 15
Cuadro del Estándar de Comunicación 802.11g

El estándar 802.11g es una unión de los estándares 802.11 "a" y "b". Contiene todos y cada uno de los tipos de modulación que éstos usan, con la salvedad de que "a" opera en la banda de los 5 Ghz, mientras que los otros dos operan en la del los 2'4 Ghz.

Cuando tenemos una red inalámbrica en la que todos los dispositivos son tipo "a" o todos de tipo "b" no hay problemas en las comunicaciones. Cada AP tipo "a" tendrá sólo TR's tipo "a" y los AP's tipo "b" tendrán sólo TR's tipo "b". Se seleccionará la mejor modulación y se transmitirá. Si la comunicación óptima no es posible debido a una excesiva distancia entre los dispositivos o por diferentes tipos de interferencias se va disminuyendo la velocidad hasta que se encuentre la primera en la que la comunicación es posible. En el caso de dispositivos AP 802.11g normalmente estará usando la modulación OFDM, modulación que es la óptima para este estándar.

En caso de que un dispositivo 802.11b quisiera hablar con otro dispositivo 802.11g, este último debería aplicar una modulación compatible con el estándar "b", cosa que es capaz de hacer. Sin embargo el dispositivo "b" no puede escuchar las transmisiones de los otros dispositivos "g" que hablan con su "partner" pues éstos usan una modulación que él no es capaz de entender. Si un dispositivo "b" comenzase a hablar a la vez que un dispositivo "g" se producirían colisiones que impedirían la transmisión, no por que interfieran ya que usan diferente modulación sino porque el AP normalmente sólo será capaz de hablar con un dispositivo a la vez.

Para evitar las colisiones, los equipos "b" usan la modulación **Barker** con **RTS/CTS** (Request To Send / Clear To Send), que básicamente significa que deben pedir permiso al AP para transmitir.

Se podría decir que en condiciones de laboratorio y a modo de ejemplo teórico, la transmisión entre dispositivos 802.11 podría ser como sigue:

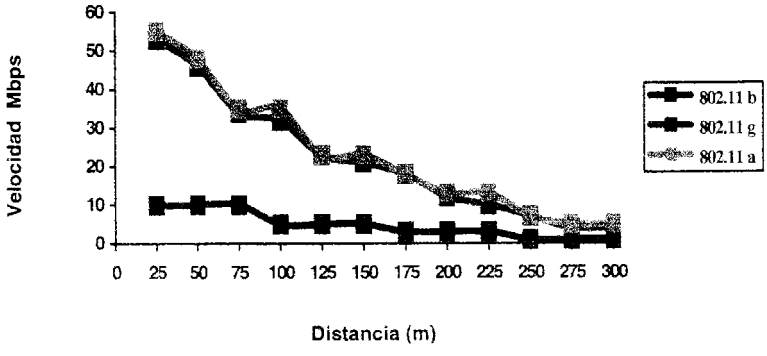


Figura III – 16

Transmisión entre Dispositivos 802.11(a, b y g)

III. 8. 5. Redes Bluetooth

Bluetooth, nombre proveniente del vikingo Harold Bluetooth, es una tecnología que está siendo usada con éxito en manos libres de los teléfonos móviles, auriculares estéreo, portátiles y PDA's.

Existe una extensa lista de productos que han sido aprobados por el grupo de interés de Bluetooth, algunos de los cuales son herramientas o componentes para crear otros productos Bluetooth. Utiliza un rango de frecuencias de los 2,4 GHz a los 2,4835 GHz, aunque la utilización exacta del espectro cambia de país en país. Por ejemplo, en Francia el rango de frecuencias utilizado va de los 2.4465GHz a los 2.4835GHz. Por eso, es probable que los productos Bluetooth adquiridos en un país no ínter operen con productos Bluetooth que estén destinados a ser consumidos en otro país.

En cuanto al ancho de banda disponible por los usuarios, la versión 1.1 permitía la comunicación a 721 Kb/s, mientras su sucesora (la 1.2) consigue hasta los 10 Mbps.

Las medidas de seguridad que incorpora son una dirección única y pública (una dirección IEEE de 48 bits) para cada usuario, dos llaves secretas y un número aleatorio nuevo para cada transacción. Sin embargo, la cobertura que ofrece este tipo de dispositivos es bastante limitada, ya que se reduce a 10 metros.

Redes Bluetooth	
Frecuencia longitud de onda	2.4GHz (2.400-2.4835)
Ancho de banda de datos	v1.1 - 721Kbps, v1.2 - 10Mbps
Medidas de seguridad	Dirección pública única para cada usuario, dos llaves secretas y un número aleatorio diferente para cada nueva transacción
Rango de Operación óptima	10 metros
Adaptado para un propósito específico o para un tipo de dispositivo	Teléfonos inalámbricos, auriculares estéreo, ordenadores portátiles, PDAs

Figura III – 17

Cuadro del Estándar de Comunicación Bluetooth

Otras redes

Existe otro tipo de redes, que aún no habiendo alcanzado la popularidad de los casos descritos con anterioridad, merecen que sean presentadas brevemente en este apartado. Estas propuestas alternativas tienen en ocasiones grandes corporaciones detrás. Por ejemplo, HomeRF cuenta con el apoyo de Intel.

III. 8. 7. HiperLAN/2

Existe otra especificación desarrollada por el ETSI (European Telecommunications Standars Institute) llamada HiperLAN (High performance radio Local Area Network) y es un estándar de comunicaciones utilizado en países Europeos. Es similar a los estándares del IEEE.

Hay dos tipos de HiperLAN:

- **HiperLAN/1**: Velocidad de transmisión de 20 Mbps en la banda de 5 GHz.
- **HiperLAN/2**: Velocidad de transmisión de 54 Mbps en la banda de 5 GHz.

Debido a que HiperLAN/2 es orientado a conexión, posee características de calidad de servicio que, combinado con las altas velocidades que aporta, facilita la transmisión de diferentes tipos de ráfagas de datos como vídeo, voz y datos.

En la actualidad, la ETSI contiene la especificación HiperLAN2 , la cual ofrece una mayor velocidad de transmisión para la capa física, 54 Mbps y que incluye QoS, seguridad e incremento del throughput cuando se necesita un ancho de banda mayor, por ejemplo para aplicaciones de vídeo. Se ha creado un grupo el HiperLAN2 Global Forum(www.hiperlan2.com), con el objetivo de sacar al mercado productos de este estándar

HiperLAN/2	
Frecuencia longitud de onda	5GHz (5.15 - 5.3GHz)
Ancho de banda de datos	6, 9, 12, 18, 27, 36, 54Mbps
Medidas de seguridad	Un esquema de cifrado-descifrado de uso opcional
Rango de Operación óptima	Máximo 150 metros
Adaptado para un propósito específico o para un tipo de dispositivo	Packetized voice, vídeo y comunicaciones de Internet

Figura III – 18

Cuadro de la Tecnología de Comunicación HiperLAN/2

III. 8. 8. HomeRF

Es un estándar híbrido de comunicaciones para redes de datos y de voz en un entorno doméstico, basada en el protocolo de acceso compartido(SWAP). La arquitectura extiende la capa MAC de manera que proporciona servicios orientados a datos, como TCP/IP y voz.

De momento el alto coste y la dificultad de instalación ha inhibido la adopción de esta especificación doméstica.

HomeRF	
Frecuencia longitud de onda	2.4GHz
Ancho de banda de datos	10Mbps, 5Mbps, 1.6Mbps, 0.8Mbps, (Planes futuros --20Mbps)
Medidas de seguridad	Cifrado de 128 bits, saltos en frecuencia, identificadores de red de 48 bits
Rango de Operación óptima	Cubre el típico entorno de casa y parcela

Figura III – 19

Cuadro de la Tecnología de comunicación HomeRF

En la siguiente figura se resumen los diferentes estándares citados indicando la situación actual y sus posibles actualizaciones futuras. Se presentan, además, algunas características técnicas muy básicas que ayudan a diferenciar unas de otras.

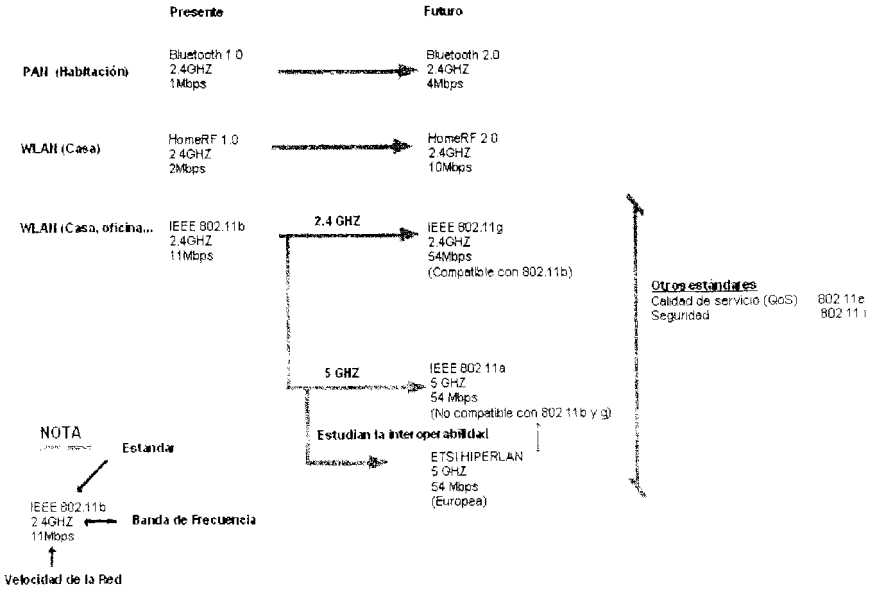


Figura III – 20

Estándares y Posible Evolución

III. 9. ¿Por qué una Red Inalámbrica?

Las redes inalámbricas comparten varias ventajas importantes, no importa cómo estén diseñados los protocolos, o incluso qué tipo de datos transporten. La ventaja irrebatible del establecimiento de una red inalámbrica es la movilidad. Los usuarios inalámbricos de la red se pueden conectar a las redes existentes e inmediatamente acceden a navegar libremente.

Avances recientes en la estandarización, han permitido el crecimiento del mercado en la conectividad de redes inalámbricas. El crecimiento de Internet, despertó el interés en el acceso inalámbrico, esto, combinado con el impulso a la estandarización de la red inalámbrica durante los últimos años a conducido a un pico de crecimiento en la industria. Aun no es una tecnología preferente, pero en nuestra actualidad los ordenadores vienen con los componentes y requerimientos necesarios (Hardware y Software) para una conectividad inalámbrica.

Los usuarios de esta tecnología tienen diversas ventajas, pueden trabajar desde una biblioteca, en una sala de conferencias, un estacionamiento, o aún en la comodidad de una cafetería. El equipo que comúnmente se encuentra disponible en el mercado puede cubrir fácilmente un campus estudiantil, se puede prolongar el alcance de una red 802.11 hasta algunas millas. Las redes inalámbricas tienen mucha flexibilidad, lo que se traduce en escalabilidad. A continuación se analizarán en detalle los aspectos en las que dichas redes aventajan a las fijas:

1) **Movilidad:** Es patente que este es el punto fuerte de las WLAN's, inalcanzable para las cableadas. Es especialmente interesante para cubrir salas de reunión, laboratorios, centros de alta itinerancia, donde haya portátiles y en general para facilitar reuniones de trabajo en cualquier punto. La movilidad en el hogar también es un valor en alza, pues permite que ese portátil que cada vez más aparece aquí sea ubicuo. Otro aspecto a considerar es la información en tiempo real en cualquier lugar.

2) **Rapidez de implantación:** Por lo general la tarea que suele consumir mayor tiempo en la instalación de una red inalámbrica es paradójicamente la parte cableada que se emplea para enlazar los puntos de acceso con la red local. En el caso de redes fijas, no son días sino habitualmente semanas. Esto es en muchos casos un factor decisivo para ciertos proyectos. También cada vez se ven más casos de despliegues primeros o ampliaciones de infraestructura que por necesidades urgentes se inician por la construcción de una red wireless para posteriormente consolidarse con una cableada, aunque manteniendo la primera para temas de movilidad y atender los requerimientos de ciertos usuarios.

3) **Estética:** Las instalaciones de redes locales se caracterizan por la existencia de infinidad de rosetas (cajas de conexiones) próximas a cada puesto de trabajo, canalizaciones generalmente visibles y cables desde los PC's hasta el punto de conexión más próximo. Como contrapartida, en una instalación wireless desaparecen los cables de las PC's y las rosetas, así como se reducen al mínimo las canalizaciones visibles. Este factor, siempre bien valorado, en ocasiones se convierte en fundamental, decidiendo la tecnología de la red a implantar. Evita obras para tirar cable por muros y techos.

4) **Reducción de costos:** El coste de despliegue de una WLAN puede estimarse entre $250 y $500 dlls por puesto de trabajo (cableado y puntos de acceso, sin contar con los adaptadores de usuario), dependiendo notablemente de los requerimientos (seguridad, calidad, bitrate) y de las características del lugar de implantación. En el caso de una red cableada, el coste es mucho más elevado, donde la gran dispersión en el presupuesto se atribuye fundamentalmente a la problemática asociada despliegue físico del cableado. 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.

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

6) **Robustez:** Las redes basadas en cableado estructurado son por lo general más robustas frente a interferencias y condiciones adversas que las inalámbricas. Sin embargo en ciertos entornos en fábricas con elevada humedad, agentes químicos agresivos, calor, etc. las instalaciones cableadas pueden sufrir una rápida degradación o ser inviables. Una instalación wireless adecuadamente ubicada para resguardarse de dichas inclemencias puede ser la alternativa idónea.

7) **Provisionalidad:** Las WLAN's tienen una gran utilidad en instalaciones que tienen carácter de provisionalidad. Ejemplos de ello son infraestructuras itinerantes (ferias, congresos, demostradores), despliegues cortos o limitados en el tiempo (oficinas temporales), para absorber fuertes picos de utilización ocasional (las WLAN pueden soportar un número elevado de usuarios transitorios, mientras que las fijas están limitadas a las conexiones ya cableadas exclusivamente) y para permitir crecimientos urgentes en una red ya establecida hasta adoptar otras alternativas. Las razones que soportan esta característica frente a la solución cableada son múltiples: economía, escalabilidad, rapidez de implantación, movilidad, etc.

8) **Mezclar las redes cableadas y las inalámbricas**: de esta manera generar una "Red Híbrida". Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

Obviamente no todas son ventajas de las redes inalámbricas frente a las cableadas: hay una serie de parámetros en las que las últimas ofrecen mayores prestaciones. La velocidad binaria es mucho mayor, obteniéndose en general límites máximos de 100 Mbps por puesto (Fast Ethernet) frente a 54 Mbps en una WLAN (802.11g) compartidos entre varios usuarios. Son asimismo más inmunes a interferencias, más seguras y requieren de un menor mantenimiento. Estas desventajas pueden ser realmente importantes o casi insignificantes dependiendo de la calidad de la implantación.

III. 10. Funcionamiento de las Redes Inalámbricas

Las redes inalámbricas utilizan un número de estaciones bases para conectar a los usuarios a una red existente. Entorno a la infraestructura inalámbrica, es equivalente si se mantiene conectado a un usuario o a miles de usuarios. Para ofrecer servicio en un área dada, se necesitan estaciones bases y antenas para dar cobertura a un lugar determinado. Una vez que se posee la infraestructura, la adición de un usuario a la red inalámbrica es solo cuestión de poseer una autorización. Tras haber localizado un AP y haberse sincronizado con él, es necesario un proceso de autentificación para evitar usuarios no autorizados. Para autentificarse se deberá mostrar el conocimiento común de una clave. Una vez autentificado el usuario, es necesario un proceso de asociación, en la asociación en la que se intercambian datos sobre las capacidades de cada uno de las partes, así el AP sabe dónde se encuentra localizado la estación. A partir de este momento ya es posible recibir y transmitir tramas (información).

Con la infraestructura montada, se le debe configurar para reconocerle y ofrecer los servicios a los nuevos usuarios, el proceso de autorización no demanda de más infraestructura. Para adicionar a un usuario a la red inalámbrica, solo es cuestión de configurar la infraestructura, en este caso ya no implica cablear.

Adentrándonos a su funcionamiento técnico, se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de WLAN los puntos de acceso conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recíbe la información, la almacena y transmite entre la WLAN. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en lo alto de las edificaciones, pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red inalámbrica a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena.

III. 11. Disposiciones a considerar en el Diseño de la Red Inalámbrica

A continuación, describiré varios puntos que se deben tener en cuenta a la hora de diseñar e implementar una red wireless.

a) Rango / cobertura.

La distancia que las ondas electromagnéticas pueden alcanzar depende de dos factores: el diseño de los dispositivos y el medio en el que se transmiten. Éste último puede ser muy variado, y modificarse a lo largo del tiempo, por lo que presenta mayores problemas a la hora de la instalación de una red wireless.

Las ondas empleadas en las redes wireless 802.11, ondas electromagnéticas mayores de 1 GHz, pueden atravesar los materiales, pero la atenuación que presenta depende del material de que esté fabricado el obstáculo, de la forma del mismo, etc.

En el caso particular de la banda ISM de los 2'4 GHz, el agua presenta un poder de absorción muy alto a esa frecuencia, por lo que los materiales con un mayor porcentaje de agua (por ejemplo, las personas) afectan muy negativamente a la propagación de las ondas electromagnéticas.

El radio de cobertura de un dispositivo wireless puede ir desde unos pocos metros, hasta alcanzar mas de 150 metros, dependiendo del entorno y el equipamiento empleado (potencia, tipos de antenas, etc).

b) Velocidad de transmisión (throughput).

La velocidad que se puede alcanzar en una red wireless depende principalmente de la norma 802.11 que utilicen los dispositivos que componen la red (2, 11, 54 Mbps como límite). Pero también otros factores como el número de usuarios, la propagación de las ondas, o la infraestructura de la red cableada (si existe) repercuten en la velocidad de comunicación en la red wireless. La velocidad en redes wireless puede alcanzar hasta los 54 Mbps con las normas 802.11a y 802.11g; existen fabricantes que anuncian alcanzar velocidades superiores, pero al emplear técnicas no normalizadas, sólo se obtienen si se emplean dispositivos de un único fabricante. Los usuarios de redes cableadas no aprecian cambios en la velocidad o en los tiempos de respuesta cuando usan redes wireless, ya que aunque poseen una velocidad inferior, es suficiente para la mayoría de las aplicaciones y servicios en red.

c) Interoperabilidad con redes cableadas.

Existe en el mercado una amplia gama de dispositivos que permiten la interconexión de redes wireless y redes cableadas. Las normas 802.11 hacen transparente al sistema operativo y de las aplicaciones de sistemas, el carácter inalámbrico en el que se comunican, y su comportamiento no varía entre una situación y otra.

d) Seguridad.

La seguridad es un tema muy importante cuando se trabaja con redes wireless, dado la característica peculiar del medio en el que viaja la información, es muy fácil para cualquier persona con el equipo adecuado (basta con un portátil y un cliente wireless) acceder a la información.

Aunque existen herramientas disponibles para obtener una transmisión segura a través de redes wireless (el protocolo WPA, por ejemplo), no se debe olvidar que, como en cualquier red de comunicación, la seguridad no se limita a la confidencialidad en el canal de comunicación, sino en una correcta administración de los recursos y servicios de la red (inalámbrica o cableada) mediante las apropiadas herramientas de seguridad desplegadas a lo largo y ancho de la red y de los equipos que la conforman.

En las últimas fechas aparecen noticias sobre lo fácil que es conseguir el acceso a redes wireless mal configuradas, aunque conviene recordar que una red inalámbrica correctamente administrada no es más que uno de los muchos puntos de seguridad que se deben mantener adecuadamente en cualquier empresa.

III. 12. Seguridad en las Comunicaciones Wireless

La seguridad en redes de tipo inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito.

Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle. Existe el término "wardriving", que se refiere a la acción de recorrer una ciudad para buscar la existencia de redes inalámbricas y ganar acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes. El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable). Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica.

La seguridad WLAN abarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquellos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Estos "hoyos" en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red alámbrica a la cual se conecta. En el apartado siguiente se mencionaran algunos mecanismos de seguridad usados en redes WLAN, así como las ventajas y desventajas de cada uno de ellos.

Mecanismos de Seguridad para Redes WLAN.

Especificación original 802.11

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas. Se hará a continuación una presentación de cada uno de ellos.

1) **SSID (identificador de Servicio):** cadena simple de 32 caracteres máximo que identifica a cada red inalámbrica. Los clientes deben tener configurado el SSID correcto para acceder a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía.

2) **Filtrado con dirección MAC (Control de Acceso al Medio):** Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Este método tiene como ventaja su sencillez. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:
   - No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.
   - El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
   - Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones
   - En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración. Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

3) **WEP (Privacidad Equivalente a Cable):** WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas, es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida.

En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de las aplicaciones:

I. La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

II. WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack 8 que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

4) **VPN Red Privada Virtual** (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP. Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

5) **802.1X** Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autenticación remota de usuarios entrantes (RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes). El protocolo 802.1x involucra tres participantes:

I. El suplicante, o equipo del cliente, que desea conectarse con la red.

II. El servidor de autorización / autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue

diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service). Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.

III. El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

6) **WPA (Wi-Fi Protected Access)** Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Protocolo de Llaves Integras–Seguras–Temporales). TKIP fue construido tomando como base el estándar WEP, este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación. Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

La norma WPA data de abril de 2003 y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello "Wi-Fi Certified" podrá ser actualizado por software para que cumpla con la especificación WPA. El uso de las VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

7) **Otros** mecanismos empleados son los siguientes:

a. **OSA vs SKA.** OSA (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el AP. SKA (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

b. **ACL.** Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

c. **CNAC.** Closed Network Access Control. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

Pasos para Asegurar una Red Inalámbrica.

En primer lugar hay que situarse dentro de lo que seguridad significa en el mundo informático. Se dice que una red es segura cuando casi nadie puede entrar la misma o los métodos de entrada son tan costosos que casi nadie puede llevarlos a cabo. Casi nadie puede significar que es segura en un 99.99%, por ello se debe desechar la idea de que los sistemas informáticos son seguros al 100%. Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener. Una vez situados se puede contemplar pasos para introducir una seguridad razonablemente alta a la red wireless. Se debe tener en cuenta que cuando se trabaja con una red convencional cableada se dispone de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos de comunicación de la misma.

- **Paso 1,** activar el WEP. Parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado. WEP no es completamente seguro, pero puede se le puede contemplar como una medida preventiva.
- **Paso 2,** seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No se debe usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando (por ejemplo) los ceros.
- **Paso 3,** uso del OSA. Esto es debido a que en la autenticación mediante el SKA, se puede comprometer la clave WEP, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.
- **Paso 4,** desactivar el DHCP y activar el ACL. Se debe asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no se permitirá que se incluyan nuevos dispositivos a la red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.
- **Paso 5,** Cambiar el SSID y modificar su intervalo de difusión. Cada propietario pre-configura el SSID en sus dispositivos, por ello es muy fácil descubrirlo. Se debe cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo prevea. Así mismo se debe modificar a la baja, la frecuencia de broadcast del SSID, deteniendo su difusión a ser posible.
- **Paso 6,** hacer uso de VPN's. Las Redes Privadas Virtuales proporcionan un extra de seguridad que va a permitir la comunicación entre dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.
- **Paso 7,** aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un firewall que filtre el tráfico entre los dos segmentos de red.

Actualmente la IEEE está trabajando en la definición del estándar 802.11i que permita disponer de sistemas de comunicación entre dispositivos wireless realmente seguros. También, en este sentido hay ciertas compañías que están trabajando para hacer las comunicaciones más seguras. Un ejemplo de éstas es CISCO, la cual ha abierto a otros fabricantes la posibilidad de realizar sistemas con sus mismos métodos de seguridad. Posiblemente algún día estos métodos se conviertan en estándar.

III. 13. Organismos en la Industria Inalámbrica

Debido al gran crecimiento de las redes inalambricas han surgido nuevas organizaciones en esta industria tales como alianzas, consorcios y forums, las cuales se encargan de proponer estándares y definir nuevas tecnologías. Se pueden dividir estas organizaciones en tres categorías: alianzas de tecnología, organizaciones de estándares y asociaciones de la industria.

I. **Alianzas de tecnología:** Típicamente, una alianza de tecnología está formada para introducir al mercado una tecnología o protocolo específico y proveer interoperabilidad y certificación de productos de diferentes compañías que utilizan esa tecnología o protocolo. Ejemplos de este tipo de organizaciones están las siguientes:

- **Bluetooth SIG:** basado en la especificación BluetoothTM especificación que utiliza la tecnología de radio para proveer conectividad a Internet a bajo costo a computadoras portátiles, teléfonos móviles o otros dispositivos portátiles.
- **HiperLAN1, HiperLAN Alliance e HiperLAN2 Global Forum:** organizaciones europeas que utilizan enlaces de radio de alto desempeño a frecuencias en el rango de 5 GHz.
- **HomeRF:** Basada en una especificación para comunicaciones inalámbricas en hogares conocida por sus siglas en inglés SWAP (shared wireless access protocol). El HRFWG (HomeRF Working Group) fue fundado para proveer los cimientos para un amplio rango de dispositivos al establecer una especificación abierta a la industria para comunicaciones digitales inalámbricas entre PC's y dispositivos domésticos alrededor de los hogares.
- **OFDM:** Esta organización está basada básicamente en una tecnología patentada conocida como W-OFDM (Wide-band orthogonal frecuency división multiplexing)
- **WLI forum:** WLIF estableció un estándar interoperable en 1996 conocido como OpenAir, el estándar está disponible a cualquier compañía que se une al Forum. OpenAir es una tecnología de espectro extendido con salto en frecuencia a 2.4 GHz
- **WECA:** La misión de la WECA (Wireless Ethernet Compatibility Alliance) es certificar la interoperabilidad del estándar conocido como Wi-Fi que es una versión de alta velocidad del estándar 802.11b de la IEEE.
- **Federal Communications Commission (FCC).** Agencia del gobierno de los EEUU encargada de regular las comunicaciones por radio, televisión, satélite y cable.
- **European Telecommunication Standards Institute (ETSI).** Organismo europeo encargada de las normas de telecomunicaciones en Europa.

- **Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.** Organismo estatal para las telecomunicaciones e Internet.

En materia de software

- **AirSnort.** Monitor pasivo de redes inalámbricas que permite conocer distinta información sobre ellas y obtener las claves WEP.
- **WepCrack.** Scripts escritos en Perl que permiten deducir la clave WEP a partir de un fichero con el tráfico recogido.

II. **Organizaciones de estándares:** Este tipo de organizaciones crean, definen y proponen estándares internacionales oficiales abiertos a la industria a través de un proceso abierto a todas las compañías. Ejemplos de estas organizaciones:

- La IEEE (Institute of Electrical and Electronics Engineers) y
- La ETSI (European Telecommunications Standards Institute)

III. **Asociaciones de la industria:** estas organizaciones son creadas para promover el crecimiento de la industria a través de educación y promoción, proveyendo información objetiva sobre la industria en general, tecnologías, tendencias, organizaciones, oportunidades independientemente de la tecnología. La organización más importante en esta categoría es la WLANA (Wireless LAN Association) cuya misión es ayudar y fomentar el crecimiento de la industria a través de la educación que puede ser caracterizada por asociaciones industriales y comerciales. Organizaciones como estás promueven la competencia y avances tecnológicos lo cual significa mejores soluciones para los usuarios de redes inalámbricas e incrementar el crecimiento de la industria.

III. 14. Tendencias

Los precios de estos equipos vienen cayendo abruptamente desde hace unos tres años, lo que ha permitido que sea ya frecuente encontrarlos en redes de hogar, produciéndose incluso la paradoja de que actualmente este segmento está siendo más activo que el empresarial.

Aunque no es sencillo adivinar la tendencia final, parece que el mercado podría quedar dividido entre router/gateways/AP's multifunción cada vez con más posibilidades (VoIP, VPN's...), muy útiles para el hogar, PYMES, universidades y pequeñas instalaciones, y, por otro lado, AP's/bridges/repeaters simples para configuraciones en los que la inteligencia de red reside en otros equipos (switches, gestores de redes inalámbricas). También cada vez más dispositivos de infraestructura están incorporando la funcionalidad PoE (Power Over Ethernet), o lo que es lo mismo, la posibilidad de alimentarse eléctricamente a través del propio cable Ethernet. Esto elimina un cableado adicional, sobre todo fundamental en instalaciones en exteriores en donde es más complejo la solución de alimentación.

En cuanto a los estándares que soportan, tanto AP's como bridges y routers suelen dividirse en dos grupos según operen bajo 802.11b/g o sobre 802.11a. Con la reciente aparición de chipsets tri-estándar, ya existen equipos 802.11a/b/g, que si prosigue la reducción de precio en los integrados, posiblemente los fabricantes opten por modelos únicos para aumentar el ahorro de costes.

Todavia hay frentes en los que se esperan importantes avances. El primero de ellos es la seguridad, con un mecanismo de seguridad avanzado (WPA) ya implantado en prácticamente todos los nuevos equipos, pero que se consolidará finalmente en unos meses como el estándar IEEE 802.11i.

El segundo es la calidad de servicio, clave para la implantación de servicios como la voz sobre IP en redes wireless (VoWLAN), difusión de televisión/vídeo/audio, juegos, etc., que probablemente se solucione para el próximo año con el 802.11e.

La tecnología inalámbrica ha ganado la aceptación universal, con el número de suscripciones inalámbrica que actualmente exceden el número de líneas fijas en muchos países.

El mercado inalámbrico es considerablemente más competitivo, se encuentra en constante crecimiento y en un vertiginoso despliegue de soluciones innovadoras que se presentan de manera acertada como núcleo de cualquier estrategia wireless .

IV. ANÁLISIS

IV. 1. Definición del Problema

Tras la experiencia personal de haber cursado la licenciatura de informática, he detectado que en el transcurso de ésta se tienen diversos problemas o situaciones de disponibilidad de servicios, centralizados en las necesidades de la comunidad y originados principalmente por las siguientes razones:

Debido a la gran población estudiantil con que cuenta la Facultad, el equipo de cómputo y los servicios en línea, no satisfacen las necesidades en la dimensión que se desearía , por lo que se limita el acceso a los servicios de la red y a los recursos del sistema (altas, bajas y cambios en el sistema de inscripciones, registro de passwords, actualización de datos, consultas de horarios de grupo e historiales académicos y comprobantes de inscripción), consultas on-line a los recursos de la Biblioteca (libros, revistas, publicaciones), a la información de la web, videoconferencias, servicio de e-mail, etc. De este modo se imposibilita el acceso a servicios, que podrían ser mucho mas flexibles a la comunidad universitaria y que favorecerían a mejorar el desempeño de sus actividades dentro de instancias como bibliotecas, centros de cómputo, laboratorios y auditorios.

Existe poca practicidad en las áreas administrativas, donde se concentra la responsabilidad de la administración de los estudiantes, registros, y todo el material de soporte para la facultad, existen ciertos elementos que pueden ser de total innovación e incrementar la eficacia en la calidad de los servicios ofrecidos, por ejemplo, el contar con una infraestructura inalámbrica que comunique cada una de las áreas internas o a las diferentes dependencias universitarias, así como la transmisión de datos, video e imágenes.

La aportación de este proyecto, es una demostración de las ventajas y aplicaciones que pueden ofrecer las tecnologías inalámbricas en cuanto al desarrollo y manejo de servicios, proporcionando una herramienta accesible y escalable para la distribución, transporte e intercambio de la información entre dispositivos sin importar su ubicación.

IV. 2. Justificación del Proyecto

Las tecnologías de redes inalámbricas requieren un extenso trabajo de investigación dado que son tecnologías en desarrollo y en constante cambio. Las primeras publicaciones en estándares oficiales IEEE se publicaron hace tres años y están sujetas a revisión dentro de los próximos cinco años.

En algún futuro no muy lejano este tipo de redes tendrán repercusiones tecnológicas y económicas muy importantes debido a su alta eficiencia y a los objetos hacia los cuales está orientada. Muchas de sus aplicaciones aún no se vislumbran y un buen estudio es fundamental para el desarrollo de nuevos servicios.

Proveer una educación de calidad a través de la diversificación de contenidos y metodologías es uno de los mayores retos para las instituciones de educación superior. Este trabajo presentará el estudio referente a tecnologías inalámbricas, y el cómo pueden facilitar a los estudiantes, académicos y docentes, sus actividades cotidianas y que involucra el uso de tecnologías de la información, servicios digitales, la interacción en la comunidad y a la obtención de conocimiento de acuerdo a sus intereses.

El manejo de tecnologías en aplicaciones para equipos móviles, abre un panorama amplio, como puede ser el aprendizaje a distancia, y del como un estudiante puede accesar a colecciones digitales, correo, realizar consultas o solicitudes al sistema y realizar trámites de manera inalámbrica.

Las redes inalámbricas están adquiriendo un éxito importante debido a una combinación de factores: una tecnología eficaz con el uso del espectro, muy orientada al despliegue de redes locales de pequeño tamaño, un entorno regulatorio que permite su libre uso, una lógica fácilmente integrable y de muy bajo coste, y una interoperabilidad de equipos generalmente exitosa. Sin embargo, la tecnología subyacente no es trivial, sino que ha requerido un estudio profundo de cómo obtener un uso muy eficiente de un rango escaso de frecuencias, cómo conseguir una amplia cobertura con potencias de emisión muy bajas, y todos los aspectos relacionados con la securización de las comunicaciones. Es importante entender las bases sobre las que se sustenta para entender sus grandes ventajas y sus inconvenientes. Teniendo en consideración las razones esbozadas en los párrafos anteriores, es precisamente esta realidad descrita la que justifica la importancia del presente trabajo de investigación.

Para el desarrollo de este proyecto de organización, no se llevará a cabo la implementación de la tecnología que permita la transmisión de datos a dispositivos inalámbricos. Sin embargo, a pesar de que no serán utilizadas dichas herramientas es importante sentar las bases para proyectos futuros.

IV. 3. Objetivos del Proyecto

IV. 3. 1. Objetivo General

Proporcionar a los alumnos, investigadores y docentes una infraestructura inalámbrica de telecomunicaciones que permita acceder, mediante una notebook o un equipo portátil (laptop o PDA Personal Digital Asistant), propiedad del usuario o de la Facultad, a las herramientas informativas necesarias y requeridas para promover, orientar y difundir en materia de docencia e investigación, así como apoyar a la Facultad en los sistemas administrativos que requiera.

IV. 3. 2. Objetivos Específicos

- **Tener una red inalámbrica,** que facilite la colaboración y el aprendizaje de los universitarios a partir de compartir recursos e información.
- **Proponer servicios a través de Internet, para la comunidad universitaria** integrada a los sistemas de información que se tengan en la misma, además de permitirle a los estudiantes acceder a servicios de apoyo e información, tanto internos como externos, para el mejor desempeño de sus labores académicas.
- **Sugerir y plantear propuestas con equipos** que sean flexibles en el acceso a nuevas tecnologías
- **La posibilidad de brindar programas educativos y capacitación** a través de la implementación de la red wireless.
- **El asegurar la confidencialidad e integridad de la información** a través del desarrollo e implantación planeada y controlada de la seguridad computacional de la red.
- **Generar un ambiente de aprendizaje** enfocado a generar medios que faciliten la labor docente y la educación virtual. Es la incorporación de tecnología que facilite el proceso de enseñanza-aprendizaje y dé un rasgo distintivo a la comunidad universitaria.
- **Sugerir las condiciones e instalaciones** para los equipos inalámbricos.

IV. 4. Alcances y Limitaciones.

IV. 4. Alcances y Limitaciones.

Alcances

Los alcances de esta propuesta involucran los siguientes puntos:

- Contar con una infraestructura inalámbrica al servicio de la comunidad universitaria para proveer aplicaciones y servicios.
- Satisfacer las necesidades de información y poner a disposición de los profesores, alumnos investigadores, graduados y público en general los servicios de consulta que ofrece la red de la FCA.
- Análisis de las herramientas y aplicaciones que estén bajo el empleo de la tecnología inalámbrica y que tengan como enfoque el aprendizaje colaborativo. Así como, el alcance real de las diferentes aplicaciones que esta tecnología puede ofrecer.
- Se propondrá una red inalámbrica fácil de escalar en un futuro.
- Funcionará con la infraestructura alámbrica existente.

Limitaciones

Entre las limitaciones de esta propuesta se encuentran los siguientes puntos:

- Contar con apoyos institucionales y privados, para la obtención de recursos en dispositivos inalámbricos, para la realización de la aplicación a desarrollarse.
- El acceso parcial o total, sobre el material técnico e informativo del equipo que se requiere, por parte de los fabricantes de los mismos, por ejemplo, las ventajas y desventajas.
- La eficiencia de la red inalámbrica estará limitada a la utilización de su capacidad dependiendo de factores como la distancia, el número de usuarios, los materiales de construcción, etc.

IV. 5. Análisis de Requerimientos

El análisis de requerimientos es el conjunto de técnicas y procedimientos que establecerán los lineamientos y mecanismos necesarios para el desarrollo y cumplimiento del proyecto.

Permitirá definir la asignación de recursos y representar el dominio y contenido de la información que será tratada por el proyecto.

En la base se encuentran las herramientas existentes hardware y software para dar soporte al esfuerzo de desarrollo. En el nivel más alto se encuentra el recurso primario que se requiere, la gente.

Análisis de Recursos

El empleo de hardware y software en este proceso de investigación, nos permitirá tener los elementos necesarios para el logro de los objetivos definidos.

Recurso Humano

Se debe planificar comenzando con la evaluación del ámbito y seleccionando las habilidades técnicas que se requieren para llevar a cabo el desarrollo.

La conformación de un equipo de trabajo encargado del desarrollo, implementación, administración gestión y de todas las actividades necesarias para la puesta en marcha de este proyecto, podría estar integrado por académicos, docentes y estudiantes de la facultad, estos últimos que se encuentren realizando el servicio social o que formen parte de un plan de becas o integrarse como personal de apoyo.

Recurso de Hardware

La arquitectura de un sistema que implementa el estándar 802.11 está constituida por los siguientes elementos:

- El punto de acceso (PA) o "Wireless Network Acces Point".
- Tarjetas inalámbricas (PCMCIA, PCI, o adaptador inalámbrico externo USB) o "Instant Wireless Network Adapter" que cumplan con el estándar IEEE 802.11
- Antenas direccionales.
- Antenas omnidireccionales.
- Componentes adicionales como cables de antena y elementos de protección contra descargas atmosféricas entre la antena y el transmisor.
- Estaciones inalámbricas.
- Adaptador de corriente.
- Cable de conexión directo UTP de Categoría 5.

Para un óptimo funcionamiento por parte de los dispositivos que se integren a la red inalámbrica, deberán contemplar los siguientes requisitos: Equipos con una interfaz 10BASE-T, 10/100, o 10/100/1000 configurada para comunicación por Internet .

Recurso de Software

La administración de los dispositivos inalámbricos está basada en navegador, asistentes de instalación inalámbrica y de detección de dispositivos; con la funcionalidad de guardar y restaurar archivos de configuración. Para un óptimo funcionamiento por parte de los dispositivos que se integren a la red inalámbrica, requerirán la instalación de los siguientes sistemas operativos:

- Windows 98,
- Windows ME,
- Windows XP o
- Windows 2000

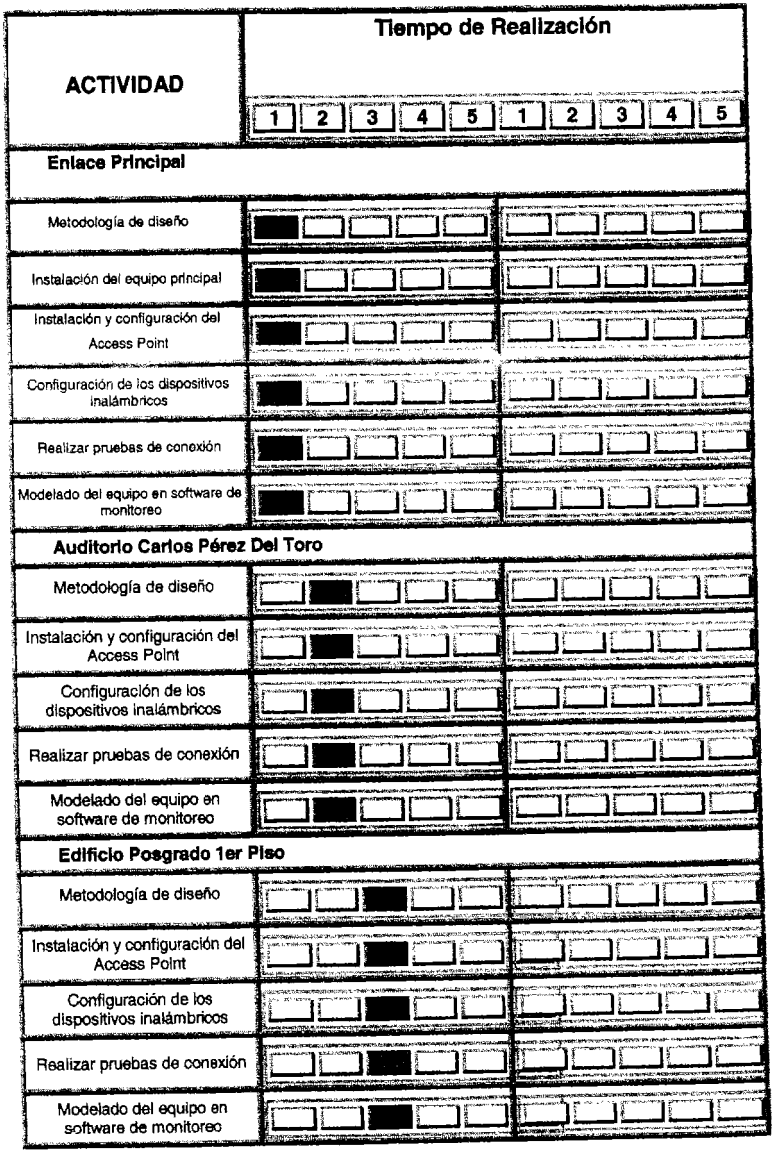
Estos sistemas operativos soportan una conexión Ethernet con una pila IP. Los puntos de acceso cuentan con la guía de instalación, CD-ROM con el programa Access Point Discovery y Guía de Usuario.

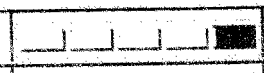
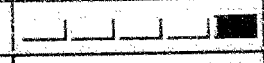
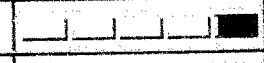
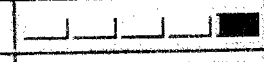
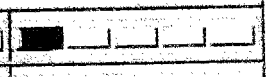
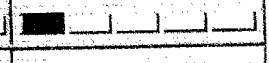
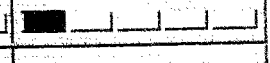
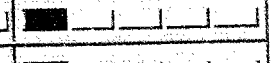
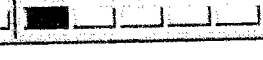
IV. 6. Especificación del Proyecto

La especificación del proyecto servirá como fundamento para el proceso de desarrollo, tomando en consideración aspectos como el hardware, el software y los recursos humanos con los que se puede contar para la elaboración del proyecto.

Se describirá la función y el rendimiento de la instalación así como las restricciones que se presentarán en el desarrollo de la investigación. Del mismo modo se delimitará el funcionamiento de cada uno de los elemento que integrará el proyecto. Es de suma importancia prestar atención a los detalles técnicos: como los estándares a emplearse y la compatibilidad de los equipos.

IV.6. Plan de Trabajo.



Edificio de Investigación Planta Baja		
Metodología de diseño		
Instalación y configuración del Access Point		
Configuración de los dispositivos inalámbricos		
Realizar pruebas de conexión		
Modelado del equipo en software de monitoreo		
Coordinaciones		
Metodología de diseño		
Instalación y configuración del Access Point		
Configuración de los dispositivos inalámbricos		
Realizar pruebas de conexión		
Modelado del equipo en software de monitoreo		
Secretaría Administrativa		
Metodología de diseño		
Instalación y configuración del Access Point		
Configuración de los dispositivos inalámbricos		
Realizar pruebas de conexión		
Modelado del equipo en software de monitoreo		
Administración Escolar		
Metodología de diseño		
Instalación y configuración del Access Point		
Configuración de los dispositivos inalámbricos		
Realizar pruebas de conexión		
Modelado del equipo en software de monitoreo		

Personal Docente	
Metodología de diseño	
Instalación y configuración del Access Point	
Configuración de los dispositivos inalámbricos	
Realizar pruebas de conexión	
Modelado del equipo en software de monitoreo	
Biblioteca	
Metodología de diseño	
Instalación y configuración del Access Point	
Configuración de los dispositivos inalámbricos	
Realizar pruebas de conexión	
Modelado del equipo en software de monitoreo	
Laboratorios de Cómputo	
Metodología de diseño	
Instalación y configuración del Access Point	
Configuración de los dispositivos inalámbricos	
Realizar pruebas de conexión	
Modelado del equipo en software de monitoreo	

V. PROPUESTA TECNOLÓGICA

V. 1. Descripción General Del Proyecto

El proyecto de Investigación para la Implementación de una Red Inalámbrica, emplea el estándar 802.11, en particular la demostración del estándar Wi-FI.

La instalación y desarrollo crearía un nuevo modelo de enseñanza más práctico y avanzado. Estaría basada en la interactividad y en el acceso permanente a la información a través un dispositivo portátil sin cables a la red, desde cualquier lugar de la facultad durante las 24 horas, lo que permitiría disfrutar a los alumnos, docentes y académicos de las siguientes ventajas:

- Aplicación de la tecnología en las clases dotándolas de una mayor interactividad entre profesor y alumno.
- Conexión a Internet.
- Tutorías.
- Acceso a correo electrónico.
- Trabajos compartidos en el servidor.
- Acceso gratuito a Internet desde cualquier punto de la facultad.
- Acceso on-line a los servicios y recursos de la Biblioteca.

Con este panorama, planteo la idea de trabajar en un proyecto con tecnología inalámbrica debido a su bajo costo, facilidad de adopción y expansión (factores que se constituyen en un aporte para aminorar la brecha de acceso a la tecnología). Si bien el objetivo principal es el de probar la tecnología wireless, se debe identificar un grupo de "usuarios" a los que les interese participar en este proyecto para utilizar el medio de transmisión que se les proporcionaría.

Grupo de Trabajo Participante

En este proyecto propongo que el grupo de trabajo que interactuaría con este modelo estaría conformado por:

1) Profesores o Investigadores. Profesores involucrados en el área de administración de la red (área de telecomunicaciones), así como en el área de desarrollo.
2) Alumnos. Se requerirá la participación de la comunidad en general, interesados en participar activamente en el proyecto. Con ello se enriquecerá la dinámica, a raíz de la naturaleza de las tareas desarrolladas.
3) Profesionales. Se necesita la participación de personas con amplia experiencia en el tema educativo para determinar el tipo de contenido, coordinar las actividades a implementar y diseñar un curso de perfeccionamiento para usar de mejor manera la tecnología en clases.
4) Coordinación. Grupo de coordinación del proyecto en todos los ámbitos (administrativos, y de control y gestión).

V.2. Situación Actual

V.2.1. Infraestructura en Materia de Telecomunicaciones

La Facultad de Contaduría y Administración cuenta con un enlace de fibra óptica a 10Mbps tendido desde la DGSCA hasta la planta baja del edificio F, donde se encuentra el switch principal el cual distribuye el servicio de red hacia el interior de la Facultad.

Internamente se cuenta con un Backbone, de fibra óptica que viene desde el switch principal hacia los edificios E, Biblioteca, Coordinaciones, Auditorio, Audiovisuales, edificios de Posgrado e Investigación, a partir de ahí a través de switches y concentradores, se proporciona servicios de red (datos y video) a todas las áreas de la FCA.

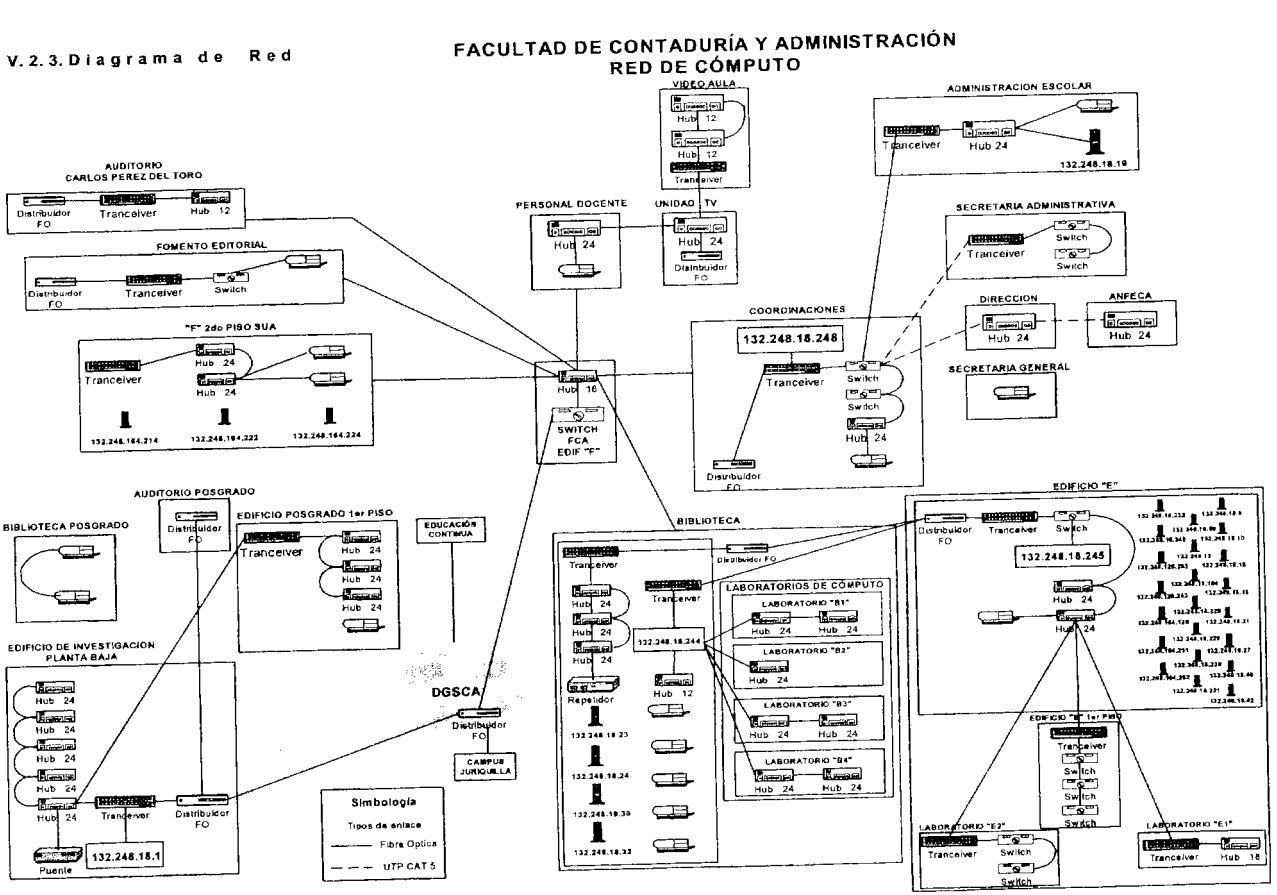
El equipo con que cuenta la Facultad es el siguiente:

- 50 Concentradores (Hubs)
- 30 Switches
- 2 Firewalls
- 2 Repetidores (Routers)
- 3 Puntos de Acceso (Access Point)

V.2.2. Servicios de la Red

- Coordinar a los alumnos, profesores, investigadores y empleados administrativos para el uso del equipo de cómputo en las salas de la Facultad, así como el servicio de impresión.
- Analizar y diseñar propuestas para el desarrollo e implantación de nuevas tecnologías en el área de Informática académica, de investigación y desarrollo.
- Administrar cuentas de alumnos, profesores y personal administrativo dentro de los servidores de la FCA.
- Administrar los servicios electrónicos de acceso a Internet, garantizando la seguridad en la transferencia de información.
- Proporcionar mantenimiento preventivo y correctivo a los equipos de cómputo y periféricos, así como soporte técnico y soporte de telecomunicaciones a la comunidad de la FCA.
- Análisis y diseño de sistemas de información para el personal administrativo y académico de la Facultad.
- Resguardar y dar seguimiento a los contratos y convenios celebrados con los diferentes proveedores de equipos de cómputo de la Facultad.
- Diseño y mantenimiento de la página Web y servicios de Internet de la Facultad.
- Diseñar, editar, digitalizar textos o imágenes para colocarlos en las páginas Web de la FCA.
- Administrar la Infraestructura de la red de cómputo Instalación y mantenimiento de la misma, según las normas establecidas por la DGSCA.
- Garantizar la eficiencia y calidad de los servicios proporcionados hacia los usuarios de la FCA.

V. 2. 3. Diagrama de Red



V. 2. 3. Descripción de la Propuesta

Dada la importancia de la red de la Facultad, es imprescindible contemplar la actualización de la tecnología para satisfacer las necesidades de crecimiento en el acceso e intercambio de información, ya que ésta es una de las partes fundamentales de la red de la facultad. De igual forma se pretende mantener la compatibilidad con la red existente, a pesar de estar basada en su mayoría por concentradores.

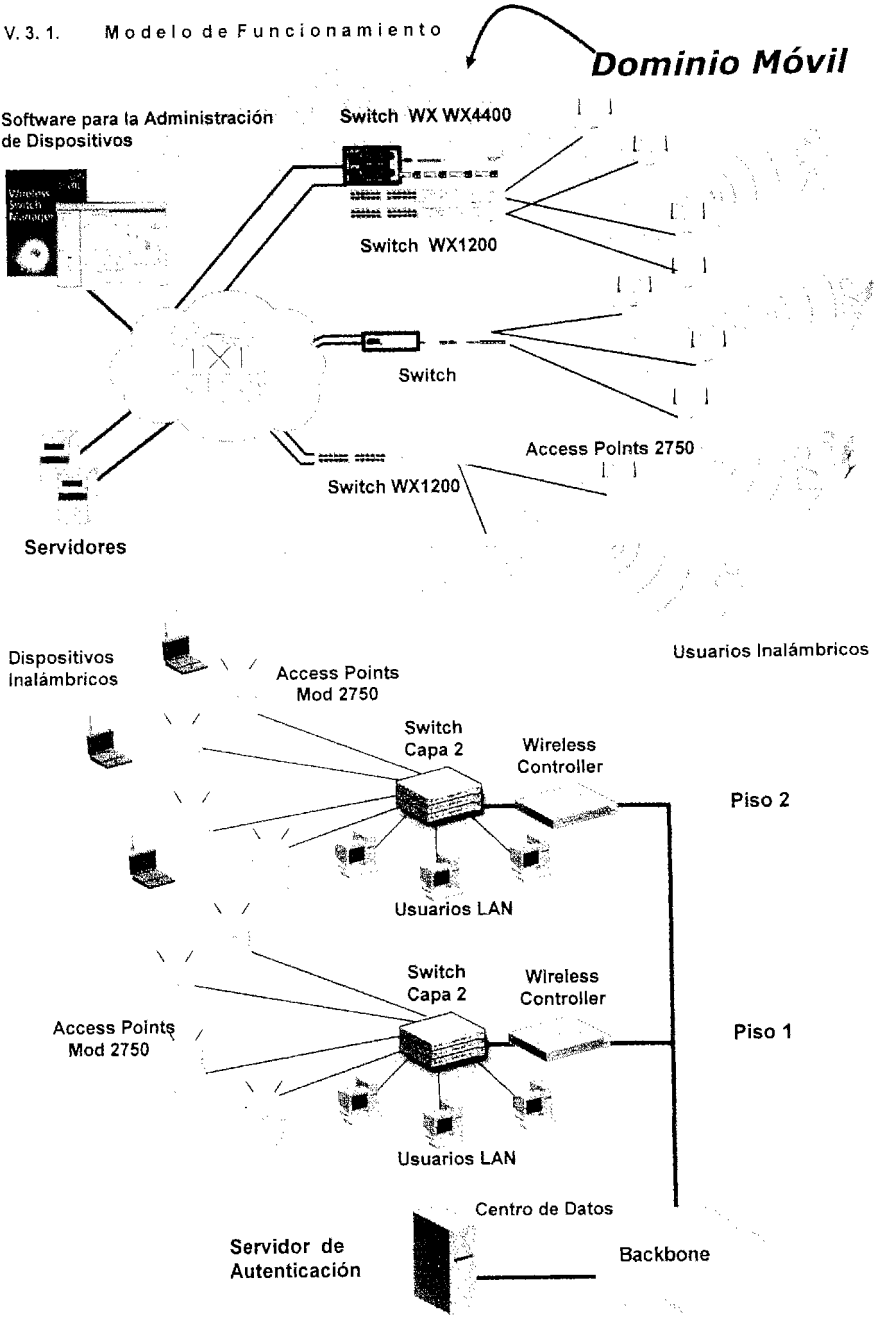
En la propuesta planeada se incluyen los siguientes elementos para la conformación de la red inalámbrica:

- Access Points, administrados de manera inalámbrica para LAN de 3Com (AP2750): Access Point con encriptación AES, administrados con 802.11a y b/g "Fit". Estos productos interoperan para proveer niveles más altos de seguridad inalámbrica y movilidad, administración simplificada y centralizada de ambientes complejos inalámbricos.
- Software para Sistemas de Movilidad (MSS, por sus siglas en inglés): Sistema operativo para sistemas de movilidad inalámbrica.
- Switches Inalámbricos WX1200 para LAN de 3Com: Switch inalámbrico de LAN para usuario y alerta de movilidad.
- Antenas omnidireccionales de banda dual 2,4/5 GHz (opcionales), para proporcionar cobertura uniforme en una amplia área en interiores o extender el alcance de transmisión.

El primer modelo propuesto obedece a las necesidades de sitios como la Biblioteca, en donde existe una gran concentración de usuarios, el equipo que se propone es el Wireless LAN Switch (WX1200) que administra y controla de forma centralizada los Puntos de Acceso (PA), además puede desplegarse sobre cualquier topología de LAN de Nivel 2 o Nivel 3 existente sin necesidad de re-configuración del troncal o de hardware. El WX1200 soporta hasta 12 MAPs, en caso de adaptarlo con controladores o conmutadores inalámbricos de 3Com, soporta futuras capacidades para LAN inalámbrica, como por ejemplo Telefonía IP inalámbrica (VoIP). Las actualizaciones de firmware son descargables y mantienen las redes al corriente de las versiones de los estándares en desarrollo, del mismo modo ofrecería múltiples esquemas de encriptación AES, TKIP y WEP, así como asignación de encriptación por usuario. Los AP2750 mantienen la encriptación local para proteger las transmisiones de red, en lugar de ser simples puntos de acceso los MAPs recopilan datos inteligentes acerca de la WLAN mediante el escaneo y la monitorización de RF. A través del Switch WX1200 se suministra alimentación y datos a los MAPs sobre el cableado Ethernet.

En el segundo modelo a implementar, se pretende situar los LAN Access Point 7250 en las siguientes puntos: en el Auditorio Carlos Pérez del Toro, en el segundo piso del SUA, en el auditorio de Posgrado, en la planta baja del Edificio de Investigación, en el edificio de Personal docente, en las Coordinaciones, Administración Escolar, en la Secretaría Administrativa, en uno de los Laboratorios de Cómputo y en el edificio E. Este modelo de AP, soporta los estándares 11a, 11b y 11g, para más detalle dirigirse a el Equipo Propuesto de este Capitulo. Se recomienda el uso de antenas para proporcionar una cobertura uniforme en una amplia área en interiores y para extenderla la misma.

V. 3. 1. Modelo de Funcionamiento



V. 3. 2. Equipo Propuesto

Se sugiere el siguiente equipo para su posible instalación en la red de la Facultad de Contaduría y Administración, el cual se apegaría a las necesidades de acuerdo al criterio de funcionamiento y operabilidad de la misma.

1) **3Com Wireless LAN Access Point 2750**

Especificaciones del producto	
Puertos totales:	Un puerto integrado PoE 10BASE-T/100BASE-TX compatible con 802.3af con auto-negociación, puerto serie de consola, conector de alimentación DC para funcionamiento sin PoE
Interfaces con los medios:	RJ-45, 802.11a, 802.11b, 802.11g, DB-9
Banda de frecuencia:	802.11a: 5 GHz , 802.11b/g: 2,4 GHz
Canales operativos:	La disponibilidad de canales depende de las regulaciones locales de los países. El administrador de sistema de LAN inalámbrica debe elegir el país correcto para poder operar. Una vez hecho esto, se configuran automáticamente los canales para cumplir con las regulaciones específicas del país
Distancia operativa:	802.11a: hasta 50 metros para transmisión y recepción; 802.11b/g: hasta 100 metros para transmisión y recepción
Consumo de alimentación:	6W máximo (puerto PoE o fuente de alimentación externa)
Seguridad:	Encriptación WEP de 48/104 bits ver. 1 y 2, WPA y AES de 128 bits, soporte de SSID de broadcast múltiple en el MAP; login de red IEEE 802.1X o autenticación RADIUS 802.1X; listas de control de acceso (ACLs); soporte de VLAN y VPN; soporte de la propuesta de estándar 802.11i en el switch/controlador
LEDs:	Alimentación, estado de enlace 10/100 Mbps, Actividad 802.11a, 11b, ó 11g
Dimensiones y peso:	Altura: 26,7 cm Anchura: 8,3 cm Fondo: 3,2 cm Peso: 0,3 kg
Administración:	Administración central con navegador Web vía consola local o de forma remota sobre SSL o HTTPS; interfaz de línea de comando vía consola local o de forma remota sobre SSH v2 o Telnet; 3Com® Wireless Switch Manager
Requisitos del sistema	Se requiere el 3Com® Wireless LAN Switch WX1200 o 3Com Wireless LAN Controller WX4400 para la operación de MAPs
Contenidos del paquete	3Com Wireless LAN Access Point 2750, Dos antenas de banda dual 2,4/5,15 GHz, Cuatro pies de goma, Hardware de montaje, Guía de inicio rápido, Documentación de garantía

2) 3Com® Wireless LAN Switch WX1200

Especificaciones del producto	
Puertos totales:	Seis puertos PoE integrados 10BASE-T/100BASE-TX, dos puertos 10BASE-T/100BASE-TX; auto-negociación en todos los puertos; puerto serie de consola
Soporte de MAPs:	Se entrega con soporte para hasta 12 MAPs por switch, dependiendo de los requisitos de capacidad y cobertura de la instalación inalámbrica
Capacidad agregada de switching:	Hasta 200 Mbps
Soporte de dirección MAC:	128 direcciones
Alimentación:	Fuente de alimentación de 200W máx.: Tensión de funcionamiento: 90-132/180-264V, 47-63 Hz Consumo máximo de corriente: 8 Arms a 120 Vrms; 3,5 Arms a 230 Vrms Power over Ethernet: Salida de tensión: 48 VDC, 15,4W por puerto
LEDs:	Estado de enlace (10 Mbps ó 100 Mbps), AP/ PoE, Alimentación
Dimensiones y peso:	Altura: 4,4 cm, ó 1U Anchura: 44,1 cm Fondo: 25,6 cm Peso: 3,8 kg
Administración:	Administración con interfaz Web mediante acceso vía consola local o de forma remota sobre SSL o HTTPS; acceso mediante interfaz de línea de comando vía consola local o de forma remota vía SSH v2 o Telnet; SNMP MIB II; 3Com® Wireless Switch Manager (producto requerido, debe pedirse por separado); inter opera con 3ND y HP OpenView
Contenidos del paquete:	3Com Wireless LAN Controller WX1200, Kit de montaje en rack Cuatro pies de goma adhesivos, Cable de consola serie DB-9 Guía de usuario, CD-ROM con documentación de usuario

3) 3Com® Wireless LAN Access Point 7250

Especificaciones del producto	
Usuarios Soportados	Hasta 253 usuarios simultáneos.
Compatibilidad con Normas Inalámbricas	Certificación Wi-Fi, IEEE 802.11g.
Velocidades de Datos Soportadas	54, 48, 36, 24, 18, 11, 9, 5,5, 2, 1 Mbps
Banda de Frecuencias	2.4 GHz.
Distancia Operativa	Hasta 100 metros (328 pies) en transmisión y recepción
Medio Inalámbrico	OFDM y DSSS (con código Barker y CCK para compatibilidad hacia atrás con 802.11b)
Protocolo de Acceso a Medios	CSMA/CA
Canales Operativos	1 - 11 (EE.UU. y Canadá), 1 - 13 (En todo el mundo: la disponibilidad de canales depende de las regulaciones locales)
Funciones de Rendimiento	Clear Channel Select, Auto Network Connect, Dynamic Rate Shifting Network Management: herramienta Site Survey, Wireless Infrastructure Device Manager, herramienta Wireless LAN Discovery, 3NS, SNMP (SNMP v1, SNMP v3, HP OpenView 6.2, 3NS)
Seguridad	IEC & EN 60950, UL / CSA 60950, NOM 019
Condiciones Ambientales Operativas	Temperatura de funcionamiento: de 0°C a 40°C (de 32°F a 104°F); con antenas externas de 15°C a 40°C (de 59°F a 104°F) Humedad: de 5 a 95% (sin condensación)

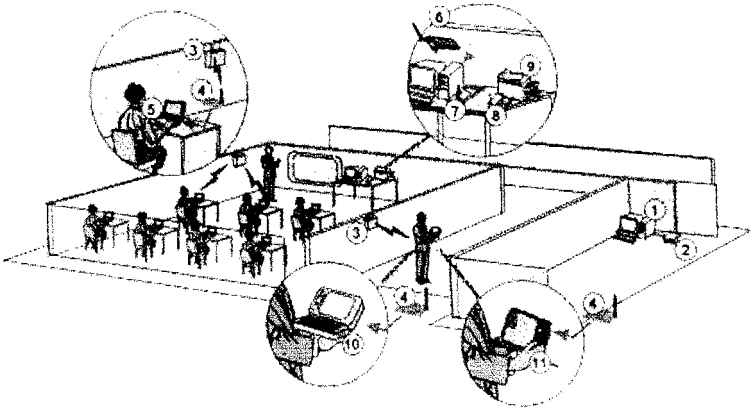
Dimensiones y Peso	Altura: 20,5 cm (8 in) Anchura: 22 cm (11") Fondo: 8 cm (3")
Requisitos del sistema	Para ejecutar las aplicaciones de administración, se necesita una computadora con CD-ROM que opere con Windows XP/2000/Me/98/95b+/NT 4.0+.
Contenidos del paquete	3Com Wireless LAN Access Point 7250 CD-ROM con utilidades de administración y la herramienta Site Survey, Adaptador de alimentación AC con cable de alimentación local, Cable Ethernet de Categoría 5 de 10 metros (33 pies) , Soporte de montaje y hardware, Guía de inicio rápido

* Si se usa el punto de acceso con una antena externa, se deberá comprar un cable de antena. Para una máxima eficiencia, se deberá usar un cable de antena el más corto posible. Los cables de antena inducen pérdidas de señal, lo que limitará la salida de potencia radiada y el alcance del punto de acceso. De entre las opciones disponibles, se recomienda el 3Com 6-pies Cable de Antena. Las opciones de antena externa amplían el alcance de las conexiones inalámbricas 802.11g a hasta 305 metros (1.000 pies)

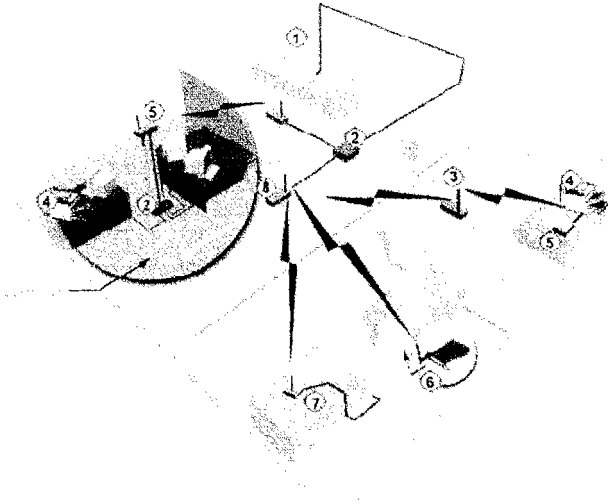
4) 3Com® 3/4dBi Dual-Band Antena

Especificaciones del producto	
Rango de Frecuencia	2300 - 2500 MHz and 5000 - 5800 MHz
Ganancia 4 GHz :	3dBi
Ganancia 5 GHz :	4dBi
Cable:	30.5 cm (12 in) RG58/U plenum cable
Tipo de conector	N Hembra
VSWR a través de la Band:	<1.35:1
Dimensiones:	Altura: los 50cm (20in); Diámetro (base del montaje): 3,2 centímetros (1,25 adentro)
Peso:	230 g (8 oz)
Contenidos del paquete	Antena, Soporte de montaje, Instrucciones de instalación

Ejemplo de Funcionamiento



1) Servidor de archivos
2) Concentrador
3) Puntos de acceso
4) Adaptador inalámbrico PCMCIA
5) Laptop / notebook
6) Adaptador inalámbrico PCI
7) Adaptador inalámbrico externo USB
8) Print server puerto paralelo o USB
9) Impresora
10) PDA / Handheld PC y 11) Tablet PC



1) Equipo con tarjeta de red para cableado estructurado
2) Concentradores para cableado estructurado con puertos disponibles
3) Extensión de Punto de Acceso para redes inalámbricas
4) Equipo de impresión sin tarjeta de red (solo puerto paralelo)
5) Punto de Acceso especializado (puerto paralelo) o punto de acceso inalámbrico USB
6) Equipo de escritorio con tarjeta inalámbrica PCI
7) Equipo con acceso inalámbrico USB (externo)

V. 4. Instalación y Configuración Básica de una Red Inalámbrica

V. 4. 1. Consideraciones de diseño en la WLAN

Este apartado contiene instrucciones detalladas diseñadas para ayudar a poner el sistema inalámbrico en funcionamiento.

El diseño general inalámbrico y los valores de configuración predeterminados facilitan la instalación y gestión rápidos. Sin embargo, la configuración requiere de conocimientos acerca del uso y empleo de equipos en telecomunicaciones ejemplo switches, distribuidores, puentes y otros dispositivos de red.

Considero que las personas que instalan, configuran y gestionan el Access Point cuentan con experiencia en las siguientes áreas:

- Protocolos de comunicación de datos.
- Seguridad
- Redes IP.
- Comunicaciones en áreas amplias.

Se recomienda contar con experiencia en la configuración de normas de direccionamiento, descarga de imágenes de software, configuración de dispositivos de red a través de lineas seriales o Telnet, y en la gestión de dispositivos basados en SNMP.

La conexión de una red de área local inalámbrica (WLAN) es relativamente fácil con equipos Wi-Fi estándar. Con unos cuantos ajustes simples, se puede configurar un portátil para compartir datos o presentaciones a través del punto de acceso de otra red.

Para un óptimo desempeño de la red inalámbrica se debe planear y contemplar diversos aspectos, entre los cuales menciono a continuación.

1) Alcance y participantes: Los sitios populares para los proyectos WLAN en la facultad incluyen, laboratorios, instalaciones administrativas y la biblioteca. Es de vital importancia obtener un buen ejemplo de cada ubicación en la cual se tiene planes de instalar la red inalámbrica. Las interacciones con objetos, paredes, metales, e incluso la gente, afectan a la propagación de la energía. Los objetos sólidos bloquean las señales de infrarrojos, esto impone limites adicionales. La mayor parte de los sistemas de redes inalámbricas usan RF porque pueden penetrar la mayor parte de lugares cerrados y obstáculos. El rango de cobertura de una Lan inalámbrica típica va de 30m. a 100m. Planificar un ejemplo realista, dependiendo del alcance, el tamaño de campo y la base de usuarios para obtener resultados que sean aplicables a una población más extensa.

2) Zonas: Planear las zonas inalámbricas que utilizarán los participantes (salas de conferencias, áreas comunes, cafeterías, oficinas, etc.), y definir el cableado LAN que se tiene en esas áreas. El punto de acceso está físicamente conectado a la LAN. Se debe trabajar de cerca con el grupo de instalaciones para incorporar la tecnología inalámbrica de manera de minimizar el trabajo mientras la WLAN se expande.

3) Entrenamiento: El éxito de la implementación se sustenta en el buen entrenamiento con que cuentan los participantes y el personal de soporte (help desk), y en la rápida respuesta a las solicitudes de ayuda por parte de su grupo de apoyo. Se debe comenzar pronto a documentar sobre cómo los usuarios deben iniciarse, cómo utilizar la tecnología, y como obtener soporte y preparar a los entrenadores y sobre las preguntas que se hacen frecuentemente para el despliegue, y entrenar detalladamente al grupo de IT y soporte técnico sobre la nueva tecnología.

4) Rendimiento: Depende de la puesta a punto de los productos así como del número de usuarios, de los factores de propagación (cobertura, diversos caminos de propagación), y del tipo de sistema inalámbrico utilizado. Igualmente depende del retardo y de los cuellos de botella de la parte cableada de la red en caso de que se opte por una red híbrida. Para la más comercial de las redes inalámbricas los datos que se tienen hablan de un rango de 1.6 Mbps. Estas proporcionan suficiente rendimiento para las aplicaciones más comunes de una LAN, incluyendo correo electrónico, acceso a periféricos compartidos, acceso a Internet, y acceso a bases de datos y aplicaciones multiusuario.

5) Integridad y fiabilidad: Estas tecnologías para redes inalámbricas se han probado durante más de 50 años en sistemas comerciales y militares. Aunque las interferencias de radio pueden degradar el rendimiento éstas son raras en el lugar de trabajo. Los robustos diseños de las tecnologías para LAN inalámbricas y la limitada distancia que recorren las señales, proporcionan conexiones que son mucho más robustas que las conexiones de teléfonos móviles y proporcionan integridad de datos de igual manera o mejor que una red cableada.

6) Otros factores que intervienen en la potencia de la señal:

- Atenuación y distorsión de atenuación
- Pérdidas en el espacio abierto
- Ruido
- Absorción atmosférica
- Multicamino
- Refracción
- Ruido térmico

V. 4. 2. Estándar Wi- Fi

Una red de área local (WLAN) usa la tecnología de radio frecuencia (RF) para transmitir y recibir datos, y está fundamentada en las especificaciones del estándar 802.11.b. Este estándar tuvo su origen a partir del el estándar 802.11, desarrollado en 1997 por la IEEE, el cual permitía velocidades de transmisión de datos hasta 2 Mbps. Con el tiempo, el estándar ha sido mejorado y las actualizaciones adicionadas al estándar son conocidas como 802.11b y g, convirtiéndose en el estándar dominante de las WLAN, (conocido también como Wi-Fi), que soporta velocidades hasta 11 Mbps o 54 Mbps en la banda de 2.4 GHz, y permite usar 14 canales dentro de los 2.4 GHz. Las especificaciones del 802.11b fueron ratificadas por la IEEE en Julio de 1999 y opera en radio frecuencias con un ancho de banda de 2.4 a 2.497 GHz. El método de modulación seleccionado por el estándar 802.11b es conocido como una secuencia directa del espectro disperso (DSSS), el cual permite velocidades de transmisión a 11Mbps.

- **Tecnología Empleada**

La tecnología que se sugiere que se emplee en la WLAN es la tecnología de espectro disperso (Spread Spectrum), la cual proveerá comunicaciones seguras y confiable, además es la empleada por la mayoría de sistemas inalámbricos.

Microsoft de acuerdo a una investigación de mercado señala que los dispositivos con el estándar Wifi. Microsoft considera actualmente que es la solución más sólida y prometedora que se puede aplicar a múltiples entornos.

- **Comparación de las tecnologías de las redes LAN inalámbricas**

Actualmente, destaca la implementación de dos soluciones LAN inalámbricas en el mundo. Se trata de los estándares IEEE 802.11, principalmente 802.11b y g, y la solución propuesta por el grupo de trabajo HomeRF. Ambas soluciones no son interoperables entre sí ni con otras soluciones de redes LAN inalámbricas. Mientras que HomeRF está diseñado exclusivamente para el entorno doméstico, 802.11b se está implementando en hogares, en la pequeña y mediana empresa, en grandes organizaciones y en un número cada vez mayor de zonas activas de redes inalámbricas públicas. Algunos de los principales distribuidores de portátiles los equipa o tiene previsto equiparlos con tarjetas NIC 802.11b internas.

Comparación de los estándares tecnológicos de LAN inalámbrica (WLAN)

	54 Mbps	11 Mbps	54 Mbps
	5 GHz	2,4 GHz	2,4 GHz
	25 a 75 pies	Más de 150 pies	100 a 150 pies
	Incompatible con 802.11b o 802.11g	802.11g	802.11b
	Compatible con puntos de conexión inalámbrica 802.11a Disponibilidad limitada	Compatible con puntos de conexión inalámbrica 802.11b Máxima disponibilidad	Compatible con puntos de conexión inalámbrica 802.11b y 802.11g Disponibilidad normal
	Teléfonos inalámbricos a 5 GHz	Hornos microondas, teléfonos inalámbricos a 2,4 GHz, Bluetooth*	Hornos microondas, teléfonos inalámbricos a 2,4 GHz

	802.11b	802.11a	802.11g
Popularidad			
Velocidad	11 Mbps	54 Mbps	54 Mbps
Costo Relativo	$		
Frecuencia	2,4 GHz	5 GHz	2,4 GHz
Rango			
Acceso Público		X	
Compatibilidad	OK	OK	OK

Figura V-2
Cuadro comparativo de tecnologías (a, b y g)

V.4.3. Diseño de la WLAN

La conexión de una red de área local inalámbrica (WLAN) es relativamente fácil con equipos Wi-Fi (estándar de Fidelidad Inalámbrica). Con unos cuantos ajustes simples, se puede configurar un portátil para compartir datos o presentaciones a través del punto de acceso de otra red, por lo que la productividad se amplía más allá de la instalación principal.

A continuación se indicarán los puntos a abordar para la configuración de la red inalámbrica:

- Instalación y configuración del Access Point
- Instalación de tarjetas inalámbricas y configuración de los dispositivos inalámbricos (PDAS, laptops, handhelds)
- Configuración del cifrado WEP (Confidencialidad equivalente al cable) o cifrado WPA (Acceso protegido inalámbrico) y demostración del cambio de la clave
- Confirmación del acceso a Internet compartido en los dispositivos inalámbricos, si hay disponible una conexión Ethernet

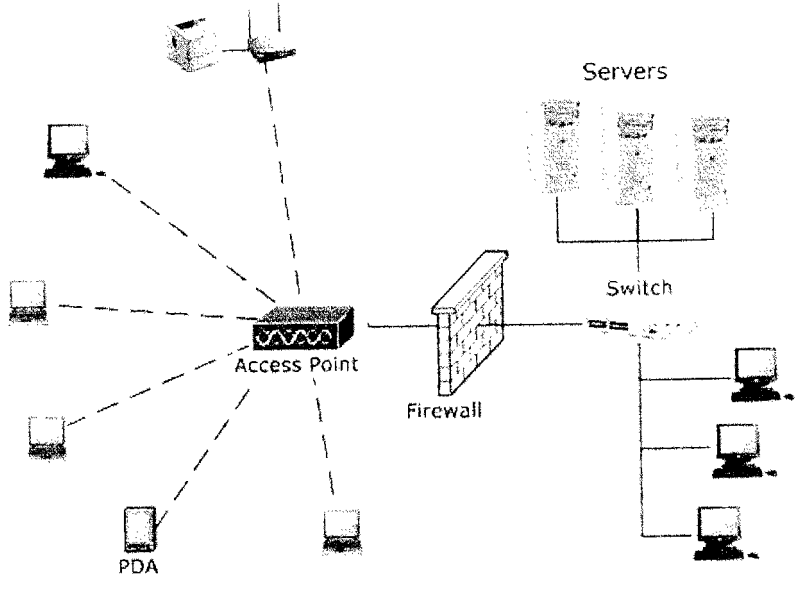


Figura V-3
WLAN

1) Consideraciones para la Instalación del Access Point

Configuración de un punto de acceso

Si se decide configurar el dispositivo inalámbrico, hay algunas acciones que se deben realizar cuando se configure el Access Point o Punto de Acceso que pueden ayudar a obtener el máximo rendimiento de la red inalámbrica.

Centrado del Access Point

- Se debe colocar el Access Point inalámbrico cerca del centro de la red.
- Se recomienda montar el Access Point en la posición más alta posible de la instalación.
- Si la red tiene que cubrir dos pisos, es posible que se necesite un Access Point distinto para cada uno.

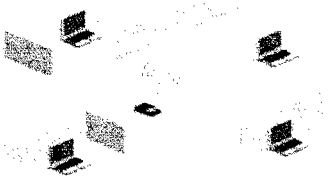


Figura V-4

Reducción de las Interferencias

- Colocar el Access Point / punto de acceso de banda ancha alejado de ordenadores, televisores, hornos microondas y teléfonos inalámbricos.
- Los productos inalámbricos en su mayoría funcionan a 2,4 GHz, la misma frecuencia que muchos dispositivos pequeños.

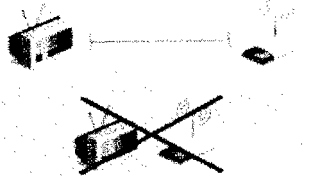


Figura V-5

Conexión del Access Point

- Se debe utilizar un cable Ethernet Cat-5 si así lo requiere para conectar el módem DSL o por cable al puerto WAN situado en la parte posterior del Access Point.
- El punto de acceso también se puede conectar a una red de área local con un cable Ethernet.

Figura V-6

2) Instalación de una tarjeta de red

Para transmitir datos a una red inalámbrica, el ordenador portátil o de sobremesa necesitará una tarjeta de red de PC. Las tarjetas de red de PC están disponibles en tres formatos:

- Interno o (Tarjetas Mini-PCI). Una tarjeta que está integrada en el portátil. También se denomina tarjeta Mini-PCI.
- Externo. Una tarjeta de red de PC independiente que se tiene que conectar a la ranura para tarjetas para PC del portátil (normalmente está situada en la parte lateral de un portátil)
- USB. Dispositivo independiente que se puede conectar en el puerto USB de un ordenador de sobremesa.

En caso de que se haya solicitado una tarjeta para PC o mini-PCI con el nuevo portátil, el software y los controladores necesarios ya deben estar instalados. Si no se está seguro, se recomienda consultar la guía del usuario del portátil o la guía de compra del fabricante.

Si se tiene un modelo antiguo, puede que se tenga que instalar las utilidades del Administrador de cliente adecuadas del CD-ROM .

Si la tarjeta para PC y los controladores están instalados correctamente, deben aparecer en la carpeta Adaptadores de red que se encuentra en Panel de control del portátil. Si no es así, se deberá consultar la guía de resolución de problemas de la guía del usuario de la tarjeta del fabricante.

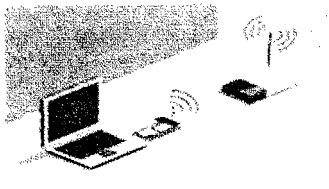


Figura V-7

Configuración del Ordenador

Una vez instalado todo el hardware de red inalámbrica, se tendrá que crear un perfil de configuración o un identificador único para acceder a la red. Esto se puede realizar mediante el software Administrador de cliente del fabricante, instalado en el portátil.

Sistemas Adicionales

Un único Access Point puede admitir hasta 30 usuarios inalámbricos dependiendo del fabricante así como el modelo de Access Point que se elija. (El alcance, la velocidad y el número de usuarios varían según el entorno y otros factores.) La conexión de ordenadores portátiles o de sobremesa adicionales a esta red inalámbrica no requiere la compra de Access Points de banda ancha adicionales. Sin embargo, cada sistema adicional precisa su propia tarjeta de red.

Los puntos de acceso se pueden enlazar entre sí para ampliar la capacidad de una red inalámbrica. Cada sistema adicional precisa su propia tarjeta de red de PC. (El alcance, la velocidad y el número de usuarios varían según el entorno y otros factores.) El punto de acceso ofrece opciones de seguridad mejorada e itinerancia. Itinerancia es un término que se utiliza para describir el modo en que un portátil cambia de un punto de acceso a otro cuando el usuario se mueve en un entorno físico distinto. Esto significa que no importa dónde se encuentre el usuario, la conexión inalámbrica siempre se establecerá con el punto de acceso más próximo para obtener una conectividad completa.

Seguridad Inalámbrica

Un elemento esencial a tener en cuenta en este tipo de redes al utilizarse la radio, es la encriptación. En general se utiliza WEP (Wired Equivalent Privacy), que es un mecanismo de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso.

La solución inalámbrica en dispositivos 802.11b/g de la mayoría de los fabricantes cumple las estrictas normas del sector. La clave de acceso estándar es de 40 bits, pero existe otra opcional de 128 bits, y se asigna de forma estática o manual (no dinámica), tanto para los clientes, que comparten todos el mismo conjunto de cuatro claves predeterminadas, como para los puntos de acceso a la red, lo que genera algunas dudas sobre su eficacia. WEP utiliza un esquema de cifrado simétrico en el que la misma clave y algoritmo se utilizan tanto para el cifrado de los datos como para su descifrado. Una combinación de las soluciones de seguridad SSID (identificador de conjunto de servicios), MAC (control de acceso a medios) y WEP (confidencialidad equivalente al cable) pueden proporcionar seguridad para la red. Para redes más grandes, una red privada virtual (VPN) permite proporcionar una seguridad más escalable y ofrecer a los usuarios un trayecto dedicado y seguro a través de otras redes.

Distribución de la WLAN

Una vez conocida la tecnología existente de una red WLAN, desempeño, características y velocidad de transmisión, se presenta la fase de diseño en la aplicación de la tecnología WLAN. Esta fase de incluye la inspección del terreno donde se va ha hacer la aplicación, la topología de red a implementar y la selección de los equipos.

La conexión de una red de área local inalámbrica (WLAN) es relativamente fácil con equipos Wi-Fi estándar. Con unos cuantos ajustes simples, se puede configurar un portátil para compartir datos o presentaciones a través del punto de acceso de otra red. Cuando se afronta este tipo de instalaciones debemos pensar bien la infraestructura.

La instalación ideal: La sencillez es un buen principio en cualquier instalación de red, bien sea cableada o inalámbrica. A fin de evitar instalaciones complejas en las que la configuración inicial y el mantenimiento puedan estar llena de variables, lo más conveniente es empezar por bases sólidas y buscar un sistema robusto. En el caso de edificaciones de la facultad, la configuración ideal sería un sistema mixto de cable e inalámbrico. El inalámbrico nos permitiría tener cobertura de red en cualquier lugar, pero el cable ayudará a una disposición homogénea de puntos de acceso.

Distribución Ideal Básica

Aquí podemos ver la distribución ideal básica (figura V-8), en la cual hay un switch en la planta baja del que sale un cable que va a parar a los puntos de acceso de cada planta. Los Puntos de Acceso de cada planta dan cobertura inalámbrica a la misma y se ven ayudados por repetidores en las áreas más alejadas. Plantas de gran superficie como una Biblioteca (Punto de Acceso mas un Repetidor)

Aquí podemos ver la distribución ideal básica, en la cual hay un switch en la planta baja del que sale un cable que va a parar a los Puntos de Acceso de cada Planta.

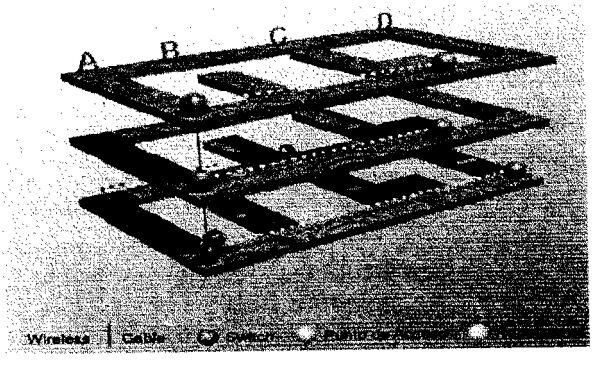


Figura V-8

En muchos casos la planta es de gran superficie o tiene formas o estructuras que no permiten que la estructura basada en un punto de acceso y un repetidor sea suficiente. En esos casos, podemos añadir más repetidores, teniendo en cuenta que un repetidor no puede hacer de "repetidor de repetidor", es decir, un repetidor repetirá la señal de un Punto de Acceso pero no la de otro repetido, así que no podemos alargar la cobertura indefinidamente con repetidores. De hecho, en la planta baja ya hemos puesto dos repetidores, podríamos hacer lo mismo en las dos plantas superiores. De todos modos, es posible que la cobertura en las habitaciones de los puntos B y D la cobertura fuese escasa. Como ya hemos comentado que un repetidor solo puede repetir señales de un Punto de Acceso, de nada serviría poner uno en D ya que no encontraría la señal del Punto de Acceso y tampoco podría repetir la señal del repetidor que tiene cerca.

Cobertura Homogénea en cada planta

Varios puntos de acceso con repetidores. En esta nueva estructura se va a necesitar poner varios PA por planta, y cada uno de ellos podrá tener uno o más repetidores. Para ello, necesitaremos poner en cada planta, lugar del PA inicial, un pequeño Switch, de él podrán salir tantos puntos de acceso como queramos.

Aquí podemos ver la distribución ideal básica, en la cual hay un switch en la planta baja del que sale un cable que va a parar a los puntos de acceso de cada planta. Los Puntos de Acceso de cada planta dan cobertura inalámbrica a la misma y se ven ayudados por repetidores en las áreas más alejadas.

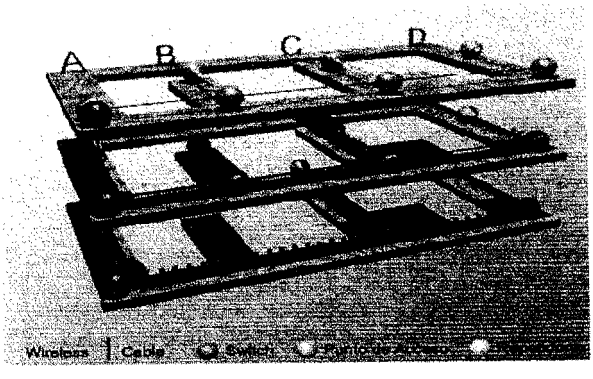


Figura V-9

Cobertura 100% Wireless

Aquí podemos ver cómo hemos sustituido todo el cableado de las plantas por combinaciones de Puntos de Acceso más un Adaptador. La complejidad y el costo son mayores que la instalación anterior, pero evitamos el cableado. Este es un caso que se da en ocasiones, buscando el extremo de la eliminación total de cables, en este caso el coste de la infraestructura sube notablemente, así como su complejidad.

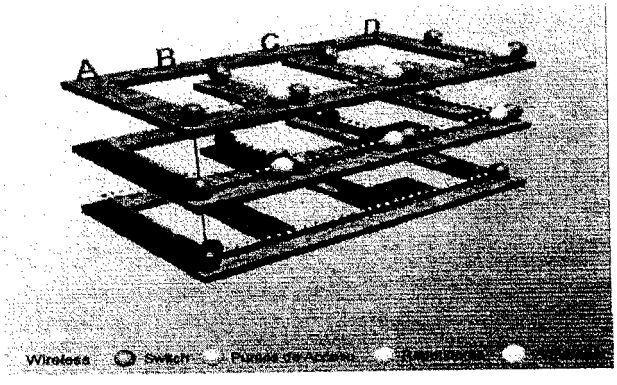


Figura V-10

Las redes inalámbricas posibilitan extender de forma económica y sencilla el acceso a Internet a áreas donde no existe la infraestructura necesaria. Los casos más comunes son las pequeñas poblaciones o urbanizaciones fuera de los núcleos urbanos.

Las ventajas son, además del acceso en sí, la posibilidad de repartir costes resultando en unas cuotas de acceso especialmente reducidas. Si bien no existen dos casos idénticos, si se dan unas condiciones comunes que pueden definir una instalación de redes inalámbricas, estas suelen ser:

- Administración segura con control de qué usuarios tienen acceso y qué cantidad de ancho de banda debe disponer cada usuario.
- Sistema de validación de usuarios que acceden a la red inalámbrica.
- Fácil instalación.
- Bajo mantenimiento.

Entrando más en detalle, también se presentan necesidades concretas como:

- Poder dar servicio a un gran número de usuarios.
- Poder dar servicio a una densidad muy alta de usuarios.

Aquí podemos ver varias infraestructuras de red inalámbrica comunitarias en las cuales transportaríamos una conexión de Internet a otras áreas.

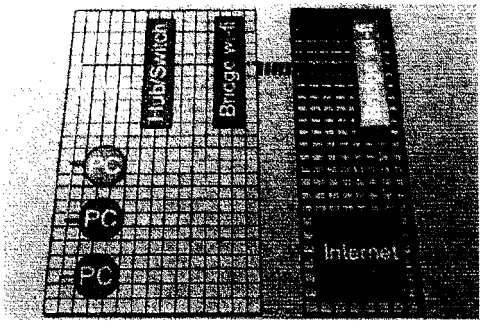


Figura V-11

Método Mixto para suministrar Acceso a Internet

La conexión a Internet llega de forma inalámbrica hasta el edificio y se reparte desde un Hub/Switch por Ethernet.

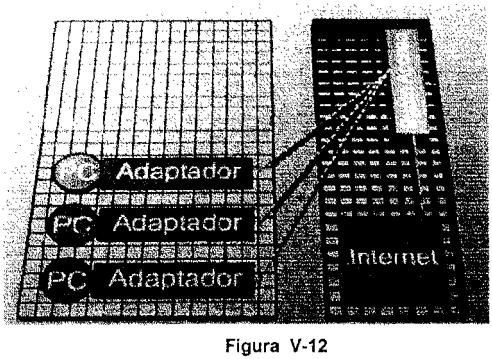


Figura V-12
Cada uno de las PC's recibe su propia conexión inalámbrica a Internet.

La conexión a Internet llega inalámbricamente hasta el edificio y se reparte desde un Hub/Switch a Puntos de acceso situados en cada planta. Los puntos de acceso suministran conexión inalámbrica a las PC's de cada planta.

Hay dos elementos que definen el material que necesitaremos para crear una red inalámbrica.

I. Las bases (Puntos de acceso o Bridges)

Los dispositivos que vertebran de forma centralizada la red inalámbrica generalmente van conectados a hub/switch (puede ser el hub/switch, por ejemplo un router ADSL), en ellos se define el tipo de red inalámbrica a realizar y además gestiona la administración de la misma.

II. Los dispositivos cliente (los adaptadores) estos son los dispositivos que permiten a un individuo o grupo de individuos conectarse a la red inalámbrica.

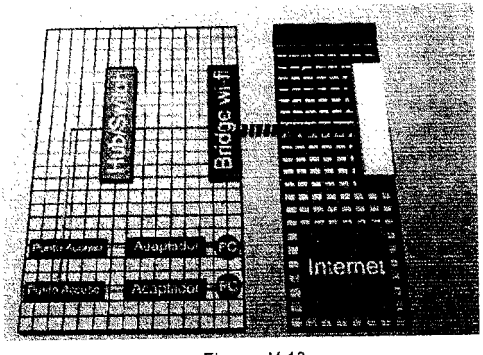


Figura V-13

La comunicación entre la señal de Internet y el edificio es obviamente en exterior. Antes de que existiese la oferta actual de dispositivos para exteriores, era una opción muy común adaptar dispositivos de interiores para un uso en exteriores.

Otra desventaja importante en el uso de sistemas para interiores en redes comunitarias es que al estar pensados para pequeños grupos no disponen del software necesario de administración de usuarios (autentificación y control del ancho de banda asignado) y obligan a la compra e instalación de una PC o periférico adicional que realice estas tareas suponiendo un importante sobreprecio y una vuelta de tuerca más en la complejidad de instalación y mantenimiento. Ante la gran demanda de redes inalámbricas, recientemente han aparecido en el mercado nuevos productos específicos para este fin.

Entornos donde Utilizar una Red Inalámbrica

Se ha comentado reiteradas veces en este capitulo la gran ventaja que supone las redes inalámbricas, al no necesitar cableado, frente a redes convencionales sobre par trenzado, cable coaxial o fibra óptica. La fácil instalación y la flexibilidad que ofrecen estas redes las hacen imprescindibles en ciertos entornos como:

- **Entornos difíciles de cablear**

  Son muchas las situaciones en las que el tendido de cables no es posible o resulta complicado. Edificios históricos o antiguos, áreas abiertas o calles muy concurridas impiden o elevan notablemente el coste de instalación de una red.

- **Equipos de trabajo provisionales**

  Zonas como exposiciones, salones de conferencias u otros emplazamientos que exigen la instalación de oficinas provisionales en donde es conveniente el establecimiento de redes locales temporales que se retiran una vez finalizado su cometido.

- **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 de área local cableadas situadas en dos edificios distintos.

- **Posibilidad de acceso a la información en tiempo real**

  La comunidad universitaria podrá acceder a la información en tiempo real.

- **Entornos que varían con frecuencia**

  Salas de exposición, salas de reunión, establecimientos de venta al público o fábricas en las que el espacio de trabajo se modifica con frecuencia.

- **Ampliaciones de redes Ethernet**

  Los administradores de redes de entornos dinámicos pueden reducir, gracias al empleo de una red local inalámbrica, los gastos generales originados por los traslados, ampliaciones de redes u otras modificaciones en sus sistemas.

- **Backup para redes de cable**

  Los administradores de redes utilizan redes locales inalámbricas como sistema de seguridad en aplicaciones críticas ejecutadas en redes de cable.

- **Instalaciones de formación / educación**

  Las salas de formación de las empresas y los alumnos de escuelas y universidades pueden recurrir a la conectividad inalámbrica para acceder e intercambiar información y aprender, sin la complejidad de cablear múltiples puestos para los alumnos.

  Podría resumir las ventajas de este tipo de sistemas en los siguiente puntos:

- Los dispositivos inalámbricos están industrialmente certificado para exteriores, soportan condiciones de temperatura y humedad sin requerir mantenimiento.
- Los dispositivos se pueden instalar directamente en el cualquier lugar óptimo ya que se puede encontrar a distancias de hasta 100 metros de la conexión principal de red/Internet.
- Existen Access Point en el que la antena va junto al dispositivo o puede estar aparte, las pérdidas llegan a ser mínimas y la cobertura máxima.
- En la propuesta sugerida el dispositivo utiliza dos CPU's, una para las conexiones inalámbricas y otra para la administración de las mismas, es decir, el equipo siempre se puede administrar o incluso re-inicializar.

- El dispositivo integra todas las herramientas necesarias para poder controlar que usuarios pueden acceder a la red inalámbrica y que velocidades de conexión cada usuario puede obtener.

  Actualmente existen Access Point avanzados que aportan además otras interesantes prestaciones tales como:

- La posibilidad de que un dispositivo dependiendo del fabricante se desdoble simultáneamente como bridge y punto de acceso, de modo que se puede añadir de forma sencilla y directa cobertura a nuevas áreas geográficas.
- La posibilidad de que un dispositivo se desenvuelva simultáneamente como bridge y repetidor, de modo que podamos dar acceso a "islas" de usuarios a distancias largas.

La potencia y versatilidad de las redes Wi-Fi nos permite ofrecer servicios de datos, voz, vídeo vigilancia, televisión, etc., en zonas donde por razones demográficas o geográficas no disponen de cableado o de banda ancha. El objetivo común de ofrecer servicios Wi-Fi es obtener una conexión a Internet con calidad similar o superior a banda ancha, para conseguirlo se barajan tres parámetros fundamentales:

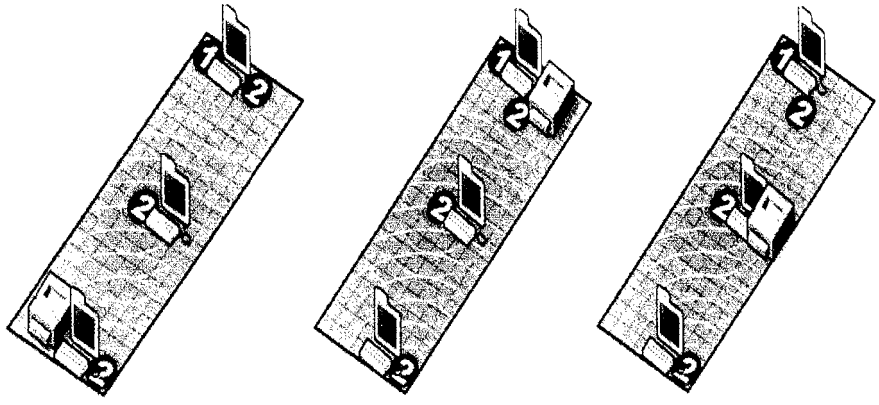
1) Cómo se conecta al Exterior-Internet.
2) Cómo se reparte la señal dentro del recinto.
3) Cómo conectan los usuarios al servicio.

V. 5. Propuestas de Diseño

Típica instalación inalámbrica opción #1 : costo bajo

(1) Acceso a Internet por módem o switch / router conectado a PC (por RJ-45 o por USB) con Windows 98SE/ME/2000/XP compartiéndolo mediante ICS

(2) Adaptador Wi-Fi PCI, USB, PCMCIA (PC Card) o Compact Flash II



Las PC´s tienen acceso a Internet por un módem o switch conectado (1) , y se comunican mediante adaptadores Wi-Fi (2) empleando la topología ad hoc o punto a punto

- **Comentarios**

En esta instalación no hay punto de acceso, la red funciona en modo Peer-to-Peer.

- **Inconvenientes**

Menos prestaciones ya que todo el tráfico de red pasa por todos los adaptadores. Otro inconveniente notable es que para acceder a Internet o a la impresora, los ordenadores que hacen de servidores de esos dispositivos deberán estar en funcionamiento.

- **Ventajas**

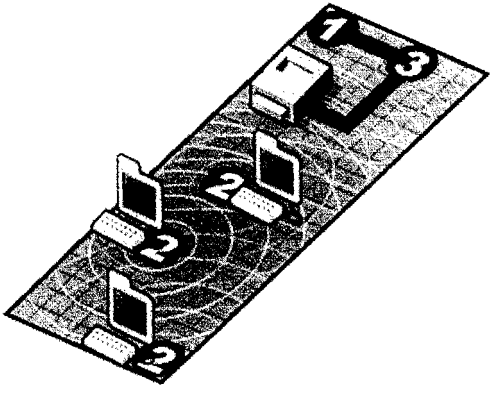
El ahorro de un punto de acceso y de un hub, switch o router.

Instalación inalámbrica opción #2 : costo medio

(1) Acceso a Internet por módem o router / switch conectado un Wi-Fi Access Point.

(2) PC's con adaptador Wi-Fi PCI, USB, PCMCIA (PC Card) o Compact Flash II

(3) Wi-Fi Punto de acceso, un dispositivo que hace de punto de acceso Wireless, haciendo que el módem /router / switch sea accesible inalámbricamente por los PC's.



Se conecta el Punto de Acceso (3) al puerto libre del switch (1) y se instala un adaptador wi-fi (2) a la PC o PC Portátil.

- **Comentarios**

En esta instalación si hay punto de acceso, la red funciona en modo centralizado.

- **Inconvenientes**

Si desea compartir la impresora, esta debe estar configurada en modo compartir, en una de las PCs, y para poder utilizarla, esa PC debe estar en funcionamiento.

- **Ventajas**

Buena velocidad y tráfico de red bien gestionado, acceso permanente a la conexión de Internet por todos los miembros de la red.

Con esto podemos pasar la instalación a Wireless y usar la PC o PC Portátil desde donde sea más cómodo. Esta configuración requiere que la línea a Internet esté conectada mediante un router.

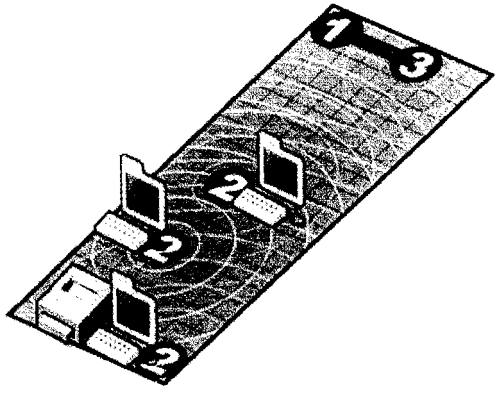
El Acceso a Internet se obtiene por módem o router conectado a PC (por RJ-45 o por USB) con Windows 98SE/ME/2000/XP compartiéndolo mediante ICS.

Instalación inalámbrica opción #3 : costo medio

(1) Acceso a Internet por módem o router conectado a un Wi-Fi Gateway. Acceso a la impresora mediante el mismo Wi-Fi Gateway.

(2) PC's con adaptador Wi-Fi PCI, USB, PCMCIA (PC Card) o Compact Flash II.

(3) Wi-Fi Gateway, que es un dispositivo que hace de punto de acceso inalámbrico, de Gateway para Internet y de servidor para impresora mediante una conexión LPT (paralelo) estándar.



- **Comentarios**

En esta instalación si hay punto de acceso, la red funciona en modo centralizado haciéndolo de punto de acceso, de switch, de servidor de acceso a Internet y de servidor de impresora.

- **Inconvenientes**

Si desea compartir la impresora, esta debe estar físicamente cerca de la conexión a Internet ya que ambos (módem / router de conexión a Internet e impresora) van conectador por cable al Wi-Fi Gateway.

- **Ventajas**

Buena velocidad y tráfico de red bien gestionado, acceso permanente a la impresora y a la conexión de Internet por todos los miembros de la red.

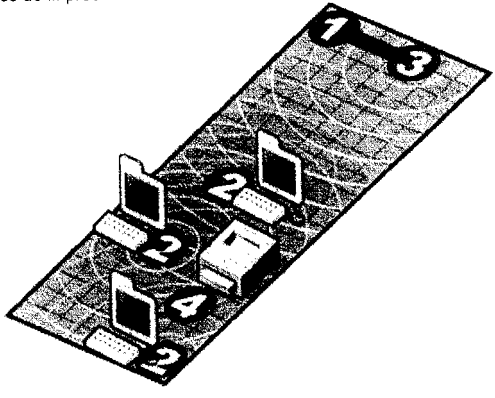
Típica instalación inalámbrica opción #4:costo medio / alto

(1) Acceso a Internet por módem / router/ switch conectado a un Access Point.

(2) PC´s con adaptador Wi-Fi PCI, USB, PCMCIA (PC Card) o Compact Flash II.

(3) Punto de Acceso Wi-Fi o AP.

(4) Servidor Wireless de impresora.



- **Comentarios**

En esta instalación la red funciona en modo centralizado sobre el punto de acceso Wireless, y el servidor wireless de impresora.

- **Inconvenientes**

Ninguno.

- **Ventajas**

Buena velocidad y tráfico de red bien gestionado, acceso permanente a la impresora y a la conexión de Internet por todos los miembros de la red. Tanto la impresora como la conexión a Internet puede estar en cualquier punto del local.

Ubicación

Los nodos de la red de enlace tienen que estar repartidos estratégicamente. Una mala ubicación de estos nodos puede hacer que el rendimiento de la red baje de manera crítica. La distancia entre nodos ha de ser la menor posible. Los cambios climáticos pueden hacer variar la potencia de la señal y por consiguiente mermar la calidad del enlace. Los nodos de la red de enlace no solo han de tener visión directa con sus nodos adyacentes, además tienen que estar ubicados en una zona donde los nodos de acceso también tengan buena cobertura.

Básicamente la ubicación física del nodo de enlace ha de cumplir estor requisitos:

- Máxima altura posible.
- Ubicación en edificio municipal o con fácil acceso en cualquier momento
- Visión directa entre nodos adyacentes.
- Poca distancia entre nodos adyacentes.
- Cobertura máxima a los nodos de acceso.

No siempre podremos poner los nodos donde nosotros queramos. Es posible que tras determinar una posible ubicación como ideal, nos encontremos que por cualquier motivo no podamos hacer la instalación. Siempre tendremos que tener en cuenta estos contratiempos y tener preparadas ubicaciones alternativas. A continuación plantearé algunas de las posibles ubicaciones óptimas donde colocar los nodos de enlace en las comunidades implicadas.

V. 6. Servicios de la Red Inalámbrica

En las áreas administrativas, donde se concentra la responsabilidad de la administración de los estudiantes, registros, nómina de profesores y todo el material de soporte para la facultad, hay ciertos elementos que pueden ser de suma practicidad e incluso de total innovación.

Por otro lado el entorno de la facultad puede ser capitalizado traspasando el lugar físico universitario, ofreciendo tanto a posibles estudiantes, a su matrícula, personal administrativo y docente diferentes opciones tecnológicas como:

- Portal universitario: Página web.
- Internet.
- Correo electrónico vitalicio a estudiantes y graduados.
- Asentamiento de calificaciones por parte de los profesores.
- Comercio electrónico: compra de libros, cursos y servicios en línea.

A continuación puntualizo algunos otros servicios que se ofrecen a través de la red inalámbrica:

- **Consultas de Catálogos de Biblioteca (material educativo e informativo) y revistas electrónicas.** Este servicio pone a disposición una colección constituida por la totalidad o una parte sustancial de la colección en formatos electrónicos y digitales, accesible por computadoras a través de las redes de la academia, y con la ayuda de motores de búsqueda que facilitan la recuperación de información pertinente, como una alternativa más de consulta al acervo de la biblioteca o como complemento del material impreso.
- **Acceso a correo electrónico.** Los profesores, los alumnos y el personal administrativo tendrán la posibilidad de acceder a sus mensajes dentro y fuera de la facultad.
- **Aprendizaje Cooperativo en línea.** Implica la sustitución del control tradicional del aula presencial, por la responsabilidad, la comunicación y el compromiso de todos los participantes. La ventaja principal de la educación en línea, es que el estudiante no sale de su entorno para formarse. Es entonces una distancia a reducir, a eliminar: la distancia a la que alude esta modalidad, no es

fundamentalmente la que existe, físicamente, entre el profesor y los alumnos, sino la que hay que eliminar, entre quien aprende y su experiencia real, concreta y cotidiana.

- **Foros de Discusión** Involucra una participación, que permitiría dar seguimiento directo a las intervenciones. La asistencia de fechas y horas de los foros se publican en el tablero de avisos del programa. Generalmente existen 2 tipos de foros, los sincrónicos (equivalentes al chat) y asincrónicos (los participantes aportan durante un período preestablecido, generalmente un día).
- **Servicios de publicación o tutorías.** Este servicio consiste en poner a disposición de los interesados, diversos documentos que puedan ser usados con fines académicos, aportados por los profesores.
- **Apoyo a procesos del departamento de Administración Escolar**. (Inscripciones, registro de passwords, actualización de datos, consultas al sistema Integral de Administración Escolar)
- **Educación a distancia.** La educación a distancia da una respuesta educativa a las necesidades de una sociedad diversificada en edad, actividad, nivel socioeconómico y lugar de residencia, mediante una enseñanza no presencial, pero flexible y abierta que utiliza al máximo las nuevas tecnologías. Enfocada a generar medios que faciliten la contribución entre personas, independiente del tiempo y el espacio físico en que ésta se realice. Son propicios para fomentar la participación en ambientes internacionales entre investigadores, docentes y estudiantes, entre otros.
- **Servicios en línea:** Revisión de calificaciones, inscripciones, evaluar el desempeño de los profesores, consultar horarios, planes de estudio, verificar la disponibilidad de eventos de carácter cultural, académico, científico o deportivo para la comunidad, transferencia de archivos.

VI. RESULTADOS ESPERADOS

VI.1. Beneficios

Los beneficios de esta propuesta involucran los siguientes puntos:

- **Una nueva Tecnologías de Información (IT)**, como lo son las redes de comunicaciones inalámbricas, permitirá a los estudiantes nuevas posibilidades para comunicarse accesando a datos e información, así como a diversos servicios (inscripciones, consultas de horarios, material educativo e informativo, correo electrónico, evaluación de servicios, consultas a la biblioteca), que puedan proveer y mejorar el ambiente de aprendizaje.

- **Ofrecer una gama de servicios y soluciones** en telecomunicaciones para la facultad, manteniéndola a la vanguardia tecnológica y le permita a sus estudiantes, profesores y personal administrativo, beneficiarse con nuevos servicios.

- **Útil en ciertas circunstancias geográficas.** A través de la tecnología inalámbrica Wi-Fi, se puede ofrecer conexión a la red de la facultad sin necesidad de estar conectado en un punto específico. La disponibilidad del servicio en una instalación, mantendrá una cobertura lo suficientemente adecuada, que cubra la zona de radio.

- **La implantación de redes inalámbricas con tecnología Wi-Fi**, es mucho más económica que otras opciones ya que un sólo punto de acceso puede dar servicio hasta a 128 usuarios o más, reduciendo los costos de equipamiento y operación así como los tiempos de instalación.

- **Contar con una conexión en tiempo real mediante dispositivos inalámbricos.** Muchos de los estudiantes que se desempeñan profesionalmente en alguna actividad requieren de servicios educativos, por lo que se facilitaría que la facultad se adapte a sus horarios, para no dejar de hacer sus actividades principales.

- **Reducir la brecha tecnológica** existente con el fin de hacer una gran y completa comunidad amplia, sin la existencia de alguna barrera, llámese tecnológica o humana.

- **Facilitar la ampliación de nuevos usuarios a la red**, sin necesidad de nuevos cables y que permita la organización de redes en sitios cambiantes o situaciones no estables (lugares de emergencia, congresos, sedes temporales, etc.).

- **Sencillez en la operación de una WLAN:**
  - ❑ Resistencia a la interferencia externa.
  - ❑ Facilidad en el mantenimiento y detección de fallas.
  - ❑ Buen nivel de integración con redes cableadas existentes.
  - ❑ Mínima capacitación para la instalación.
  - ❑ Red fácil de escalar en un futuro.

VI.2. Limitaciones

Las limitantes que se vislumbran en este proyecto inalámbrico se encuentran en los siguientes puntos:

- En la actualidad se requiere de infraestructura tecnológica conveniente, con el propósito de proveer y ser capaz de dar este servicio
- Los costos de los equipos, dispositivos y de los enlaces respectivos, también son una limitante, esperando que con el tiempo, dichos costos bajen considerablemente, de tal forma, que estén accesibles para todos los estudiantes.
- Es necesario que exista voluntad y un apoyo conjunto del sector académico y administrativo de la facultad, que sumados a los apoyos otorgados por empresas privadas, puedan hacer que en un plazo inmediato, se pueda contar con una facultad inalámbrica.
- Una implementación Inalámbrica, obliga a tener en cuenta los costos de comunicaciones y los bajos rangos en la trasmisión de información.
- Problemas de seguridad. La mala configuración de un acceso inalámbrico es, desgraciadamente, una cosa muy común. Se enumeran tres vulnerabilidades diferentes: robo de sesión (que afecta sobre todo a nodos de acceso públicos y más aún si no se hace uso de WEP), ataques de hombre en el medio (donde el atacante se hace pasar por el punto de acceso al atacado y como cliente al punto de acceso real) y negación del servicio (perturbaciones voluntarias del tramo de frecuencias utilizado por la red). Podemos ver que el tema de la seguridad es todavía uno de los puntos débiles de las redes inalámbricas en el que habrá que invertir muchos esfuerzos.
- Otras
  - Potencia y distancias limitadas.
  - Velocidad de transmisión limitada.
  - Es una tecnología relativamente nueva en nuestro país.
  - Dependencia tecnológica en ciertos equipos de algunas marcas y fabricantes (ejemplo el fabricante Symbol)

VII. COSTO DEL PROYECTO

VII. 1. Estimaciones del Proyecto

La instalación de una LAN inalámbrica incluye los costos de infraestructura para los puntos de acceso, antenas y el software de administración y planeación. Los costos de infraestructura dependen fundamentalmente del número de puntos de acceso desplegados. El valor de los puntos de acceso oscila entre 200 y 800 dólares dependiendo el fabricante. El número de puntos de acceso dependerá de la cobertura requerida y del número y tipo de usuarios.

El área de cobertura es proporcional al cuadrado del rango de productos adquirido. Los adaptadores son requeridos para las plataformas estándar de ordenadores y su precio oscila entre 80 y 150 dólares. El costo de instalación y mantenimiento de una WLAN generalmente es más bajo que el costo de instalación y mantenimiento de una red cableada tradicional, por dos razones:

En primer lugar una red WLAN elimina directamente los costos de cableado y el trabajo asociado con la instalación y reparación.

En segundo lugar una red WLAN simplifica los cambios, desplazamientos y extensiones, por lo que se reducen los costos indirectos de los usuarios sin todo su equipo de trabajo y de administración.

VII. 1. 1. Costo de los Dispositivos para la Red

El modelo de red utilizado en el proyecto consiste básicamente en lo siguiente:

Dependiendo de la topografía del terreno y del diseño de la red inalámbrica, puede ser necesario incorporar valores de referencia de todos los componentes usados.

Cantidad	Descripción	Precio Unitario	Precio Total
1	3com Wireless Switch Manager	$ 4200 dlls	$ 4200 dlls
10	AP7250 802.11g Access Point	$ 769 dlls	$ 7690 dlls
10	3/4 Dual-Band Ceiling Mount Antenna	$ 119 dlls	$ 1190 dlls
1	Wireless LAN Switch WX120	$ 3299 dlls	$ 3299 dlls
3	Wireless LAN Switch Managed Access Point AP2750	$ 299 dlls	$ 897 dlls

Nota: Por concepto de instalación y mantenimiento el fabricante cobra 10% del valor del equipo

Costo Total **$ 17276 dlls***

* Se deberá actualizar de acuerdo al tipo de cambio en pesos a la fecha.

VII. 1. 2. Costo de los Servicios

La explotación de un servicio de ingreso a una red inalámbrica como la desplegada en el proyecto, requiere tomar en cuenta, además del monto de la inversión, otros elementos para lograr el éxito deseado.

Entre los factores importantes de considerar se pueden mencionar la depreciación de los equipos, los costos de mantenimiento, los costos operacionales, el enlace a Internet o a la red fija a la que se quiera integrar la red inalámbrica, etc.

En cuanto al costo de uso de espacios, es un elemento muy importante dependiendo de la topografía del terreno o de la topología de la red a desplegar. Los switches o inclusive los puntos de acceso dentro de una red inalámbrica requieren instalarse en espacios físicos que no necesariamente están acondicionados. Pueden no contar con energía eléctrica o con un nivel adecuado de seguridad y lo más usual es que se deba arrendar el espacio o inclusive tener que adquirir el terreno necesario para poder disponer del punto de irradiación necesario y desplegar adecuadamente la red inalámbrica.

VII. 1. 3. Costo de Mantenimiento

Como todo proyecto tecnológico, la red inalámbrica requiere tareas de revisión que garanticen un correcto funcionamiento durante el tiempo estipulado del servicio. En este tipo de redes hay dos tipos de mantenimiento: el equipamiento interno desplegado (antenas y Punto de Acceso).

En general, las instalaciones exteriores no requieren mayor mantenimiento, sobre todo si al inicio la instalación se hizo de buena manera. Lo que suele suceder es que se deba revisar la alineación de las antenas para lograr una buena señal, por lo que el costo asociado a este tipo de actividades es más bien a solicitud o necesidad y dependerá del valor de la mano de obra de quien lo realice. Se desechó el mantenimiento de los equipos que forman la red inalámbrica como un servicio dentro del proyecto. Debido al bajo valor de los componentes, en particular el punto remoto, fue mejor mantener algo de stock de los componentes y no pagar por un servicio que no se justificaba. En general, una red inalámbrica requiere, al igual que cualquier otra red, elementos de supervisión (monitoreo, estadísticas, sistema de autorización, etc.), servidores, sistemas de energía ininterrumpida, sistemas de almacenamiento, etc. Si éstos ameritan labores o contratos de mantenimiento, sus costos quedan sujetos a lo que ofrece el respectivo mercado.

VII. 1. 4. Costos a Considerar

- Costos en materiales de instalación.
- Costos de contratación de energía eléctrica al punto de acceso o repetidor.

VII. 1. 5. Costo Total del Proyecto

Costo de los Dispositivos para la Red

Cantidad	Descripción	Precio Unitario	Precio Total	Tipo de Cambio en Pesos $ 11.20	$ 11.80
1	3com Wireless Switch Manager	$ 4200 dlls	$ 4200 dlls	$ 47,040	$ 49,560
10	AP7250 802.11g Access Point	$ 769 dlls	$ 7690 dlls	$ 86,128	$ 9,074.2
10	3/4 Dual-Band Ceiling Mount Antenna	$ 119 dlls	$ 1190 dlls	$ 13,328	$ 14,042.2
1	Wireless LAN Switch WX120	$ 3299 dlls	$ 3299 dlls	$ 36,949	$ 38,928.2
3	Wireless LAN Switch Managed Access Point AP2750	$ 299 dlls	$ 897 dlls	$ 10,047	$ 10,584.2
		TOTAL	$ 17276 dlls	$193,491.2	$203,856.8

Costo Extra para la Instalación de la Red

Concepto	Precio Total
- **Materiales de Instalación**	$ 18,857
Canaletas	
Cinchos	
Cajas Protectoras	
Herramientas de uso común (pinzas, desarmador, cutter)	
- **Material opcional**	
Probador de Cable	
TOTAL	$ 18,857
COSTO TOTAL DEL PROYECTO	---------- $212,348.2** $ 222,713.8 **

** Se maneja un presupuesto con cierto margen de variación, debido a que se está utilizando un tipo de cambio estimado, considerando una posible fluctuación.

Costos Generados para el Fucionamiento de la Red

Energía. Por concepto de energía eléctrica se generarán gastos mensuales para el funcionamiento de los dispositivos que integrarán la red, los cuales se estimarán de acuerdo a las tarifas vigentes por consumo de energía generada por cada dispositivo.

Mantenimiento. El mantenimiento de los equipos se evaluará en un periodo anual estimándose en un 10% del valor del equipo.

Sueldo del personal de Redes. No se contratará personal, puesto que el personal responsable de la gestión y administración de la red de la Facultad, se considera apta y con los conocimientos necesarios para el funcionamiento de dicha red.

VIII. NORMATIVIDAD

VIII. 1. Políticas de Seguridad

Las políticas de seguridad son reglas electrónicamente programadas y almacenadas en equipos de seguridad para controlar áreas tales como los privilegios de acceso. Obviamente, las políticas de seguridad también consisten en reglamentaciones escritas o verbales que delimitan el funcionamiento de un centro de cómputo. Además, los centros de cómputo deben asignar a las personas responsables de implementar y administrar estas políticas, determinar el modo en que se informará a los usuarios acerca de las reglas y realizar los controles necesarios.

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que se confrontan hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos.

Política HW-01: Dispositivos inalámbricos de la red

Propósito: Definir las políticas relacionadas con la instalación de equipos inalámbricos a la red de la facultad y establecer los procedimientos para su instalación, administración y configuración. Algunas de las metas de esta política son:

1) Mantener la integridad y seguridad de la información y de la infraestructura de la red.
2) Evitar el mal uso de la red universitaria a través de sistemas y el robo de señales.
3) Establecer normas para la instalación de antenas externas para uso con equipos de red inalámbricos.
4) Prevenir la interferencia con otros usuarios que utilicen el mismo espectro de frecuencias.

Políticas: El mantenimiento de la seguridad e integridad de la red de la facultad requiere de medios adecuados para asegurar que solamente los usuarios autorizados puedan hacer uso de ella. Los dispositivos de red inalámbricos que utilizan la infraestructura de la red, deben cumplir con ciertos estándares para que solamente usuarios autorizados y autentificados se puedan conectar y que dichos dispositivos no queden expuestos a ser utilizados personas no ajenas.

1) Se entiende por un dispositivo inalámbrico de red un equipo que permite acceder de forma inalámbrica a la red universitaria. En adelante se hará referencia a estos con el nombre DIR (Dispositivo Inalámbrico de Red).
2) Los DIR pueden ser de varios tipos:

   a) Punto de acceso (Access Point). – Actúa como un Hub inalámbrico al cual se conectan computadoras.

   b) Tarjetas inalámbricas para computadora.- Permiten a una computadora conectarse a un punto de acceso.

   c) Punto a punto.- Enlazan de forma inalámbrica dos sitios diferentes. Usualmente se utilizan para distancias largas y usan antenas externas direccionales u omnidireccionales.

   d) Punto-multipunto.- Enlazan de forma inalámbrica más de dos sitios diferentes. Usualmente se utilizan para distancias largas y requieren antenas externas direccionales u omnidireccionales.

3) Nadie está autorizado a instalar dispositivos inalámbricos de red (DIR) sin la autorización del administrador del Centro de Cómputo de la facultad. Cuando se detecte un equipo instalado ilegalmente se procederá a deshabilitar el equipo en donde se detecte, independientemente si existen otros equipos de red legalmente conectados a ese puerto.
4) Cuando se deseé instalar un DIR, se deberá presentar una solicitud por escrito al Centro de Cómputo Universitario, firmada por el titular de la dependencia. El caso en particular será analizado conjuntamente con la persona asignada por la dependencia que solicita, esto no garantiza la autorización para conectarlo.
5) Los DIR están sujetos a las mismas regias y políticas que se aplican a otros dispositivos electrónicos de comunicación instalados.
6) El abuso o interferencia con otras actividades es una violación al uso aceptable. La interferencia o disrupción de otras comunicaciones autorizadas o la intercepción de otros tipos de tráficos constituye una violación a las políticas.
7) Una dependencia solamente podrá instalar DIRs para proporcionar servicio en espacios interiores de edificios pertenecientes a dicha dependencia. El servicio entre edificios solamente lo podrá proporcionar el Centro de Cómputo Universitario.

Seguridad

1) El acceso a la infraestructura de la red, incluyendo la infraestructura inalámbrica está limitada a personas autorizadas a usar los recursos de Internet de la Facultad de Contaduría y Administración.
2) Debe ser mantenida una seguridad física con la finalidad de evitar el robo de los equipos o el acceso a los puertos de datos.
3) La infraestructura inalámbrica punto a punto o punto-multipunto no proporciona codificación o autentificación. El password y la protección de los datos es responsabilidad de la aplicación.
4) Los puntos de acceso deben utilizar autentificación de usuarios y además restringir la aceptación de la conexión mediante la verificación de la dirección MAC de las computadoras.

Interferencia

El funcionamiento correcto de una instalación inalámbrica que cubre edificios completos o áreas más amplias, requiere que todo el equipo está correctamente instalado y configurado para evitar interferencias entre los componentes de otros segmentos de red o entre otros equipos. El Centro de Cómputo será el encargado de regular y administrar la configuración de las frecuencias. Las interferencias que pudieran resultar serán resueltas por el Centro de Cómputo de acuerdo a las prioridades, las cuales son las siguientes: académicos, administración, investigación y acceso público.

VIII. 2. Responsabilidad del Centro de Cómputo

I. Crear, mantener y actualizar las políticas y los estándares de seguridad.
II. Mantener un registro de todas las tarjetas y equipos inalámbricos en la facultad.
III. Resolver los problemas de interferencia en la comunicación.
IV. Administrar e instalar los sistemas inalámbricos en áreas comunes de la facultad.
V. Aprobar el software y hardware usado en las dependencias y extensiones universitarias.
VI. Informar a los usuarios de sistemas inalámbricos las políticas de privacidad y seguridad relacionados con el uso de comunicación inalámbrica en áreas comunes.
VII. Proporcionar asistencia a las dependencias para la instalación de sistemas inalámbricos.
VIII. Monitorear la seguridad y eficiencia de las redes inalámbricas en las áreas comunes y mantener estadísticas, así como prevenir los accesos no autorizados.
IX. Resolver cualquier caso no previsto.

Las dependencias tienen como obligación.

1. Respetar las políticas para redes inalámbricas.
2. Informar a sus usuarios sobre estas políticas.

VIII. 3. Plan de Contingencia

Es una herramienta que cualquier institución debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le afectara, y ocasionara una interrupción parcial o total en sus funciones.

La tecnología de red evoluciona tan rápidamente, que debe planificarse la actualización del plan de contingencia periódicamente, por ejemplo una vez al año. Aunque la redacción del plan inicial supondrá una gran cantidad de trabajo, una vez que se dispone del plan, las actualizaciones son relativamente fáciles.

Contenido del Plan de Contingencia para la Red Inalámbrica

El plan de contingencia debe intentar definir las cinco áreas siguientes:

1) Listas de notificación, números telefónicos, mapas y direcciones.
2) Prioridades, responsabilidades, relaciones y procedimientos.
3) Información sobre adquisiciones y compras.
4) Diagramas de las instalaciones.
5) Sistemas, configuraciones y copias de seguridad en cinta.

Las principales actividades requeridas para la planificación e implementación de una capacidad de recuperación de desastres.

1. **Identificación de riesgos.** La primera fase del plan de contingencia, la preocupación está relacionada con tres simples preguntas: ¿qué está bajo riesgo? por ejemplo, información crítica o recursos materiales, ¿qué puede ir mal en la red? y ¿cuál es la probabilidad de que suceda?

2. **Evaluación de riesgos.** Es el proceso de determinar el costo de sufrir un desastre que afecte la actividad diaria de la red. Los costos de un desastre pueden clasificarse en las siguientes categorías: Costos reales de reemplazo del equipo de telecomunicaciones, costos por inactividad de la red.

3. **Asignación de prioridades a las aplicaciones o servicios inalámbricos.** Después de que acontezca una interrupción del servicio y se inicie la recuperación, debe conocerse qué aplicaciones recuperar en primer lugar, es decir las aplicaciones esenciales.

4. **Establecimiento de los requerimientos de recuperación.** La clave de esta fase del proceso es definir un periodo de tiempo aceptable y viable para lograr que la red esté de nuevo activa.

5. **Elaboración de la documentación.** Los diagramas de red simplifican en gran medida la labor de construir una red. Un diagrama detallado de la red alámbrica como de la inalámbrica, necesaria para las primeras aplicaciones, facilita y agiliza la reanudación de las actividades.

6. **Verificación e implementación del plan.** Una vez redactado el plan, hay que probarlo. Hay que estar seguro de que el plan va a funcionar. Para ello, se debe ser escéptico sobre el propio trabajo, de manera que pueda uno probarse a sí mismo que funciona.

7. **Distribución y mantenimiento del plan.** Por último, cuando se disponga del plan definitivamente ya verificado, es necesario distribuirlo a las personas que necesitan tenerlo. Se debe controlar las versiones del plan, de manera que no exista confusión con múltiples versiones.

VIII. 4. Autorización

Debido a que las comunicaciones inalámbricas son en cierto nivel inseguras, el tráfico que circula por ellas es susceptible de ser interceptado y examinado. La autorización para el acceso debe contemplar lo siguiente:

I. Es obligatorio utilizar la autentificación mediante direcciones MAC.
II. Los usuarios que trabajen con información confidencial, deben utilizar protocolos de cifrado, por ejemplo: SSL (Secure Socket Layer), Secure Shell (versión más reciente), IPSEC.

VIII. 5. Amenazas a la Información y Recursos de Cómputo de la Facultad

El escaneo de la red, si se utiliza adecuadamente, es una valiosa herramienta para proteger nuestra información y recursos de cómputo. Por otro lado, los escaneos no autorizados de la red representan una seria amenaza a la disponibilidad, integridad y confidencialidad de nuestra información electrónica y nuestros recursos de cómputo. Los escaneos no autorizados pueden resultar en:

1. **Revelar información sensitiva**: Los escaneos de red recopilan una cantidad importante de información acerca de los dispositivos conectados a la misma. Esta información es crucial para los atacantes (hackers) en su intento de comprometer los sistemas de computo. Si un sistema critico es comprometido, un atacante puede tener acceso ilimitado a información confidencial.

2. **Pérdida de servicio**: Los ataques a la red varían enormemente en su naturaleza. La meta de un atacante puede ser obtener el control de un sistema de computo o simplemente hacer que nadie mas lo puede acceder. Incluso el proceso de escaneo para verificar la vulnerabilidad de un sistema puede ocasionar que este se comporte de manera errática o que quede de fuera de servicio.

3. **Pérdida de conexión a la red y del rendimiento de la misma**: Los escaneos pueden involucrar a cientos o hasta a miles de sistemas de cómputo. El abrupto volumen de tráfico puede ocasionar un tremendo esfuerzo en los recursos de los sistemas de computo y de la red universitaria, resultando en un bajo desempeño lo cual afecta directamente a los usuarios.

4. **Pérdida de reputación**: Como un miembro de la comunidad global de Internet nuestras acciones afectan directamente la seguridad de la información y los recursos de información alrededor del mundo. Si se permite que los recursos de la universidad sean utilizados para comprometer sistemas externos, nuestra reputación como miembro responsable del Internet se verá empañada.

VIII. 6. Monitoreo

Aplican las políticas sobre monitoreo y escaneo (ED-01)

Política ED-01: Escaneo de dispositivos conectados a la red

Propósito: Prohibir el uso de los recursos de la red (computadoras o cualquier otro recurso) para efectuar escaneos basados en red de cualquier dispositivo o sistema de computo sin el permiso por escrito de la persona o dependencia que lo tiene a su cargo. Esta política aplica para todos los dispositivos conectados a la red de la facultad.

Estas políticas proporcionan información relacionada con la práctica del escaneo de la red. El cumplimiento de las políticas aquí mencionadas es un requisito para poderse conectar a la red de cómputo. Persona(s) con responsabilidades primaria(s): La responsabilidad primaria corresponde al jefe del Centro de Cómputo. El encargado de seguridad informática coordinará las investigaciones de los incidentes de escaneo a la red.

Políticas: Un sistema puede ser escaneado por el propietario o por el administrador de dicho sistema. Una persona puede escanear un sistema ajeno solamente si recibe permiso por escrito del propietario o administrador de ese sistema. El documento debe incluir el periodo de tiempo específico durante el cual se efectuarán los escaneos. Cualquier escaneo adicional requiere una nueva autorización por escrito.

- El personal de telecomunicaciones del Centro de Computo puede efectuar escaneos de la red con la finalidad de resolver problemas de servicio, como parte de las operación normal del sistema y del mantenimiento, o para mejorar la seguridad de los sistemas. Siempre en coordinación con el área de seguridad en cómputo.
- El personal del área de seguridad en computo, del Centro de Cómputo Universitario, puede efectuar escaneos para monitorear, efectuar estudios de seguridad o para investigar incidentes de seguridad.

Violaciones:

Cuando se detecten violaciones a esta política, se procederá a armar un expediente el cual será enviado a las autoridades correspondientes para que se proceda legalmente.

CONCLUSIONES

La transmisión inalámbrica, es una tecnología en pleno desarrollo, que nació como respuesta a las necesidades de movilidad en los campos de la educación, la industria y el comercio, por mencionar solo algunas áreas. Por sus características y múltiples aplicaciones, las redes inalámbricas han ido incursionando poco a poco en el mercado actual, ganando cada día más adeptos.

Las redes inalámbricas no surgen como un reemplazo de las redes cableadas, sino como un complemento de ellas, puesto que la verdadera ventaja de las redes inalámbricas son las diferentes opciones de accesibilidad y movilidad que ofrecen frente a las cableadas. Las comunicaciones inalámbricas ya son una parte muy importante de la vida del ser humano, cada día el hombre se vuelve más dependiente de ellas y viendo el progreso de las mismas en tan poco tiempo, podría decir con certeza de que el objetivo de las comunicaciones es conectar a todo dispositivo electrónico de manera inalámbrica.

Las Nuevas Tecnologías de Información, como lo son las redes de comunicaciones inalámbricas, permitirán, nuevas posibilidades para comunicarse, accesando a datos e información, así como a diversos servicios que pueda proveer al ambiente de aprendizaje.

Para las universidades, como instituciones educativas, uno de sus principales objetivos con la sociedad y la industria, son: la enseñanza y la investigación. Una universidad, debe estar a la vanguardia en el aspecto tecnológico. Las universidades de todo el mundo, unen fuerzas en común con empresas de comunicaciones, con el propósito de llevar tecnologías a las instalaciones educativas.

Este trabajo logró presentar información integrada y relevante, resultado de una investigación referente a las tecnologías inalámbricas, para proponer su aplicación en ambientes académicos. Se pudieron plantear lineamientos en el desarrollo de una infraestructura inalámbrica, en la cual los usuarios se integrarán de manera transparente con cualquier dispositivo móvil y accesar a servicios disponibles. Por ejemplo, en la Facultad se podría implementar una red wireless que permita la integración de dispositivos móviles y en la que un alumno o un profesor pueda accesar a servicios como horarios, calendarios de exámenes, fechas importantes información sobre la facultad, etc.

La labor realizada consiguió detectar claramente cuáles son las tecnologías inalámbricas disponibles, el modelado, el desarrollo y su aplicación, así como las oportunidades de investigación y el contexto para ambientes de aprendizaje, facilitándole al usuario el poder interactuar en una comunidad virtual y ser miembro activo de ésta.

La teoría anywhere, anytime, será el preámbulo de la nueva educación en México y el mundo entero. De acuerdo al INEGI se estima que para el año 2010, notaremos un crecimiento del 22% en la educación superior y postgrado, incrementándose de 2.5 millones en el 2004, a 3.0 millones en el 2010.

A medida que la tecnología avanza los procesos, ideas, herramientas, deben evolucionar a la par para lograr una mejor sincronización de todas las partes involucradas. Proveer una educación de calidad a través de la diversificación de contenidos y metodologías es uno de los mayores retos para el mercado de las instituciones de educación superior.

Durante todo este proceso de investigación, pude tomar conciencia de las limitantes en materia de tecnologías de información y como, la brecha digital, desde mi personal punto de vista, representa mas una limitante social que una tecnológica. Mediante el análisis de la infraestructura de los equipos de la facultad, se podría llevar a cabo una actualización de la red pero se deben tomar en cuenta, aspectos como, las aplicaciones actualmente existentes, la compatibilidad de los equipos así como la integración de servicios.

Las WLAN poseen un futuro prometedor, debido a la gran aceptación que están recibiendo por parte del mercado.

Las instituciones deben aprovechar las nuevas tecnologías para satisfacer las necesidades educativas del siglo XX, deben brindar modelos educativos modernos para mejorar el proceso de aprendizaje y que a su vez, le permitan cautivar nuevos alumnos.

Propuestas para Trabajos Futuros

A través del desarrollo del presente proyecto fué posible entender la dirección que toman las tecnologías que se están implementando en la actualidad. Basándose en el análisis de las mismas, pero sobre todo en las tendencias y necesidades del mundo moderno, se sugieren algunas propuestas para la implementación de proyectos futuros, ya sea para mejorar la aplicación de este proyecto o para desarrollar nuevos que empleen tecnologías ya mencionadas.

Para mejorar la solución implementada en este trabajo se sugiere extenderlo a dispositivos reales, donde puedan ser integradas otras tecnologías inalámbricas como Bluetooth o WAP, para aplicaciones en Internet.

Algunos otros servicios que se proponen son los que manejen tipos de datos multimedia (audio y video) que son un poco más complejos, para que puedan ser utilizados para servicios básicos como impresoras o fax.

ANEXO I

Actualmente uno de los usos más extendidos de Wi-Fi es en los hotspots, que son lugares públicos los cuales cuentan con la infraestructura necesaria para que usuarios que poseen una laptop o un PDA puedan navegar en Internet a una velocidad superior a la que normalmente se conectan por medio de una línea telefónica; en el mundo los hotspots están creciendo de forma acelerada, tan sólo en Estados Unidos de Norteamérica existen más de 3000 y en el mundo se calcula hay 20 000.

En este anexo se presentan las universidades y sitios públicos donde se brindan servicios con tecnología inalámbrica en México.

Nombre	Ciudad	Estado
CETYS Tijuana	Tijuana	Baja California Norte
CUDEC	Querétaro	Querétaro
Instituto Pedagógico de Estudios de Posgrado	Celaya	Guanajuato
IPADE	México	Distrito Federal
IPADE - Monterrey	Monterrey	Nuevo León
ITAM	México	Distrito Federal
Tec de Monterrey- Querétaro	Querétaro	Querétaro
Tecnológico de Monterrey, Campus Hidalgo	Pachuca	Hidalgo
Universidad Autónoma De Nuevo León	Monterrey	Nuevo León
Universidad Bonaterra	Aguascalientes	Aguascalientes
Universidad Contemporánea de Querétaro	Querétaro	Querétaro
Universidad Del Valle De México Campus Tlalpan	México	Distrito Federal
Universidad Del Valle De México Campus Chapultepec	México	Distrito Federal
Universidad Del Valle De México Campus San Ángel	México	Distrito Federal
Universidad Del Valle De México Campus San Rafael	México	Distrito Federal
Universidad Del Valle De México Campus SLP	San Luis Potosí	San Luis Potosí
Universidad Del Valle De México Campus Villahermosa	Villahermosa	Tabasco
Universidad del Valle de México-Querétaro	Querétaro	Querétaro
Universidad Latina de México	Celaya	Guanajuato
Universidad Panamericana Cd. De México	México	Distrito Federal

Nombre	Categoría	Ciudad
Aeropuerto Internacional de la Cd. de México	Aeropuerto	México
Área de Restaurante Galerí Cuisine	Otros	México
Banqueta Wi-Fi Polanco (desde Garabatos	Restaurante	México
Beer Factory	Restaurante	México
Best Western Estoril	Hotel	Distrito Federal
Café Café	Restaurante	México
Centel	Otros	México
Centro Comercial Centro Insurgentes	Otros	México
Centro Comercial Pabellón Altavista	Otros	México
Centro Comercial Pabellon Polanco	Restaurante	México
Centro Comercial Plaza Inbursa	Otros	México
Centro Comercial Plaza Loreto	Otros	México
Centro Comercial Plaza Mazarik	Otros	México
Cinemex Santa Fé	Otros	México
Fiesta Americana Grand Chapultepec	Hotel	Distrito Federal
Fiesta Inn Periférico Sur	Hotel	México
FISHER'S	Restaurante	México
Fonda de Santa Clara Polanco	Restaurante	México
Galeria Plaza Ciudad de México	Hotel	México
Gloria Jean's Loreto	Restaurante	Distrito Federal
Hard Rock Café Ciudad De México	Restaurante	México
Hilton Ciudad de México Aeropuerto	Hotel	México
Hospital Ángeles del Pedregal	Hospital	México
Hospital de México	Hospital	México
Hospital Español	Hospital	México
King's Plaza	Hotel	México
Konditori	Restaurante	México
La Chiluca Santa Fe	Restaurante	México
Las Virtudes de la Condesa	Restaurante	México
Librería de Porrua Hermanos y Cia DF	Librería	México
Librería El Péndulo Polanco y Zona Rosa	Restaurante	México
Librería Gandhi Lomas	Librería	México
Librería Gandhi M A de Quevedo 121	Librería	México
Papalote- Museo del Niño	Otros	México
Park Nilo Hotel Suites	Hotel	México
Plaza Universidad	Otros	México
Restaurante Rainforest Santa Fe	Restaurante	México
Sanborn's	Restaurante	Distrito Federal
Salones Ejecutivos de Mexicana	Aeropuerto	Distrito Federal
Algunos VIPS	Restaurante	México
Xtratechnet	Restaurante	México

ANEXO II

Las instrucciones de esta guía de instalación y configuración son para ordenadores inalámbricos, laptops e inclusive para PDA's con Microsoft® Windows® XP Professional.

Su ordenador con WLAN 802.11 WLAN integrada (red de área local inalámbrica).

CONSEJO: Si no se ha adquirido un portátil preparado para conexiones inalámbricas, se puede comprar una tarjeta PC Card inalámbrica para incorporar

Mis ajustes de Red
Punto a punto a través de Ethernet
Nombre de usuario
Nombre del host
Contraseña
Nombre del servicio

Access Point inalámbrico compatible .Consultar la tabla "Comparación de los estándares tecnológicos de LAN inalámbrica (WLAN)". Durante la configuración del AP, se deberá utilizar la tabla siguiente para anotar el nivel de seguridad.

Nivel de seguridad general del Access Point		
Nivel de seguridad del Access Point	**Resultado**	**Acción**
WEP (privacidad equivalente de cable)	Clave de codificación suministrada	Anote la clave de codificación. _____
WPA-PSK (clave precompartida de acceso Wi-Fi protegido)	Necesita una frase de acceso.	1 Cree una frase de acceso. 2 Registre la frase de acceso. _____ 3 Descargue la actualización WPA más reciente para Microsoft® Windows® XP visitando la página Windows Update de Microsoft en http://windowsupdate.microsoft.com. Busque "WPA".

Instale el hardware y el software

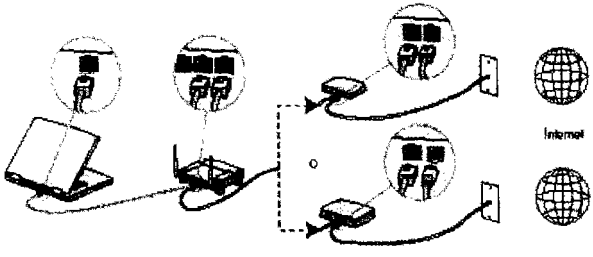
Ahora que se dispone de los componentes necesarios, se puede pasar a conectar los elementos de la red y configurar el Access Point inalámbrico.

1. Conecte y encienda el dispositivo portátil siguiendo las instrucciones suministradas con el mismo. Cerciórese de que el dispositivo está conectado a una toma de c.a. durante es procedimiento de configuración. Encienda, el Access Point inalámbrico y luego el dispositivo portátil.

2. Asegúrese de que el indicador luminoso situado junto al icono de conexión inalámbrica está apagado. Si está encendido, apáguelo pulsando el botón de activación / desactivación de la capacidad inalámbrica.

La ubicación del botón y del indicador luminoso de conexión inalámbrica depende del modelo.

3. Conecte el AP inalámbrico siguiendo las instrucciones del fabricante. (Durante este proceso el ordenador se conecta temporalmente al AP usando el cable Ethernet suministrado con el AP. Las instrucciones indicarán cuándo debe conectar y desconectar el cable.)



Conexiones de red con el cable Ethernet del Access Point conectado temporalmente (la ubicación del conector varía)

4. Configure el Access Point inalámbrico siguiendo las instrucciones del fabricante. Consulte la información que ha anotado en la tabla "Mis ajustes de red".

Durante la configuración del Access Point, compruebe si el nivel de seguridad del Access Point está ajustado en desactivado, WEP o WPA-PSK. Consulte la información de la tabla "Nivel de seguridad del Access Point". Compruebe la conexión a Internet abriendo su navegador de Web y accediendo a una página Web.

Tras comprobar la configuración con el cable Ethernet del Access Point inalámbrico conectado, desenchufe el cable del ordenador y del Access Point.

COMPROBACIÓN DEL PROGRESO
Si ha completado con éxito el paso 6, el Access Point está configurado correctamente. Si no puede acceder a una página Web, repita los pasos del 1 al 5 o póngase en contacto con el fabricante del Access Point.

Complete la red inalámbrica

Ahora que se ha terminado la configuración del hardware y software del Access Point, está preparado para añadir dispositivos a la red.

Pulse el botón de activación / desactivación de la capacidad inalámbrica del ordenador para activarla.

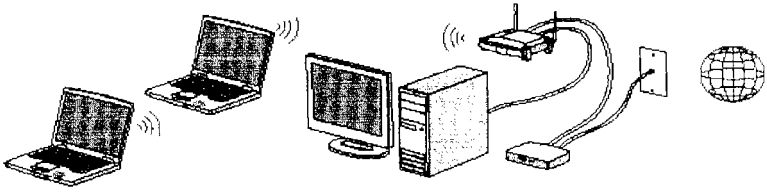
Conéctese a la red inalámbrica seleccionando Inicio > Connect To (Conectar) > Wireless Network Connection (Conexión de red inalámbrica). Marque el nombre de su red en la lista Available wireless networks (Redes disponibles).

Lleve a cabo los pasos siguientes que se correspondan con el nivel de seguridad del su Access Point inalámbrico (codificación):

Nivel de seguridad general de los Access Point	En la pantalla de conexión con red inalámbrica:
Desactivar (ninguna seguridad)	1 Seleccione la casilla Allow me to connect to the selected wireless network, even though it is not secure (Permitir la conexión con la red inalámbrica seleccionada incluso si no es segura). 2 Elija Connect (Conectar).
WEP	1 Elimine la marca de la casilla Enable IEEE 802.1x authentication for this network (Activar autenticación IEE 802.1x para esta red). 2 Escriba la clave de codificación WEP en el campo Network key (Clave de red). (Anotó esta clave en la tabla "Nivel de seguridad de mi AP") 3 Vuelva a escribir la clave de codificación en el campo Confirm network key (Confirmar clave de red). 4 Elija Connect (Conectar).
WPA-PSK	1 Escriba la frase de acceso WPA-PSK en el campo Network key (Clave de red). (Anotó esta clave en la tabla "Nivel de seguridad de mi AP") 2 Vuelva a escribir la frase de acceso en el campo Confirm network key (Confirmar clave de red). 3 Elija Connect (Conectar).

Compruebe la conexión a Internet abriendo el navegador de Web y accediendo a una página Web.

Conecte y configure cualquier otro ordenador adicional preparado para conexión inalámbrica u otros dispositivos, incluidos los cableados, que desee añadir a la red.



Ejemplo de red con portátiles inalámbricos y PCS de escritorio cableados

COMPROBACIÓN DEL PROGRESO
Si ha completado con éxito el paso 4, la red inalámbrica está configurada correctamente. Si no puede acceder a una página Web, reinicie el ordenador y repita los pasos del 1 al 3. Si sigue teniendo el mismo problema, póngase en contacto con el fabricante del Access Point o con su proveedor de servicios de Internet para obtener asistencia técnica.

Ejecute el Asistente para configuración en red en cada uno de los ordenadores de la red:

a Seleccione Inicio > Panel de control> Network and Internet Connection (Conexión de red e Internet) > Set up or change your home or small office network (Configurar una red doméstica o para pequeña oficina).
b Siga las instrucciones que se muestren en pantalla.

COMPROBACIÓN DEL PROGRESO
Si ha completado con éxito el paso 6, todos los dispositivos de la red podrán acceder a una página Web.

Importante: Si pierde la conexión inalámbrica mientras trabaja, seleccione Inicio > Connect (Conectar) > Wireless Network Connection (Conexión de red inalámbrica). (El icono y mensaje de estado de conexión de la red inalámbrica se muestran en la barra de tareas cuando logra volver a conectar.)

Conexión en red, movilidad, seguridad

No se puede arriesgar a entrar en el ciberespacio sin seguridad.

En función del nivel de seguridad del Access Point inalámbrico, considere el empleo de una o varias de las medidas de seguridad siguientes:

- **Activar la codificación.** Si aún no ha activado la codificación de seguridad, siga las instrucciones del fabricante para ajustar el nivel de seguridad más alto posible. WEP y WPA son protocolos de codificación de seguridad.

- **Cambiar el SSID (el nombre de su red) predeterminado en el dispositivo inalámbrico y en todos los ordenadores de la red.** El SSID debe ser un nombre único que no se pueda asociar fácilmente con usted.

Importante: Es necesario especificar el mismo SSID en el Access Point y en los ordenadores para qu los dispositivos puedan comunicarse.

1) Para cambiar el SSID, consulte sus instrucciones correspondientes.
2) Para cambiar el SSID en cada ordenador de la red:
a Seleccione Inicio > Panel de control > Network and Internet Connection (Conexión de red e Internet > Network Connections (Conexiones de red).
b Haga clic con el botón derecho del ratón en la opción Wireless Network Connection (Conexión de red
inalámbrica) y seleccione Properties (Propiedades). (Se abre la ventana de propiedades.)
c Seleccione la ficha Wireless Networks (Redes inalámbricas).
d Cambie el SSID.

- **Activar el filtro de direcciones MAC.** Consulte las instrucciones.
- **Usar un cortafuegos.** Un cortafuegos es una solución esencial de seguridad que protege sus datos y su ordenador de hackers destructivos, ladrones de datos, anexos maliciosos de correo electrónicos y demás riesgos incipientes de Internet.
- **Ajustar la seguridad en su navegador de Web.** El ajuste del nivel más alto de seguridad en su navegador es la forma más segura de navegar, pero limitará sus posibilidades de acceso y recepción de ciertos tipos de información.

Nota: Existen otros medios adicionales para securizar su red inalámbrica. Dependiendo del fabricante del Access Point se puede consultar las instrucciones del equipo para obtener más información al respecto

GLOSARIO

802.11

802.11, o IEEE 802.11, es un grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN).
802.11 se compone de distintas normas que operan a diferentes frecuencias, con distintas velocidades y capacidades.

AES (Advanced Encryption Standard).

Algoritmo de encriptación del gobierno de EE.UU., basado en el algoritmo Rijndael, método de encriptación simétrica con clave de 128 bits desarrollada por los belgas Joan Daemen y Vincent Rijmen.

Access Point (AP, Punto de Acceso)

Estación base o "base station" que conecta una red cableada con uno o más dispositivos wireless.
Existen muchos tipos de Access Point en el mercado, con diferentes capacidades: bridge, hubs, gateway, router, y las diferencias entre ellos muchas veces no están claras, porque las características de uno se pueden incluir en otro. Por ejemplo, un router puede hacer bridge, y un hub puede hacer switch. Además, los Access Points pueden mejorar las características de la WLAN, permitiendo a un cliente realizar roaming entre distintos AP de la misma red, o compartiendo una conexión a Internet entre los clientes wireless.

Ad-Hoc, modo.

Un tipo de topología de WLAN en la que sólo existen dispositivos clientes, sin la participación de ningún Access Point, de forma que los clientes se comunican de forma independiente punto a punto, peer-to-peer. Dado que no existe un dispositivo central, las señales pueden ocasionar mayores interferencias reduciendo las prestaciones de la red.

Ancho de banda (Bandwidth)

Fragmento del espectro radioeléctrico que ocupa toda señal de información.

Autentificación.

Proceso de identificación de un equipo o usuario. El estándar 802.11 define dos métodos de autentificación: open system y shared key.

Bluetooth.

Tecnología desarrollada para la interconexión de portátiles, PDA's, teléfonos móviles y similares a corta distancia (menos de 10 metros) con una velocidad máxima de 11Mbps a la frecuencia ISM de 2'4 GHz.

Bridge.

Dispositivo que conecta dos segmentos de red que emplean el mismo protocolo de red (por ejemplo, IP) pero con distintos medios físicos (por ejemplo, 802.11 y 10baseT).

BSSID, Basic Service Set Identification.

Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo Ad-Hoc.

Clave de encriptación.

Conjunto de caracteres que se utilizan para encriptar y desencriptar la información que se quiere mantener en privado. El tipo de clave y la forma de emplearla depende del algoritmo de encriptación que se utilice.

Cliente, o dispositivo cliente.

Cualquier equipo conectado a una red y que solicita servicios (ficheros, impresión, etc.) de otro miembro de la red. En el caso de las WLAN, se suele emplear para referirse a los adaptadores que proporcionan conectividad a través de la red inalámbrica, como tarjetas PCMCIA, PCI o USB, que permiten al equipo acceder a la red.

Codificación

Proceso de cifrado de los datos para evitar que los lean destinatarios no autorizados.
Normalmente se precisa una clave exclusiva para descodificar los datos. WEP y WPA son protocolos de codificación de seguridad.

Decibelios, dB.

Unidad logarítmica empleada habitualmente para la medida de potencias. Se calcula multiplicando por diez el resultado del logaritmo en base 10 de la potencia (en watios): $10 * \log_{10}$ (W). También puede usarse como medida relativa de ganancia o pérdida de potencia entre dos dispositivos.

DHCP, Dynamic Host Configuration Protocol.

Protocolo para la configuración automática de los parámetros de red de los equipos. La información se almacena en un servidor DHCP al que los equipos, al encenderse, solicitan los parámetros de configuración.

Directividad.

Capacidad de una antena para concentrar la emisión en una determinada región del espacio. Cuanto más directiva sea la antena, se obtiene un mayor alcance a costa de un área de menor cobertura.

Diversidad.

Un equipo puede utilizar varias antenas distintas para mejorar la calidad en la recepción de la señal, al aprovechar las mejores características de cada una para cada situación.

DNS (servidor de nombres de dominio)

La dirección IP del servidor de su proveedor de servicios de Internet que traduce los nombres de páginas Web en direcciones IP.

DSL (línea de suscripción digital)

Dispositivo que conecta un ordenador a una línea telefónica, que a su vez conecta con Internet.

DSSS, Direct Sequence Spread Spectrum.

Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en el uso de bits de redundancia.

ESID.

Identificador del punto de acceso, utilizado por los clientes para conectarse a el.

Espectro radioeléctrico.

El espectro radioeléctrico es toda la escala de frecuencias de las ondas electromagnéticas. Considerado como un dominio de uso público, su división y utilización esta regularizado internacionalmente.

ESSID, Extended Service Set Identification.

Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

Ethernet.

Ethernet es el nombre común del estándar IEEE 802.3, que define las redes locales con cable coaxial o par trenzado de cobre. Existen distintas versiones, desde la original 10Base5 (cable coaxial con 10 Mbps hasta 500 metros), pasando por la 10Base2 (coaxial, 10Mbps, 200m), 10BaseT (par trenzado, 10 Mbps, 100m) y 100BaseT (trenzado, 100Mbps, 100m) conocida como Fast Ethernet, el más utilizado hoy en día en redes locales.

ETSI, European Telecommunications Standard Institute http://www.etsi.org.

Organización europea sin ánimo de lucro para el desarrollo de estándares de telecomunicación, agrupa 699 miembros de 55 países.

FCC, Federal Communication Commision http://www.fcc.gov.

Agencia gubernamental de los EE.UU. para la regularización de las comunicaciones por radio, televisión, cable y satélite.

FHSS, Frequency Hopping Spread Spectrum.

Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en cambios sincronizados entre emisor y receptor de la frecuencia empleada.

Firewall.

Sistema de seguridad que previene el acceso no autorizado a la red, restringiendo la información que entra o sale de la red. Puede ser un equipo específico o un software instalado en una máquina de uso general.

Gateway.

Dispositivo que conecta a distintas redes entre sí, gestionando la información entre ellas.

Hot Spot.

También conocidos como lugares de acceso público, son áreas geográficas a las que da cobertura un punto de acceso, para puntos de acceso normales esta área suele cubrir un radio de 100 metros. Pueden estar en cyber-cafés, aeropuertos, centros de convenciones, hoteles, y otros lugares de encuentro, para proporcionar acceso a su red o a Internet a los visitantes o invitados.

Hub.

Dispositivo de red multipuerto para la interconexión de equipos vía Ethernet o wireless. Los concentradores mediante cables alcanzan mayores velocidades que los concentradores wireless (Access Points), pero éstos suelen dar cobertura a un mayor número de clientes que los primeros.

Hz, Hertzios.

Unidad internacional para la frecuencia, equivalente a un ciclo por segundo. Un megahertzio (MHz) es un millón de hertzios; un gigahertzio (GHz) son mil millones de hertzios.

Infraestructura, modo.

El modo de infraestructura es una topología de red inalámbrica en la que se requiere un Punto de Acceso. A diferencia del modo Ad-Hoc, toda la información pasa a través del Punto de Acceso, quien puede además proporcionar la conectividad con una red cableada y controlar el acceso a la propia red wireless.

IEEE, Institute of Electrical and Electronics Engineers (http://www.ieee.org).

Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones.
Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN.

IP, dirección.

Un número de 32 bits que identifica a un equipo, a nivel de protocolo de red en el modelo ISO. Se compone de dos partes: la dirección de red, común a todos los equipos de la red, y la dirección del equipo, única en dicha red.

ISM, Industrial, Scientific and Medical band.

Bandas de frecuencias reservadas originalmente para uso no comercial con fines industriales, científicos y médicos. Posteriormente, se empezaron a usar para sistemas de comunicación tolerantes a fallos que no necesitaran licencias para la emisión de ondas. 802.11b y 802.11g operan en la ISM de los 2'4 GHz, así como otros dispositivos como teléfonos inalámbricos y hornos microondas, por ejemplo.

ISO, modelo de red.

La ISO, International Standards Organization (http://www.iso.org), desarrolló un modelo para describir a las entidades que participan en una red. Este modelo, denominado Open System interconnection (OSI), se divide en 7 capas o niveles, que son:

1) Físico.
2) Enlace.
3) Red.
4) Transporte.
5) Sesión.
6) Presentación.
7) Aplicación.

Con esta normalización de niveles y sus interfaces de comunicación, se puede modificar un nivel sin alterar el resto de capas. El protocolo 802.11 tiene dos partes, una denominada PHY que abarca el nivel físico, y otra llamada MAC, que se corresponde con la parte inferior del segundo nivel del modelo OSI.

LAN (Local Area Network).

Es una red de comunicación de datos que está situada habitualmente en un mismo edificio (o tiene grandes dimensiones) y que posibilita que las máquinas conectadas transmitan información de unas a otras mediante alguno de los protocolos existentes.

MAC (Media Access Control), dirección.

En las redes wireless, el MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2) en el modelo ISO. Cada dispositivo wireless posee una dirección para este protocolo, denominada dirección MAC, que consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta,

mientras que los restantes 24, a la tarjeta en sí. Este modelo de direccionamiento es común con las redes Ethernet (802.3).

Modulación.

Técnicas de tratamiento de la señal que consiste en combinar la señal de información con una señal portadora, para obtener algún beneficio de calidad, eficiencia o aprovechamiento del ancho de banda.

Multitrayecto (multipath).

Fenómeno que ocurre cuando una señal rebota en las superficies y alcanza el destino final por varios caminos, con efecto positivo o negativo sobre la potencia de señal recibida difíciles de controlar.

Network name, nombre de red.

Identificador de la red para su diferenciación del resto de las redes. Durante el proceso de instalación y configuración de dispositivos wireless, se requiere introducir un nombre de red o SSID para poder acceder a la red en cuestión.

Omnidireccional, antena.

Antena que proporciona una cobertura total en un plano (360 grados) determinado.

Open System, autentificación.

Método de autentificación por defecto del estándar 802.11, en la que no se realiza ningún proceso de comprobación de identidad; simplemente, se declaran, por lo que no ofrece ninguna seguridad ni control de acceso.

Parabólica, antena.

Antena en forma de disco curvado. Este tipo de antenas ofrecen la directividad más alta, lo que las hace ideales para enlaces punto a punto a larga distancias.

PHY.

Nombre abreviado del nivel más bajo del modelo ISO, el nivel físico, que describe el medio físico en el que se transmite la información de la red. En el caso de las redes inalámbricas, las normas 802.11 definen el nivel PHY que utilizan, el aire libre, y los parámetros empleados como la velocidad de transmisión, tipo de modulación, algoritmos de sincronización emisor / receptor, etc.

PPPoE (protocolo punto a punto por Ethernet).

Tipo de conexión de banda ancha que proporciona autenticación además de transporte de datos.

Roaming.

Nombre dado a la acción de moverse del área de cobertura de un Punto de Acceso a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.

RF.

Abreviatura de Radio Frecuencia. Este término se refiere a una corriente alterna (AC) con la característica especial de que, si ésta sirve de entrada a una antena, se genera un campo electromagnético (EM) adecuado para las comunicaciones inalámbricas. Estas frecuencias cubren

una porción significativa del espectro de radiaciones electromagnéticas, extendiéndose desde los 9 KHz a miles de gigahertzios.

Router.

Dispositivo de red que traslada los paquetes de una red a otra. Basándose en las tablas y protocolos de enrutamiento y en el origen y destino, un router decide hacia dónde enviar un paquete de información.

Sensibilidad.

Potencia mínima de señal que el receptor puede transformar correctamente en datos.

Shared Key, autentificación.

Proceso de autentificación por clave secreta. Habitualmente, todos los dispositivos de la red comparten la misma clave.

Spread Spectrum, espectro disperso.

Técnica de trasmisión consistente en dispersar la información en una banda de frecuencia mayor de la estrictamente necesaria, con el objetivo de obtener beneficios como una mayor tolerancia a las interferencias.

SSID, Service Set Identification.

Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad. Dependiendo de si la red wireless funciona en modo Ad-Hoc o en modo Infraestructura, el SSID se denomina ESSID o BSSID.

Términos de radio frecuencia: GHz, MHz, Hz.

La unidad internacional de medida de frecuencia es el Hertzio (Hz) el cual es equivalente a la unidad antigua de ciclos por segundo. Un MHz es un millón de Hertzios y un GHz son mil MHz (mil millones de Hz). Como referencia: La frecuencia eléctrica utilizada en Europa son 50 Hz y en EEUU son 60 Hz. La banda de frecuencia de radiodifusión AM es 0.55 - 1.6 MHz. La banda de frecuencia de radiodifusión FM es 88 - 108 MHz. Los hornos microondas típicamente operan a 2.45 GHz.

TCP/IP (protocolo de control de transmisiones / protocolo de Internet).

Protocolo de red para la transmisión de paquetes de datos en una red.

TKIP, Temporal Key Integrity Protocol.

Algoritmo empleado por el protocolo WPA para mejorar la encriptación de los datos en redes wireless. Sus principales características son la renovación automática de la clave de encriptación de los mensajes y un vector de inicialización de 48 bits, lo que elimina el problema del protocolo WEP.

UNII, Unlicensed National Information Infraestructure.

Banda de frecuencia en los 5 GHz reservada por la FCC para las comunicaciones wireless según el estándar 802.11a. No existe una regularización internacional común sobre los aspectos de esta banda y los dispositivos que operan en ella.

Velocidad de transmisión (Throughput)

Capacidad de transmisión de un medio de comunicación en cualquier momento, se suele medir en bits por segundo (bps). Depende de múltiples factores, como la ocupación de la red, los tipos de dispositivos empleados, etc, y en el caso de redes wireless, se añaden los problemas de propagación de microondas a través de la que se transmite la información.

VPN, Virtual Private Network.

Herramienta de seguridad que permite mantener en privado una comunicación a través de una red pública. Puede ofrece otros servicios como autentificación de los extremos involucrados, integridad, etc.

War chalking.

Proceso de realizar marcas en las superficies (paredes, suelo, señales de tráfico, etc) para indicar la existencia de redes wireless y alguna de sus características (velocidad, seguridad, caudal, etc).

War driving.

Localización y posible intrusión en redes wireless de forma no autorizada. Sólo se necesita un portátil, un adaptador wireless, el software adecuado y un medio de transporte.

WEP, Wired Equivalent Privacy.

Algoritmo de seguridad, de uso opcional, definido en el estándar 802.11. Basado en el algoritmo criptográfico RC4, utiliza una clave simétrica que debe configurarse en todos los equipos que participan en la red. Emplea claves de 40 y 104 bits, con un vector de inicialización de 24 bits. Se ha demostrado su vulnerabilidad y que su clave es fácilmente obtenible con software de libre distribución a partir de cierta cantidad de tráfico recogido de la red.

Wi-Fi, Wireless Fidelity.

Nombre dado al protocolo 802.11b. Los dispositivos certificados como Wi-Fi son interoperables entre sí, como garantía para el usuario.

Wi-Fi Alliance, también llamada Wireless Ethernet Compability Alliance (WECA) (http://www.wi-fi.org).

Asociación internacional formada en 1999 para certificar la interoperatibilidad de los dispositivos wireless basados en el estándar 802.11, con el objetivo de promover la utilización de dicha tecnología.

WLAN (Wireless Local Area Network).

Subdivisión de las redes de área local que se caracteriza porque sus usuarios pueden conectarse de forma inalámbrica a la red física. Más reducidas aún son las WPAN (Wireless Personal Area Network), caracterizadas por utilizar la tecnología Bluetooth.

WPA, Wi-Fi Protected Access.

Protocolo de seguridad desarrollado por la WECA para mejorar la seguridad de la información en las redes wireless y permitir la autentificación de usuario, puntos débiles del WEP.