RESUMEN EJECUTIVO

Durante el desarrollo de esta investigación se encontraron muchos aspectos muy interesantes, las ventajas y beneficios de utilizar la tecnología inalámbrica así como su facilidad de implementación fueron unos de los más importantes. Otro factor a tomar en consideración son las diferentes variantes de estándar 802.11 con lo cual se puede cubrir cualquier requerimiento, dependiendo de las características del lugar y la inversión que se desee realizar. Las seguridades que quizás son el punto más bajo de esta tecnología, muestran que con un poco de atención y utilización de los debidos estándares se puede obtener un sistema muy robusto y confiable.

El análisis de mercado realizado deja resultados satisfactorios, en el sentido de que la gran mayoría de los estudiantes cuentan con dispositivos inalámbricos y estarían gustosos de acceder a esta tecnología, lo que les permitiría utilizar y sacar provecho perfectamente al servicio propuesto en el tema investigado.

Implementar un ISP inalámbrico no es tarea fácil , por cuanto intervienen básicamente tres factores que tienen que estar perfectamente configurados como son: El Access Point, el servidor RADIUS y los clientes; si alguno de ellos falla simplemente no se podría acceder o brindar el servicio.

CAPÍTULO I

INTRODUCCIÓN

1.1- Introducción

En un ambiente globalizado en el cual nos desenvolvemos hoy en día, todo el mundo necesita utilizar Internet, la mayoría de empresas y organizaciones utilizan este servicio como medio principal de comercio y publicidad. En nuestro país existen muchos proveedores de Internet con diferentes tipos de tecnologías como lo son: Dial up, cable modem, líneas dedicadas, ADSL, Internet satelital, Internet móvil, entre otros.

Actualmente la tecnología inalámbrica está suscitando no sólo el interés teórico de mercado, por las novedades tecnológicas que aporta, sino también interés práctico, ya que se le suponen crecimientos y cifras de negocio a los que la industria de Tecnologías de la Información se está adaptando.

Las redes inalámbricas están adquiriendo un éxito sin precedentes 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 seguridad de las comunicaciones.

Este trabajo de investigación abarcará temas muy importantes en las telecomunicaciones modernas como lo son el estándar Wi-Fi (802.11b), y sus diferentes variantes ya que éstos son protocolos que permite conexiones inalámbricas a altas velocidades y con gran fidelidad.

Además se verán tópicos sobre, cuáles son los pasos a seguir para poner un ISP inalámbrico en funcionamiento, costos de equipos, un estudio de factibilidad de mercado y por último una aplicación de ejemplo del uso y funcionamiento de la tecnología Wi-Fi.

El tema de este proyecto es "Análisis y Diseño para implementar un ISP inalámbrico utilizando un nodo Wi-Fi", el cual busca satisfacer conocimientos a través de una amplia investigación en telecomunicaciones inalámbricas, previo a la obtención del título de Ingeniero de Sistemas e Informática de acuerdo a los requerimientos de la Facultad de Sistemas e Informática de la Escuela Politécnica del Ejército.

1.2- Justificación

La importancia de las telecomunicaciones como motor de la Sociedad de la Información es indiscutible. Las tecnologías de las telecomunicaciones tienen implicaciones revolucionarias en la vida cotidiana y las relaciones empresariales y ello con un ritmo de cambio nunca antes conocido; todo esto multiplica la importancia de la investigación y el desarrollo en este sector.

La tecnología inalámbrica verdaderamente ha llegado para quedarse, se ha ido convirtiendo poco a poco en la solución a muchos problemas o incomodidades que representaban tantos cables, no sólo estéticamente sino también en cuestiones de trabajo.

El Ecuador es un país en vías de desarrollo por lo que no puede estar ajeno a las nuevas tendencias tecnológicas en lo que ha telecomunicaciones se refiere, es por ésta razón que el autor considera muy importante hacer un estudio que permita implementar una infraestructura tecnológica inalámbrica adecuada y moderna, de tal manera que los usuarios puedan navegar en Internet sin necesidad de cables, de manera rápida y a un costo conveniente, además este es un tema prácticamente virgen y rentable en nuestro mercado.

1.3- Objetivos

1.3.1- Objetivo Principal

Realizar el análisis y el diseño necesarios para implementar un Proveedor de Servicios de Internet Inalámbrico utilizando un nodo con tecnología Wi-Fi.

1.3.2- Objetivos Específicos

- Profundizar los conocimientos sobre telecomunicaciones inalámbricas.
- Conocer las ventajas de la tecnología Wi-Fi como estándar de las telecomunicaciones inalámbricas.
- Establecer gastos operativos y de instalación para implantar un ISP inalámbrico.
- Elaborar una guía técnica de implementación.
- Realizar una aplicación práctica y demostrativa de la utilización del estándar Wi-Fi.
- Realizar un análisis para conocer las tendencias del mercado en cuanto a necesidades inalámbricas.

1.4- Alcance

El alcance de este proyecto de investigación consiste en realizar el estudio y la planificación necesario, para la implementación de un nuevo servicio de Internet inalámbrico con tecnología de punta llamada Wi-Fi, esta tecnología garantiza alta fidelidad en telecomunicaciones inalámbricas y por esta razón está siendo muy utilizada en otros países de América y Europa.

Al terminar esta investigación se obtendrá un documento guía o manual que servirá de base para poder implantar un ISP inalámbrico utilizando un nodo Wi-Fi, es decir, el documento tendrá todos los pasos a seguir y consideraciones a tomar para cualquier ISP que desee brindar servicios inalámbricos en cualquier parte del país.

Por último se realizará un ejemplo aplicativo en la Escuela Politécnica del Ejército, en cual se pondrán en práctica los pasos antes mencionados y se realizará la conexión inalámbrica a través del nodo Wi-Fi.

1.5- Metodología

La metodología de la investigación combina de manera armónica lo cualitativo y lo cuantitativo, obteniendo así una mayor riqueza de información basada en la realidad del sector. A través de los datos cuantitativos se pretende conocer los hechos tal y como se dan en realidad, intentando obtener una visión objetiva de tales hechos e identificando las posibles relaciones que se dan entre ellos, así como las causas que los originan y las consecuencias que de ellos se derivan.

Mediante los métodos cualitativos se intentará obtener una información relevante acerca de cómo los protagonistas de la realidad del sector viven los acontecimientos. A través de ésta metodología se obtendrá una visión subjetiva apoyada en las opiniones de expertos que conocen los aspectos más complejos de la realidad y de los problemas del sector de las telecomunicaciones inalámbricas.

1.5.1- Técnicas de Recogidas de Datos

Los datos de la investigación se recogerán a través de la combinación de técnicas cualitativas y cuantitativas. A través de esta metodología, se obtendrá una información mayor acerca del objeto de estudio, puesto que las técnicas cualitativas proporcionan una profundidad en el conocimiento de la realidad que se estudia que las cuantitativas no ofrecen, mientras que las cuantitativas permiten realizar inferencias y aproximaciones exactas a la realidad, permitiendo en consecuencia un acercamiento mucho más objetivo.

Las técnicas de carácter cualitativo que se utilizarán estarán basadas en entrevistas en profundidad y grupos de discusión. Como instrumento de recogida de datos

cuantitativos en fuentes primarias se utilizarán cuestionarios cerrados que se aplicarán a estudiantes de la Facultad.

En el proceso de la investigación se utilizarán en primer lugar las técnicas cualitativas, puesto que proporcionarán al investigador un amplio conocimiento del sector; de tal forma que, con la información que se obtendrá a través de ellas junto con la que se obtendrá a través del análisis en fuentes secundarias, faciliten en gran medida el diseño de instrumentos de recogida de datos en fuentes primarias de carácter cuantitativo, adecuado a la realidad del sector.

1.5.2- Definición y cuantificación del universo

El universo de estudio de ésta investigación, estará constituido por la mayoría de empresas que brindan servicios de Internet que operan en la ciudad de Quito. Serán objeto de estudio aquellas empresas que estén dentro del siguiente ámbito:

- Operadores de comunicaciones móviles.
- Operadores de cable.
- Proveedores de Internet

1.5.3- Tamaño de la muestra, procedimientos de muestreo y fiabilidad

Partiendo del universo anteriormente mencionado, se calcula una muestra de unas 5 empresas con un nivel de confianza del 90%. El muestreo que se plantea es aleatorio y estratificado por el ámbito geográfico de la ciudad de Quito. Además se considerará una muestra de unos 100 estudiantes de la ESPE.

1.5.4- Selección de los entrevistados

La selección de los entrevistados a través de técnicas cuantitativas será aleatoria en la elección de los usuarios, y posteriormente concretada a una serie de perfiles profesionales capacitados para contestar la encuesta por su especial conocimiento del tema y todas la actividades que se desarrollan en su organización o entorno.

1.5.5- Análisis de los datos

El análisis del contenido de las entrevistas se realizará a partir de las anotaciones y/o grabaciones que el entrevistador (investigador) tomará durante el proceso. El carácter semiestructurado y semidirigido de las entrevistas posibilitarán la comparación de la información obtenida, de la cual se irá consiguiendo un relativo consenso conforme se vaya avanzando con la investigación. En el caso concreto de los cuestionarios se utilizarán análisis estadísticos que serán facilitados por la propia estructura definida en el diseño de los cuestionarios.

Dado que el nivel de explicación de la investigación es básicamente descriptivo, sus principales objetivos se centran en el estudio y planificación así como un análisis detallado y profundo del sector de las telecomunicaciones inalámbricas a distintos niveles (situación económica, situación actual, situación administrativa).

1.6- Herramientas

En éste proyecto de investigación se utilizarán las siguientes herramientas:

- Microsoft Word 2000
- Microsoft Excel 2000
- Microsoft Project 2000
- Microsoft Visio
- Internet Explorer
- Adobe Acrobat Reader

1.7- Factibilidad

1.7.1- Técnica

Al implantar un ISP inalámbrico en la ESPE (Escuela Politécnica del Ejército), se estaría brindando un nuevo servicio que se vendría a agregar al sistema existente en el mercado nacional. Con esto se generaría competitividad entre los proveedores de servicios

de Internet generando mejor calidad de servicio, en donde los únicos beneficiados serían los usuarios ya que contarían con más alternativas de acceso a Internet, encontrarían mejores costos y servicios más óptimos.

Una de las principales herramientas técnicas con que el autor cuenta para la realización de este proyecto de investigación es Internet; la cual para este tema es la principal fuente de información bibliográfica.

Para poder realizar una aplicación práctica utilizando un nodo Wi-Fi el autor cuenta con el apoyo del Ing. José Luis Torres quien se ofreció a facilitar los equipos necesarios para realizar una aplicación de ejemplo que permita poner en práctica el estudio realizado.

1.7.2- Económica

El autor le dedicará al desarrollo de este proyecto un tiempo promedio de 8 horas diarias durante un período aproximado de 6 meses, con la finalidad de cubrir todas las metas trazadas y los objetivos planteados; para esto se han considerado los siguientes costos aproximados:

Cuadro 1.1: Factibilidad Económica

No.	Descripción	P. Unitario	P. Total
1	Computador Portátil (con puerto Wi-Fi)	1500,00	1500,00
2	Uso de Internet (6 meses)	20,00	120,00
3	Uso del teléfono (conexión a Internet vía Dial-Up)	70,00	420,00
4	Compra de libros (2)	50,00	100,00
5	Otros		50,00
		Total:	**2190,00**

1.7.3- Operativa

Lo que se busca al final del desarrollo de esta investigación es generar un documento base o guía técnica que le permita a cualquier persona o empresa implementar

un ISP inalámbrico en el Ecuador, utilizando tecnología de punta como lo es el estándar Wi-Fi.

Además se realizará una aplicación demostrativa, que permita poner en práctica todo lo investigado, de tal manera que se pueda tener un acceso a Internet inalámbrico utilizando un nodo Wi-Fi.

CAPITULO II

MARCO TEÓRICO

2.1- Introducción

La expectativa creada en torno al estándar IEEE 802.11 ha motivado un gran interés por conocer el modo en que este tipo de tecnologías podrían ser aplicadas dentro del sector empresarial como un agente catalizador de nuevas aplicaciones y negocios.

El estándar está orientado al desarrollo de redes de área local inalámbrica con aplicación dentro de espacios interiores. Esto no ha sido impedimento de que existan aplicaciones Wi-Fi más allá de su concepción inicial, llegándose incluso a pensar en la posibilidad de dar cobertura inalámbrica a áreas metropolitanas, cubriendo por entero una pequeña ciudad.

El hecho de utilizar una banda de frecuencias no regulada y la interoperación entre dispositivos de diversos fabricantes, junto con la reducción de precios, ha hecho que su aplicación y expectativas de uso se hayan desarrollado enormemente.

La economía en el despliegue en este tipo de redes, así como el carácter de uso libre del espectro, ha hecho que algunos vean estas soluciones como una amenaza o alternativa al servicio de acceso Internet inalámbrico a través de tecnologías UMTS (Universal Mobile Telecommunications System – Sistema Universal de Telecomunicaciones Móviles) ofrecido por los operadores de redes móviles.

Tanto en EEUU como en el resto del mundo, están apareciendo iniciativas para el desarrollo de las denominadas PWLAN (Public Wireless LAN – Redes LAN Públicas Inalámbricas). Bajo este tipo de uso de Wi-Fi (Wireless Fidelity – Fidelidad Inalámbrica) están apareciendo compañías denominadas WISP (Wireless Internet Service Provider – Proveedor de Servicios de Internet Inalámbrica), que ofrecen un servicio de acceso a

Internet dentro de espacios de uso público llamados Hotspots (Puntos de acceso con conexión inalámbrica de alta velocidad en emplazamientos públicos) como pueden ser hoteles, aeropuertos, restaurantes. El modelo de negocio está aún por ser validado, aunque algunos operadores de telecomunicaciones empiezan a definir una estrategia dentro de este mercado. Es muy probable que exista un exceso en cuanto a la valoración de estas oportunidades de negocio.

Las empresas pueden beneficiarse de la tecnología Wi-Fi en una doble vertiente, por una parte, son muchas las facilidades que Wi-Fi ofrece en cuanto a conectividad inalámbrica, por lo que cada día se reconoce su capacidad como alternativa o complemento a las redes locales cableadas. Paralelamente, las aplicaciones asociadas a Wi-Fi suponen una oportunidad de negocio en actividades como integración, desarrollo, soporte y mantenimiento.

La incorporación de Wi-Fi a dispositivos de usuario como ordenadores personales, PDAs, proyectores, teléfonos; implica que la existencia de una alternativa de acceso Wi-Fi a las redes locales presente una gran ventaja, ya que muchos dispositivos se conectarán conservando su movilidad.

Antenas direccionales, equipamiento especializado y otros elementos hacen que Wi-Fi pueda ser aplicado para la interconexión de edificios tanto en ámbito urbano como rural. En el hogar Wi-Fi crece a medida de que la electrónica de consumo va incorporando esta tecnología a televisores, cadenas de música, reproductores multimedia, teléfonos celulares.

Las empresas en general podrán utilizar Wi-Fi como elemento integrante de su infraestructura de informática y telecomunicaciones. Además, el desarrollo de Wi-Fi hace que esté llegando a integrarse en servicios finales ofrecidos por terceras compañías, como por ejemplo vídeo vigilancia, tele seguridad o hilo musical. Por otro lado, las empresas que

trabajan en el sector TIC (Tecnologías de la Información y las Comunicaciones) tienen la oportunidad de actuar como canales de distribución de este tipo de componentes, desarrolladores de aplicaciones, o incluso llegar a actuar como empresas proveedoras de la solución completa: desarrollo de aplicación, integración, instalación y mantenimiento.

2.1.1- WECA (Wireless Ethernet Compatibility Alliance)

A mediados del año 1997, el IEEE (Institute of Electrical and Electronics Engineers – Instituto de Ingenieros Eléctricos y Electrónicos) hizo público el estándar 802.11 que definía las especificaciones para las WLAN, y poco después, a finales de 1999, vio la luz el estándar 802.11b que daría lugar posteriormente a la denominación Wi-Fi. Básicamente, esto significa que, vía radio se mantienen las características de una conexión Ethernet cableada. El grupo de trabajo 802.11 es el responsable del desarrollo de los estándares de redes de área local inalámbricas bajo los auspicios del Comité de Estándares del proyecto 802 de LAN/MAN del IEEE.

La WECA (Wireless Ethernet Compatibility Alliance – Alianza Ethernet de Compatibilidad Inalámbrica) fue fundada por 3Com, Cisco, Intersil, Agere, Nokia y Symbol Techonologies en Agosto de 1999, con el compromiso de impulsar el desarrollo a nivel mundial de la tecnología de LAN inalámbrica bajo el estándar IEEE 802.11. La lista de miembros se ha incrementado a más de 200. Desde entonces, Intermec, Microsoft e Intel han formado el comité de dirección de WECA.

2.1.2- Wi-Fi Alliance

Wi-Fi Alliance (Alianza Wi-Fi) anteriormente WECA, es una organización internacional, sin ánimo de lucro, formada en 1999 para certificar la interoperabilidad de productos inalámbricos de redes de área local basados en la especificación del IEEE 802.11.

Actualmente la Wi-Fi Alliance tiene más de 200 miembros alrededor del mundo, que representan a un nutrido grupo de relevantes empresas y más de 1.500 productos han recibido la certificación Wi-Fi® desde que el proceso de certificación empezase en Marzo de 2.000. El objetivo de los miembros de la Wi-Fi Alliance es enriquecer la experiencia de los usuarios a través de la interoperabilidad de sus productos.

Wi-Fi Alliance establece un procedimiento de certificación para garantizar la interoperatividad de los dispositivos entre fabricantes. Aquellos equipos con el logo Wi-Fi gozan de esa garantía de interoperatividad que básicamente consiste en:

- Ahorro de energía
- Encriptación WEP
- Control RTS/CTS
- Manejo de sistemas de polling
- Tiempo de respuesta de paquetes
- Tasas de transmisión
- Manejo de tramas inesperadas

Figura 2.1: Logotipos de certificación de productos de la Wi-Fi Alliance

Como se observa en los logotipos existe un código de color denominado SII (Standard Indicator Icons – Indicador Estándar de Íconos), que sirve para identificar a

todos los productos certificados por la Wi-Fi Alliance, lo cual sería muy importante tomar en cuenta antes de realizar cualquier compra de un dispositivo inalámbrico.

El logo de certificación Wi-Fi es la única garantía de que el producto ha pasado por rigurosos procedimientos de prueba para garantizar su compatibilidad con productos de otras marcas; este logotipo significa que se está realizando una compra segura. El código de color asignado garantiza al comprador que los productos adquiridos son interoperables.

2.1.3- Características

Las redes LAN inalámbricas están obteniendo actualmente una base de usuarios que se encuentra en una rápida expansión. A lo largo de los años, la LAN inalámbrica ha pasado por un proceso de estandarización y ha mejorado su velocidad además de alcanzar un precio asequible. También se puede utilizar conjuntamente con LAN cableada, como Ethernet, por lo que ahora tiene sentido utilizar un sistema inalámbrico.

Dentro de sus características mas importantes están:

Movilidad.- Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red alámbrica.

Simplicidad y rapidez en la instalación.- La instalación de una red inalámbrica puede ser tan rápida y fácil y además que puede eliminar la posibilidad de tirar cable a través de paredes y techos.

Flexibilidad en la instalación.- La tecnología inalámbrica permite a la red ir donde la alámbrica no puede ir.

Costo de propiedad reducido.- Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN alámbrica, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente

inferior. Los beneficios y costos a largo plazo, son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

Escalabilidad.- Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones especificas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

Desventajas.- Es importante destacar los principales inconvenientes o desventajas que están presentes en las redes inalámbricas 802.11:

- Costo de instalación, el costo inicial es mucho más alto que el de una red cableada.
- Rango de conectividad, el alcance va a depender del número de access points o routers instalados.
- Velocidad, con las WLANs no se alcanza todavía las velocidades que tienen las redes cableadas.
- Regulación, depende de cada país y generalmente son muy altos los costos de funcionamiento.
- Seguridad, los estándares de seguridad no son tan fiables como los de una red cableada.

2.1.3.1- ¿Qué es Wi-Fi?

Una WLAN 802.11b es una red de hosts (PDAs, PCs, etc) interconectados entre si principalmente a través de frecuencias radioeléctricas, permitiendo a un dispositivo conectarse sin cables a Internet y comunicarse con otros aparatos en un radio determinado sin cables. La red tiene dos principales componentes que son:

Terminales de usuario que son los clientes, llamados WC (Wireless Client – Cliente Inalámbrico) ó ROR (Remote Office Router – Router de Oficina Remoto) ó Remote Base, este nombre va a depender del fabricante. Los clientes están dotados de una tarjeta interfaz

de red NIC (Network Interface Card – Tarjeta de Interfase de Red) que incluye un transceptor radio y la antena.

Los nodos que son los puntos de acceso también llamados AP (Access Points – Puntos de Acceso), COR (Central Office Router – Router de Oficina Central), Base Unit, nombres que también dependen del fabricante. Los puntos de acceso actúan como puerta de enlace entre la parte cableada de la red y la parte inalámbrica.

La existencia en el mercado de dichos dispositivos capaces de interconectarse de forma barata y sencilla ha dado origen a una gran variedad de aplicaciones que sobrepasan ampliamente el ámbito de utilización en entornos empresariales para el que nacieron las WLAN.

En un principio, la expresión Wi-Fi era utilizada únicamente para los aparatos con tecnología 802.11b, el estándar dominante en el desarrollo de las redes inalámbricas, de aceptación prácticamente universal, que funciona en una banda de frecuencias de 2,4 GHz y permite la transmisión de datos a una velocidad de hasta 11Mbps y un alcance desde 10 hasta 100mts. en ambientes indoor dependiendo del área.

Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término Wi-Fi se extendió a todos los aparatos provistos con tecnología 802.11 que son: 802.11a, 802.11b, 802.11g, 802.11e, 802.11f, 802.11h, 802.11i.

2.1.3.2- Banda ISM

Las redes inalámbricas 802.11 ocupan la banda de frecuencias ISM (Industry, Scientific and Medical – Industrial Científica y Médica) considerada como de uso libre, es decir que, en general, no requiere licencia específica para su utilización.

Las utilizadas son la de 2,4 GHz y la de los 5 GHz. Hay que tener en cuenta que la banda de 2,4 GHz es utilizada por la tecnología Wi-Fi, como por otros estándares de

comunicaciones, como Bluetooth, Home RF para Home Networking. La utilización de la banda de 5 GHz permite incrementar tanto el ancho de banda como la capacidad de tráfico disponible, dando lugar a nuevas dimensiones para esta tecnología.

Las asignaciones de frecuencia son las siguientes:

- 433 Mhz para productos de poco alcance como puertas de garaje, etc.
- 850 Mhz para dispositivos de mayor ancho de banda, teclados, mouses, etc.
- 902 Mhz – 928 Mhz para transmisión de voz.
- 2400 Mhz – 2483,5 Mhz para WLAN.
- 5725 Mhz – 5850 Mhz para WLAN.

2.2- Clasificación de las redes inalámbricas

Dentro de la consideración genérica de redes inalámbricas se pueden encontrar distintas categorías en función del rango o alcance en que una tecnología presta un servicio:

2.2.1- Red de área personal inalámbrica (WPAN)

Un dispositivo PAN inalámbrico normalmente tiene un alcance de hasta 20m, lo que lo libera de las limitaciones de los cables.

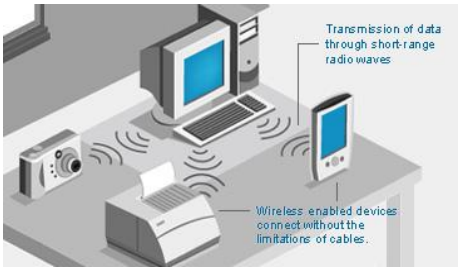


Figura 2.2: Esquema de una red de área personal inalámbrica

Con una red de área personal inalámbrica, puede:

- Conectar su sistema a una impresora

- Sincronizar un PDA
- Descargar imágenes de una cámara digital
- Transferir archivos MP3
- Conectarse a un teléfono móvil compatible con Bluetooth
- Conectarse a otro PC compatible con Bluetooth

2.2.2- Red de área local inalámbrica (WLAN)

Una WLAN crea un alcance que puede llegar hasta 100m. Puede conectarse a una WLAN desde su oficina o instalaciones de acceso público.

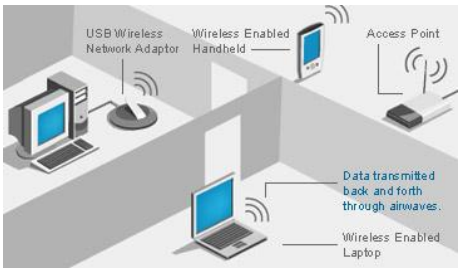


Figura 2.3: Esquema de una red de área local inalámbrica

En una red de área local inalámbrica, un dispositivo de comunicaciones por radiofrecuencia, denominado punto de acceso, conecta los ordenadores de la red. El punto de acceso es pequeño y ligero, con una antena conectada que envía los datos de un lugar a otro a través de las ondas del aire. La ilustración anterior muestra el funcionamiento de una WLAN en un entorno de oficina típico.

2.2.3- Red de área amplia inalámbrica (WWAN)

El alcance de una WWAN puede llegar hasta 30Km., lo que ofrece a los usuarios un modo de seguir conectados mientras se desplazan o están alejados de otra infraestructura de red.

Figura 2.4: Esquema de una red de área amplia inalámbrica

Las redes de área amplia inalámbricas transmiten los datos mediante señales de telefonía móvil, a través de un proveedor de servicios de telefonía móvil, con velocidades de conexión iguales a las de acceso telefónico de 56K.

2.3- Tecnologías alternativas a 802.11b

2.3.1- Tecnología Home RF

Home RF (Home Radio Frecuency - Radio Frecuencia para el Hogar) es una tecnología que ha sido definida por un grupo de compañías que se reúnen bajo el nombre de HRFWG (Home RF Working Group – Grupo de Trabajo RF para el Hogar) y que se encargan de mantener la interoperabilidad entre productos de diferentes empresas, tal y como hace "Wi-Fi Alliance" en Wi-Fi.

Home RF está basada en el Protocolo de Acceso Inalámbrico Compartido SWAP (Shared Wireless Access Protocol – Protocolo de Acceso Inalámbrico Compartido), que define una interfaz inalámbrica diseñada para soportar voz y datos, y especialmente pensada tanto para operar con los operadores de telefonía e Internet, como para la comunicación con teléfonos, periféricos o electrodomésticos dentro del hogar sin la necesidad de utilizar los cables.

Entre las características técnicas de este estándar se puede mencionar que añade un subconjunto de estándares DECT (Digital Enhanced Cordless Telecommunications –

Telecomunicaciones Digitales Realizadas sin Cordones), para proporcionar los servicios de voz (hasta seis conversaciones).

Home RF utiliza la misma banda de frecuencia que los estándares 802.11b y 802.11g, pero cuenta con un método de salto de frecuencia (SWAP) para no interferir con conexiones Bluetooth. Sus principales aplicaciones se encuentran en el ámbito doméstico, con la conexión sin cables para dispositivos como reproductores de vídeo o DVD, teléfonos, juguetes, etc. Su alcance es de alrededor de 50 metros, consiguiendo unas velocidades de transferencia que pueden variar entre 1,2,10 Mbps, conectando un total de hasta 127 dispositivos.

2.3.2- HiperLAN/2

Este es el nombre que se le ha dado a la nueva generación de la tecnología WLAN desarrollada por ETSI (European Telecommunications Standards Institute – Instituto de Estándares Europeo de Telecomunicaciones), un organismo similar al IEEE pero a nivel europeo.

Se trata de un sistema de comunicación inalámbrica basado en ATM (Asynchronous Transfer Mode – Modo de Transferencia Asincrónico), similar a UMTS pero que incorpora toda una serie de características adicionales como QoS (Quality of Service – Calidad de Servicio), orientación de la conexión para obtener una mayor eficiencia en la utilización de los recursos de radio, búsqueda automática de la frecuencia a utilizar (similar a los teléfonos móviles), y sobre todo una elevada velocidad de transmisión, que puede llegar hasta 54 Mbps.

Esta tecnología opera sobre la banda de frecuencia de los 5 GHz y utiliza el método de modulación OFDM (Ortogonal Frequency Division Multiplexing – Multiplexación Ortogonal por División de Frecuencia) al igual que ocurre con el estándar 802.11a, contando también con un radio de alcance similar, tanto en interiores (alrededor de 30 metros) como en exteriores (hasta 150 metros.).

2.3.3- Bluetooth

El Grupo de Interés Especial (SIG) Bluetooth se fundó a principios de 1998. Es un consorcio formado por aproximadamente 2000 empresas de las industrias informática, de telecomunicaciones y de redes.

El principal objetivo del SIG Bluetooth fue la creación de la especificación básica Bluetooth y una serie de perfiles que definen cómo implementar la especificación de forma estandarizada, de modo que los productos de diferentes fabricantes puedan trabajar conjuntamente sin ningún problema. El SIG Bluetooth está liderado por nueve empresas Promotoras: 3Com, Ericsson, Intel, IBM, Lucent, Microsoft, Motorola, Nokia y Toshiba.

Bluetooth es un radio enlace de corto alcance que aparece asociado a las redes de área personal inalámbricas o WPAN (Wireless Personal Area Network – Red Inalámbrica de Área Personal). Este concepto hace referencia a una red sin cables que se extiende a un espacio de funcionamiento personal o POS (Personal Operating Space - Espacio Operativo Personal) con un radio de hasta 20 metros.

Bluetooth tiene un mercado objetivo que esta compuesto por equipos informáticos y de comunicación portátil y móvil, como ordenadores, PDAs, impresoras, ratones, micrófonos, auriculares, lectores de código de barras, censores, displays, localizadores, teléfonos móviles y otros dispositivos de electrónica de consumo. El objetivo es que todos estos equipos se puedan comunicar e interoperar entre sí sin interferencias.

El estándar actual de Bluetooth es 802.15 (IEEE) y trabaja en el rango de frecuencias de 2,402 GHz a 2,480 GHz. La primera versión de Bluetooth, la que implementan los circuitos disponibles actualmente, puede transferir datos de forma asimétrica a 721 Kbps y simétricamente a 432 Kbps. Se puede transmitir voz, datos e incluso vídeo. Para transmitir voz son necesarios tres canales de 64 Kbps. Para transmitir

vídeo es necesario comprimirlo en formato MPEG-4 y usar 340 Kbps para conseguir refrescar 15 veces por segundo una pantalla VGA de 320x240 puntos.

Además, utiliza un sistema de saltos de frecuencia a 1600 saltos por segundo, todo esto junto con su ajuste automático de la potencia de salida para reducir el alcance exactamente a lo requerido hace que sea extremadamente difícil interceptar el sistema.

2.3.4- Cuadro comparativo de tecnologías inalámbricas

Cuadro 2.1: Cuadro comparativo de tecnologías inalámbricas

	BlueTooth	**HyperLan/2**	**HomeRF**	**WLAN 802.11**
Organización e Interoperabilidad	BlueTooth SIG	H2GF	HRFWG	Wi-Fi Alliance
Tasa de Transmisión	1Mbps	54 Mbps	1,2,10 Mbps	11 Mbps, 54 Mbps
Rango de Frecuencia	2.4 Ghz	5.8 Ghz	2.4 Ghz	2.4 Ghz, 5.8 Ghz
Canalización	FHSS	OFDM	FHSS	DSSS, FHSS, OFDM
Alcance	10 – 30 mts.	30	50 mts.	10 a 100 mts. Indoors
Portátil	Si	Si	Si	Si

2.4- Estándares del 802.11 IEEE

Como estándares adicionales dentro del grupo 802.11, dignos de mención por su importancia en la mejora y evolución de las normas básicas o por cubrir aspectos no contemplados en esas normas se destacan los siguientes:

2.4.1- 802.11

Este fue el primero de los estándares definidos por la IEEE para aplicaciones WLAN, y fue publicado en 1997. Funciona sobre los 2,4 GHz (de 2.400 MHz a 2.483,5 MHz) y utiliza dos tipos de modulación: DSSS (Direct Sequence Spread Spectrum – Propagación de Espectro por Secuencia Directa) y FHSS (Frequency Hopped Spread Spectrum – Propagación de Espectro por Salto de Frecuencia). La velocidad de transmisión que es capaz de alcanzar está entre 1 ó 2 Mbps, dependiendo del fabricante.

Este estándar está prácticamente en desuso, debido a la aparición de una serie de variantes que mejoran no sólo la velocidad de transferencia, sino que además dan cobertura a funciones especiales de seguridad y de integración con redes de cable.

2.4.2- 802.11b

Es la evolución natural del anterior estándar. Básicamente, se diferencian en el uso exclusivo de la modulación DSSS con el sistema de codificación CCK (Complementary Code Keying – Código de Llaves Complementarias) que sólo funciona con esta modulación. Esto le permite ofrecer hasta 11 Mbps. Las velocidades de transmisión que es capaz de ofrecer podrán variar desde 1, 2, 5.5, y 11 Mbps, dependiendo de diferentes factores.

Esta característica, denominada DRS (Dynamic Rate Shifting – Cambio de Transferencia Dinámico) permite a los adaptadores de red inalámbricos reducir las velocidades para compensar los posibles problemas de recepción que se pueden generar por las distancias o los materiales que es necesario atravesar.

Según la Wi-Fi Alliance, la velocidad del estándar 802.11b decrece dependiendo de la distancia a la cual se encuentra el cliente de la estación base. Por ejemplo, cuando el cliente se encuentra cerca de la estación base puede estar en capacidad de conectarse a la máxima velocidad de 11Mbps; a medida que empieza a alejarse y dependiendo del ambiente, su velocidad de conexión puede bajar a 5.5Mbps.

Si el cliente se alejara más la velocidad bajaría a 2Mbps y finalmente a 1Mbps. Aún así, si se llegara a la velocidad más baja del estándar, ésta brinda un rendimiento perfectamente aceptable ya que 1Mbps es mucho más rápido que la mayoría de las conexiones DSL y cableadas, lo que significa que todavía es una velocidad de conexión aceptable ya que se puede tranquilamente enviar o recibir emails o navegar por Internet desde un cliente portátil.

Cuadro 2.2: Cuadro de rangos estimados de alcances de 802.11b según Wi-Fi Alliance

	Máximo Rango a 1Mbps	**Máximo Rango a 11Mbps**
Ambientes Outdoors	225 a 300 mts.	45 a 105 mts.
Ambientes Indoors	10 a 105 mts.	18 a 45 mts.

Otros datos a tener en cuenta sobre este estándar es el soporte para 3 canales sin solapamiento y su reducido nivel de consumo, que le hace perfectamente válido para su uso en PCs, portátiles o PDAs.

Es importante la comprensión acerca de los canales ya que estos afectan la capacidad total de una WLAN. Un canal representa una banda angosta de frecuencia de radio. Debido a que la frecuencia de radio modula dentro de una banda de frecuencias, existe un limite de ancho de banda dentro de cualquier rango dado para transportar datos.

Es importante además que las frecuencias no se solapen porque el rendimiento se reduciría significativamente mientras la red clasifica y arma de nuevo los paquetes de datos enviados por el aire.

Cada canal transportará un máximo rendimiento para su estándar. Por lo tanto, el estándar 802.11b cuenta con un máximo de 3 canales no solapados que transportan un rendimiento de 11 Mbps cada uno, equivalente a un rendimiento total de 33 Mbps.

En el caso de Estados Unidos y de Europa la tecnología de espectro ensanchado por secuencia directa, DSSS, opera en el rango que va desde los 2.4 GHz hasta los 2.4835 GHz, es decir, con un ancho de banda total disponible de 83.5 MHz. Este ancho de banda total se divide en un total de 11 canales con un ancho de banda por canal de 22 MHz de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular.

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema, si la separación entre las frecuencias centrales es como mínimo de 30 MHz.

Esta independencia entre canales permite aumentar la capacidad del sistema de forma lineal con el número de puntos de acceso operando en un canal que no se esté utilizando y hasta un máximo de tres canales. Se suelen ocupar los canales 1,6 y 11.

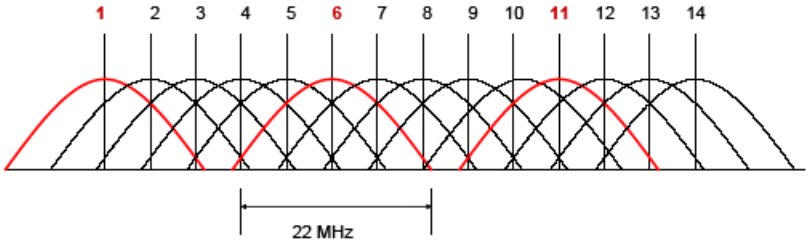


Figura 2.5: Esquema del Método de canalización

Es necesario mencionar que parte de la información transmitida en el aire es específica de la transmisión radio (cabeceras, codificación, etc.) y por lo tanto no forma parte de la capacidad útil para el usuario. Es decir que los valores de velocidad máxima de 11 Mbps ó de 54 Mbps no son equivalentes al concepto de velocidad aplicado en las redes LAN cableadas.

Según los proveedores de tecnología 802.11b, en aplicaciones wireless se estima que el overhead puede llegar a un 60% del total de datos procesados. Por ende, el ancho de banda real de datos de información (throughput) se ubicará entre los 4 a 6 Mbps en un enlace 802.11

Cuadro 2.4: Cuadro comparativo de Throughput WLAN

Norma	**Velocidad Máxima (Mbps)**	**Velocidad Efectiva (throughput) Mbps**
802.11b	11	4.8 ~ 6
802.11a	54	32

802.11g	54	~20

Además la capacidad mencionada debe ser compartida por los distintos usuarios que comparten un mismo Punto de Acceso (AP). Cuando la capacidad resultante para cada usuario no es suficiente para la aplicación requerida es necesario incrementar el número de AP´s en una misma celda (utilizando diferentes canales radio) y así permitir mayores densidades de tráfico.

2.4.3- 802.11a

Es una evolución del 802.11b, fue ratificado en el año 2000 y también se lo conoce como Wi-Fi5, presenta como diferencia fundamental su funcionamiento sobre la banda de frecuencia U-NII de 5.8 GHz, utilizando la técnica de modulación de radio OFDM, que utiliza 64 sub-portadoras en un tamaño de canal de 20MHz y una modulación de 64 QAM (64 Level Quadrature Amplitude Modulated – 64 Niveles de Amplitud Modulada), además tiene 12 canales no solapados.

Estos productos soportan hasta 54 Mbps / 30 Mbps efectivos en datos. 802.11a no es compatible con 802.11b o 802.11g, ya que opera en una diferente frecuencia. Estos dispositivos soportan usualmente la más nueva seguridad como WPA, WPA2, WEP, SSID, 802.1x y filtración MAC.

La frecuencia de funcionamiento más alta del estándar 802.11a tiene como consecuencia un alcance relativamente más corto. Se necesitarán más puntos de acceso 802.11a para cubrir la misma zona. Pero incluso con estos inconvenientes, las pruebas iniciales demuestran que los productos 802.11a ofrecen un rendimiento casi tres veces superior al de los 802.11b en cuanto a alcances en interiores.

Aunque este aumento en la velocidad presenta una excelente ventaja, lo cierto es que esta norma cuenta también con algunas desventajas con respecto a su antecesora, como es el mayor nivel de consumo (que la hace menos idónea para su instalación en portátiles o

PDA´s), o la falta de compatibilidad con el 802.11b debido al cambio de frecuencia, aunque esto último ya se ha resuelto a través de puntos de acceso que ofrecen soporte para ambos estándares.

Otro dato que se puede resaltar sobre este estándar es que las distancias de cobertura se ven reducidas significativamente, alcanzando entre 30 mts. (54 Mbps) y 300 mts. (6 Mbps) en exteriores, y entre 12 mts. (54 Mbps) y 90 mts. (6 Mbps) cuando se utiliza en interiores.

Un punto de acceso 802.11b de 2,4 GHz, por ejemplo, no podrá trabajar con una tarjeta de interfaz de red 802.11a de 5 GHz. No obstante, estos estándares pueden coexistir perfectamente

2.4.4- 802.11g

En Junio del año 2003 se aprobó un nuevo estándar, el 802.11g, que se basa en la norma 802.11b. Más avanzada que su predecesora, trabaja sobre la misma frecuencia de los 2,4 GHz y es capaz de utilizar dos métodos de modulación DSSS y OFDM, lo cual lo hace compatible con el estándar 802.11b ya que también utiliza CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance – Sentido Portador de Múltiple Acceso / Evitar Colisión) y MAC.

Al soportar ambas codificaciones, este nuevo estándar utiliza 3 canales no solapados por lo cual será capaz de incrementar notablemente la velocidad de transmisión, pudiendo llegar hasta los 54 Mbps que oferta la norma 802.11a, usando un tamaño de canal de 20 MHz así como una modulación de 64 QAM; además manteniendo las características propias del 802.11b en cuanto a distancia, niveles de consumo y frecuencia utilizada.

De este modo, la mayor bondad de esta nueva norma es el incremento de velocidad manteniendo una total compatibilidad con el estándar Wi-Fi, permitiendo la coexistencia

entre ambos estándares en una misma instalación, algo realmente significativo si se toma en cuenta la importancia de la base instalada.

Los dispositivos 802.11g soportan usualmente las más nuevas características de seguridad como WPA, WPA2, 802.11i, WEP, SSID, 802.1x y filtración MAC.

En comparación con el estándar IEEE 802.11a, el 802.11g tiene un ancho de banda utilizable más bajo, lo que redunda en un menor número de usuarios WLAN de alta velocidad. Aunque las modulaciones OFDM permiten una velocidad más alta, el ancho de banda disponible total en la banda de frecuencia de 2,4 GHz no varía. El motivo es que el IEEE 802.11g todavía está restringido a tres canales en la banda de 2,4 GHz.

Los productos IEEE 802.11g son capaces de conseguir velocidades de datos más elevadas y con mayor alcance que los productos con tecnología 802.11a. La combinación de OFDM y la mejor capacidad para atravesar paredes de sus 2,4 GHz confieren a los productos 802.11g una ventaja clara sobre otras tecnologías WLAN de alta velocidad. La capacidad para proporcionar una cobertura de gran rendimiento, en un área comparativamente grande desde un único punto de acceso, supone un factor importante de coste.

2.4.5- 802.11e

Se podría definir como la implementación de características de QoS (Quality of Service – Calidad de Servicio) y multimedia para las redes 802.11b. Esta especificación que está haciendo el IEEE será aplicable tanto a 802.11b como a 802.11a.

2.4.6- 802.11f

Básicamente, es una especificación que funciona bajo el estándar 802.11g y que se aplica a la intercomunicación entre puntos de acceso de distintos fabricantes, permitiendo el *roaming* o itinerancia de clientes.

2.4.7- 802.11h

Una evolución del IEEE 802.11a que permite asignación dinámica de canales y control automático de potencia para minimizar los efectos de posibles interferencias.

2.4.8- 802.11i

Este estándar que hasta la fecha de ésta investigación no ha sido oficializado, permite incorporar mecanismos de seguridad para redes inalámbricas, ofrece una solución interoperable y un patrón robusto para asegurar datos.

Actualmente, ya existen en el mercado gamas completas de productos multibanda y multimodo que cumplen con estos estándares y que, al mismo tiempo, facilitan sus prestaciones y permiten mayor flexibilidad e interoperabilidad entre distintas redes.

Uno de los mayores proveedores de equipamiento, 3Com, ya anunció el pasado año una solución con los tres estándares Wi-Fi. Los nuevos puntos de acceso y los dispositivos cliente tribanda 802.11 a/b/g para WLAN incorporan seguridad inalámbrica avanzada.

La integración de estos tres estándares en una solución permitirá a los usuarios empresariales proteger su inversión, a la vez que disponen de una red segura, flexible y fiable a múltiples velocidades y frecuencias sobre una misma infraestructura.

2.4.9- Resumen IEEE

Cuadro 2.5: Cuadro comparativo de las tres variantes más importantes de 802.11

	802.11b	**802.11g**	**802.11a**
Compatibilidad	IEEE 802.11b Wi-Fi Certificado	IEEE 802.11b y 802.11g Wi-Fi Certificado	IEEE 802.11a Wi-Fi Certificado
Numero de canales	3 canales no solapados	3 canales no solapados	12 canales no solapados (4 en algunos países)
Rango típico Ambientes Indoor	45 mts. a 11 Mbps; 105 mts. a 1 Mbps	30 mts. a 54 Mbps; 91 mts. a 6 Mbps	12 mts. a 54 Mbps; 91 mts a 6 Mbps
Rango típico Ambientes Outdoor	105 mts. a 11 Mbps; 300mts. a 1 Mbps	105 mts. a 54 Mbps; 300 mts a 6 Mbps	30mts. a 54 Mbps; 305mts. a 6 Mbps

Tasas de transferencia	11, 5..5, 2 y 1 Mbps	54, 48, 36, 24, 18, 12, 9 y 6 Mbps	54, 48, 36, 24, 18, 12, 8 y 6 Mbps
Medio Wireless	DSSS, 2.4 GHz	OFDM/DSSS, 2.4 GHz	OFDM, 5 GHz

2.5- Topologías WLAN

El elemento fundamental de la arquitectura de las redes 802.11 es la celda, la cual se puede definir como el área geográfica en la cual una serie de dispositivos se interconectan entre sí por un medio aéreo. A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión es posible combinar las celdas de estas señales para cubrir de forma casi total un área más extensa.

En general, esta celda estará compuesta por estaciones y un único punto de acceso. Las estaciones son adaptadores que permiten la conversión de información, generalmente encapsulada bajo el protocolo Ethernet, existente en terminales o equipos clientes, y su envío y recepción dentro de la celda. El punto de acceso es el elemento que tiene la capacidad de gestionar todo el tráfico de las estaciones y que puede comunicarse con otras celdas o redes. Es a todos los efectos un bridge (puente) que comunica a nivel 2 (capa de enlace) los equipos, tanto de su celda de cobertura, como a otras redes a las cuales estuviese conectado. A esta configuración se le denomina BSS (Basic Service Set - Grupo de Servicio Básico).

El BSS es, por tanto, una entidad independiente que puede tener su vinculación con otros BSS a través del punto de acceso mediante un DS (Distribution System - Sistema de Distribución). El DS puede ser interrogado (comunica el BSS con una red externa), cableado (con otros BSS a través de cable como por ejemplo una red Ethernet fija convencional), o también inalámbrico, en cuyo caso se denomina Sistema de distribución inalámbrica (Wireless Distribution System).

Existen algunas variantes de BSS que se describen a continuación:

BSS Independiente (IBSS, "Independent Basic Service Set").- Consiste en una celda inalámbrica en la cual no hay sistema de distribución y, por tanto, no tiene conexión con otras redes. Es utilizado en redes tipo Ad-Hoc.

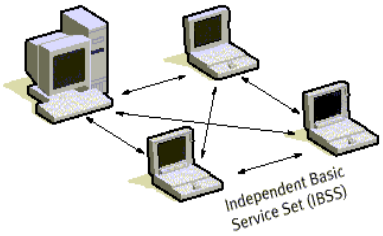


Figura 2.6: Esquema de IBSS en una red Ad-Hoc

BSS Extendido (ESS, "Extended Service Set"). Es un caso específico del modo infraestructura, representado por un conjunto de BSS asociados mediante un sistema de distribución. Esto permite una serie de prestaciones avanzadas opcionales como el *roaming* entre celdas. Se presentan como una LAN simple para el nivel LLC (Link Layer Control – Capa de Control de Enlace), sin notar que forman diferentes puntos de la red.

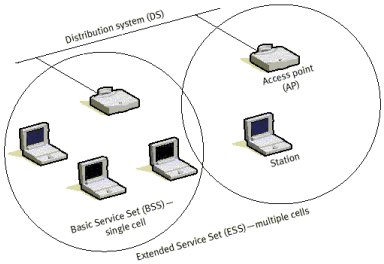


Figura 2.7: Esquema BSS extendido y DS

Es conveniente hacer una división entre la topología y el modo de funcionamiento de los dispositivos Wi-Fi. Topología se refiere a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo

de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida; es decir es la forma como se configura la red inalámbrica considerando los distintos ambientes de entorno. En el mundo Wireless existen dos topologías básicas que son:

- Modo Ad-Hoc
- Modo Infraestructura

2.5.1- Modo Ad-Hoc o Red Autónoma Ad-Hoc

Estas redes nacen bajo el concepto de autonomía e independencia, ya que no se requiere contar con algún tipo de infraestructura física preexistente (en su definición formal); no opera bajo esquemas de control centralizado; su topología cambia de forma dinámica y de manera aleatoria; se conecta a los demás dispositivos de la red regularmente a través de múltiples saltos radio eléctricos; los nodos que conformen una red Ad-Hoc operarán como dispositivos finales (emisores o receptores de información) y/o como enrutadores, funcionando básicamente en un ambiente colaborativo de conectividad.

Una red Ad-Hoc, definida de manera amplia es un conjunto de nodos móviles (en general) e inalámbricos, los cuales se unen voluntariamente formando una red entre ellos, sin la necesidad de ninguna entidad administrativa centralizada o soporte físico de red existente (en su forma básica). Visto desde otro enfoque una red Ad-Hoc es Auto Creada (Self Creating), Auto Organizada (Self Organizing) y Auto Administrada (Self Administering).

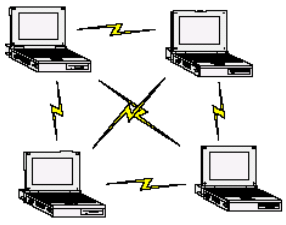


Figura 2.8: Esquema de una red de Ad-Hoc

Los ordenadores de la red inalámbrica que quieren comunicarse entre ellos necesitan usar el mismo canal radio y configurar un identificador específico de Wi-Fi (denominado SSID) en "Modo Ad-Hoc"; una buena alternativa para este tipos de redes son los entornos SOHO (Small Office Home Office – Pequeña Oficina Pequeño Hogar) o temporal.

2.5.2- Modo Infraestructura

En esta topología existe un nodo central AP Wi-Fi, que sirve de enlace para todos los demás (Tarjetas de red Wi-Fi). Este dispositivo es el punto de acceso inalámbrico a la red de PC´s (LAN) cableada. Es decir, es la interfaz necesaria entre una red cableada y una red inalámbrica, es el traductor entre las comunicaciones de datos inalámbricas y las comunicaciones de datos cableadas.

Figura 2.9: Esquema de una red inalámbrica en modo Infraestructura

Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP.

Estos modos de funcionamiento sugieren que básicamente los dispositivos Wi-Fi son todos iguales, siendo los que funcionan como APs realmente tarjetas de red a las que se les ha añadido cierta funcionalidad extra vía firmware o vía software.

Esta afirmación se ve confirmada, al descubrir que muchos APs en realidad lo que tienen en su interior es una placa de circuitos integrados con un firmware añadido a un adaptador PCMCIA, en el cual se le coloca una tarjeta PCMCIA idéntica a las que funcionan como tarjetas de red inalámbricas.

2.5.3- Redes Mesh

Las redes Mesh 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 APs, están dentro del rango de cobertura de algún cliente (tarjeta de red inalámbrica) que directa o indirectamente está dentro del rango de cobertura del AP.

En las redes Mesh, las mallas emergen de los mismos dispositivos inalámbricos que las conforman enviando señales de dispositivo en dispositivo. En el caso de una red Wi-Fi, un nodo en la malla buscaría automáticamente a otro que está conectado a un punto de acceso desde el cual, por ejemplo, se obtiene acceso a Internet. En resumidas cuentas los dispositivos terminales se convierten en la red propiamente dicha.

Dependiendo de la cantidad de dispositivos inalámbricos que son parte de la red, las redes en malla puede extenderse a través de vastas áreas, utilizando muy pocos nodos conectados a Internet para proveer acceso a todos los clientes que conforman la infraestructura.

Las redes en malla tienen además otros beneficios como ser altamente adaptables y escalables. Pueden ser redundantes de manera que cada dispositivo tenga dos o más caminos para enviar datos, lo cual las hace altamente confiables. Se pueden agregar más nodos sencillamente agregando otro dispositivo a la red, también pueden escalarse para contener un gran número de dispositivos y puntos de acceso a Internet.

En cuanto a la conexión entre nodos existen varias alternativas que se describen a continuación:

1. Radioenlace dedicado
    - Se puede aprovechar de antenas direccionales.
    - Se gana mayor ancho de banda, 11Mbps con 802.11b.
2. Radioenlace compartido con la red de clientes
    - Peor rendimiento por el aumento de tráfico.
3. Enlace a través de Internet usando una VPN
    - Opción más económica e inicialmente más factible.
4. Múltiples enlaces de un nodo con la red
    - Es un sistema más robusto.
    - La conectividad de la red no depende de un solo nodo.

2.6- Configuraciones de redes WLAN

En todo sistema 802.11 se establece un diálogo entre los adaptadores (CPEs Customer Premise Equipment ó Tarjeta de acceso a la red inalámbrica) y el Punto de Acceso (AP) a través de una comunicación radioeléctrica a una frecuencia de 2.4 Ghz (802.11b). La propagación a estas frecuencias es muy susceptible a atenuaciones producidas por obstáculos existentes en la trayectoria entre el CPE y el AP.

Una opción para conseguir una mayor cobertura en redes inalámbricas 802.11b consiste en utilizar diversos AP, interconectados entre sí, y donde cada uno de ellos proporciona una célula de cobertura. Solapando células se consigue aumentar la cobertura. Entre diversas células es posible disponer de una capacidad de “hand over”, de esta forma un terminal puede moverse de una célula a otra sin perder la conexión, consiguiéndose el efecto de una cobertura celular.

2.6.1- Ambientes Indoors

En estas aplicaciones donde la antena está integrada a la tarjeta de red inalámbrica, la distancia entre el CPE y el AP puede llegar a los 300 metros cuando no existen paredes u obstáculos en la trayectoria entre ambos. Cuando existen obstáculos estas distancias se disminuyen en proporción directa al grosor y material del obstáculo.

En las aplicaciones en interiores puede suceder, que con el fin de incrementar el área de servicio interno en un edificio, sea necesaria la instalación de más de un AP. Cada AP cubrirá una área de servicio determinada y las computadoras tomarán servicio de LAN a través del AP más cercano.

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

Es importante mencionar ejemplos de posibles obstáculos que interferirían en una red WLan en un ambiente indoor; a continuación se destacan algunos de ellos:

Cuadro 2.6: Ejemplos de posible obstáculos

MATERIAL	ATENUACIÓN
Pared de ladrillo	2dB
Pared de metal o vidrio dentro de un edificio	6dB
Pared de oficina	6dB
Puerta de metal en una pared de oficina	6dB
Puerta metálica en pared de ladrillo	12.4dB
Pared de ladrillo al lado de una puerta metálica	3dB

2.6.2- Ambientes Outdoors

En estas aplicaciones se recomienda que la trayectoria entre el CPE y el AP este totalmente libre de obstáculos. A este requisito se lo denomina LoS (Line of Sight - Línea

de Vista). Es decir, ubicados en donde se encuentra la antena externa del CPE se tiene que poder ver la antena del AP (nodo de la red).

En estas aplicaciones los rangos de cobertura pueden llegar a varios kilómetros (por ejemplo : 5 Km) según la configuración total de la red.

Dentro de las variables que determinan la cobertura de un sistema Outdoor se puede mencionar:

- Longitud y tipo de cable instalado entre el CPE y la antena externa.
- Ganancia de la antena del CPE. Usualmente se trabaja con antenas cuya ganancia oscila entre 7 dBi a 24 dBi de acuerdo a la distancia entre el CPE y el nodo donde se instala el AP.
- Ganancia de la antena del nodo donde se ubica el AP. Dicha ganancia oscila entre los 6 dBi a los 13 dBi. La antena puede ser Omnidireccional o sectorizada.
- Uso de amplificadores bidireccionales junto a la antena del nodo. Este dispositivo activo incrementa la cobertura de un sistema.
- Longitud y tipo de cable instalado entre la antena del nodo y el AP.

2.6.2.1- Ambientes Outdoor Punto-Punto

En esta configuración se tiene aplicaciones de enlaces punto a punto 802.11b uniendo dos LANs a 11 Mbps ó 22 Mbps que pueden distar varios kilómetros entre sí; enlaces uniendo una PC con una LAN remota o enlaces uniendo dos PC entre sí. Permite conectar puntos distantes (varios kilómetros) a través de un vínculo de datos a 11 Mbps ó 22 Mbps.

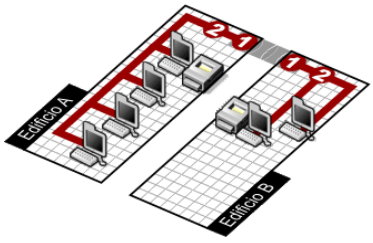


Figura 2.10: Enlace Outdoor Punto – Punto

En donde:

(1) Es un AP funcionando en modo Bridge y conectado a una antena exterior direccional.

(2) Es un Switch

2.6.2.2- Ambientes Outdoor Punto-Multipunto

En esta configuración se tiene aplicaciones de enlaces punto a multipunto, permitiendo conexiones de datos a 11 Mbps ó 22 Mbps entre distintos nodos de una ciudad. Ahora se puede unir las redes de varias sucursales de manera sencilla y económica.

Proveer servicio de Internet inalámbrica en una comunidad o población, con suma facilidad se puede ser Proveedor de Servicio de Internet Inalámbrica (WISP) en pequeñas poblaciones, cooperativas, universidades, edificios, sucursales de una forma sencilla y económica.

En las aplicaciones de Internet Inalámbrica para exteriores puede darse el caso que la cantidad de abonados CPE sea elevado, y debido al alto tráfico que ellos generan, se requiera instalar más de un AP con el fin de poder brindar servicio de alta calidad; en lo que se refiere a mejorar el área de cobertura, puede instalarse en el nodo central un amplificador bidireccional a tope de torre. A continuación se muestra un ejemplo de una típica instalación inalámbrica con cobertura de exteriores:

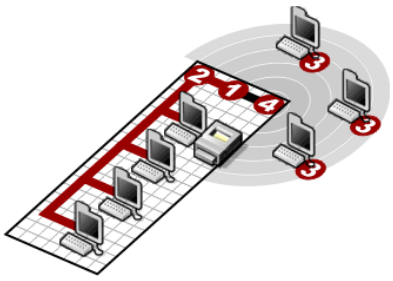


Figura 2.11: Enlace Outdoor Punto - Multipunto

En donde:

(1) AP funcionando en modo AP y conectado a una antena exterior omnidireccional con 8 dBi de ganancia y cobertura horizontal de 360º

(2) Switch

(3) Ordenadores con acceso a la red inalámbrica mediante adaptadores Wi-Fi, disponibles en PCI, USB, PCMCIA (PC Card) o Compact Flash II. Los ordenadores pueden estar en un área de hasta 1 km. del punto (1)

(4) Antena OmniDireccional

Vale la pena destacar que aunque la antena tenga una cobertura horizontal de 360º, es decir total, no habrá recepción en el otro lado del edificio debido a las múltiples paredes que hay en medio. En el gráfico no aparece la cobertura interior, esto es porque la antena (de muy reducidas dimensiones) irá en el exterior, y en consecuencia, la cobertura en el interior en el área adyacente a la antena será variable.

2.7- Funcionamiento de la Tecnología WLAN 802.11b

Las redes inalámbricas se diferencian de las convencionales principalmente en la Capa Física (PHY) y en la Capa de Enlace de Datos (MAC), según el modelo de referencia OSI.

La Capa Física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos, se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse. Los dos métodos para remplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

2.7.1- Capa Física (PHY)

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos. En la capa física, se definen dos métodos de transmisión RF y un infrarrojo. El funcionamiento de la WLAN en bandas RF ilícitas,

requiere la modulación en banda ancha para reunir los requisitos del funcionamiento en la mayoría de los países.

Los estándares de transmisión RF son:

Propagación de Espectro por Frecuencia de Saltos (FHSS).- Esta modulación utiliza una portadora de banda estrecha, que cambia la frecuencia utilizando un patrón conocido únicamente por transmisor y el receptor. Si se sincronizan bien ambos, el efecto es equivalente a mantener un único canal lógico. Un receptor que desconozca el patrón verá una señal compuesta de impulsos de corta duración, idecodificable y por tanto interpretada como ruido.

Propagación de Espectro por Secuencia Directa (DSSS).- En este caso, se genera un patrón redundante llamado ***señal de chip***, para cada bit que se transmite. Como más largo sea, mayor será la probabilidad que los datos originales se puedan recuperar en el receptor; aunque el ancho de banda requerido para la transmisión lógicamente será mucho mayor. Aunque algún bit de este patrón se pierda, puede ser recuperado mediante técnicas estadísticas. Para un receptor desconocido la señal DSSS le parecerá como un ruido de baja potencia, que será rechazado por la mayoría de receptores.

DSSS tiene definidos tres tipos de modulaciones para aplicar a la señal de información una vez que se sobrepone la señal de *chip* tal y como especifica el estándar IEEE 802.11:

- La modulación DBPSK, Differential Binary Phase Shift Keying que proporciona una tasa de transferencia de 1 Mbps.
- La modulación DQPSK, Differential Quadrature Phase Shift Keying que proporciona una tasa de transferencia de 2 Mbps.

- La modulación CCK (Complementary Code Keying) que consiste en un conjunto de 64 palabras código de 8 bits proporcionando velocidades de transferencia de 5,5 y 11 Mbps.

2.7.2- Capa de enlace de datos (MAC)

La capa de gestión MAC, controlará aspectos tales como las funciones de entrega segura de datos con la reserva del canal (por ser éste un medio compartido), se encarga de la privacidad de los datos transmitidos, sincronización y los algoritmos del sistema de distribución, que se define como el conjunto de servicios que precisa o propone el modo infraestructura.

La arquitectura MAC del estándar 802.11 se compone de dos funcionalidades básicas que son:

- La Función de Coordinación Distribuida (DFC), que gestiona el acceso al medio mediante un proceso de contención (acceso contienda).
- La Función de Coordinación Puntual (PCF), que gestiona el acceso al medio mediante un proceso centralizado en el AP.

2.8- Cálculo de Enlaces

El desempeño de las redes inalámbricas de área local, o cualquier otro sistema inalámbrico, se ve fuertemente influenciado por las características de sus puntos de acceso (antenas transmisoras), como lo son su cantidad, ubicación y potencia de transmisión. Por esta razón es muy importante realizar una planeación cuidadosa de estas características para optimizar los recursos que se tienen y brindar una mejor calidad de servicio, ya que estos dispositivos usualmente representan la mayor inversión en el montaje de una WLAN, no sólo por su costo sino también por la instalación del cableado de energía y de datos que estos requieren.

Para realizar el cálculo de los enlaces en el montaje de una red inalámbrica hay que partir del siguiente concepto:

"La ganancia del sistema debe ser mayor o igual que la suma de todas las ganancias y pérdidas incurridas por una señal, conforme se propaga de un transmisor a un receptor".

Entonces: $$G_s = P_t - C_{min}$$

En donde:

- G_s = Ganancia del sistema (dB).
- P_t = Potencia de salida del transmisor (dBm).
- C_{min} = Potencia mínima de entrada del receptor para un objetivo de calidad determinado (umbral recepción).

Partiendo de la fórmula anterior y desglosando cada uno de los factores que intervienen en el cálculo del enlace se tiene:

Pr = Pt + Ganancias – Pérdidas

Pr = Pt + At + Ar – Lc – Lp – Fm - Int

En donde:

- Pr = Potencia del receptor.
- Pt = Potencia de salida del transmisor.
- At = Ganancia de la antena de Tx.
- Ar = Ganancia de la antena de Rx.
- Lc = Pérdidas en los cables, pigtails, pararrayos y demás elementos.
- Lp = 92.5 + 20log(F) + 20log(D) = Pérdidas en el espacio libre;
    - F = Frecuencia en Ghz.
    - D = Distancia en Km.

- Fm = Margen de desvanecimiento para un determinado objetivo de confiabilidad (10dB). Para menos de 10 Km.
- Int = Parámetro opcional que representa la interferencia si es que existiera.

Figura 2.12: Esquema de cálculo de un enlace

2.8.1- Zona de Fresnel

La Zona de Fresnel, es el volumen vacío que tiene que haber entre el emisor y el receptor. La altura mínima a la que se tendrán que colocar las antenas será ***r,*** es decir, la distancia del objeto más alto a la línea que forman las dos antenas. Esta distancia nunca debe ser mayor del 60% de ***r*** más la curvatura de la tierra.

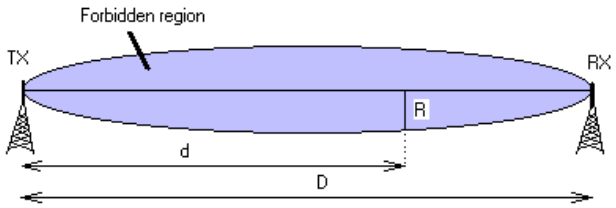


Figura 2.13: Esquema de la Zona de Fresnel

No basta con ver la otra antena, es preciso tener una visión ‘amplia’, en realidad se requiere una elipse libre de obstáculos entre antenas. La vegetación puede crecer y obstaculizar la visión en alguna época del año

Para evitar pérdidas NO deberían haber obstáculos dentro de esta zona (región prohibida) porque un obstáculo alterará el flujo de energía. Es importante destacar además la atenuación por lluvia en las diferentes bandas:

En 2.4 Ghz:

- Lluvia torrencial (4 pulg/hora)
  - 0.05 dB/Km
- Lluvia ligera
  - 0.02 dB/Km

En 5.8 Ghz:

- Lluvia torrencial (4 pulg/hora)
  - 0.05 dB/Km
- Lluvia ligera
  - 0.07 dB/Km

2.9- Dispositivos inalámbricos y antenas

Las redes inalámbricas se pueden configurar de diversas maneras, para lo cual se necesitan algunos elementos fundamentales basándose en las posibles arquitecturas y estructuras de red descritas anteriormente.

Actualmente hay dos tipos de componentes Wi-Fi que se necesitarían para armar una red de hogar o de oficina:

- Dispositivos de radio Wi-Fi (también conocidos como dispositivos del cliente) que son PC´s, Laptops, PDAs, etc.
- Access points o gateways que actúan como estaciones base.

Un tercer tipo de periféricos con tecnología Wi-Fi han aparecido y muy pronto serán de uso común como impresoras, scanners, cámaras, teléfonos celulares, etc.

2.9.1- Adaptadores de red inalámbricos

Las redes Wi-Fi utilizan radio frecuencia para emitir datos a otros equipos habilitados con tecnología Wi-Fi; siendo los dispositivos más comunes las tarjetas de red inalámbricas. Hay algunas variantes pero las más estandarizadas son:

Tarjeta de red inalámbrica PCMCIA o PC Card Radio.- Estas tarjetas están diseñadas para ser insertadas en la ranura Tipo II del puerto PCMCIA (Personal Computer Memory Card International Association) que tienen las computadoras portátiles (Laptops). Estas tarjetas antes eran conocidas como PCMCIA pero ahora son simplemente llamadas PC cards.

Figura 2.14: PC Cards

Las Wi-Fi PC Cards están diseñadas con una antena incluida, usualmente es una antena miniatura que utiliza un sistema que reduce la interferencia y maximiza la recepción y calidad de transmisión; algunas de estas antenas traen un pequeño conector al final que permite conectarse con otra antena más poderosa para maximizar el rango de cobertura.

En muchas de las computadoras portátiles el software y los drivers para estas PC Cards ya vienen por defecto en el sistema operativo, basta con introducir la tarjeta en la laptop y el software automáticamente se cargará. También se puede utilizar las PC Cards en algunas cámaras, sistemas de audio, PDA´s y otros dispositivos inalámbricos que tiene una ranura para PC Card.

Módulos Mini-PCI.- Actualmente algunas laptops o PC´s están viniendo con la tecnología Wi-Fi habilitada; esto es debido a que muchos fabricantes están instalando módulos Mini-PCI Wi-Fi como parte del hardware del equipo

Figura 2.15: Módulo Mini-PCI

Adaptadores USB.- La mayoría de las PC´s no están provistas con ranuras para PC Cards, este problema se puede solucionar utilizando adaptadores de bus PCI/ISA o USB. Para la mayoría de usuarios con PC´s la forma más fácil de agregar tecnología Wi-Fi a su equipo es usando un adaptador USB, ya que este dispositivo combina en una sola pieza una tarjeta de red inalámbrica y un convertidor de circuitos USB.

Figura 2.16: Adaptadores USB

Adaptadores de bus PCI e ISA.- Muchos fabricantes de dispositivos Wi-Fi proveen de tarjetas inalámbricas que trabajan en arquitecturas ISA o PCI, permitiendo de esta manera habilitar la tecnología Wi-Fi en PC´s para que puedan trabajar en un entorno de red inalámbrico. Vale la pena acotar que la arquitectura de bus ISA en los PC´s se encuentra prácticamente descontinuada en la actualidad.

Figura 2.17: Adaptadores PCI/ISA

Compact Flash y otros formatos para clientes pequeños.- Estas tarjetas son diseñadas para PDA´s de menor tamaño y otros dispositivos móviles de computación. La tecnología PC Card Wi-Fi puede ser construida en dispositivos más pequeños denominados Compact Flash (CF) que los típicos PC Card tipo II. Estas pequeñas tarjetas tienen el mismo rango y rendimiento que las PC Cards normales.

2.9.2- Estaciones Base Inalámbricas

Aunque los clientes Wi-Fi pueden ser configurados para interactuar unos con otros (Red Ad-Hoc), una red con tecnología Wi-Fi opera de una manera más eficiente cuando se usa una estación base central para coordinar las comunicaciones

Hay dos tipos de estaciones base inalámbricas Wi-Fi que son: Gateways y Access Points. Diferenciarlas no siempre está muy claro, en parte porque las funciones que ellas realizan pueden sobreponerse, o porque muchas redes cableadas y otras aplicaciones de hogar como Internet las llaman gateways.

Un gateway inalámbrico tiene como objetivo administrar en su totalidad los ambientes de hogar o pequeñas oficinas; mientras que los AP están destinados para cubrir ambientes que integran redes Ethernet con redes inalámbricas en grandes empresas, campus o corporaciones.

Los gateways y APs se pueden diferenciar en lo que se refiere a sus capacidades para administrar funciones de seguridad, protección de firewall y manejo de tráfico y tareas en la red.

Lo dicho anteriormente no quiere decir que las funciones descritas para cada uno son propietarias de cada dispositivo, sino por el contrario, ambos pueden realizar las mismas funciones y es por esta razón que se prestan para confusiones; lo importante aquí es que el administrador de la red tenga claro en qué ambiente (indoor, outdoor) se va a instalar la red, con qué otras redes o dispositivos va a interactuar y la inversión que desea realizar.

Gateways o Ruteadores inalámbricos.- Una red tipo infraestructura contiene uno o más APs separados, conectados directamente a una red cableada existente. Estos APs son llamados "**gateways**" o "**routers inalámbricos**".

Los gateways a menudo incluyen los servicios de ruteo NAT (Network Address Translation – Traductor de Direcciones de Red) y DHCP (Dynamic Host Control Protocol – Protocolo Dinámico de Control Principal). Estos servicios crean y proveen una dirección IP individual para todos los clientes tanto inalámbricos como cableados en la red, y también habilitan un único gateway Wi-Fi que simultáneamente provee de acceso a Internet, a numerosos usuarios a través de una única conexión compartida. Los Gateways pueden también incluir otras aplicaciones y características como encriptación y seguridad, VPN, firewalls y voz sobre IP (VoIP)

Puntos de Acceso (AP - Access Points).- Usualmente los APs no brindan los servicios de ruteo NAT o DHCP, esto es debido a que los routers de la red cableada ya están configurados para brindar dichos servicios. Los APs trabajan simplemente como puentes transparentes entre la red cableada y varios usuarios inalámbricos brindándoles facilidad de interconexión. Los APs usualmente habilitan el servicio de Roaming

(capacidad de moverse de un AP a otro sin perder conexión a la red), altos niveles de seguridad y altos niveles de control y administración de la red.

Algunos Gateways también proveen estos servicios, de hecho muchas estaciones base pueden operar como Gateways o como APs. Pero un Gateway es usualmente la única estación base inalámbrica en ambientes de pequeñas oficinas o de hogar; mientras que para grandes oficinas o campus puede haber cientos o miles de AP formando una o múltiples redes inalámbricas solapadas.

Figura 2.18: Gateways y Access Points

2.9.3- Otros dispositivos

Asistente Personal Digital (PDA - Personal Digital Assistants).- Como Palm™, Visor™ y Pocket PC™ tienen una ranura para el formato Compact Flash Wi-Fi descrito anteriormente. En la actualidad existen también nuevos formatos Wi-Fi más pequeños para PDA´s y dispositivos móviles de datos, que ofrecen opciones de conexión inalámbricas adicionales para el futuro.

Figura 2.19: PDA

Servidores de impresoras.- Permiten la instalación de una o varias impresoras en red, a través de la conexión Wi-Fi realizando funciones de buffering y gestión de colas.

Figura 2.20: Servidores de Impresión Wi-Fi

Cámaras de video vigilancia.- Estas cámaras soportan conexión a la red a través de una interfaz inalámbrica. Permiten la monitorización remota de locales y espacios con el simple uso de un navegador. Algunos equipos incluyen software para la detección de presencia con envío de alertas vía e-mail. Instalaciones multicámara son también posibles, permitiendo el acceso vía Internet desde cualquier lugar remoto.

Figura 2.21: Cámara de Video vigilancia Wi-Fi

Dispositivos de conexión multimedia.- Permite establecer conexión con las librerías multimedia almacenadas en un PC de la red, y ser reproducidas en el televisor o equipo de música a través de la red inalámbrica. Estos dispositivos trabajan con el estándar 802.11g, llegando a alcanzar velocidades de 54 Mbps.

Figura 2.22: Dispositivo de conexión multimedia Wi-Fi

Cámaras digitales Wi-Fi.- Algunos fabricantes de cámaras digitales (Ejm. Sanyo), comienzan a desarrollar cámaras capaces de conectarse a un servidor en red para descargar las imágenes almacenadas. Igualmente este dispositivo está preparado para realizar la conexión a través de un AP Público PWLAN.

Figura 2.23: Cámaras digitales Wi-Fi

Marco digital Wi-Fi.- Dispositivo que soporta la visualización de fotografías a través de la LAN local inalámbrica. Permite en casa o en la oficina realizar una presentación dinámica de contenidos fotográficos almacenados en la red.

Figura 2.24: Marco digital Wi-Fi

Dispositivos de conexión Wi-Fi a fuentes MP3 y Streaming de audio.- Comienzan a aparecer mini cadenas y equipos de audio con conexión Wi-Fi integrada. Estos

dispositivos facilitan el acceso a contenidos de audio (MP3 y streaming), tanto a los almacenados en servidores de Internet, como a aquellos almacenados en la red local.

Figura 2.25: Dispositivo de conexión Wi-Fi a fuentes MP3

Terminales telefónicos inalámbricos Wi-Fi.- Dispositivos de voz sobre IP que permiten desarrollar comunicaciones integradas de voz y datos tanto en entorno local, como líneas telefónicas de voz sobre IP. Su empleo más inmediato es dentro del ámbito corporativo de empresas y campus.

Su importancia radica en el hecho de transformar el sistema de comunicaciones tradicional de las empresas. Las soluciones de voz sobre IP tienen un gran impacto en el modelo de comunicaciones empresariales, ya que implica fuertes cambios respecto al equipamiento clásico de PBX así como la relación con el proveedor de telecomunicaciones. Aquí Wi-Fi viene a añadir la conectividad inalámbrica a los terminales de voz.

Figura 2.26: Terminales telefónicos Wi-Fi

2.9.4- Antenas, cables y conectores

Los sistemas de radio modulan, o codifican, la información en el transmisor. Estas señales moduladas se transmiten a través de una antena que convierte la señal de radiofrecuencia en una onda electromagnética. El medio de transmisión de la onda electromagnética es el espacio libre, el aire. La antena receptora intercepta la onda electromagnética y la convierte de nuevo en una señal de radiofrecuencia. Idealmente, esta señal de radiofrecuencia es igual que la original generada por el transmisor.

Existen básicamente dos variantes de antenas que son:

- Antenas Omnidireccionales
- Antenas Direccionales

La señal que emite una antena omnidireccional puede ser comparada con el haz de luz que emite una vela, mientras que la señal de una antena direccional puede ser comparada con el haz de luz que emite una linterna.

La ganancia de una antena es la potencia de salida, en una dirección particular, comparada con la potencia producida en cualquier dirección por una antena omnidireccional ideal (isotrópica).

Antena Omni direccional.- Irradia la señal en un círculo de dos dimensiones. Este tipo es el más común de todas las antenas externas ya que la mayoría de los AP y tarjetas PCI traen integrada una pequeña antena de estas características. Con este tipo de antenas se puede obtener una ganancia entre 3 y 12dB. En una red punto multipunto, una antena omni direccional es usada en el gateway del nodo central para permitir a los usuarios un acceso a la red de 360 grados.

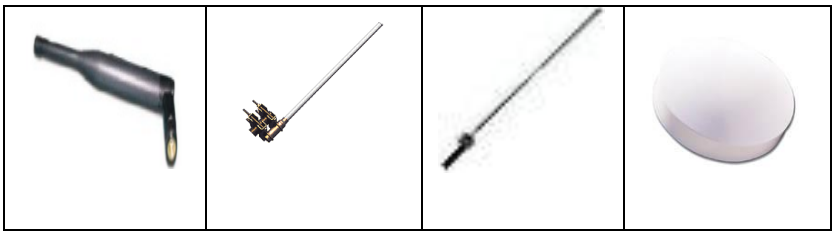
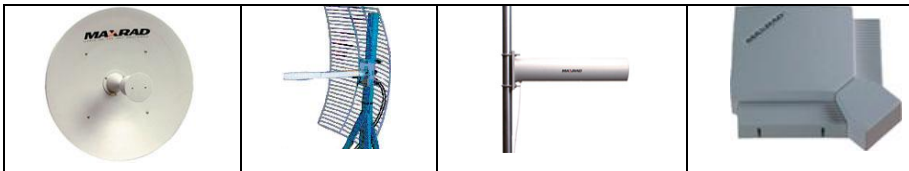


Figura 2.27: Antenas Omnidireccionales

Para grandes áreas como hoteles, campus, etc. antenas omnidireccionales pueden ser una buena solución si son colocadas en la mitad del área que se desea cubrir, ya que éstas irradian la señal prácticamente en todas las direcciones.

Antena Direccional.- Provee alta ganancia pero con un rayo muy estrecho. Estas antenas deben ser cuidadosamente apuntadas al objetivo. Son usadas en aplicaciones punto a punto o en nodos remotos de aplicaciones punto multipunto. Antenas tipo dish, yagi, parabólicas, de panel y rejilla son ejemplos comunes de antenas direccionales. La ganancia que se puede obtener con este tipo de antenas va a ser mayor en lugares pequeños y menor en lugares más grandes, valores típicos pueden estar entre los 5 y 20 dB.



Parabólica	**Rejilla**	**Yagi**	**Panel**

Figura 2.28: Algunos Tipos de Antenas Direccionales

Las antenas direccionales se suelen utilizar para unir dos puntos a largas distancias, mientras que las antenas omnidireccionales se suelen utilizar para dar señal en los alrededores.

Antenas Sectoriales.- Son una variación de las antenas direccionales, pensadas para ser combinadas en arreglos de varias unidades que dan la cobertura de los 360º del plano horizontal, pero con más apertura vertical y más ganancia que las antenas omnidireccionales.

	
Sectorial Tipo Panel	**Antena Sectorial**

Figura 2.29: Algunos Tipos de Antenas Sectoriales

Son usualmente usadas para cubrir áreas largas como grandes pasillos, patios o supermercados, etc. La mayor ganancia de estas antenas se logra colocando la antena en el eje vertical de radiación, el patrón de radiación de este tipo de antenas está entre los 10 y 20 grados HPBW (Half Power Beam Width – Ancho del haz a mitad de Potencia).

HPBW .- Es el ángulo en grados al cual la señal ha fallado de la mitad del valor al máximo. Usualmente ese ángulo es considerado como el área en la cual es lograda la mejor cobertura. Para un mejor entendimiento acerca de antenas y enlaces es importante aclarar los siguientes conceptos:

Polarización de una antena.- La polarización de una antena se refiere sólo la orientación del campo eléctrico radiado desde ésta. Una antena puede polarizarse en forma lineal (por lo general polarizada horizontalmente o verticalmente, suponiendo que los

elementos de la antena se encuentran dentro de un plano horizontal o vertical), en forma elíptica o circular. Si una antena irradia una onda electromagnética polarizada verticalmente, la antena se define como polarizada verticalmente; si la antena irradia una onda electromagnética polarizada horizontalmente, se dice que la antena está polarizada horizontalmente; de igual manera para la polarización elíptica y circular.

Patrón de radiación.- Representación gráfica en coordenadas polares o rectangulares de la distribución espacial de la potencia de una antena.

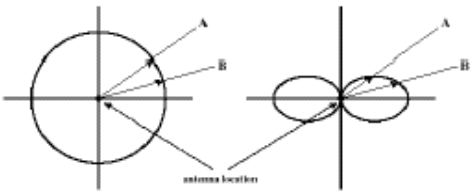


Figura 2.30: Patrón de Radiación Omnidireccional y Direccional

Sensibilidad de receptor.- Medida de la señal más débil que un receptor puede recibir y convertir correctamente en datos.

Ganancia de antena.- La ganancia de una antena es una medida de la capacidad de la antena para dirigir o concentrar la energía de radio en una región espacial. Las antenas de alta ganancia tienen un patrón de radiación más concentrado en una dirección concreta.

Cuadro 2.7: Ángulos respecto a cada tipo de antena con su respectiva ganancia

Ganancia dBi	**Tipo de Antena**	**Half Power BeamWidth (HPBW)**	
		Horizontal	**Vertical**
2	Omnidireccional	± 180°	± 60°
6	Omnidireccional	± 180°	± 10°
8.5	Unidireccional	± 37°	± 37°
12	Unidireccional	± 11°	± 11°
18	Unidireccional	± 7°	± 7°
24	Unidireccional	± 3.7°	± 3.7°

dB.- El decibel es una medida logarítmica de algo comparado con un punto definido de referencia. Un incremento de 10 dB corresponde al valor multiplicado por 10. Un decremento de 10 dB corresponde al valor dividido para 10.

dBi.- Proporción de decibelios de una antena isótropa, utilizada normalmente para medir la ganancia de antena. Cuando mayor sea el valor dBi, más alta será la ganancia y más preciso el ángulo de cobertura.

dBm.- Expresa la potencia absoluta mediante una relación logarítmica; el dBm se define como el nivel de potencia en decibelios en relación a un nivel de referencia de 1 mW.

A continuación se muestra una tabla tomando como referencia una antena de 14 dbi con sus respectivos valores de distancia y tasa de transferencia según la ETSI:

Cuadro 2.8: Cuadro con valores referenciales según la ETSI

Antenna Gain	Data rate	14 dBi	12 dBi	10 dBi	7 dBi
14 dBi	1 Mb/s	7.0 km 4.3 mi	6.9 km 4.3 mi	5.5 km 3.4 mi	4.0 km 2.5 mi
	2 Mb/s	5.0 km 3.1 mi	4.9 km 3.0 mi	4.0 km 2.5 mi	2.7 km 1.7 mi
	5.5 Mb/s	3.5 km 2.2 mi	3.5 km 2.2 mi	2.7 km 1.7 mi	1.9 km 1.2 mi
	11 Mb/s	2.5 km 1.6 mi	2.5 km 1.6 mi	2.0 km 1.2 mi	1.4 km 0.9 mi

Relación Señal Ruido (SNR - Signal to Noise Ratio).- La relación señal ruido es una medida de la calidad de la señal, usualmente es medida en decibeles ya es ésta es una medida logarítmica. La relación señal ruido en dB es la diferencia entre señal y ruido si ambos están medidos en la misma unidad de dB.

Célula.- Área de alcance o cobertura de la radio dentro de la cual los dispositivos inalámbricos pueden comunicar con la estación base. El tamaño de la célula depende de la

velocidad de la transmisión, del tipo de antena utilizado y del entorno físico, entre otros factores.

Pérdida de señal.- La pérdida de señal se puede producir por un gran número de factores: ruido de radiofrecuencia, erupciones solares, variaciones atmosféricas, ruido interno del sistema, etc.

Una consideración importante que hay que tomar en cuenta, es tratar de minimizar la atenuación que se produce en el cable entre el equipo Wi-Fi y la antena, ya que se pueden perder fácilmente 3 dB usando un cable de pobre calidad. Se recomienda usar cables de baja pérdida y de alta calidad tomando en cuenta que éstos pueden ser muy costosos. Las pérdidas también podrían ser minimizadas usando en lo posible cables de poca longitud. Cables largos pueden ser tirados siempre y cuando sean Ethernet o USB ya que éstos son menos sensibles a las pérdidas

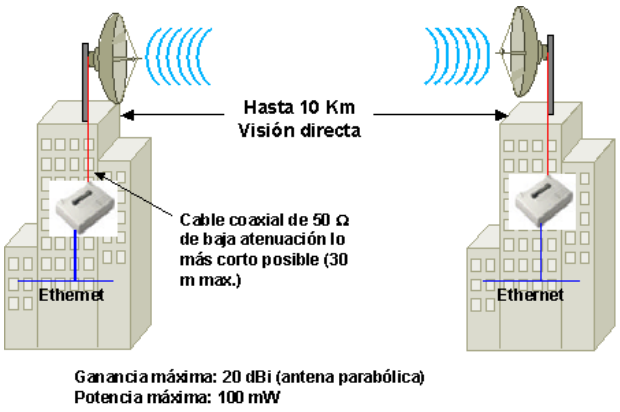


Figura 2.31: Esquema de cableado idóneo para colocación de una antena

2.9.4.1- Cables

Son un factor crítico a la hora de montar una estación cliente o un nodo. Los cables, *todos*, tienen pérdidas, sólo que unos más que otros. Generalmente se recomienda el uso del cable LMR400 que, aunque existen otras alternativas, sigue siendo el cable ideal para

este uso. Del cable depende que la señal llegue correctamente desde la tarjeta o AP a la antena, y viceversa, y es recomendable usar siempre el mínimo cable posible, independientemente de que el cable sea muy bueno. Esto es debido evidentemente a que cuanto menos cable se use, menores pérdidas de señal habrán.

Mientras más fino es el cable mayor atenuación tendrá, aunque se desea su flexibilidad, su atenuación no. La atenuación del cable es medida en dB/100m; mientras mayor es la atenuación mayor energía se perderá, la atenuación trabaja en ambos sentidos, para transmitir y recibir señales.

La única salida para bajar la atenuación es usar cables más gruesos que pueden ser fácilmente colocados en las antenas que ya se encuentran montadas, la desventaja con estos cables es que son mucho más rígidos y en la mayoría de los casos no pueden ser conectados a las portátiles o dispositivos inalámbricos por su grosor. Para solucionar éste problema se utilizan unos pequeños cables denominados pigtails.

En soluciones Outdoor comúnmente se utilizan tres tipos de cables que son:

Pigtail.- Son pequeños, flexibles y delgados cables coaxiales que usualmente miden 20 o 30 cm. de largo, se conectan entre el cable largo que está conectado a la antena y el dispositivo inalámbrico; aunque éstos introducen más atenuación es la única manera de conectarse con la antena, salvo en algunos modelos de antenas diseñadas expresamente para usar en interiores, que ya vienen con ese conector de serie. El pigtail tiene 2 conectores especiales y diferentes; el propietario de cada tarjeta en un extremo, y por el otro un conector N estándar en la mayoría de los casos. El pigtail depende del fabricante de la tarjeta, por lo que no se trata de un estándar.

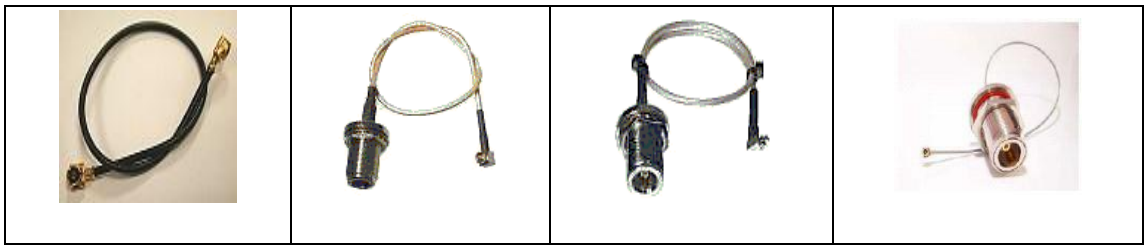


Figura 2.32: Algunos modelos de Pigtails

Cables coaxiales de baja atenuación.- Especiales para la banda de frecuencias de trabajo, que permiten separar tanto como sea necesario los equipos de radio de las antenas, con vistas a poder ubicar éstas en la altura y posición adecuadas.

Cables de red UTP o STP.- Que en algunos casos conectan el dispositivo Wi-Fi a la red de ordenadores, y pueden incluso servir de medio para la alimentación eléctrica de dichos dispositivos.

Como se mencionó anteriormente todos los cables sufren atenuación, aunque se recomienda utilizar cables de 50 ohm; a continuación se describen algunos valores típicos de pérdida para cables coaxiales comunes en la frecuencia de 2.4 Ghz:

- RG 58 (muy común, usado para Ethernet): -1 dB/m.
- RG 214 ("negro grande", muy común): -0.6 dB/m.
- LMR-400: -0.22 dB/m
- Tipo Heliax: -0.14 dB/m

La atenuación típica de cables coaxiales para una frecuencia de 3.5 Ghz es:

- RG 58: -1.3 dB/m
- RG 214: -0.7 dB/m
- Tipo Heliax: -0.2 dB/m

2.9.4.2- Conectores

Muchos fabricantes de accesorios Wi-Fi usan conectores poco comunes en sus equipos. Esto es debido a que la US FCC (Federal Communications Comisión – Comisión Federal de Comunicaciones de Estados Unidos) pidió a los fabricantes que no usen conectores comunes para detener a la gente que utiliza antenas de alta ganancia, y para proteger la frecuencia del espectro de emisiones ilegales. Por lo tanto lo primero que hay que hacer es averiguar que tipo de conector utiliza el equipo Wi-Fi que se va a usar; aunque la mayoría de tipos usados en las redes inalámbricas son conocidos.

Figura 2.33: Conectores más comunes

Con algunos tipos de conectores es común utilizar adaptadores, pero como regla general es mejor evitarlos en lo posible ya que éstos introducen más atenuación, en un conector normal la atenuación está alrededor de 0.2 dB.

Dentro de los conectores más comunes se encuentran:

Conector Tipo N.- Los conectores tipo N son de tamaño medio con acoplamiento roscado, es el conector utilizado para instalaciones profesionales, prácticamente todas las antenas Outdoor lo usan, está disponible para casi todos los tipos de cables. Estos conectores tipo N soportan perfectamente situaciones donde intervienen choques y vibraciones.

Figura 2.34: Conector Tipo N

Conector Tipo MC.- Este conector es oficialmente llamando "MC Card Conector", se podría decir que es uno de los conectores más importante y también más caros, pertenece a ORINOCO. Es uno de los más pequeños que se encuentra en el mercado.

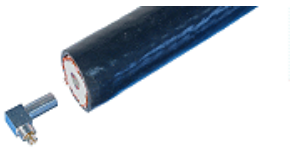


Figura 2.35: Conector Tipo MC

Conector Tipo SMA.- Es un conector pequeño que tiene la particularidad de que invierte la polaridad por lo que son ampliamente usados en los equipos Wi-Fi.

Invertir la polaridad significa que el centro del conductor es invertido, esto quiere decir que donde se espera un pin macho se encuentra un jack hembra y viceversa. Son usualmente llamados RP-SMA o Reverse SMA.

Los conectores SMA están disponibles en una amplia variedad de estilos de montaje, cuerpos de latón o acero inoxidable, y diversos métodos de fijación del cable.

Figura 2.36: Conectores tipo SMA Jack y Plug

Aunque no siempre se usan, a veces son necesarios otros elementos accesorios tales como:

- Amplificadores, a veces necesarios para lograr mayores alcances o para compensar las pérdidas de cables muy largos.

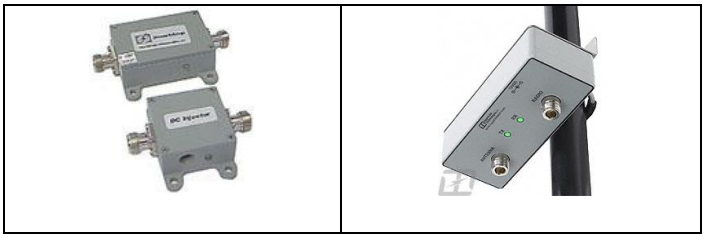


Figura 2.37: Amplificadores

- Splitters, permiten acoplar varias antenas a una misma radio, dividiendo entre ellas la potencia transmitida y sumando las recibidas.

Figura 2.38: Splitters

- Protecciones, hay dispositivos para aislar eléctricamente la antena del equipo electrónico, para evitar en lo posible el daño por rayos.

Figura 2.39: Protectores contra descargas eléctricas

2.10- Tendencias de nuevas tecnologías

En la actualidad, las redes WLAN 802.11a/b/g proporcionan el rendimiento adecuado para las aplicaciones de conexiones de redes actuales, donde la conveniencia de una conexión inalámbrica puede proporcionar gran valor al usuario. A medida que la próxima generación de aplicaciones inalámbricas emerge, se requerirá un rendimiento superior para los datos de WLAN y es por esta razón que aparecen nuevos estándares como los que se mencionan a continuación:

2.10.1- WiMAX

A pesar de que el proyecto para la creación de un nuevo estándar se gestó hace 6 años en el IEEE, no fue hasta abril de 2002 que la primera versión del mismo, la 802.16, se publicó, y se refería a enlaces fijos de radio con visión directa (LoS) entre transmisor y receptor, pensada para cubrir la "última milla" (o la primera, según desde que lado se mire), utilizando eficientemente varias frecuencias dentro de la banda de 10 a 66 GHz.

WiMAX (Worldwide Interoperability for Microwave Access – Interoperabilidad a lo Largo del Mundo para el Acceso Microonda) es el nombre del estándar 802.16a, aprobado en enero del año 2003 por el WiMAX forum y fue entonces cuando WiMAX como una tecnología de banda ancha inalámbrica, empezó a cobrar relevancia. También se pensó para enlaces fijos, pero llega a extender el rango alcanzado desde 40 a 70

kilómetros, operando en la banda de 2 a 11 GHz, parte del cual es de uso común y no requiere licencia para su operación.

El WiMAX Forum está compuesto por más de 230 miembros (representantes del conjunto necesario de empresas para introducir los productos WiMAX en el mercado) es decir, fabricantes de equipos y componentes, proveedores de servicios y aplicaciones.
El hecho de que WiMAX no sea todavía una tecnología de consumo ha permitido que el estándar se desarrolle conforme a un ciclo bien establecido, lo que garantiza su estabilidad y cumplimiento de sus especificaciones, algo parecido a lo que sucedió con la tecnología GSM (Global System for Mobile Communications – Sistema Global para Comunicaciones Móviles*)* en años pasados, con su total garantía de estabilidad.

Este nuevo concepto de banda ancha permitirá que los proveedores de servicios puedan ofrecer acceso a Internet directamente a las casas, además está considerada como una alternativa más barata a las líneas de suscripción digital (DSL) ya que los costes de instalación son mínimos.

Es válido para topologías punto a multipunto y, opcionalmente, para redes en malla, y no requiere línea de visión directa. Emplea las bandas de 3,5 GHz y 10,5 GHZ, válidas internacionalmente, y las de 2.4 GHz y 5,725-5,825 GHz que son de uso común y no requieren disponer de licencia alguna.

Un aspecto importante del estándar 802.16x es que define un nivel MAC (*Media Access Layer*) que soporta múltiples enlaces físicos (PHY). Esto es esencial para que los fabricantes de equipos puedan diferenciar sus productos y ofrecer soluciones adaptadas a diferentes entornos de uso.

Pero WiMAX también tiene competidores, y así una alternativa es el estándar Hiperaccess (>11 GHz) e HiperMAN (<11 GHz) del ETSIT, pero el auge que está tomando WiMAX ha hecho que se esté estudiando la posibilidad de armonizarlo con esta

última norma, que también utiliza una modulación OFDM. Sin dejar de lado Mobile-Fi, el estándar 802.20 del IEEE, específicamente diseñado desde el principio para manejar tráfico IP nativo para un acceso móvil de banda ancha, que provee velocidad entre 1 y 16 Mbps, sobre distancias de hasta 15 o 20Km, utilizando frecuencias por debajo de la banda de 3,5 GHz.

Cuadro 2.9: Cuadro comparativo de WiMAX frente a otras tecnologías

	WiMAX 802.16	**Wi-Fi 802.11**	**Mobile-Fi 802.20**	**UMTS y cdma2000**
Velocidad	124 Mbit/s	11-54 Mbit/s	16 Mbit/s	2 Mbit/s
Cobertura	40-70 Km.	300 m-20 Km.	20 Km.	10 Km.
Licencia	Si/No	No	Si	Si
Ventajas	Velocidad y Alcance	Velocidad y Precio	Velocidad y Movilidad	Rango y Movilidad
Desventajas	Interferencias?	Bajo alcance	Precio alto	Lento y caro

2.10.2- 802.11n

En respuesta a la demanda del mercado creciente para redes de áreas locales inalámbricas (WLAN) de alto rendimiento, el Instituto de electrónica e ingenieros electrónicos - Asociación de estándares (IEEE-SA) ha aprobado la creación del Grupo de enfoque N (802.11 TGn) del IEEE 802.11 durante el segundo semestre del año 2003.

Cuadro 2.10: Comparación de distintas velocidades de transferencia en 802.11. Fuente: Intel Labs.

Estándar para WLAN de IEEE	**Cotizaciones Over-the-Air (OTA)**	**Cotizaciones de la Capa de control del acceso de medios, Servicio en punto de acceso (MAC SAP)**
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (en ausencia de .11b)
802.11a	54 Mbps	25 Mbps
802.11n	200 Mbps o más	100 Mbps

El alcance del objetivo del TGn consiste en definir modificaciones para la Capa física y la Capa de control del acceso medio (PHY/MAC) que generan resultados de un mínimo de 100 megabits por segundo (Mbps) en el MAC SAP (encima del MAC).

Los resultados mínimos requeridos representan un incremento 4 veces superior, aproximadamente, en el rendimiento de WLAN en comparación con las redes 802.11a/g actuales. El propósito de TGn para este próximo paso en el rendimiento de WLAN consiste en mejorar la experiencia del usuario con las aplicaciones WLAN existentes a tiempo de habilitar aplicaciones nuevas y segmentos del mercado recientes. Al mismo tiempo, TGn espera una transición lúcida para su adopción al requerir compatibilidad retroactiva con las soluciones IEEE WLAN legadas existentes (802.11a/b/g).

La Wi-Fi Alliance considera que este nuevo estándar no estará listo hasta Noviembre del año 2006, los nuevos productos que los fabricantes desarrollen para la norma 802.11n también serán certificados por la Wi-Fi Alliance.

Las consideraciones clave en la definición de la arquitectura de la próxima generación de redes WLAN son los costos y el rendimiento robusto. Intel cree que tanto la tecnología MIMO así como los canales de ancho de banda más amplio serán requeridos para satisfacer fiablemente las demandas de resultados superiores. Al mismo tiempo, el rendimiento general de la MAC SAP será habilitado con las características nuevas de la MAC, lo cual maximizará la eficiencia del rendimiento.

CAPITULO III

ANÁLISIS DE MERCADO

3.1- Antecedentes

El impacto socio-económico a nivel mundial provocado por los constantes y acelerados cambios que se han suscitado en los últimos años en las áreas de informática y telecomunicaciones, permiten asegurar que el desarrollo de una nación está determinado por su grado de inserción y adaptación a los nuevos descubrimientos tecnológicos.

No es posible definir políticas que permitan un desarrollo económico sostenido sin considerar el desarrollo tecnológico. El desarrollo de Internet en Ecuador a diferencia de otros países en América Latina se realizó de manera independiente de los operadores dominantes. Cada ISP buscó una alternativa de conexión internacional más económica que la que ofrecían los operadores; esto ocasionó la formación de algunos ISP´s. De los operadores dominantes, Andinatel ofrece servicio de Internet desde el 2000 y Pacifictel desde el mes de Marzo de 2001.

El crecimiento de Internet ha sido en los últimos años acelerado; sin embargo, la densidad está por debajo de la media de América Latina, la penetración de Internet en Ecuador es mucho más baja que la de Colombia o Perú. La baja densidad de computadoras, la falta de oferta de líneas telefónicas, la poca capacidad adquisitiva de la ciudadanía, la falta de cultura en el uso de tecnología son algunos de los factores que influyen en el uso de Internet.

El país debería tener como objetivo a corto plazo el de que todo estudiante de educación secundaria tenga acceso a Internet y tenga una cuenta de correo electrónico gratis con la finalidad de que el estudiante y su familia empiecen a hacer uso de esta tecnología. Internet es un medio para democratizar la información y el conocimiento.

La brecha digital es la distancia que separa a quienes tienen acceso a la información y a las nuevas tecnologías de quienes no la tienen. Esto da como resultado que la apropiación del conocimiento y desarrollo económico y social no sea equitativo.

La brecha digital no se relaciona solamente con aspectos de carácter tecnológico, es el reflejo de una combinación de factores socioeconómicos y de la falta de infraestructura de telecomunicaciones e informática.

3.1.1- Penetración de Internet

La globalización de la economía mundial no sólo se explica por la dramática disminución de barreras a los flujos internacionales de bienes, servicios y capitales desde mediados del siglo pasado, sino por el cambio tecnológico. A este respecto, el papel que está jugando Internet en la expansión de las comunicaciones globales y la multiplicación de las transacciones económicas ha sido extraordinario, y será cada vez más importante a la luz del potencial de usuarios y del aprendizaje tecnológico. En 1990 menos de un millón de personas tenía conexión a Internet. En el 2004 se pasó a más de 785 millones, con una tasa de aumento de usuarios del 120 por ciento en el período 2000-2004.

El Ecuador tiene una penetración a la Internet significativamente baja con respecto a otros países latinoamericanos, lo que incide en su competitividad y afecta su desarrollo. Por ello se explica la limitación de acceso al conocimiento en forma actualizada y constante; a una mejor calidad de vida y a una mayor atención en educación. Según el informe presentado por la ITU (International Telecomunication Union) en Marzo del 2005 las estadísticas en Internet en América incluyendo a Ecuador están de la siguiente manera:

Cuadro 3.1: Usuarios de Internet y Estadísticas de Población para América.

Fuente: ITU actualización al 24 de Marzo del 2005.

Usuarios de Internet y Estadísticas de Población para América						
América	Población (2005 Est.)	% Pob. América	Usuarios de Internet, Últimos datos	Crecimiento (2000-2005)	Penetración (% Población)	% Uso América
América Central	142,671,074	16.3 %	14,984,100	365.7 %	10.5 %	5.4 %
América del Sur	365,389,570	41.8 %	38,480,557	169.2 %	10.5 %	13.9 %
Caribe	38,856,548	4.4 %	2,760,300	393.4 %	7.1 %	0.9 %
América del Norte	328,387,059	37.5 %	221,437,647	104.9 %	67.4 %	79.8 %
TOTAL AMERICA	875,304,251	100.0 %	277,662,604	120.1 %	31.7 %	100.0 %

Cuadro 3.2: Uso de Internet en Sudamérica.

Fuente: ITU actualización al 24 de Marzo del 2005.

Uso de Internet en Sudamérica					
Sudamérica	**Población (Est. 2005)**	**Usuarios Internet Últimos Datos**	**Crecimiento (2000-2005)**	**% Población (Penetración)**	**% Usuarios Sudamer.**
Argentina	37,584,554	5,600,000	124,0 %	14.9 %	14.6 %
Bolivia	9,073,856	270,000	125.0 %	3.0 %	0.7 %
Brasil	181,823,645	17,945,437	258.9 %	9.9 %	46.6 %
Chile	15,514,014	4,000,000	127.6 %	25.8 %	10.4 %
Colombia	45,926,625	2,732,200	211.2 %	5.9 %	7.1 %
Ecuador	**12,090,804**	**581,600**	**223.1 %**	**4.8 %**	**1.5 %**
Falkland Islands	2,661	-	-	-	n/a
French Guiana (FR)	194,277	3,200	60.0 %	1.6 %	0.0 %
Guyana	877,721	125,000	4,066.7 %	14.2 %	0.3 %
Paraguay	5,516,399	120,000	500.0 %	2.2 %	0.3 %
Perú	28,032,047	2,850,000	14.0 %	10.2 %	7.4 %
Surinam	460,742	23,000	96.6 %	5.0 %	0.1 %
Uruguay	3,444,952	1,190,120	221.7 %	34.5 %	3.1 %
Venezuela	24,847,273	3,040,000	220.0 %	12.2 %	7.9 %
TOTAL	365,389,570	38,480,557	169.2 %	10.5 %	100.0 %

En la actualidad el panorama de Internet en el Ecuador ha cambiado debido a su lenta pero constante evolución, dándose lugar a nuevos enfoques, perspectivas y falencias que se los puede resumir en los siguientes puntos:

Enfoques:

- Internet es ahora "PROTAGONISTA".
- Banda Ancha consolidándose.
- Promedio de 18 usd por mes en conexiones Dial Up.
- PC es como un electrodoméstico.
- Tarifas de Internet cada vez más accesibles.
- Crecimiento de sitios informativos y tiendas virtuales (catálogos on-line).
- Mayor número de proveedores de Internet está conectándose a la fibra óptica y no por vía satelital.
- Mediano crecimiento pero sostenido

Perspectivas:

- El mercado Dial Up, se está buscando una conexión al Internet sin tarifa telefónica (tarifa plana).
- Mayor velocidad de navegación .
- Mayor tiempo de conexión por un menor costo.
- Evitar la congestión telefónica.
- Estar permanentemente conectado.
- **Uso de tecnología inalámbrica (soluciones Anytime-Anywhere).**
- Costos mensuales de Banda Ancha más bajos.

Falencias:

- Necesidad de sistemas de seguridad y marco legal más robusto.
- Pocos sitios transaccionales, básicamente BANCA EN LINEA.

- Ley retrasada a adelantos tecnológicos y tendencias globales de sistemas de información y comunicaciones.
- Aplicaciones B2B escasas.
- Ecuador consumidor, no productor de tecnología.
- Poca información en el mercado sobre tecnología, lo que se presta a confusión.

Se estima que para el año 2007, más de 20 millones de personas utilizarán accesos a Internet inalámbricos en todo el mundo, según se informó en el reciente encuentro de la Unión Internacional de Telecomunicaciones, dependiente de Naciones Unidas.

3.1.1.1- Internet con Dial Up

Dial Up es el servicio convencional de acceso a Internet que utiliza un módem telefónico y una línea telefónica para establecer la conexión. Esta conexión tiene un límite de 56Kbps de DownStream y 33.6Kbps de UpStream, además en esta tecnología es el usuario quien llega a la central o ISP, por lo que la velocidad no se puede asegurar, así como tampoco la conectividad.

Cuadro 3.3: Resumen anual de acceso a Internet 2004.

Fuente: SUPERTEL.

Resumen anual de acceso a Internet 2004				
Mes	**Cuentas Dial Up**	**Cuentas Corporativas**	**Usuarios estimados de Cuentas Corporativas**	**Total de usuarios estimados**
Julio	107.414	8.782	74.127	181.541
Agosto	108.373	8.956	72.932	181.305
Septiembre	103.005	9.848	77.065	179.997
Octubre	103.514	9.849	77.183	180.624
Noviembre	107.348	11.455	79.806	187.154
Diciembre	**108.169**	**11.599**	**83.734**	**191.903**

Cuadro 3.4: Resumen anual de acceso a Internet 2005.

Fuente: SUPERTEL.

Resumen anual de acceso a Internet 2005				
Mes	**Cuentas Dial Up**	**Cuentas Corporativas**	**Usuarios estimados de Cuentas Corporativas**	**Total de usuarios estimados**
Enero	107.391	11.890	94.377	201.768
Febrero	**107.901**	**11.848**	**94.016**	**201.917**

Según datos presentados por la SUPERTEL (Superintendencia de Telecomunicaciones), a inicios del año 2004 el 94% de los usuarios en Ecuador accedían a Internet a través de líneas telefónicas; haciendo un análisis comparativo en base a los cuadros (2.13 y 2.14) arriba presentados, en la actualidad las cosas han cambiado significativamente ya que al finalizar el año 2004 el 56% de los usuarios eran de tipo Dial Up y en lo que va del año 2005 el 53% sigue perteneciendo a estos usuarios; esto quiere decir que el 54.5% (promediando los dos anteriores) pueden ser usuarios que acceden a Internet a través de Banda Ancha cableada o a través de Internet Inalámbrica.

3.1.1.2- Internet con Banda Ancha

En el amplio sentido de la palabra, Banda Ancha puede ser comparado con una autopista de múltiples pistas, en la que se puede viajar más rápido y con mayor seguridad; ya que se puede usar el teléfono mientras se navega, debido a que la información viaja por distintos sectores del mismo cable.

La masificación de tecnologías ha hecho que el usuario final cuente con conexiones a Internet de alta velocidad. Hoy en día, son cuatro las tecnologías a través de las cuales se ofrece comercialmente Internet de Banda Ancha al usuario final en el mundo:

- xDSL, cuya modalidad más conocida es el ADSL, que usa los pares telefónicos de cobre;

- Cable Coaxial, a través del cual se entregan los servicios de televisión pagada;
- WLL (Wireless Local Loop), tecnología inalámbrica fija, que igualmente sirve para ofrecer servicios de telefonía; y,
- PLC, tecnología que ocupa la red eléctrica para la transmisión de datos.

Aunque disímiles, estas tecnologías entregan básicamente el mismo servicio, con una calidad y velocidad de conexión similar. Ello marca la primera pauta en el modelo de negocios de los proveedores de servicios de Internet.

3.1.2- Proveedores y costos de Servicios de Internet

En el Ecuador existen en la actualidad alrededor de 60 ISP´s registrados en la SUPERTEL, todos ellos brindando más o menos los mismos servicios y similares tarifas, para este estudio se tomó como referencia algunos de los más importantes que se describen a continuación:

Cuadro 3.5: Cuadro de Tarifas de algunos Proveedores de Internet en Quito.

Proveedor	Servicios	Tarifas
Interactive	Dial Up Ilimitado Mensual	17,00 + IVA
	ADSL 128 Kb Home (2 Cuentas de Correo) ➢ Sin costo de instalación	65,00 + IVA
	Empresarial ADSL Platinum 128/64 (5 cuentas de correo) ➢ Valor instalación 200,00 usd ➢ Incluye Modem	75,00 + IVA
Ecuanet	Dial Up Ilimitado Mensual	18,99 + IVA
Andinanet	Dial Up Ilimitado Mensual	18,00 + IVA
	ADSL Home 128 X 64	65,00 + IVA
Paradyne	**Tarjetas prepago para acceso a Internet inalámbrico**	
	1 Hora	4,00

	2 Horas	7,00
	4 Horas	12,00
	Ilimitado	50,00

Es importante destacar que en la ciudad de Quito ya se encuentran algunos Hot Spots brindando servicios de Internet inalámbrica, dentro de los más importantes se pueden mencionar:

- Centro histórico
- Plaza de las Américas
- CEMEXPO
- Cumbayá
- Aeropuerto Mariscal Sucre
- Hotel Quito
- Hotel Across

3.2- HIPÓTESIS

Con este estudio se pretende demostrar que el grado de aceptación del uso de la tecnología inalámbrica Wi-Fi, para acceso a Internet entre los estudiantes de la Facultad de Sistemas de la ESPE es del 40%.

3.3- OBJETIVOS

3.3.1- General

Obtener de un segmento de mercado constituido por estudiantes de séptimo, octavo y noveno nivel de la Facultad de Sistemas de la ESPE, criterios y opiniones acerca de tecnología inalámbrica que utiliza nodos Wi-Fi para conectarse a Internet ilimitadamente .

3.3.2- Específicos

- Evaluar si los estudiantes cuentan con dispositivos inalámbricos y si los utilizan como alternativa para conexión a Internet.
- Conocer las características de demanda del mercado de Internet inalámbrica en los estudiantes respecto al uso de Internet convencional.
- Determinar si el servicio ofrecido es atractivo y práctico para los estudiantes.
- Determinar si los estudiantes tienen conocimientos acerca de la tecnología Wi-Fi.
- Realizar una cuantificación aproximada del tamaño de mercado en dólares, para el servicio de Internet inalámbrica con tecnología Wi-Fi.

3.4- Síntesis del Análisis

3.4.1- Enfoque de Mercado

El propósito de este estudio se centra en el uso privado de la tecnología Wi-Fi, pero es importante realizar una aclaración sobre su aplicación dentro de un entorno público. En una red Wi-Fi pública PWLAN (Public Wireless LAN), existe una compañía proveedora de servicios de Internet llamada WISP (Wireless ISP). Los lugares donde se presta el servicio se denominan Hot Spots Públicos y suelen ocupar lugares estratégicos como son: aeropuertos, estaciones de ferrocarril, plazas, etc.

Se puede encontrar Hot Spots gratuitos, donde el gestor de espacio decide desplegar una infraestructura Wi-Fi y ofrecer el servicio como un valor agregado a su oferta; este el caso de ciertos hoteles, universidades, bibliotecas, etc.

El mercado objetivo para este estudio está formado por los estudiantes de séptimo, octavo y noveno nivel de la facultad de Sistemas de la ESPE, que disponen de dispositivos inalámbricos, y que utilizan el acceso a Internet como parte de su rutina diaria, ya sea para investigación, estudio, trabajo u ocio.

3.4.2- Definición de población y muestra

El presente análisis se basa en un universo de estudio conformado por 1250 estudiantes (entre séptimo, octavo y noveno nivel) que constituyen posibles usuarios del sistema de Internet inalámbrica. La muestra utilizada para realizar la encuesta del estudio de mercado se basa en un muestreo probabilístico aleatorio simple en el cual se calculó la muestra tomando la fórmula de poblaciones finitas, de la siguiente manera:

$$n = \frac{\sigma^2 * N * p * q}{e^2 * (N-1) + \sigma^2 * p * q}$$

En donde:

- **σ** = 1.96 para α = 0.05. Para un 95% de seguridad de la muestra
- **N** = tamaño conocido de la población
- **p** = Prevalencia esperada del parámetro a evaluar, si de desconoce utilizar 0.05 que hace mayor el tamaño de la muestra.
- **q** = 1 – p
- **e** = error que se prevé cometer, para este caso 0.1 que equivale al 10%.

Entonces:

$$\mathbf{n} = \frac{1.96^2 \text{ x } 1250 \text{ x } 0.5 \text{ x } 0.5}{0.1^2 \text{ x } 1249 + 1.96^2 \text{ x } 0.5 \text{ x } 0.5} = 89$$

Una vez introducidos los datos en la fórmula, da como resultado una muestra de 89 unidades, esto quiere decir que serán encuestados 89 estudiantes para el análisis correspondiente.

3.4.3- Desarrollo del plan de investigación

Como fuentes de información se ha aprovechado los datos primarios y secundarios obtenidos de Internet; como mecanismo de investigación se utilizó el método de investigación experimental por su mayor valor científico. Para ello se seleccionó temas acordes que permitan obtener datos certeros y confiables.

Como instrumento de investigación se utilizó el cuestionario por ser la herramienta más común y flexible de manejar; su tabulación es fácil y proporciona ayuda para la obtención de datos primarios.

3.4.4- Conclusiones

- El 100% de los encuestados utiliza normalmente Internet como instrumento de trabajo, estudio u ocio.
- El 4.8% de los encuestados tienen como alternativa de acceso a Internet un dispositivo móvil o inalámbrico
- El 58% de los encuestados escogió a la Universidad como el lugar donde más le gustaría tener acceso inalámbrico a Internet.

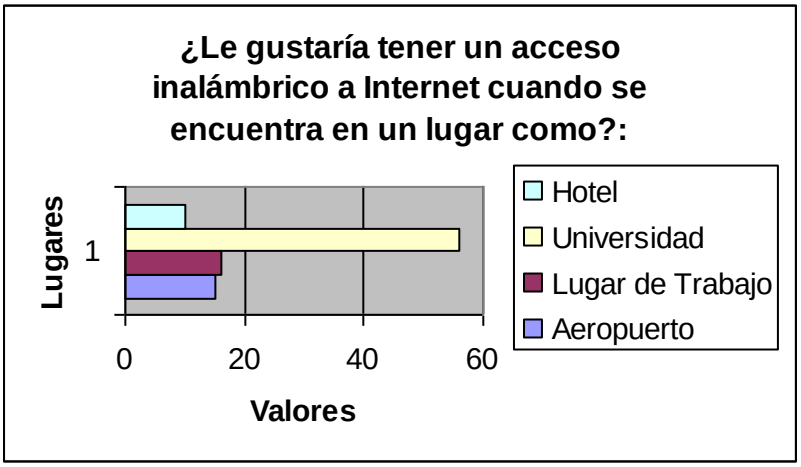
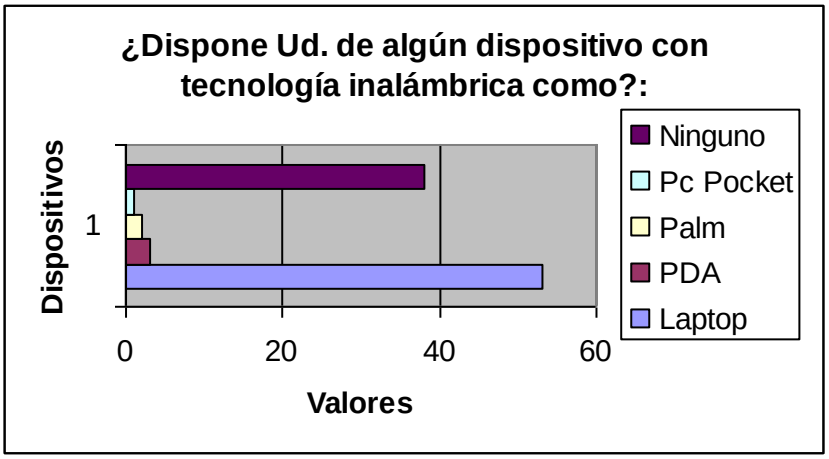


Figura 3.1: Gráfico de barras que representa valores vs. lugares

- El 56% de los encuestados poseen dispositivos inalámbricos.



3.2: Gráfico de barras que representa valores vs. Dispositivos

- El 69% de los encuestados considera como muy beneficioso el hecho de tener un acceso inalámbrico a Internet desde la Universidad, y sólo el 3% no lo considera beneficioso.
- El 70% de los encuestados estaría dispuesto a contratar un servicio inalámbrico de acceso a Internet.

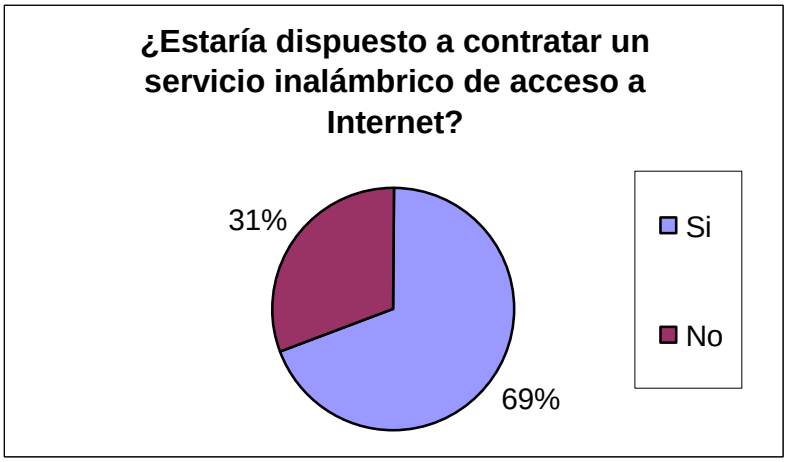


Figura 3.3: Gráfico de pastel que representa la aceptación del servicio

- El 85% de los encuestados no conoce ninguna empresa que en la ciudad de Quito brinde el servicio de Internet inalámbrica.
- El 62% de los encuestados adquiriría el servicio de acceso a Internet inalámbrica exclusivamente por la "movilidad" que éste brinda, mientras que el 9.6% lo haría por la "velocidad" de conexión.
- El 30% de los encuestados nunca ha escuchado o no tiene ningún conocimiento acerca de la tecnología inalámbrica Wi-Fi.
- El 98% de los encuestados consideran entre extremadamente interesante e interesante la conceptualización de Wi-Fi.
- Finalmente, el 58% de los encuestados consideran que los costos planteados son caros mientras que el 20% considera que son justos.

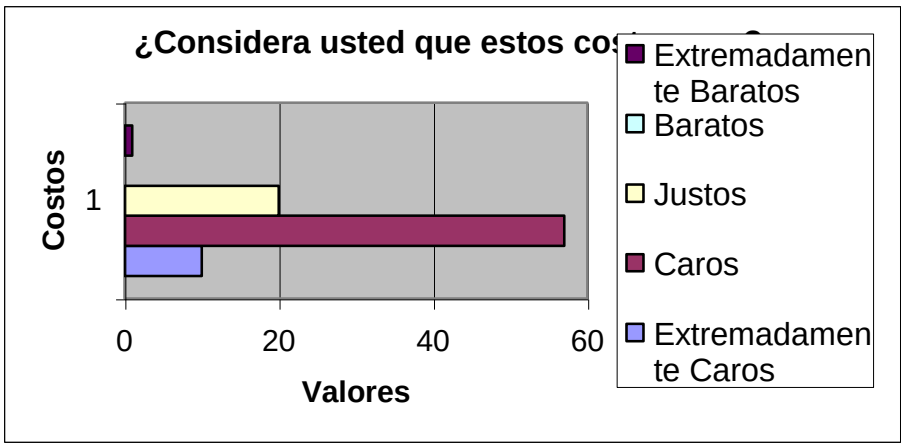


Figura 3.4: Gráfico de barras que representa valores vs. Costos

- En resumen, si se toma en cuenta que el grupo objetivo son 1500 estudiantes y según los datos arrojados por la encuesta, 870 quisieran tener un acceso inalámbrico a Internet desde la Universidad, se podría concluir que se justifica plenamente la realización del proyecto.

3.5- Análisis FODA

Luego de un largo proceso de investigación y estudio, tomando en cuenta los pros y contras de esta nueva tecnología, se podría resumir un análisis FODA de la siguiente manera:

3.5.1- Fortalezas

- Una nueva alternativa de acceso a Internet.
- Movilidad y escalabilidad.
- La capacidad de banda ancha.
- Rápido despliegue de redes inalámbricas.
- No se requieren grandes inversiones.
- IEEE respalda la evolución de los estándares.
- Soporte al sector informático y comercial.

3.5.2- Oportunidades

- La creciente demanda del mercado.
- Acceso a entornos de carácter rural.
- Aplicaciones y servicios para entorno rural.
- Entrada en la administración pública local.
- Alianzas y complementos a otras tecnologías.
- Introducción a nuevos mercados/clientes.
- Desarrollo de aplicaciones.
- Desarrollo de calidad de servicio.

3.5.3- Debilidades

- Interferencias e inseguridad en la transmisión de datos.
- Estándar IEEE 802.11 en evolución.
- Estándar 802.11i para seguridades no lanzado oficialmente todavía.

- Escasa penetración de ordenadores o dispositivos portátiles.
- No existe un estándar para soluciones Outdoor.
- Poca difusión en el mercado.
- Desconocimiento de la tecnología.
- Legislación muy complicada, sobre todo en lo que se refiere a homologaciones.
- En ocasiones, crecimiento incontrolado e ilegal.
- Inseguridad física debido a la delincuencia del país.

3.5.4- Amenazas

- Sector tecnológico en recesión o evolución.
- Fuerte competencia en entorno urbano.
- Marco regulatorio indefinido.
- UMTS/ operadores móviles.
- Desorden en su desarrollo, despliegue.
- Falta de profundidad en la ejecución de soluciones.

3.6- Marco Regulatorio

La SUPERTEL en cumplimiento del Reglamento General a la Ley Especial de Telecomunicaciones ejerce control a las operadoras de Servicios de Valor Agregado, incluido el Acceso a Internet, efectuando inspecciones técnicas; solicitando información a los operadores; aplicando sanciones; conociendo casos de denuncias; y, evaluando la calidad.

La Superintendencia de Telecomunicaciones inspecciona a los operadores ubicados en el territorio nacional, con el objeto verificar:

- Que los permisos no hayan caducado.

- Que los prestadores de Servicios de Valor Agregado - SVA, se encuentren operando legalmente y aquellos cuyos medios de transmisión incluyan el espectro radioeléctrico o tengan infraestructura propia internacional, tengan los respectivos títulos habilitantes.
- Que en el caso de infraestructura propia, esta no este siendo alquilada a terceros sin un titulo habilitante para la prestación de servicios portadores.
- Que los operadores en el plazo establecido en el permiso haya iniciado sus operaciones.
- Que operen en las áreas de cobertura autorizadas.
- Que no se estén realizando subsidios cruzados.
- Que si una empresa tiene varios servicios de telecomunicaciones se manejen de forma independiente al servicio del titulo habilitante de SVA.
- Que en el caso de encontrarse con un permisionario que haya cambiado sus características haya emitido la notificación escrita a la Secretaría Nacional de Telecomunicaciones.

Según la "Norma para la Implementación y Operación de Sistemas de Espectro Ensanchado", publicada en el Registro Oficial No. 215 del 30 de noviembre del 2000, las consideraciones a tener en cuenta para los interesados en instalar y operar sistemas de espectro ensanchado son las siguientes:

3.6.1- Homologación de Equipos

Todos los equipos de espectro ensanchado que se utilicen en el país deberán ser homologados por la SNT. La homologación de equipos terminales individuales se realizará únicamente para aquellos que hayan sido adquiridos fuera del país y debe efectuarla el propietario del equipo terminal. En caso de imposibilidad física, el peticionario deberá anexar la autorización correspondiente.

- Solicitud firmada por el propietario del equipo que constará en el formulario correspondiente. Esta información ingresará en la base de datos del Sistema de Homologación de la Superintendencia de Telecomunicaciones.
- Original y copia de la cédula de Ciudadanía del propietario del equipo;
- Original de la factura de compra del equipo terminal

Requisitos para homologación de equipos importados (desde el quinto equipo):

- Formulario de solicitud para homologación de equipos terminales con la información requerida. (Esta información se ingresará directamente en el Sistema de Homologación de la Superintendencia de Telecomunicaciones);
- Manuales técnicos que aporten la información necesaria para la realización de pruebas;
- Características de funcionamiento y modo de conexión a la red;
- Un certificado de características técnicas emitido por un laboratorio reconocido por la Superintendencia de Telecomunicaciones de que los equipos o aparatos cuya marca y modelo se quiere importar cumplen con las especificaciones de la Norma técnica correspondiente o un certificado de un organismo internacional de homologación reconocido;
- Un documento con el compromiso de la empresa responsable de la importación, respecto de la garantía técnica del mantenimiento de los equipos importados;
- Documentos de importación y nacionalización pertinentes (copias certificadas) DUI; y,
- Información del modelo y número de serie de los equipos a homologar, de preferencia en medio magnético.

Costos por homologación

El peticionario para obtener el certificado de homologación deberá cancelar a la Superintendencia de Telecomunicaciones, los siguientes valores:

a) Para equipos individuales (hasta 4 equipos)

Derechos de homologación:	US $ 13,14
Etiqueta:	US $ 0,79

b) Para equipos importados

1. Por primera vez:

Derechos de homologación:	US $ 131,45
Registro y verificación en laboratorio de los parámetros del equipo terminal:	US $ 40,00
Etiqueta	US $ 0,79

2. En las siguientes ocasiones por cada etiqueta opcional:

por cada etiqueta:	US $ 0,79

En caso de requerirse pruebas técnicas adicionales, el solicitante pagará los costos de laboratorio que correspondan.

3.6.2- Permisos y Limitaciones

Los interesados en instalar y operar sistemas de espectro ensanchado de gran alcance, en cualquier parte del territorio nacional, deberán presentar la solicitud para el registro correspondiente, dirigida a la SNT (Secretaría Nacional de Telecomunicaciones), adjuntando el estudio de ingeniería, elaborado por un ingeniero en electrónica y/o telecomunicaciones, describiendo la configuración del sistema a operar, el número del certificado de homologación del equipo a utilizar, las características del sistema radiante, las coordenadas geográficas donde se instalarán las estaciones fijas o de base del sistema

móvil, localidades a cubrir, y los demás datos consignados en el formulario que para el efecto pondrá a disposición la SNT.

El registro será por un período de 5 años y podrá ser renovado previa solicitud del interesado, dentro de los treinta (30) días anteriores a su vencimiento.

Se aprobará la operación de sistemas de radiocomunicaciones que utilicen la técnica de espectro ensanchado, en las bandas de frecuencias ICM indicadas a continuación:

- 902 - 928 MHz
- 2.400 - 2.483,5 MHz
- 5.725 - 5.850 MHz

Los sistemas que utilicen la tecnología de espectro ensanchado no deberán causar interferencia a otros sistemas de radiocomunicaciones que trabajen en estas bandas. La operación de los sistemas en modo de espectro ensanchado de secuencia directa, salto de frecuencia o híbridos, se aprobará con las siguientes configuraciones:

- Sistemas fijos punto a punto;
- Sistemas fijos punto - multipunto;
- Sistemas móviles;

Los sistemas que utilicen espectro ensanchado para aplicaciones de transmisión de datos en redes de área local (LAN), telemetría, lectura remota, PBX y teléfonos inalámbricos cuya potencia de salida del transmisor sea menor o igual a 100 milivatios (mW) no requerirán de aprobación expresa. En todo caso, la antena deberá ser omnidireccional con una ganancia máxima de 1 dBi y encontrarse adherida al equipo.

Limitaciones de Potencia (para los radios)

- Ambientes Indoors: Max 100mw(20dBm)
- Ambientes Outdoors: Max 1w(30dBm)

Limitaciones de Antenas

Outdoor Pto – Pto, Pto - Mpto

- 2.4Ghz
  - Ganancia máxima de la antena 6dBi.
  - Por cada 3dbi extras en la ganancia de la antena se reducirá en 1dBm la potencia de salida del Tx.
- 5.8 Ghz
  - Se puede usar una ganancia mayor a 6dBi en la antena, no hay límites.

Outdoor Pto – Pto, Pto - Mpto

- 5.8 Ghz
  - Se puede usar una ganancia mayor a los 6dBi en la antena

Sistemas Móviles

Los sistemas que usen antenas con ganancia superior a los 6dBi deberán reducir la potencia en el Tx en el mismo número de dBm que sobrepase la ganancia de la antena.

3.6.3- Pagos a la SUPERTEL (Superintendencia de Telecomunicaciones)

Para el registro de los sistemas espectro ensanchado de gran alcance, el solicitante o usuario deberá cancelar anualmente por anticipado, por concepto de uso del espectro radioeléctrico, durante el periodo de cinco (5) años, el valor en dólares de los Estados Unidos de América, que resulte de la aplicación de la fórmula que se indica a continuación:

$$\mathbf{IA = 4 * K * B * NTE}$$

Donde:

IA = Imposición Anual

B = 12 (Para sistemas Pto – Pto, Pto – Mpto)

B = 0.7 * NA (Para los sistemas móviles. Para el cálculo de IA se considerará un NTE mínimo de 50 estaciones entre bases y móviles)

K = Índice de inflación anual

NA = Número de áreas de operación

NTE = Número de estaciones

Haciendo un análisis desde el punto de vista técnico – práctico se tiene lo siguiente:

ISP.- Para que un ISP funcione como tal se necesitan los siguientes requisitos:

- Permiso de ISP.- Para lo cual se necesita:
  - RUC
  - Anteproyecto colegiado
- Permiso de enlace satelital.- El cual tiene un costo de 750,00 usd.
- Permiso de Servicios Portadores para clientes que no pertenecen a la misma red.- Es decir hay que contratar una empresa de servicios portadores para que provea del enlace de última milla.

CAPÍTULO IV

ANÁLISIS Y DISEÑO DEL WISP

4.1- Definición de un HotSpot

Funcionalmente, un HotSpot es un lugar público donde está disponible una conexión inalámbrica de red, de tal manera que usuarios con dispositivos inalámbricos compatibles como PDA´s, teléfonos celulares, laptops, etc., pueden conectarse a Internet o a una red privada, enviar y recibir emails o descargar archivos, todo esto sin la necesidad de utilizar cables.

Un HotSpot puede ser temporal o permanente sin perder su funcionalidad y seguridad, en otras palabras debe ser transparente para el usuario en todo aspecto como por ejemplo la conexión inicial a la red. Una de las principales razones por las que los usuarios acuden a los HotSpots, es porque están seguros que ahí van a encontrar una conexión de alta velocidad de navegación en Internet.

Es importante entender el entorno de un HotSpot para poder desarrollar una configuración que contemple los requerimientos de los usuarios. Hay tres factores que determinan qué tipo de entorno de HotSpot crear:

1. **El tamaño físico de la ubicación.-** Esto se refiere al número de AP que deben ser colocados para dar cobertura al lugar.
2. **El número de usuarios simultáneos.-** Se refiere al número de usuarios por unidad de área, como mínimo el HotSpot debe estar en capacidad de proveer 100Kbps por cada usuario activo. Un AP puede dar cobertura en un área física para 20 o 25 usuarios.
3. **Tipos de usos esperados.-** Esto se refiere al tipo de aplicaciones que el usuario ejecutará una vez que esté conectado a la red.

4.2- Seguridades

La especificación original del estándar 802.11b incluía tres mecanismos para seguridad inalámbrica conocidos como seguridad básica. La seguridad básica incluía primeramente el uso de un SSID (Identificador de Conjunto de Servicios), el cual tiene una llave abierta que se comparte al momento de autenticar un cliente, segundo una llave estática WEP, y por último una autenticación opcional de filtrado de direcciones MAC. Esta combinación proveía un rudimentario nivel de control de privacidad, que podía ser fácilmente vulnerado.

1.- Identificador de Servicio de Red (SSID - Service Set Identifier).- Para poder tener conexión a una red inalámbrica se necesita un identificador denominado SSID (Identificador de Conjunto de Servicios), un identificador único de 32 caracteres. El SSID diferencia una red inalámbrica de otra. Todos los puntos de acceso y todos los dispositivos que intenten conectarse a una WLan determinada deben utilizar el mismo SSID. 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 (beacon frame), por lo que es recomendable cambiarlo periódicamente.

Beacon Frames.- Los AP mandan constantemente anuncios de la red, para que los clientes móviles puedan detectar su presencia y conectarse a la red wireless. Estos anuncios son conocidos como Beacon Frames, si se rastrea (a través de un sniffer) las tramas de una red wireless se puede ver que normalmente los AP mandan el SSID de la red en los Beacon Frames, aunque esto se puede deshabilitar por software en la mayoría de los AP que se comercializan actualmente.

2.- Filtrado de direcciones MAC.- Con el fin de incrementar la seguridad en la Wlan es posible programar un AP para permitir el acceso solo a ciertos dispositivos de los

cuales conoce sus respectivas direcciones MAC. Esto se logra creando lo que se conoce con el nombre de ACL (Listas de Control de Acceso), en donde se encuentran registradas todas las direcciones MAC de los dispositivos Wi-Fi que forman parte de la red. Esto quiere decir que si un equipo que no tiene registrada su dirección MAC en la ACL intenta conectarse con el AP, éste no se lo permitirá. Las listas de control de acceso deben ser llenadas manualmente en cada uno de los AP´s , lo cual puede ser una ardua tarea dependiendo del tamaño de la red.

3.- Privacidad Equivalente Cableada (WEP - Wired Equivalent Privacy).- WEP proporciona a 802.11 servicios de autenticación y cifrado; 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.

Una limitación importante de este mecanismo de seguridad es que el estándar no define un protocolo de administración de claves para la distribución de las mismas. Esto supone que las claves secretas compartidas se entregan a la estación inalámbrica a través de un canal seguro independiente. El reto aumenta cuando están implicadas un gran número de estaciones, como es el caso de un campus corporativo.

Se ha demostrado su vulnerabilidad y han aparecido aplicaciones que escuchando las comunicaciones iniciales de un cliente que realiza el acceso a la red inalámbrica, son capaces de averiguar la clave y a partir de aquí pueden realizar escuchas en claro de lo transmitido por la red.

Métodos Estándares de Autenticación y Autorización

Para que un punto de acceso permita a las estaciones tener acceso a la red, las estaciones móviles deben asociarse con el punto de acceso. Antes de permitir la asociación, las estaciones y el punto de acceso deben autenticarse mutuamente.

Los métodos de autenticación por defecto del estándar 802.11 original son:

- Open System Authentication, éste método autorizaba el acceso a todas las estaciones registradas con un determinado nombre SSID. El sistema de autenticación abierto es muy común porque es fácil de usar.
- Shared Key Authentication, este mecanismo utiliza una clave secreta compartida que conoce el AP y el cliente. El AP envía una cadena de texto en un mensaje al cliente, el cliente es requerido para encriptar la cadena usando una clave WEP y enviarla de vuelta al AP. Una vez que el cliente ha sido autenticado está listo para ser asociado al AP y por consiguiente interactuar en la red.

Figura 4.1: Proceso de autenticación de un cliente en un AP

4.2.1- Requerimientos de seguridad

Los requerimientos básicos para la protección de una WLAN incluyen: control de acceso, mantenimiento de privacidad de usuarios, integridad de los datos y protección contra ataques conocidos de cualquier tipo.

Para cumplir con estos requerimientos la red debe proveer tecnología (sea hardware o software) que implemente las siguientes funciones:

- Tener una estructura total para juntar la implementación de las funciones mencionadas a continuación:
- Autenticación.
- Autorización
- Confidencialidad
- Integridad de los datos
- Administración de claves
- Protección contra ataques conocidos

Control de acceso a la estructura.- El control de acceso a la estructura provee la base para la implementación de todos los otros servicios. La especificación original de WEP no incluye una estructura para autenticación y autorización. Con WAP, WAP2 y RSN, el grupo de trabajo de 802.11i introdujo el estándar 802.1X como la estructura para autenticación y autorización.

Autenticación.- La autenticación se refiere a la verificación de credenciales provistas por una entidad que busca autenticación en la red. El método de autenticación usado en la implementación de una red, depende de algunos factores como son, si la red es corporativa o pública y qué servicios presta a los usuarios. Por ésta razón se necesita que de alguna manera la red soporte múltiples métodos de autenticación. 802.1X utiliza el protocolo EAP (Extensible Authenticaction Protocol), lo que significa que soporta múltiples métodos de autenticación.

Autorización.- La autorización se refiere a permitir a unidades autenticadas el acceso a recursos específicos de la red. 802.1X especifica la autorización basada en puertos. Una vez que un cliente autorizado (laptop o cualquier cliente inalámbrico) ha sido autenticado los puertos a través de los cuales puede acceder a los recursos de la red, son habilitados.

Confidencialidad.- Esta función indica cómo mantener en forma confidencial la información que es intercambiada entre uno o más clientes que se comunican. En otras palabras, solo los clientes a los cuales se les ha enviado un mensaje están en capacidad de leerlo. Esta función es complementada por un fuerte algoritmo de encriptación de frames inalámbricos.

WEP utiliza una pre clave compartida para encriptación, lo que presenta muchas debilidades que no fueron descubiertas sino hasta que el estándar fue lanzado al público. 802.11i utiliza un Estándar Avanzado de Encriptación (AES) corrigiendo así estas debilidades.

Integridad de los datos.- Esta función asegura que el receptor de un mensaje tenga la manera de detectar si el mensaje ha sido alterado mientras se enrutaba a su destino. En WEP, la integridad de los datos es implementada a través del uso de el algoritmo de Chequeo de Redundancia Cíclica (CRC), el cual no es criptográficamente seguro ya que sus resultados son predecibles, esto quiere decir que matemáticamente se puede predecir el CRC cuando uno o más bits en el mensaje son cambiados. WAP y WAP2 utilizan un algoritmo más robusto llamado Chequeo de Integridad del Mensaje (MIC).

Administración de claves.- La administración de claves se refiere a la capacidad para automatizar la forma como las claves de autenticación y encriptación son generadas, transferidas y utilizadas en el sistema, para asegurar la comunicación del enlace. Con WEP, 802.11 no proveía un manejo automático de claves. En WEP, una pre clave compartida es ingresada manualmente en todos los AP´s y en todos las estaciones inalámbricas que utilizan esos AP´s. Obviamente la falta de un manejo automático de claves es un gran vacío en la especificación. 802.11i soluciona este problema relevándolo a las funciones de administración de claves de 802.1X.

Protección contra ataques conocidos.- El diseño de un buen sistema de seguridad protegerá la red contra cualquier tipo de ataques que sean conocidos. 802.11i incluye protecciones contra ataques conocidos como Spoofing de capa MAC y el ataque del hombre en el medio (Man In The Middle). La resistencia a estos ataques es usualmente el resultado de la combinación de características como autenticación, autorización, confidencialidad y administración de claves.

4.2.2- Evolución de estándares para seguridad

La primera especificación para seguridades en el estándar 802.11 fue el protocolo WEP, pronto después fue completado ya que se determinó que éste tenía serias debilidades que prácticamente lo hacían vulnerable en ambientes donde la seguridad es crítica. El comité de 802.11 siguió adelante para proveer una especificación de seguridad más robusta para el estándar inalámbrico; y es así como definió la siguiente generación de estándares de seguridad para 802.11. El nuevo estándar es llamado "Robust Security Network" (RSN) también conocido como 802.11i.

RSN a incrementado los requerimientos computacionales del básico estándar WEP. Estas mejoras de requerimientos provienen de utilizar un algoritmos mucho más complejos de encriptación y de la inclusión de administración automática de claves. El nuevo requerimiento también significa que los equipos ya desplegados no pueden ser actualizados por la falta de tecnología para manejar estos requerimientos.

La alianza Wi-Fi concluyó entonces, que era necesario proveer una vía de migración a través de la cual los proveedores de servicio inalámbrico, pudieran hacer sus redes más seguras sin que tengan que reemplazar completamente todos sus equipos (AP´s, NIC´s, etc.), por cuestiones de costo definitivamente. Esta vía también fue necesaria ya que era poco razonable pretender que todos los clientes sean actualizados simultáneamente.

Para proveer una solución a este problema, la alianza Wi-Fi en un esfuerzo conjunto con el comité de la IEEE 802.11 desarrollaron la especificación "Wi-Fi Protected Access" (WPA) y luego WPA2. Estas dos especificaciones fueron desarrolladas utilizando partes finales de la todavía no ratificada especificación 802.11i.

802.11i.- La solución que plantea el estándar 802.11 para las falencias de WEP es Robust Security Network (RSN). RSN está siendo desarrollado por el grupo de trabajo denominado "i" de la IEEE, se tenía planificado su lanzamiento para mediados del año 2004, pero hasta la fecha de esta investigación no ha sido implementado.

RSN esta basado en el Estándar Avanzado de Encriptación (AES) para encriptación de frames inalámbricos y 802.1X para autenticación, autorización y administración de claves.

AES es un fuerte algoritmo de encriptación al que no se le conocen defectos, hasta donde han llegado las formas de criptoanálisis; sin embargo es computacionalmente exigente y podría consumir la mayoría de recursos computacionales en muchos de los AP´s que se comercializan actualmente en el mercado.

Laptops que utilizan tarjetas inalámbricas y descargan la encriptación al procesador principal podrían ser capaces de soportar AES; por otro lado a nivel de PDA´s posiblemente la mayoría de ellas no tienen los recursos necesarios para soportar AES.

Para proveer una ruta de migración que mejore la seguridad de sitios con AP´s no tan poderosos, el grupo de trabajo de la 802.11i también ha desarrollado un set de programas basados en la seguridad WEP, para trabajar en dispositivos que no tienen mucha capacidad computacional. Esta solución es llamada Wi-Fi Protected Access (WPA).

WPA fue desarrollado por la Wi-Fi Alliance como una solución interina a los requerimientos de seguridad de 802.11 y está basado en el borrador 3.0 del estándar 802.11i. Vale la pena destacar que WPA no es parte del estándar 802.11i.

Estándar Avanzado de Encriptación (AES – Advanced Encriptation Standard).- AES es el resultado del esfuerzo del Instituto Nacional de Estándares y Tecnología (NIST) en conjunto con la industria y la comunidad de criptografía para desarrollar el Estándar Federal de Procesamiento de Información (FIPS) que especifica un algoritmo de encriptación capaz de proteger sensitivamente información gubernamental. Este estándar está designado para reemplazar a la actual especificación de encriptación FIPS, llamada DES. AES es obligatorio para información gubernamental y opcional para la industrial. AES especifica el uso del algoritmo de Rijndael.

802.11i seleccionó a AES como el algoritmo básico para proveer encriptación a 802.11i, ya que es un algoritmo de encriptación muy robusto al cual no se le conocen fallas a pesar de que ha sido sometido a pruebas muy rigurosas de criptoanálisis.

AES tiene un alto grado de requerimientos de recursos computacionales (mucho más que WEP solo) y requerirá que la asistencia de hardware forme parte de los componentes de la red. El uso de AES como un algoritmo de encriptación requerirá la utilización de todas las capacidades computacionales de los AP´s, como por ejemplo AP´s con algún tipo de procesador en su tarjeta principal.

En el lado de las estaciones móviles, las computadoras portátiles estarán en capacidad de manejar el incremento de los requerimientos computacionales del algoritmo, mientras que por el lado de las PDA´s no será posible. Por esta razón el comité del 802.11 desarrolló la especificación TKIP para proveer una solución al hardware existente.

Protocolo de Integridad Temporal de Claves (TKIP – Temorary Key Integrity Protocol).- Diseñado como una envoltura para WEP, TKIP fue desarrollado para direccionar las debilidades de WEP y proveer una ruta de migración para mayor seguridad de las redes inalámbricas que utilizan el hardware existente.

TKIP requiere más de una actualización de software y/o firmware, ya que mientras por un lado utiliza el algoritmo RC4 (el mismo algoritmo de WEP) por otro lado agrega mejoras a la seguridad como:

- Nueva función de mezcla de claves por paquete.
- Nuevo chequeo de integridad de mensajes (MIC), llamado Michael.
- Vector de inicialización más grande (de 24 bits en WEP a 48 bits en TKIP).
- Nuevo mecanismo de reasignación de claves (sesión de claves renovada de la base regular).

TKIP inicia una sesión con una clave temporal de 128 bits que es conocida tanto por la estación móvil como por el AP, esta clave cambia después de cada 10,000 paquetes transmitidos. La clave de sesión es usada como un generador básico de claves por paquete. Las claves por paquete son generadas usando una combinación de funciones que usan una clave de sesión temporal, la dirección MAC de la estación móvil y la IV.

802.1X.- .- Con el fin de proporcionar un método más sólido de autenticación y autorización, Microsoft y una serie de proveedores han propuesto un marco de seguridad de WLAN mediante el protocolo 802.1X. 802.1X es una especificación que describe una arquitectura para un mecanismo de autenticación y autorización basado en control de puertos de acceso. 802.1X es parte de la familia de estándares para redes de área local y metropolitana, y está siendo adaptado por el grupo de trabajo "i" de la IEEE como la base para un nuevo modelo de seguridad Wi-Fi.

802.1X está basado en el Protocolo de Autenticación Extensible (EAP), éste permite a los administradores de la red escoger entre algunos métodos de autenticación, el más apropiado para su entorno.

El protocolo 802.1X implica al usuario de la red, un dispositivo de acceso a la red (o puerta de enlace) como un punto de acceso inalámbrico y un servicio de autenticación y

autorización en forma de servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota). El servidor RADIUS desempeña la labor de autenticar las credenciales de los usuarios y de autorizar el acceso de éstos a la WLAN.

RADIUS.- RADIUS (*"Remote Authenticated Dial-In User Service"*) es la infraestructura recomendada por la Wi-Fi Alliance como sistema de gestión centralizada que da una solución de autenticación para entornos con un elevado número de usuarios.

Teniendo en cuenta que este tipo de entornos utilizará normalmente estructuras mixtas (cable tradicional y WLAN), la utilización de este protocolo permitirá mejorar la capacidad de autentificación del usuario inalámbrico, proporcionando un nivel de seguridad superior, escalable y una gestión centralizada.

A través de este sistema se podrá obtener un Certificado de Cliente Universal para permitir la autentificación mutua (autentificación del cliente al AP y del AP al cliente), gestión de clave protegida a través del soporte para RADIUS-EAP-TLS, así como la integración en entornos RADIUS existentes que soporten el protocolo MD-5 con sistemas de autenticación múltiples con protocolo EAP.

Protocolo de Autenticación Extensible (EAP - Extensible Authentication Protocol).- Es una estructura genérica de autenticación que como su nombre lo dice, soporta una gran variedad de protocolos de autenticación.

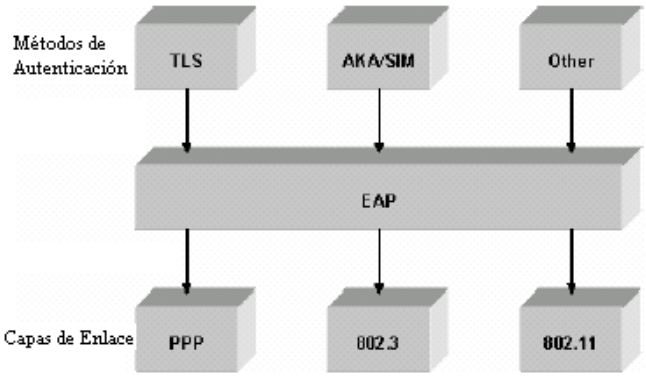


Figura 4.2: Diagrama del Protocolo EAP

EAP fue desarrollado originalmente para usarlo con PPTP. 802.1X utiliza EAP como parte de su mecanismo de control de acceso para redes inalámbricas, por esta razón EAP puede ser utilizado sobre una gran variedad de enlaces de datos. El protocolo actual de autenticación para ser usado para autenticación es seleccionado a través de un proceso de negociación entre la estación móvil y el servidor de autenticación.

Cada dispositivo hace la selección del proceso de autenticación basado en los protocolos que ellos soportan, y las políticas que pueden ser configuradas en cada dispositivo por el administrador. Un ejemplo de una política podría ser la selección de un protocolo específico de autenticación para conexiones dentro de la red de empresa y otro protocolo para conexiones fuera.

El soporte para la selección de políticas de autenticación depende de la implementación. Algunos dispositivos podrían no soportar esta característica, mientras otros pueden tener soporte extenso. Hay muchos protocolos de autenticación EAP, siendo los más importantes: MD5, LEAP, TLS, TTLS y PEAP.

Resumen de Mensaje 5 (MD5 - Message Digest 5).- MD5 es el método más simple de las variantes de autenticación EAP, pero cuando se usa sobre redes inalámbricas es el menos seguro. MD5 es un método de autenticación de una sola vía , es decir, de la estación móvil de la red al AP que usa una clave y una cadena para proveer pruebas de identidad.

La desventaja principal de MD5 radica en el almacenamiento de claves en modo texto limpio para el autenticador de acceso; siendo un método de autenticación de una sola vía, sólo la estación móvil es autenticada dejándolo vulnerable a ataques del tipo hombre en el medio (man in the middle). MD5 no provee administración de claves, por lo que los atacantes pueden olfatear y crackear la claves WEP. El soporte para MD5 es obligatorio en la especificación EAP.

EAP Ligero (LEAP - Lightweight EAP).- LEAP es un método EAP de autenticación desarrollado por Cisco que soporta autenticación mutua. Se usa el nombre de usuario y la contraseña de la estación móvil o cliente y credenciales del AP para ser autenticado por un servidor RADIUS.

Sobre autenticación, LEAP genera claves WEP una vez para usos de sesión, usando LEAP cada usuario conectado a la red inalámbrica usa una única clave WEP. Las claves de sesión pueden ser renovadas por una característica de tiempo fuera del servidor RADIUS que causa que el usuario se vuelva a logear, éste puede ser un proceso transparente para el usuario.

La vulnerabilidad de LEAP viene dada por el uso de MS-CHAPv1 para autenticación mutua, ya que éste protocolo es conocido por ser vulnerable a ataques. La desventaja principal de LEAP es que es un protocolo propietario de Cisco que sólo trabaja en redes end-to-end de Cisco. Otros fabricantes tienen agregado soporte para LEAP en sus servidores finales ensanchando así la interoperabilidad.

De cualquier manera, este protocolo no ayuda en un ambiente de Hotspot donde se necesita dar soporte a una gran cantidad de clientes y sus respectivos sistemas.

Nivel de Seguridad de Transporte (TLS - Transport Level Security).- TLS es un método de autenticación estándar de IETF (Internet Engineering Task Force) que utiliza certificados de X.509 para proveer autenticación mutua. En la generación TLS, la distribución y administración general de certificados requieren lo que se conoce como Public Key Infraestructure (PKI). TLS genera claves WEP por sesión y provee a la estación móvil reautenticación y reasignación de claves sin intervención del cliente.

La principal desventaja de TLS viene dada por sus requerimientos para el cliente que espera ser certificado. Administrar certificados para un gran número de clientes puede ser una tarea difícil y es suficiente razón para evitar este método de autenticación

Túnelado TLS (TTLS - Tunneled TLS).- TTLS, creado por Funk Software y ahora conocido como un estándar IETF (Internet Engineering Task Force), es uno de dos métodos de autenticación (el otro es PEAP) desarrollado para superar la demanda de requerimientos de certificación de clientes del protocolo TLS. En TTLS, las estaciones móviles se identifican a sí mismas a través de un nombre de usuario y una contraseña, mientras que el AP continúa usando certificados como en TLS.

TTLS es capaz de transmitir credenciales de una manera segura usando un túnel SSL (Secure Sockets Layer) establecido entre el cliente y el servidor de autenticación. Ya que se usa éste túnel seguro, TTLS está en capacidad de soportar múltiples mecanismos de respuesta (PAP, CHAP, MS-CHAPv1, MS-CHAPv2, PAP/Token Card o EAP). TTLS implementa diferentes métodos de autenticación por intercambio "atributo-valor-pares" (AVP) que son similares a los utilizados por el protocolo RADIUS. Otra ventaja de TTLS sobre TLS es que la identificación del usuario no es expuesta a fisgoneadores porque la información es enviada a través de un túnel establecido.

TTLS es considerado un protocolo muy seguro, ha sido implementado por algunos fabricantes y es ampliamente desplegado, son muy pocos los que no lo han aceptado como el método definitivo de autenticación del estándar 802.11; su principal rival es PEAP.

EAP Protegido (PEAP - Protected EAP).- PEAP, creado por Microsoft, Cisco y RSN es ahora un estándar IETF (Internet Engineering Task Force), es uno de dos métodos de autenticación (el otro es TTLS). En PEAP, como en TTLS la estación móvil se identifica a sí misma con un nombre de usuario y una clave, mientras que el AP continúa usando certificados. La diferencia principal entre TTLS y PEAP es que PEAP utiliza un túnel de cliente RADIUS para establecer un segundo intercambio EAP. Esto permite que PEAP soporte todos los métodos de autenticación de EAP.

Es importante destacar que PEAP es un protocolo propietario desarrollado por Cisco, que únicamente sirve cuando Cisco provee protocolos que están disponibles tanto en el cliente como en el servidor. Sin embargo, algunas compañías tienen licencias PEAP que les permiten incorporar el protocolo en sus servidores de autenticación.

Acceso Protegido Wi-Fi (WPA - Wi-Fi Protected Access).- WPA es un poderoso estándar basado en una tecnología de seguridad interoperable para redes Wi-Fi. Provee una fuerte protección para los datos a través de encriptación así como un fuerte control de acceso y autenticación de usuarios. WPA puede ser habilitado en dos versiones: WPA Personal y WPA Empresarial.

WPA Personal protege de accesos no autorizados a la red a través de claves; WPA Empresarial verifica a los usuarios de la red a través de un servidor. WPA utiliza claves de encriptación de 128 bits y claves dinámicas de sesión para asegurar la privacidad y seguridad de la red inalámbrica.

Acceso Protegido 2 Wi-Fi (WPA2 - Wi-Fi Protected Access 2).- Provee a los administradores de la red con un alto grado de seguridad que solo usuarios autorizados puedan ingresar. WPA2 está basado en el estándar ratificado IEEE 802.11i, y provee grado de seguridad gubernamental ya que fue implementado por el Instituto Nacional de Estándares y Tecnología (NIST).

Se lo puede habilitar en dos versiones: personal y empresarial. La versión personal evita accesos no autorizados a la red utilizando claves establecidas; la versión empresarial verifica a los usuarios de la red a través de un servidor. Yendo hacia atrás WPA2 es compatible con WPA.

Red Privada Virtual (VPN - Virtual Private Network).- La mejor forma de tratar a los usuarios de las redes Wi-Fi es hacerlo como usuarios “no confiables”, procediendo a manejarlos como usuarios venidos de Internet. En este sentido las soluciones empleadas

para las redes cableadas, cuando se las pone en contacto con Internet, son perfectamente aplicables a un entorno Wi-Fi. La protección en base a firewalls activos con soporte VPN hace que la solución sea económica, compatible con los diferentes fabricantes y sistemas operativos.

Una VPN trabaja a través de un servidor VPN creando un protocolo de encriptación para transferir datos a usuarios que se encuentran fuera de las oficinas. El software especial de VPN en el cliente remoto utiliza el mismo protocolo de encriptación, habilitando los datos para que sean transmitidos de forma segura sin oportunidad de intercepción.

Hay muchos tipos y niveles diferentes de tecnología VPN, algunos de los cuales son muy caros y requieren componentes tanto de software como hardware, sin embargo Microsoft provee una configuración gratis pero básica de tecnología VPN en sus servidores avanzados de sistemas operativos.

Kerberos.- Es otra manera de proteger a las redes inalámbricas de datos. Es un sistema de autenticación basado en distribución de claves, esto permite a las entidades que se comunican a través de cables o inalámbricamente probar sus identidades unas a otras previniendo ataques escondidos.

Luego de que un cliente y un servidor han utilizado Kerberos para probar su identidad, también pueden encriptar todas sus comunicaciones para asegurar la privacidad e integridad de los datos.

Kerberos provee a los usuarios o servicios tickets digitales que ellos pueden utilizar para identificarse a sí mismos en la red, y para claves secretas de encriptación para comunicaciones seguras. Un ticket es una secuencia de unos pocos cientos de bytes que pueden estar embebidos virtualmente en cualquier otro protocolo de red.

4.2.3- Principales amenazas para la seguridad de las WLAN

4.2.3.1- Interceptación (revelación de datos)

La interceptación de transmisiones de la red puede dar lugar a la revelación de datos confidenciales y de credenciales de usuario sin protección, además de a una posible usurpación de la identidad. Permite también que intrusos expertos recopilen información sobre los entornos de TI y la utilicen para atacar otros sistemas o datos que, de otra forma, no serían vulnerables.

4.2.3.2- Interceptación y modificación de los datos transmitidos

Si un atacante logra obtener acceso a la red, puede introducir un equipo falso que intercepte y modifique los datos comunicados entre dos usuarios autorizados.

4.2.3.3- Imitación

El acceso directo a la red interna permite que el intruso falsifique datos que parecen legítimos de manera que no sería posible desde fuera de la red, por ejemplo, un mensaje de correo electrónico de un usuario imitado. Los usuarios, incluso los administradores de sistemas, suelen confiar en los elementos originados dentro de la red mucho más que en los que proceden del exterior de la red corporativa.

4.2.3.4- Denegación del servicio (DoS)

Un agresor determinado puede activar un ataque de DoS de diversas maneras. Por ejemplo, la interrupción de las señales de radio se puede activar mediante algo tan simple como un microondas. Existen ataques más complejos cuyo objetivo son los protocolos inalámbricos de bajo nivel, y otros menos complejos cuyo objetivo son las redes mediante un gran incremento del tráfico aleatorio en la WLAN.

4.2.3.5- Carga libre (o robo de recursos)

Es posible que los intrusos sólo deseen utilizar su red como punto de libre acceso a Internet. Si bien esto no es tan grave como las demás amenazas, hará que, como mínimo,

no sólo empeore el nivel de servicio prestado a los usuarios autorizados sino también que puedan introducirse virus y otras amenazas.

4.2.3.6- Amenazas accidentales

Algunas características de las WLAN facilitan la aparición de amenazas no intencionadas. Por ejemplo, un visitante autorizado podría iniciar el equipo portátil sin la intención de conectarse a la red, pero se conecta a su WLAN automáticamente. Así, el equipo portátil del visitante se convierte en un punto de entrada de virus en la red. Este tipo de amenaza sólo se da en WLAN desprotegidas.

4.2.3.7- WLAN no autorizadas

Si una empresa no dispone oficialmente de una WLAN, es posible que siga estando bajo la amenaza de las WLAN sin administrar que surjan en su red. El hardware de WLAN adquirido a bajo precio por parte de empleados entusiastas puede abrir vulnerabilidades no intencionadas en su red.

4.3- ISP inalámbrico utilizando un nodo Wi-Fi

Con la venida del estándar base 802.11 las comunicaciones trajeron nuevas oportunidades de negocio, entre ellas el requerimiento de un nuevo tipo de Proveedor de Servicio de Internet (ISP), llamado Proveedor de Servicios de Internet Inalámbrico (WISP). Dentro de los servicios que un WISP puede proveer se encuentran:

- Diseño del HotSpot.
- Administración
  - Monitoreo remoto del estado del HotSpot.
  - Dirección de actualización de hardware y software.
  - Administración de la configuración de la red.
  - Administración de cuentas de usuario.
- Control de Acceso y Monitoreo

- ❖ Aprovisionamiento
- ❖ Autenticación
- ❖ Seguridad

- ➢ Contabilidad y Facturación: Pre pago, post pago y pagos de servicios Roaming.
- ➢ Acceso WAN.

Los HotSpots pueden ser implementados en lugares como cafeterías, hoteles, universidades, aeropuertos, etc. No necesariamente los WISP´s tienen que ser los dueños de la ubicación del HotSpot, los WISP´s y los dueños de la ubicación podrían establecer relaciones comerciales para entregar comunicaciones inalámbricas a través de un HotSpot.

En algunos casos, los dueños de diferentes espacios físicos contratan a algunos WISP´s para entregar servicios inalámbricos en sus áreas. Un ejemplo de esto es una cadena de hoteles, ya que ésta podría escoger diferentes WISP´s dependiendo de su ubicación geográfica o de otras razones comerciales.

4.3.1- Entorno Wireless

Mantener una buena calidad de comunicación entre la estación móvil y el AP en el HotSpot es típicamente el aspecto más ignorado a la hora de implementar el HotSpot, es muy importante considerar el entorno para poder dar una buena cobertura de radio frecuencia y una alta calidad de transmisión real de paquetes (throughput).

Una red wireless puede ser implementada satisfactoriamente considerando los siguientes puntos:

- ➢ Investigar los requerimientos del sitio para determinar el tipo de HotSpot que se va a implementar.
- ➢ Realizar una inspección del sitio para determinar los posibles problemas que involucra instalar la red wireless.
- ➢ Evaluar el sitio para la cobertura y ubicación de los AP´s.

- Escoger la tecnología adecuada.
- Escoger los equipos cuidadosamente dependiendo del entorno del lugar.
- Tomar debidamente las precauciones para proporcionar un alto grado de seguridad de la red inalámbrica.

4.3.2- Realizar la inspección del espectro (RF) en el sitio

La inspección del sitio es una de las partes más importantes de cualquier red inalámbrica, para esto se requiere de tres equipos que son:

- Un AP estándar
- Un analizador de radio frecuencia
- Una computadora portátil

La prueba del AP podría ser una muestra representativa de lo que se está planeando implementar en el entorno. Si no se está seguro de qué AP usar, un AP certificado por Wi-Fi es más que suficiente en la mayoría de los casos.

Los analizadores de radio frecuencia vienen en muchas formas y tamaños, algunos de los más conocidos son AirMagnet, Wildpackets AiroPeek NX y Network Instruments Observer. Si se está planeando implementar un entorno 802.11 únicamente, AirMagnet tiene una buena solución para PDA´s (haciendo mucho más fácil la inspección del sitio). Además, hay muchos programas gratis que se pueden descargar de Internet como por ejemplo NetStumbler, MiniStumbler (para PDA´s), Kismet (para Linux) y Elixar AirTraf (para Linux). Hay que tomar en cuenta que estos programas son muy útiles y recomendables aunque sean gratis, pero en muchos casos no son tan completos y funcionales como los programas comerciales.

Inspeccionar la radio frecuencia de un sitio requiere mucha paciencia y ser muy cuidadoso con los detalles, muchas veces equipos como hornos microondas, teléfonos inalámbricos, monitores de video inalámbricos, paredes de metal, etc. pueden interferir en

el espectro aunque la herramienta de análisis no los detecte. Usualmente los teléfonos inalámbricos causan interferencia sólo cuando están en uso, al igual que los hornos microondas. Si la frecuencia del AP, es decir, el canal en el cual está configurado para trabajar, está cerca de la frecuencia de éstos dispositivos, la radiación de ruido podría presentar problemas más serios que los descritos anteriormente.

Como punto final es importante considerar que se debería realizar la inspección del sitio cuando la red esté casi lista para ser usada, si es posible varias visitas al sitio ayudarían a asegurarse que no existen fuentes adicionales de interferencia. Hacer un archivo de cualquier actividad incluyendo canales, direcciones MAC e intensidad de la señal, esto con el objetivo de llevar un registro de parámetros correctos o idóneos.

4.3.3- Consideraciones de rendimiento

Mientras que para el estándar 802.11b la máxima tasa de transferencia es 11 Mbps para el estándar 802.11g es 54 Mbps, pero hay que considerar que hay varios factores que pueden afectar el rendimiento de la tasa de transferencia. Aparte de las consideraciones de diseño del hardware, los dos factores más influyentes que pueden afectar el rendimiento son la distancia (entre el transmisor y el receptor) y los métodos pro-activos usados por los protocolos para negociar con la interferencia de la señal. Hay algunos mecanismos de compensación en la especificación 802.11 para posibles errores de transmisión que podrían resultar por una baja intensidad de señal y/o alta interferencia.

Por ejemplo, mientras más se alejen el transmisor y el receptor la tasa de transferencia puede bajar automáticamente desde 11 Mbps a 5.5, 2 o inclusive a 1 Mbps. La tasa más baja de transferencia actúa para asegurar que hayan menor cantidad de errores cuando la señal de radio frecuencia está más débil.

Otra forma de disminuir la tasa de errores es usando el control de mensajes (RTS/CTS) que tiene el estándar 802.11, para reservar el canal antes de la transmisión de

los frames; esto quiere decir que el transmisor puede automáticamente cambiar usando estos mensajes cuando detecta una alta tasa de transferencia de error; después de esta consideración para evadir de errores, se recuperan mecanismos y protocolos de cabeceras, por lo cual la tasa efectiva de transferencia va a ser menor.

El estándar 802.11 además requiere que cada paquete enviado sea reconocido, más allá de que esto reduce más la tasa efectiva de transmisión. Por lo tanto la máxima tasa de transferencia para el estándar 802.11b estará alrededor de los 5.5 Mbps, mientras que para los estándares 802.11a o 802.11g estará alrededor de los 27 Mbps.

4.3.4- Tamaño de la célula del AP, diseño y ubicación

Siempre se está tentado en agregar más AP´s para resolver problemas de cobertura, pero habría que tener mucho cuidado antes de tomar este tipo de decisiones; ya que en muchos casos las redes inalámbricas son usadas para atraer personas dentro de lugares de negocios. Si ésta es la estrategia, ubicar un AP cerca de una pared exterior o ventana, podría ocasionar que usuarios no deseados que están fuera del lugar utilicen la red o peor que eso la ataquen.

La ubicación de los AP´s necesita ser cuidadosamente estudiada, usando datos de una inspección del espectro con consideraciones del lugar, para ubicar los AP´s en los lugares más apropiados. Ubicar AP´s en lugares donde puedan generar señal fuera de donde se quiere, también puede causar problemas con otras redes inalámbricas y alterar las expectativas de cobertura.

Cuando se coloca un AP se debe tomar en consideración el canal y el tamaño de la célula, ya que debido a la naturaleza de la banda ICM sólo hay 3 canales no solapados disponibles para las redes 802.11b. Para implementar un canal apropiado se debe estar familiarizado con la esfera de espectro que irradia el AP dado, de lo contrario habría que

revisar el manual de fábrica o visitar el sitio web del producto para determinar el área típica de cobertura en una configuración determinada.

4.3.5- Consideraciones para el diseño de la infraestructura de canales

Cuando se utilizan diferentes capacidades del estándar 802.11 es importante recordar el impacto que estos pueden tener en el diseño de la red inalámbrica. Actualmente, muchos de los AP´s que se encuentran en el mercado vienen con capacidades de múltiple frecuencia como b/g y a/g. Es importante recordar que el tamaño efectivo de la célula de los AP´s que soportan diferentes frecuencias (802.11a vs 802.11g , 802.11g infiere 802.11b) son completamente diferentes y si soportan ambos tipos de conexión, esto debe ser considerado.

El estándar 802.11a utiliza el espectro de frecuencia de 5Ghz y es más limitado en la cobertura efectiva de la distancia comparado con el estándar 802.11g (2.4 Ghz); esto es debido a la frecuencia y limitaciones de intensidad de la señal. Se necesitarían tres AP´s 802.11a para cubrir la misma área que cubre un AP 802.11g.

4.3.6- Tipos de Access Points

Básicamente los AP´s están clasificados en tres tipos que son: Small Office/Home Office (SOHO), empresariales y suichables por lo que hay que tener mucho cuidado a la hora de seleccionar un AP para una aplicación en particular.

Los AP´s SOHO son ante todo productos de baja administrabilidad que están diseñados para trabajar por sí solos, y no poseen las mismas características y funcionabilidad que se podría encontrar en los AP´s del tipo empresarial. Por ejemplo, es improbable que se necesite soporte RADIUS o administración SNMP en un entorno de hogar; sin embargo es más probable que se pueda necesitar DHCP, ruteo básico y capacidades de NAT. En muchos casos los AP´s del tipo SOHO no poseen las últimas o

más robustas consideraciones de seguridad, aunque tienen por lo menos los estándares básicos.

Los AP´s de la clase empresarial están diseñados para usuarios más exigentes ya que manejan alta administrabilidad e interoperabilidad de dispositivos. Estos AP´s son para trabajar en redes muy grandes con múltiple soporte para roaming de usuarios, varias capacidades de seguridad y soporte detallado de datos en tiempo real.

Una nueva categoría de AP´s son los Suitches Empresariales Inalámbricos, que son conocidos como Dispositivos Gordos por la abundante capacidad de procesamiento y la individualidad que poseen. Son muy útiles ya que en vez de tener un paquete completo de AP´s, se puede tener pequeñas combinaciones de antenas y puentes que bajan la señal de radio frecuencia, a un protocolo Ethernet estándar que utiliza cable categoría 5 para transmitir datos a la cabecera del dispositivo.

Estos suitches pueden soportar decenas de antenas desplegadas en toda una área y reducen significativamente el número de dispositivos que necesitan ser manejados. Ellos también mejoran el balance y roaming desde que el suitch y las antenas actúan como dispositivos individuales. Adicionalmente, muchos de estos dispositivos soportan auto configuración del entorno de radio frecuencia y pueden ubicarse por sí solos en la intensidad de señal más baja si no detectan a ningún cliente; sin embargo estos equipos pueden ser un poco caros y requieren mucha energía y mantenimiento.

4.3.7- Características que hay que buscar en un Access Point

Las características que hay que buscar en un AP en la mayoría de los casos depende del tipo de implementación que se va a realizar. En general, las siguientes características son ideales para que entorno inalámbrico sea utilizable y manejable:

La intensidad de la señal del espectro debería ser ajustable.- En muchos AP´s del tipo SOHO esta característica no está disponible, la falta de ella lidera los problemas en

implementar un entorno multi AP. Típicamente un AP del tipo empresarial soporta un rango de potencia que está entre los 5 a 100 miliWatts.

Múltiples tipos de antenas.- Los AP´s deberían soportar una variedad de tipos de antenas, y ser ajustables para encender o apagar la propiedad de diversidad de la antena. La diversidad de antenas es un método para minimizar el desvanecimiento multiruta que se produce usando múltiples antenas; el sistema de radio escoge la señal de la antena con mejor recepción, esto específicamente útil en áreas de alta interferencia.

En algunos AP´s SOHO 802.11a/b no se podría encender la propiedad de diversidad ya que están divididos en dos antenas. Algunos AP´s tienen inclusive antenas que están cableadas haciendo imposible cambiar a una antena direccional o remota.

Administración Remota.- Los AP´s deberían tener algunas formas de administrabilidad mediante acceso remoto como SSH2 o HTTPS, ya que éstas son más seguras contra atacantes. Si éstas no están disponibles, deberían tener otros métodos para prevenir posibles ataques en la interfase de administración. Algunas tácticas para prevenir ataques pueden ser poner los AP´s en subredes restringidas y controlar el acceso mediante ACL´s (Access Control List).

Soporte SNMP.- El soporte para SNMP debe estar en cualquier solución de nivel empresarial. Siempre hay que asegurarse que SNMP esté deshabilitado y recordar cambiar las cadenas y contraseñas que vienen por defecto.

Energía sobre Ethernet (PoE).- PoE puede marcar la diferencia entre los costos de una implementación de HotSpot para que éste sea efectivo o no. PoE permite que la energía llegue directamente a los dispositivos remotos a través de cable Ethernet categoría 5. Desde que los AP´s son a menudo puestos en lugares donde es difícil conseguir energía (techos y largos corredores) PoE es una solución mucho más deseada que tener un nuevo, costoso y poderoso acceso instalado. Desde que PoE fue ratificado por la IEEE como el

estándar 802.3af muchos fabricantes lo utilizan en sus dispositivos para satisfacer requerimientos de los clientes.

Soporte para preámbulo largo y corto.- La primera generación del estándar 802.11, indicaba el uso de un preámbulo de 144 bits que era usado para ayudar a los receptores, a prepararse para la adquisición de señales inalámbricas. Como 802.11direccionó altas tasas de transferencia y consideró el uso de nuevos modelos como VoIP, introdujo también un preámbulo más corto pero más eficiente de 54 bits.

Luego de la introducción de este preámbulo, los primeros AP´s y NIC´s en el mercado incluyeron una opción de configuración para usar cualquiera de los dos, el corto o el largo. Esto causó problemas de interoperabilidad para usuarios de estaciones móviles que no tenían esa opción. Si el AP utiliza para la comunicación el preámbulo corto y el cliente utiliza el preámbulo largo, ellos no se podrían asociar y el cliente no se podría conectar. Reconocer este problema de interoperabilidad hizo que los fabricantes de hardware, desarrollaran sistemas que puedan reconocer automáticamente cualquier seteo; es decir, la opción para administradores o clientes para seleccionar el preámbulo desapareció de la interfase de configuración del dispositivo.

En la actualidad, todavía se encuentran dispositivos en los cuales hay que escoger el preámbulo; si ese fuera el caso, es recomendable usar el preámbulo largo ya que provee la capacidad de interoperabilidad con estaciones móviles que todavía usan NIC´s.

4.3.8- Formas como se registra un cliente en un AP

Registro de los clientes a un AP.-

1. El cliente manda una señal de prueba.
2. Los AP mandan una respuesta a la prueba del cliente, y éste evalúa el mejor AP.
3. El cliente manda una petición de autenticación al AP seleccionado (AP A).
4. El AP A confirma la autenticación y registra al cliente.

5. El cliente manda una petición de asociación al AP seleccionado.
6. El AP A confirma la asociación y registra al cliente.

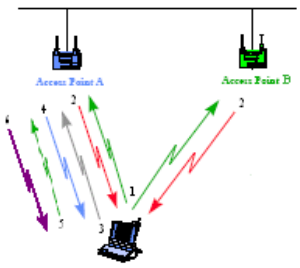


Figura 4.3: Registro de los clientes a un AP

Reasociación de un cliente a otro AP.-

1. El adaptador escucha las señales desde los AP, y selecciona el mejor AP en base a dichas señales.
2. El adaptador manda la petición de asociación al seleccionado AP.
3. El AP B confirma la asociación y registra al adaptador.
4. El AP B informa al AP A acerca de la asociación con el AP B.
5. El AP A reenvía los paquetes en el buffer al AP B y desregistra al adpatador.

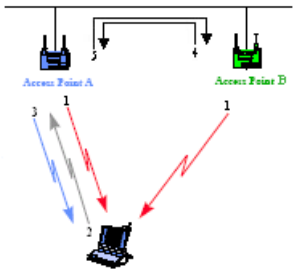


Figura 4.4: Reasociación de un cliente a otro AP

4.3.9- Factores condicionantes

Los factores que van a condicionar y determinar el funcionamiento y el rendimiento del enlace inalámbrico son los siguientes:

Potencia de transmisión de las tarjetas.- Según la potencia de transmisión de las tarjetas, se las puede clasificar en dos tipos generales:

- 30 mW de potencia de transmisión (aprox. 15 dB)
- 100 mW de potencia de transmisión (aprox. 20 dB)

Cuanto mayor sea la potencia de transmisión, mayor será el alcance del enlace, siempre teniendo en cuenta los demás factores condicionantes.

Calidad de los conectores.- Hay que ser cuidadoso a la hora de realizar las conexiones, crimpados y soldaduras de los conectores. Es preferible gastar algo más de dinero en conectores y herramientas de calidad y ganar en estabilidad del enlace y evitar pérdidas de señal. Para este tipo de cableado se suele utilizar conectores de tipo N.

Longitud y calidad del pigtail.- Este conector suele ser de tipo N, cuanto más corto y de más calidad sea el pigtail, menor será la pérdida de señal. El pigtail se lo puede comprar hecho o bien hacer uno a medida. Se aconseja que en ningún caso el pigtail supere los 2 metros de longitud, si bien unos 20cm pueden ser suficientes.

Longitud y calidad del cable coaxial.- El cable coaxial es uno de los factores más importantes a la hora de elegir el tipo de montaje que se va a realizar. El coaxial deberá recorrer desde la antena (colocada habitualmente en el exterior del edificio y en el punto más alto de este) hasta la ubicación del PC o AP (normalmente dentro del edificio).

Hay que tener en cuenta:

- Cuanto más largo sea el cable coaxial, mayor será la pérdida de señal.
- La calidad del cable afecta a la pérdida de señal / metro. Se podría decir que:

cable de menor pérdida = cable más grueso y rígido = cable más caro

No existe longitud máxima para el cable coaxial, pero a mayor longitud, mayor pérdida. A continuación, una pequeña tabla que muestra la relación entre modelos de cable LMR y pérdida de señal / metro longitudinal a una frecuencia de 2.4GHz:

Cuadro 4.1: Cuadro de cables y sus respectivas pérdidas

Cable	Pérdida en dB/100m
LMR-200	54.2
LMR-240	41.5
LMR-400	21.7
LMR-600	14.2
LMR-900	9.58
LMR-1200	7.27
LMR-1700	5.51

Ganancias y tipos de antenas.- De acuerdo a la fórmula vista anteriormente en la sección de cálculo de enlaces, la ganancia de las antenas determina la calidad final del enlace, así como el tipo de antena elegida.

Distancia entre antenas.- Cuanto mayor sea la distancia entre antenas, obviamente mayor será la pérdida de señal. La distancia máxima puede variar desde varios metros hasta decenas o cientos de kilómetros. Es altamente recomendado que haya una línea de visión directa entre las antenas.

Zona de Fresnel.- La zona de Fresnel expresada en la tabla que se muestra a continuación (la que se usa en la práctica), es calculada según el 70% de la 1ª zona de Fresnel a una frecuencia de 2.4GHz más la curvatura terrestre para cada distancia.

Cuadro 4.2: Cuadro de distancias entre antenas en Zona de Fresnel

Distancia entre antenas (en Km)	Zona de Fresnel (en metros)
1	3.9
5	9.7
10	16.4
15	24.4
20	34.0
25	45.4

30	58.7

Condiciones del terreno y meteorológicas.- Los árboles, los edificios, tendidos eléctricos, etc. influyen en la recepción de la señal. La señal se reflecta en los objetos y llega con retardo de fase a la antena receptora, pudiendo provocar pérdidas de señal. Se puede corregir este efecto desplazando 6cm longitudinalmente hacia delante o hacia atrás la antena receptora (6cm es la mitad de la longitud de onda, es decir, desde un pico hasta un valle de la senoide).

El hielo y la nieve influyen negativamente en las antenas cuando están en contacto directo con éstas. La lluvia en sí tiene poco impacto sobre la pérdida por propagación, pero en el caso de las antenas "flat-pannel", puede disminuir su rendimiento si se crea una película de agua en el panel de la antena.

Para un enlace de correcto, la sensibilidad debe ser:

- Para 11Mbit: -82dBm
- Para 5.5Mbit: -87dBm
- Para 2Mbit: -91dBm
- Para 1Mbit: -94dBm

El margen ha de ser:

- Mínimo: 10dB
- Enlaces expuestos a interferencias (ciudad): 15dB
- Enlaces con condiciones climáticas adversas: 20dB

4.3.10- Equipamiento básico

Una solución básica para implementar un ISP inalámbrico debería estar constituida por los siguientes elementos:

Hardware:

- Un proveedor de servicios de Internet.- Es decir, se necesita tener una conexión permanente a Internet de por lo menos 256 Kbps o más rápida.
- Un Servidor.- Un computador bastante potente, de preferencia un servidor donde va a estar alojado el servidor RADIUS, así como también la base de datos.
- Por lo menos un Access Point.- Para realizar la gestión inalámbrica del WISP, dependiendo del área de cobertura y de la cantidad de usuarios que se vaya a administrar.
- Un Switch.- Para administrar la parte cableada de la red.
- Un Router.- Que servirá como puerta de enlace hacia Internet, podría ser un modem-router inclusive.
- Una antena de alta ganancia.- Ya que se usan radios de bajo poder y antenas de alta ganancia para los enlaces inalámbricos, con el objetivo de dar mejor cobertura.
- Cliente.- Que utilicen el servicio de Internet inalámbrica.

Software:

- Un servidor RADIUS.- Este software es el que va a permitir gestionar la autenticación, autorización y la contabilidad para cada usuario que acceda a la red. Permitirá gestionar el tiempo de conexión para cada usuario así como claves de acceso.
- Windows 2000 Server o Windows 2003 Server
- Una base de datos o un manejador de archivos.- Para la gestión de la información de los clientes.
- Licencias.- Son todas las licencias de software necesarias para que la información pueda ser debidamente procesada.

Consideraciones adicionales

- Que los clientes se localicen en un radio de 2km alrededor del sitio central; esta distancia dependerá de la ganancia de la antena que se utilice; utilizando repetidores se pueden cubrir distancias de hasta 30 Km.
- Una línea de vista directa entre el sitio del cliente y la antena central.
- El uso de las frecuencias 2.4GHz ó 5.7GHz según las regulaciones locales.
- Se debe considerar una ubicación alta para instalar la antena central, para que todas sus antenas clientes puedan ver la antena central sin ningún obstáculo, es decir, ellos deben tener línea de vista directa con la antena central. Algunas sugerencias para las mejores ubicaciones de la antena de la estación base podrían ser:
    - La cima de un edificio alto en alguna parte en la ciudad.
    - La cima de un edificio localizado en una colina.
    - Una torre alta (TELEVISIÓN o alguna torre de comunicación)
- Es muy importante, que encontrar la ubicación dónde puedan instalarse estrechamente la antena de la Estación base y la Unidad de la Radio Base, por ejemplo:
    - La antena en el techo de un edificio y la unidad base en el ático,
    - La antena en una torre de comunicación y la unidad base en una caja impermeable (Waterproof box) atada a esta torre.

Un esquema básico de un ISP inalámbrico debe lucir de la siguiente manera:

Figura 4.5: Esquema básico de un IPS inalámbrico (Tomado de una solución D-Link)

4.4- Análisis Financiero

En una infraestructura inalámbrica urbana los costes dependen linealmente del precio del equipamiento, la cantidad de equipamiento necesario y la posibilidad de incrementar la cobertura de forma escalonada y pareja al incremento de las necesidades.

Para el caso de estudio planteado los equipos necesarios junto con sus costos aproximados serían los siguientes:

Cuadro 4.3: Cuadro de Análisis Financiero

Cant.	Descripción	P. Unitario	P. Total
1	Antena Omnidireccional de 15 dbi	380.00	380,00
1	Access Point RoamAbout AP3000	700.00	700,00
41	Access Points Air Premier 2.4 Ghz D-Linik	90.00	3690,00
1	ISP enlace microonda de 1Mbps	2000.00	2000,00
1	Pc o servidor	1000.00	1000,00
1	Licencias WinRadius para 1500 usuarios	1,5.00	2250.00

100	Cable coaxial LM200 con conectores	0,60	60,00
		TOTAL:	10080.00

Los valores presentados en la tabla anterior han sido tomados de los distribuidores de equipos y/o servicios inalámbricos locales, dichos precios están sujetos a cambios sin previo aviso; por lo tanto el resultado final es un valor estimativo.

La diferencia de costo entre el AP RoamAbout de Enterasys con el AP Air Premier de D-Link es debido a sus diferencias de valor agregado, por ejemplo es un radio multibanda, tiene soporte para mayor número de usuarios entre otras ventajas por lo cual es más costoso y funcional.

Los costos de las licencias se desprenden de la siguiente tabla proporcionada por la empresa comercializadora del software ITCONSULT2000:

Cuadro 4.4: Cuadro de costos de licencias de WinRadius

Tarifa Básica	US$500 / 100 users (100 users license)	US$1200 / k users (3- 4k users license)
	US$400 / 100 users (200 users license)	US$900 / k users (5-9k users license)
	US$320 / 100 users (300 - 900 users license)	US$600 / k users (10-99k users license)
	US$1500 / k users (1- 2k users license)	US$400 / k users (100k- users license)
	Por ejemplo, el precio de la licencia para 5000 usuarios será US$900 X 5 = US$4500.	
	(Nota: Usuarios quiere decir usuarios totales, todos los usuarios pueden entrar al mismo tiempo; para un número ilimitado de usuarios escoger la versión Linux.	

Para mayor información acerca de este producto puede referirse a la siguiente dirección electrónica: http://www.itconsult2000.com.

Nota: Este análisis de costos se ha hecho partiendo de una infraestructura de red cableada existente, es decir, si se empezara desde cero habría que aumentar todos los costos de los equipos necesarios para implementar la parte cableada de la red.

4.5- Gestión y/o administración del ISP

Antes de empezar a describir la administración del WISP, es importante primero aclarar la forma como será interconectado todo el hardware necesario para que la solución inalámbrica planteada sea óptima.

4.5.1- Distribución e interconexión de equipos

Según el diagrama de la Red LAN de la ESPE campus Sangolquí, la universidad tiene una infraestructura de 11 edificios que conforman el Backbone principal, todos ellos conectados mediante fibra óptica como se muestra a continuación:

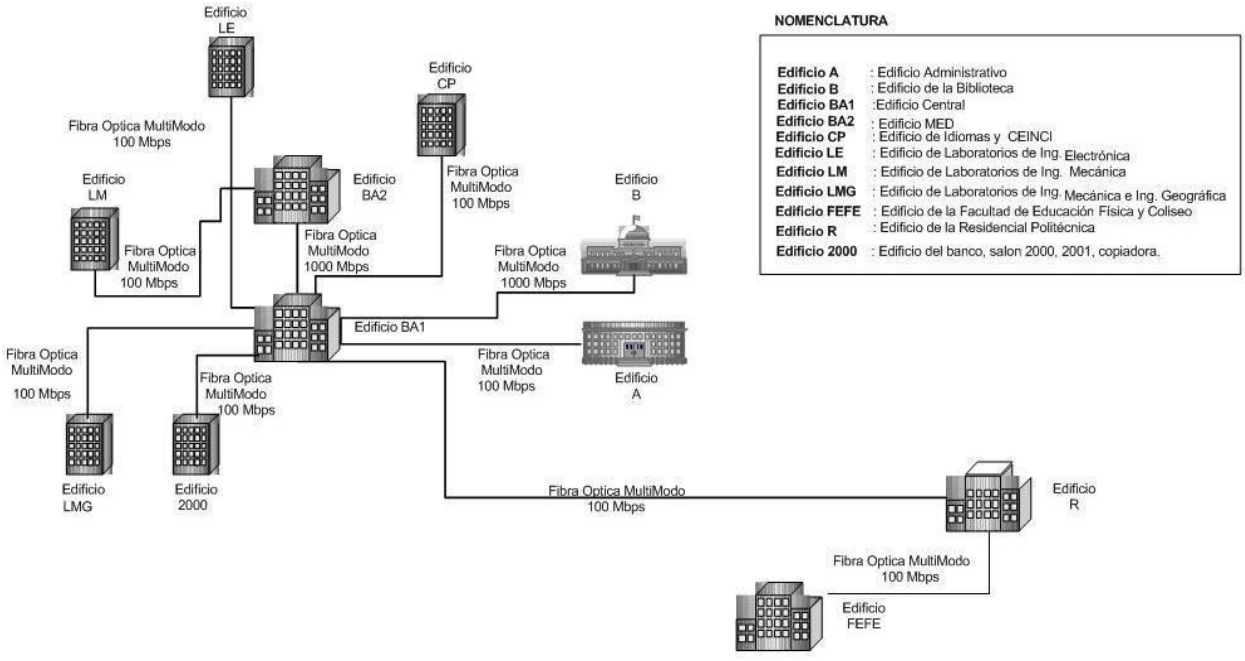


Figura 4.6: Diagrama Red LAN - Campus ESPE Sangolquí

Cada edificio tiene cuatro pisos a excepción del Edifico 2000 que tiene un piso con dos salones 2000 y 2001, de esta observación se desprende que se necesita un AP para dar

cobertura a cada piso, con lo que se estaría cubriendo el entorno indoor completamente y se estaría justificando los 42 AP´s mencionados anteriormente. La solución completa va ha estar dividida en dos áreas fundamentales que son interiores y exteriores.

Ambientes Interiores (Indoors)

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 mantenimiento pueden ser estar llenas de variables, lo más conveniente es empezar por bases sólidas y buscar un sistema robusto.

En el caso de los edificios de la ESPE, la configuración ideal sería un sistema mixto de cable e inalámbrico. El inalámbrico nos permitiría tener cobertura del red en cualquier lugar, pero el cable ayudará a una disposición homogénea de puntos de acceso.

En dicha instalación en alguna parte de las oficinas debería haber un switch. El Switch será el centro de la infraestructura tanto cableada como inalámbrica. En cada planta debería haber un Punto de Acceso inalámbrico que diese cobertura a esa planta. Si la planta tuviese una extensión importante, se deberá añadir un segundo Punto de Acceso trabajando en modo repetidor.

Ahora lo que hay que hacer es llevar la señal de red al punto de acceso de cada planta. Los Puntos de Acceso emiten una señal de red inalámbrica, pero esa señal de red les tiene que llegar vía cable (a menos que estén trabajando en modo repetidor).

La configuración recomendable es que el punto de acceso de cada planta esté unido vía cable al switch. A continuación se muestra un diagrama con la solución planteada:

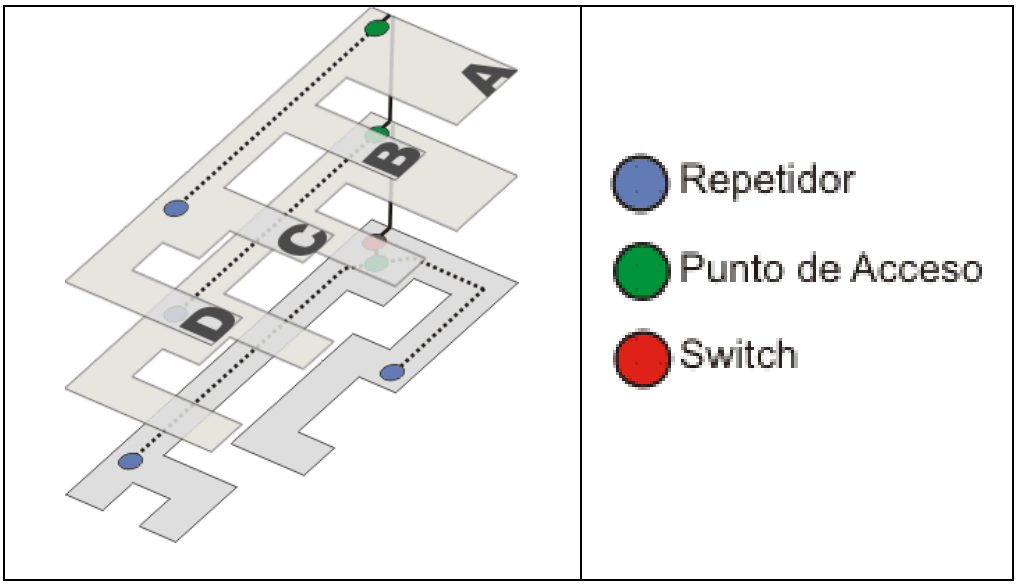


Figura 4.7: Diagrama de distribución de los AP´s en cada piso

En el gráfico de arriba se puede ver la distribución básica de los equipos, en la cual hay un switch en la planta baja del que salen n cables que van a parar a los Puntos de Acceso de cada Planta. Los AP de cada planta dan cobertura inalámbrica a la misma y se ven ayudados por repetidores en las áreas más alejadas.

Cada AP se conecta al switch a través de cable de red ethernet (categoría 5 o 6) con conector RJ-45, bajo los mismos criterios de redes LAN, es decir, el cable no debe pasar los 100 mts. de distancia que exige el estándar; debe estar configurado en modo Access Point y hay que activar la casilla de cliente DHCP para recibir una dirección IP automáticamente del servidor DHCP de la red. Si por alguna razón los requerimientos fueran tener más de un AP en modo AP por piso, lo que se debería hacer es poner un pequeño switch en cada planta, y conectar a él tantos puntos de acceso como se necesite.

Ambientes Exteriores (Outdoors)

La aproximación más habitual a la hora de distribuir Internet en un área extensa es el uso de los llamados "Nodos Centrales" y "Nodos de Distribución".

La idea consiste en que desde un lugar donde habitualmente se encuentra la conexión a Internet (no es necesario) se instala el "Nodo Central" (NC) cuya función consiste en hacer llegar la conexión en modo Bridge Punto-a-MultiPunto a diversos "Nodos de Distribución" (ND). Los ND, basados en sistemas de doble radio con control de abonados y ancho de banda recibirán desde su Radio A configurada en modo Bridge la conexión proveniente del NC y la repartirán a los abonados de los alrededores mediante la Radio B configurada en modo "Access Point" (AP).

Lo más común es que el nodo central esté equipado con antenas sectoriales, las antenas sectoriales tienen la eficacia de una antena direccional y a la vez cubren una extensa área (hasta 180º horizontalmente).

La Radio A del ND estará conectada a una antena direccional de bajo costo (solo necesita recibir la señal de un punto muy concreto). La Radio B del ND estará conectada a una antena omnidireccional de buena calidad y ganancia.

Los ND tiene muchas ventajas respecto a los clásicos repetidores, en primer lugar los repetidores suelen tener que aplicar una solución de compromiso en cuanto a la antena, ya que por un lado tienen que llegar al emisor central (conveniente utilizar una antena direccional) y a la vez servir a los usuarios distribuidos en los alrededores (conveniente antena omnidirecional). Lo que se gana por un lado se pierde por el otro, y la utilización de splitters (más de una antena por dispositivo) en equipos de una sola radio supone pérdidas y hace mas compleja la instalación. Otra desventaja muy importante del repetidor frente al ND es que el repetidor utiliza el mismo canal que el NC, es decir que hay que vigilar que no esté demasiado cerca ni del NC ni de otro repetidor de la misma red inalámbrica. En cambio un ND se puede situar donde se desee ya que emite en un canal seleccionable distinto al que le vincula al NC, de este modo, se puede dar incluso cobertura por capas, es

decir, que en un área un abonado reciba señal de dos ND y pueda seleccionar la que más calidad ofrezca.

Para el caso específico de la ESPE esta solución queda un poco grande ya que el área del campus es de aproximadamente 2 Km², la solución que se propone sería colocar una antena omnidireccional de 15 dbi en la terraza del edificio de la MED, ya que en dicho edificio se encuentra el cuarto principal de comunicaciones. De esta manera se estaría dando cobertura a todo el perímetro del campus sin ningún inconveniente.

La antena debe estar conectada al AP principal mediante cable coaxial y un pigtel; hay que considerar que mientras más grueso y rígido el cable coaxial hay menos atenuación pero es más costoso, a su vez el AP debe estar conectado a la red cableada mediante el switch que gestiona la red. Podría ser recomendable colocar el AP en el último piso del edificio para que esté mas cerca de la antena y de esta manera evitar las pérdidas antes mencionadas. A continuación se muestra una gráfica que resume todo lo mencionado anteriormente:

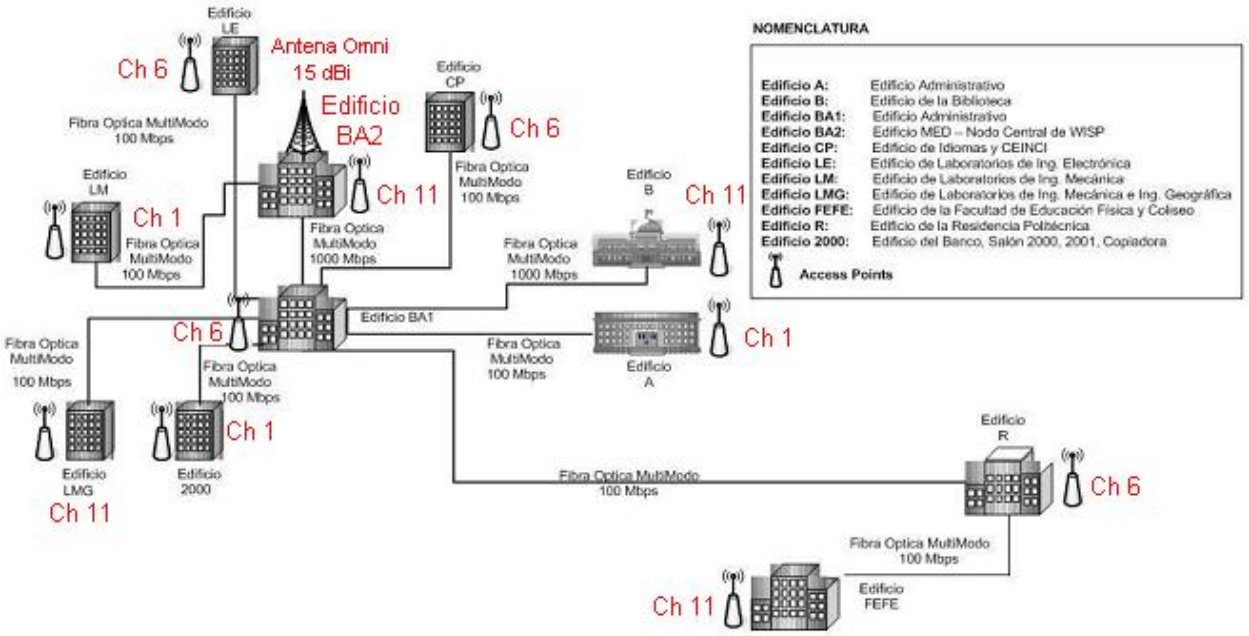


Figura 4.8: Esquema de cobertura del Nodo Wi-Fi – Campus ESPE Sangolquí

De esta manera estaría cubierta toda la parte física de la red inalámbrica faltando únicamente realizar la configuración del servidor RADIUS, los AP´s y los clientes.

4.5.2- Configuración del Servidor RADIUS (AAA)

Es importante aclarar la función de cada uno de los procesos que están involucrados dentro de un servidor RADIUS.

Autenticación.- Es el proceso de identificar una unidad (dispositivo o usuario) que desea tomar el servicio de una red basada en transacciones. La autenticación puede ser mutua y puede tomar lugar utilizando cualquiera de los varios protocolos de autenticación como EAP, TTLS o PEAP.

Autorización.- Es la habilitación del acceso a un recurso específico de la red, una vez que la unidad (dispositivo o usuario) ha sido autenticado. Por ejemplo, la autorización puede tomar lugar habilitando un puerto en el switch que dé acceso a servicios Web o bases de datos, etc.

Contabilidad.- Se refiere al seguimiento de la utilización de recursos de cada cliente; éstos datos pueden ser usados con propósitos de cargar valores, rendimiento u otras razones.

RADIUS (*Remote Authentication Dial-In User Service*) es un protocolo ampliamente utilizado que proporciona autenticación y autorización centralizadas para acceso a redes de todo tipo. Su funcionamiento detallado se describe en los RFC 2865 y 2866 del IETF [http://www.ietf.org/]. Aunque inicialmente se desarrolló para habilitar el acceso telefónico remoto (como su propio nombre indica) en la actualidad se usa para multitud de aplicaciones adicionales tales como servidores de redes privadas virtuales (VPN), acceso mediante ADSL, y por supuesto redes inalámbricas entre otras.

Una infraestructura RADIUS está formada básicamente por los clientes que requieren el acceso, los clientes RADIUS y los servidores RADIUS. En el caso que se

estudia el cliente RADIUS será un AP que actúa, en efecto, como cliente RADIUS desde el punto de vista de la red interna, pero actúa como servidor de acceso desde la perspectiva de los clientes inalámbricos. El servidor RADIUS concede o deniega el acceso de los clientes a la red interna utilizando para la autenticación y autorización la información contenida en un controlador de dominio. En el caso de la plataforma Windows, tanto Windows 2000 Server como Windows 2003 Server incluyen un servidor RADIUS que se conoce como Servicio de Autenticación de Internet o IAS (*Internet Authentication Service*).

En una solución Windows la configuración de un servidor RADIUS está compuesta por cuatro pasos que son:

1.- Instalación de una entidad certificadora (CA – Certification Authority).- La instalación de un CA es necesaria para la autentificación de los usuarios con el servicio RADIUS. Sobre todo cuando el protocolo de seguridad que se vaya a utilizar así lo requiera como es el caso de WPA (EAP-TLS) por ejemplo.

2.- Instalación y configuración de RADIUS.- Para la instalación del servidor RADIUS hay que instalar Internet Authentication Services (IAS) que deberá ser configurado con protocolo RADIUS.

3.- Configuración de los AP´s.- A los cuales hay que configurarlos indicando donde se encuentra el servidor RADIUS, es decir, asignándoles la dirección IP de dicho servidor. La configuración de los AP´s puede hacerse tanto desde un browser o por línea de comandos (CLI – Command Line Interface – Línea de Interfase de Comandos).

4.- Configuración de los clientes.- Los clientes deben configurarse con el mismo certificado que está alojado en el servidor IAS. Luego configurar el SSID y el protocolo de seguridad que debe ser el mismo que está configurado en el AP y en el servidor RADIUS.

Los pasos mencionados anteriormente corresponden a un resumen de una solución

netamente Windows muy segura y funcional; pero para el caso de estudio se realizó una pequeña aplicación en la cual se utilizaron los siguientes elementos:

- Un PC con Windows 2000 Profesional, hará las veces de servidor.
- Un Access Point Air Premiere D-Link de 2.4 Ghz.
- Un Hub 3Com de 8 puertos
- Una computadora portátil Toshiba Satellite A-40, con una tarjeta de red inalámbrica Atheros AR5001X.
- Un servidor RADIUS llamado WinRadius propietario de "ITCONSULT2000", del cual se puede bajar una versión gratis con funcionalidad para cinco usuarios en la dirección: http://itconsult2000.com.

La aplicación realizada incluye la configuración del servidor WinRadius, del Access Point y de los clientes.

Configuración del servidor WinRadius

1.- Instalar el servidor winRadius en el PC que va a alojarlo, en el caso del servidor WinRadius que se utilizó solo hay que descargar la versión gratis y ejecutarla en el computador.

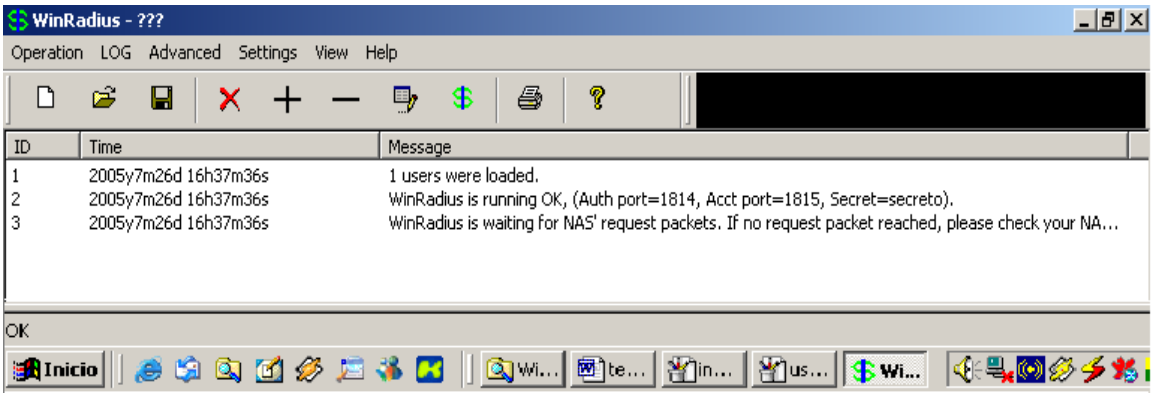


Figura 4.9: Servidor WinRadius en ejecución y a espera de solicitudes del NAS

Un término muy utilizado a la hora de hablar de servidores RADIUS es NAS. NAS (Network Attached Storage – Almacenamiento Agregado a la Red) es usado para describir

un sistema completo de almacenamiento, el cual está designado para estar agregado a la red de datos tradicional. En términos generales una NAS será el Access Point que envía peticiones al servidor RADIUS, cada vez que un cliente inalámbrico intente conectarse a la red.

2.- Configurar el servidor WinRadius, para ello hay que asignarle los puertos que van a ser utilizados para autenticación y cuentas; además hay que configurar una palabra clave o "secreto" que tendrá que estar tanto en el servidor RADIUS como en el NAS para que se puedan ver el uno al otro. Normalmente el puerto asignado por defecto para la autenticación es el puerto 1812 y para cuentas es el puerto 1813, pero por motivos de pruebas se utilizó el puerto 1814 y 1815 para autorización y cuentas.

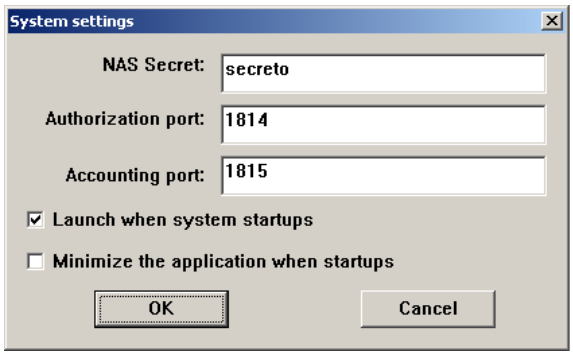


Figura 4.10: Configuración de puertos en servidor WinRadius

3.- Configurar la base de datos, este es un detalle muy importante en este tipo de soluciones porque es aquí donde se van a almacenar todos los datos de clientes y cuentas. Normalmente los servidores RADIUS tienen incorporada una base de datos por defecto con ciertas tablas y campos; se puede utilizar ésta u otra independiente que haya sido creada anteriormente de acuerdo a las necesidades y servicios que va a prestar el WISP. En el caso de WinRadius trae por defecto una base de datos realizada en Access, para

conectarla con el servidor WinRadius hay que generar un ODBC que gestione la conexión a la base.

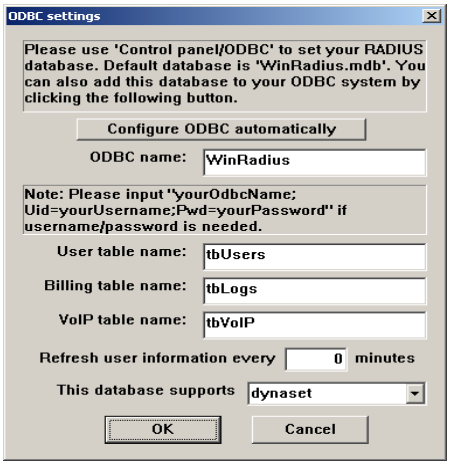


Figura 4.11: Conexión a la base desde WinRadius

Es importante acotar que WinRadius permite también trabajar con SQL Server, ORACLE y MySQL. La característica de tener soporte para varias bases de datos es muy común en la mayoría de servidores RADIUS existentes en el mercado. WinRadius tiene una herramienta muy útil que permite generar usuarios con sus respectivas claves, direcciones IP´s, montos y fechas de expiración.

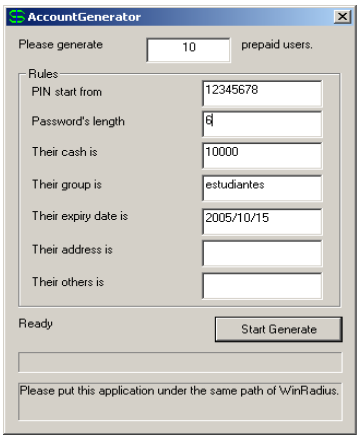


Figura 4.12: Generador de cuentas de WinRadius

Todos estos datos obtenidos automáticamente pasan a formar parte de la base de datos apenas son generados, y se pueden ver en pantalla a manera de búsquedas o reportes.

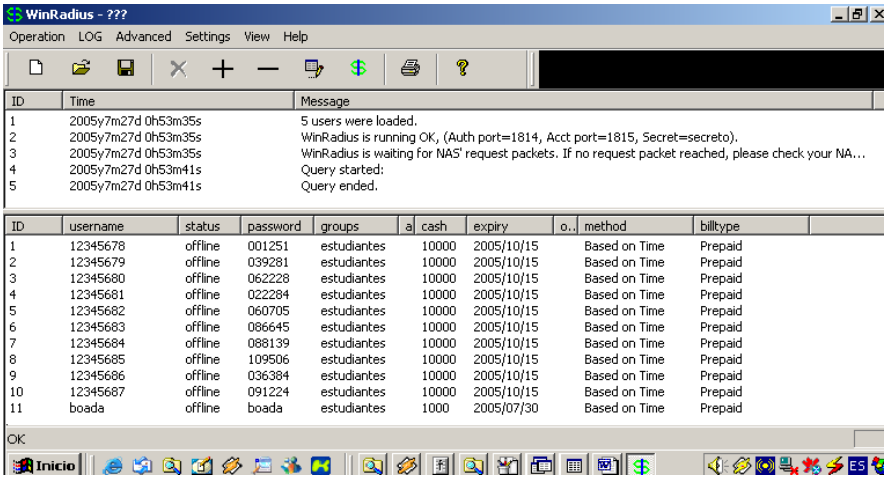


Figura 4.13: Pantalla de reporte de estatus de WinRadius y usuarios generados

4.- Luego hay que configurar la parte de autenticación de usuarios; para esto hay que determinar si los usuarios van a ser autorizados mediante su nombre de usuario y contraseña; ó, a través del identificador de la máquina que hace la solicitud denominado (Calling Station Id). Para esta aplicación se utilizó el nombre de usuario y contraseña como método de autenticación.

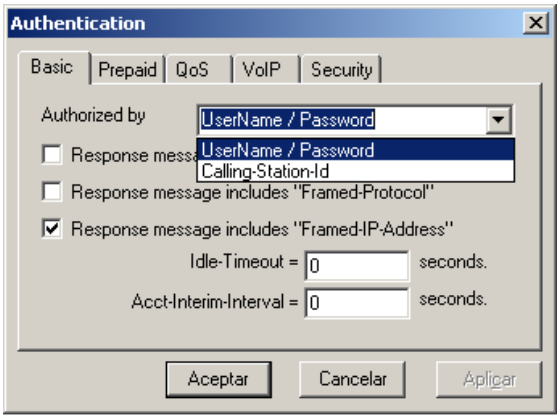


Figura 4.14: Autenticación de usuarios en WinRadius

5.- Por último hay que configurar la parte de cuentas, aquí se puede establecer si el débito del usuario será por el tiempo de consumo o por la cantidad de bytes transmitidos; así como también se podrá establecer los costos del minuto o de la cantidad de bytes.

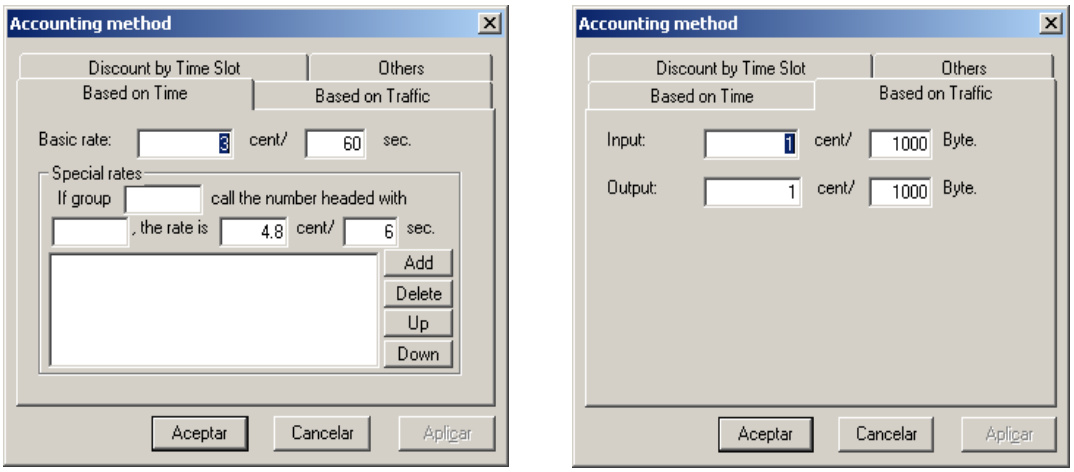


Figura 4.15: Configurando los parámetros de cuentas en WinRadius

Es importante comentar que el protocolo de seguridad que utiliza WinRadius es EAP-DM5, por ser esta una versión de prueba está configurado por defecto y no se lo puede cambiar. Todos los pasos descritos anteriormente, son un pequeño resumen de los aspectos más importantes que hay que tomar en cuenta a la hora de configurar un servidor RADIUS. También se recomienda que la dirección IP de la máquina que aloja al servidor RADIUS sea fija para evitar pérdidas en la conexión.

Configuración del Access Point

Para esta aplicación se utilizó un AP AirPremier 2.4 Ghz D-Link el cual tiene las siguientes características:

- Capacidad para 80 usuarios.
- Soporte para estándar 802.11b.
- Antena con 2.0 dB de ganancia.
- Tasa de transferencia de 1,2,5.5,11 Mbps y 22 Mbps en un modo turbo propietario.

- Potencia de salida del transmisor 15dBm + ó – 2dB.
- Rango de cobertura de 100 mts para interiores y 400 mts para exteriores.

1.- Para configurar el AP lo primero que hay que hacer es abrir un browser y digitar la dirección IP que viene por defecto que es 192.168.0.50. Luego de esto aparecerá la pantalla de ingreso de nombre de usuario que es "admin" y el password que hay que dejarlo en blanco. Estos valores se pueden cambiar más adelante.

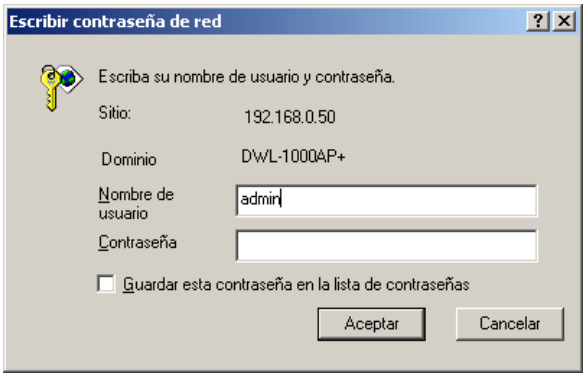


Figura 4.16: Ingreso de usuario y contraseña para configurar el AP

2.- Luego hay que configurar el secreto compartido que debe ser el mismo que se configuró anteriormente en el servidor WinRadius, e indicarle al AP la dirección IP de la máquina donde se encuentra alojado dicho servidor. Para esto se habilita 802.1X que es el protocolo que permitirá ingresar dicha información.

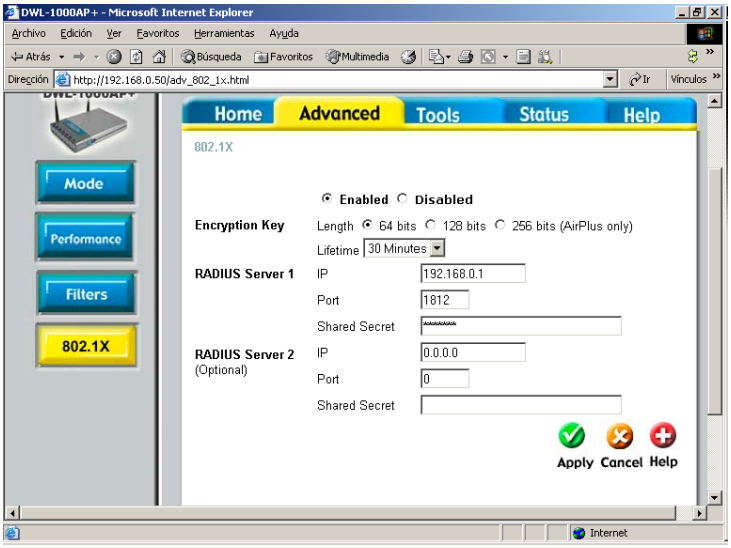


Figura 4.17: Pantalla de configuración de 802.1X

Se puede configurar un servidor RADIUS secundario bajo los mismos criterios, por si existiera algún problema con el principal, pero esto es opcional.

3.- El siguiente paso es configurar la parte wireless del AP. Aquí es recomendable cambiar el nombre por defecto del AP sobre todo por cuestiones de seguridad. Hay que asignar un nombre de SSID que para esta aplicación fue "campus_espe", escoger un canal en el cual va a trabajar el AP en este caso fue "6" y por último dejar deshabilitado el protocolo WEP. La encriptación WEP es utilizada cuando se trata de usuarios fijos como por ejemplo los que pertenecen a un empresa, para usuarios aleatorios y desconocidos que acceden a un HotSpot es recomendable dejar deshabilitada esta opción porque de lo contrario no podrían conectarse a la red.

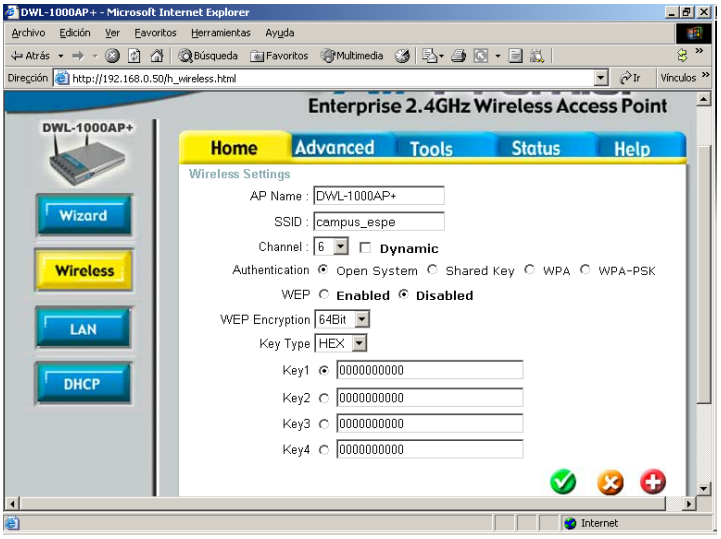


Figura 4.18: Pantalla de configuración de la parte wireless del AP

4.- Configurar DHCP, en esta aplicación se configuró el AP para que sea el servidor DHCP, en redes grandes esto ya debe estar previamente configurado en algún dispositivo que pertenece a la parte cableada de la red. Para configurar el servicio solo hay que habilitarlo e indicar el rango de IP´s que puede asignar. Una vez hecho esto aparecerán en pantalla todos los equipos que se vayan conectando a la red.

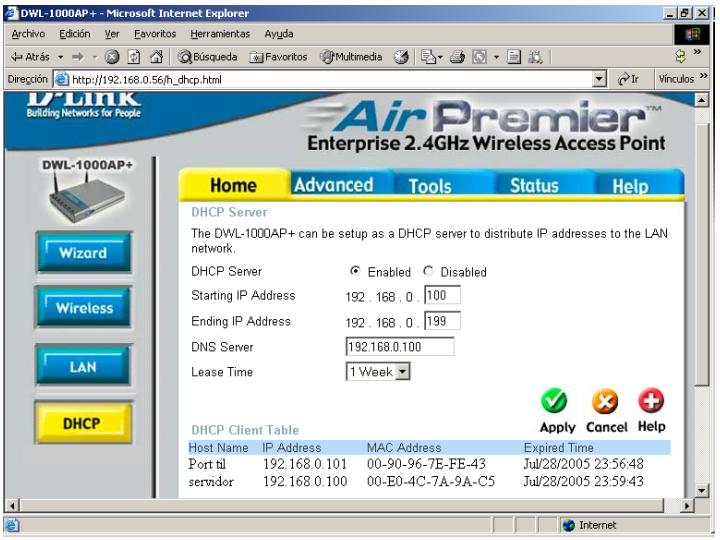


Figura 4.19: Servidor DHCP configurado en el AP

5.- Por último es muy importante configurar ciertos parámetros generales como lo son:

- Escoger que antena utilizar y con qué potencia.
- Los intervalos de tiempo con los cuales serán transmitidos los beacom frames.
- Un detalle muy importante es que se recomienda deshabilitar la opción SSID Broadcast. Con esto lo que se está haciendo es evitar por cuestiones de seguridad que sea enviado el nombre del SSID en cada emisión de los beacom frames.
- Con qué tasa de transferencia se desea hacer la conexión.

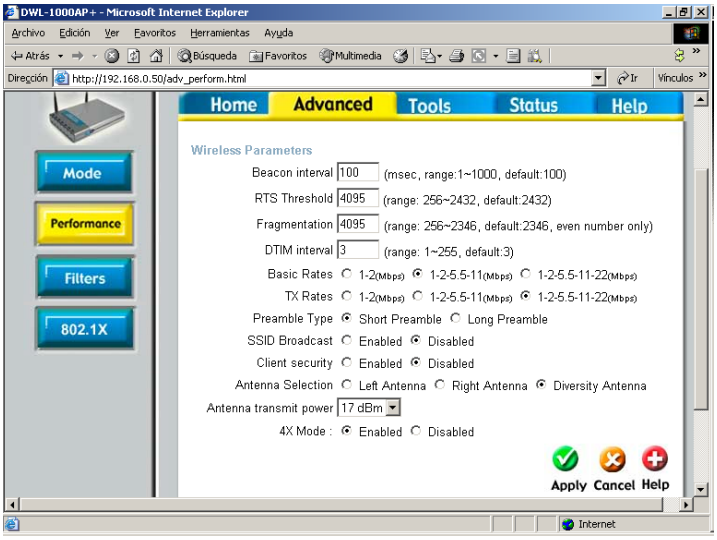


Figura 4.20: Pantalla de configuración de aspectos generales del AP

Existen muchos otros parámetros que se pueden configurar dependiendo de las necesidades de la red, pero los pasos descritos anteriormente son suficientes para poner en marcha la aplicación antes mencionada.

El momento en que está debidamente configurado el AP se puede acceder a través de él a todos los servicios de la red, en este caso se tiene una conexión compartida a Internet desde el servidor principal; es decir, que cuando un usuario inalámbrico se conecte y sea debidamente autenticado y autorizado a través del servidor RADIUS verificando su nombre, contraseña y saldo podrá navegar sin ningún inconveniente.

Configuración del cliente

La configuración del cliente es más sencilla por cuanto Windows se encarga de gestionar casi todo lo necesario para conectarse; es decir, detecta el SSID y normalmente trabaja en modo infraestructura, lo único que habría que considerar es deshabilitar la casilla de modo WEP por cuanto el AP y WinRadius se encargarán de las seguridades. El AP detectará la presencia del cliente inalámbrico y el servidor RADIUS inmediatamente solicitará permisos de ingreso a través de su nombre de usuario y contraseña. Si estos valores son incorrectos de acuerdo a los guardados en la base de datos entonces el cliente no podrá ingresar a la red. Lo ideal es evitar que el cliente tenga que configurar su dispositivo inalámbrico, por cuanto en muchos de los casos no tendrá los conocimientos necesarios para poder hacerlo.

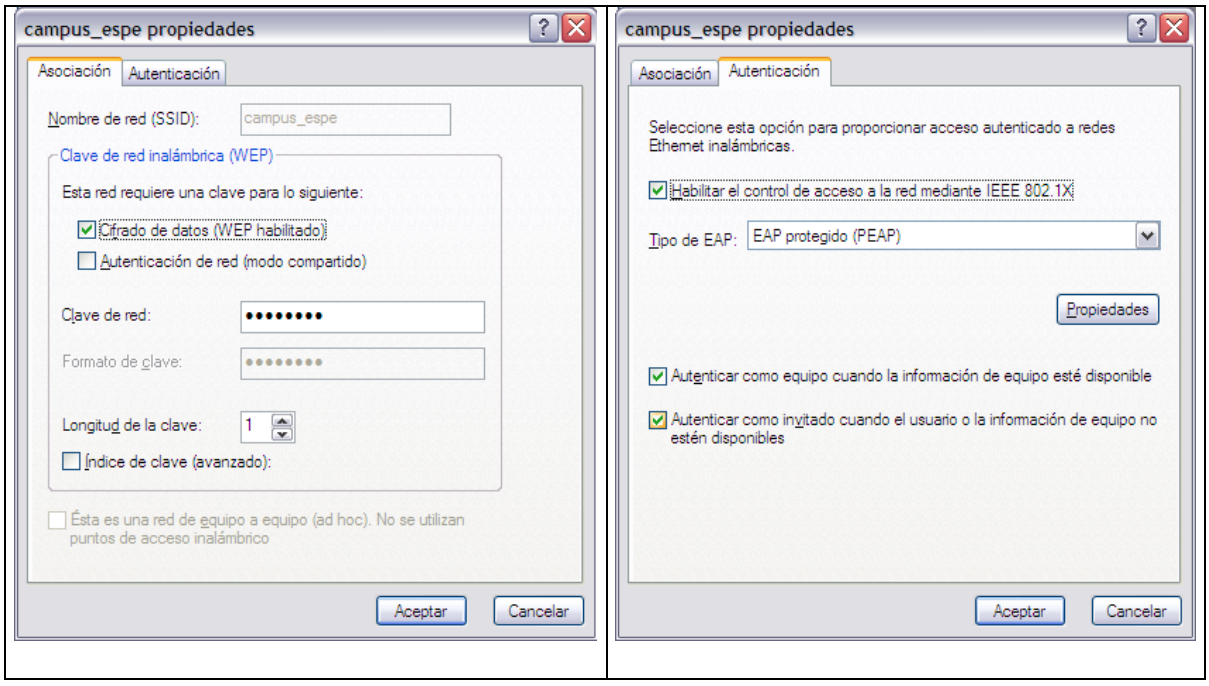


Figura 4.21: Pantallas de configuración WEP en el lado del cliente

4.5.3- Métodos de pago

A la hora de administrar un WISP se pueden considerar tres formas de pago definidas para el servicio que son:

Tarjeta prepago 24h.- Mediante la cual se podrá acceder a Internet desde cualquier parte del Hotspot por un período de 24h continuas desde la primera conexión realizada con la misma. Es decir, si el primer uso de la tarjeta se realiza a las 20:00:00 horas del 15 de Julio del 2005, se podrá navegar por Internet hasta las 19:59:59 horas del 16 de Julio del 2005.

Suscripción mensual de acceso con tarifa plana.- Con este tipo de tarjeta se podría navegar por Internet sin límite de tiempo ni de tráfico durante todo el mes.

Por tiempo de acceso.- Esta tarjeta permite el pago por uso del servicio de Internet en períodos de 10 min., es decir, cuando empiece a navegar se descontará el equivalente en dinero a un período de tiempo de 10 min. de la tarjeta. Transcurrido este tiempo, si se sigue navegando se descargarán nuevamente 10 min. de la tarjeta de manera transparente.

Estas opciones han sido tomadas de una solución planteada por Telefónica llamada "Zona ADSL Wi-Fi", para dar servicio de banda ancha a Internet a usuarios que dispongan de un dispositivo inalámbrico.

Vale la pena acotar que en la mayoría de los casos el WISP debe poseer un sitio Web donde se realizan todas las altas de los usuarios que utilizan el servicio.

Para el caso específico de la ESPE, ésta solución podría ser igualmente implementada; aunque quizás lo más conveniente sea el cobro directo en la matrícula de cada estudiante como un rubro de Internet inalámbrica ilimitada.

4.5.4- Consideraciones adicionales útiles para seguridad

Adicionalmente a todos los protocolos de seguridad descritos anteriormente es muy importante realizar la protección de la red de los clientes, para lo cual hay que implementar

una política de cortafuego (Firewall) estricta para garantizar que las 3 redes (Internet, red Corporativa y red de Servicio) queden protegidas de los posibles ataques internos o externos. Un cliente de la red de Servicio, solo puede salir a Internet con las restricciones definidas en el cortafuego. Ningún usuario de Internet puede acceder a un cliente de la red de Servicio si no está explícitamente definido por el administrador del sistema a través de una regla de redireccionamiento de puerto.

También la red Corporativa se queda protegida detrás del cortafuego y puede acceder a Internet de manera totalmente segura sin que le entre un cliente de la red de Servicio ni un usuario desde Internet. Con el aislamiento físico de esas 3 redes se tiene un sistema mucho más seguro y controlado.

Si se necesitara utilizar encriptación WEP lo único que hay que hacer es abrir la ventana de propiedades de redes inalámbricas y habilitar el cifrado mediante WEP, gracias al uso del servidor RADIUS, la clave de cifrado será proporcionada de manera automática. La otra pestaña, Autenticación, servirá para configurar el acceso mediante 802.1X y EAP. Hay que marcar la casilla correspondiente para habilitar este protocolo y en la lista de tipos de EAP disponibles hay que seleccionar EAP Protegido (PEAP). Por omisión se empleará PEAP-MS-CHAP v 2 que es el protocolo que está habilitado por defecto. Si se realiza esta configuración del lado del cliente debe haberse habilitado la encriptación WEP del lado del AP o servidor RADIUS dependiendo de las características de cada uno de ellos.

El mantenimiento de la seguridad e integridad de la red universitaria 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 por personas ajenas.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1- Conclusiones

- Al finalizar la investigación se logró implementar una guía técnica bastante útil y clara acerca de los pasos a seguir y las consideraciones a tomar a la hora de implementar un ISP inalámbrico.
- El mercado se muestra bastante interesado en estas nuevas tecnologías y dispuesto a invertir en ellas.
- Las redes de datos 8021.11b utilizan la banda de frecuencias ISM (2.4 Ghz – 5.8 Ghz), con una modulación CCK que permite llegar a 11 Mbps. Son interoperables y permiten una cómoda integración con las redes cableadas.
- Los estándares inalámbricos establecidos hasta el momento son muy claros y precisos en cuanto a lo que ambientes indoor se refiere; cuando se trata de ambientes outdoor no existe un estándar; es decir, dependiendo de la infraestructura que se monte se pueden alcanzar mayores o menores distancias.
- En la actualidad todavía las redes inalámbricas no son tan rápidas ni tan seguras como las redes cableadas, pero gracias a su rápido desarrollo y evolución son una excelente alternativa como solución de comunicaciones para cualquier entorno empresarial.
- Los estándares inalámbricos cuentan con varios protocolos de seguridad que si son administrados de forma adecuada, brindarán un alto grado de seguridad y estabilidad a la red.

- Los estudiantes de la Facultad de Sistemas de la ESPE, en aproximadamente un 60% están dispuestos y tienen los equipos necesarios para utilizar un servicio de Internet inalámbrica dentro del campus de la Universidad.
- Es un proyecto factible de realizar por cuanto en aproximadamente un año se podría recuperar la inversión, empezar a obtener utilidades por el servicio y estar a la par con la tecnología de punta.
- Las redes inalámbricas pueden interactuar perfectamente con las redes Ethernet, permitiendo de esta manera aprovechar las ventajas de las redes cableadas junto con la funcionalidad y movilidad de las redes sin cables.
- Distintos organismos (WECA, IEEE, ETSI, etc.) continúan trabajando en la búsqueda de soluciones para mejorar las limitaciones actuales de la tecnología inalámbrica. Su actividad garantiza que en los próximos años los aspectos de seguridad y "roaming" estarán plenamente resueltos desde la infraestructura de red.
- Las redes inalámbricas en primera instancia son mas costosas que las redes cableadas, pero debido a su barato mantenimiento y escalabilidad se convierten en soluciones más económicas que las redes Ethernet.

5.2- Recomendaciones

- Realizar un estudio previo del espectro para poder determinar de forma acertada, la infraestructura que se necesita para cumplir con los requerimientos planteados, evitando de esta manera pérdidas o desperdicios en cuanto a lo que equipamiento se refiere y permitiendo un control total del espectro.
- Tomar en cuenta todas las consideraciones necesarias de seguridad, mientras más seguridades se implementen y más precauciones se tomen, más difícil será que la red pueda ser violada.
- Investigar y acatar la legislación vigente en el país en el cual se pretende implementar una infraestructura de red inalámbrica, básicamente en lo que a soluciones outdoor se refiere ya que esto implica el uso de antenas de alta potencia y radios de largo alcance.
- No comprar equipos que pertenezcan a fabricantes que no tengan el sello de compatibilidad e interoperabilidad de la Wi-Fi Alliance, ya que esta es la única garantía que se tiene de que se pueden obtener los resultados establecidos por el estándar.
- Comparar precios y características de los equipos antes de comprarlos, un factor muy importante es el valor agregado que ofrece cada fabricante independientemente de la marca, parámetros como que los radios sean multibanda, manejen QoS, servidor DHCP, entre otros son factores muy importantes que se deben analizar para realizar la mejor compra.
- Cambiar los valores por defecto que están configurados en los AP, sobre todo lo que es nombre de usuario y clave de administrador, nombre del SSID y BroadCast de SSID. Esto ayudará a tener una red más segura y confiable.

- Incentivar la investigación de las redes inalámbricas en los estudiantes de la ESPE debido a su rápido crecimiento, importancia, funcionalidad e incursión en el mercado a nivel mundial. Se sugiere que en la Facultad de Sistemas se cree una materia optativa que cubra estos conceptos de tal manera que los estudiantes tengas ventajas competitivas en el mercado nacional o internacional.
- Comprar cables y conectores de la mejor calidad posible si se va a conectar antenas, esto va a garantizar que haya una menor pérdida de la señal y garantizará mayor tiempo de vida en los equipos.

BIBLIOGRAFÍA

Colegio Oficial de Ingenieros de Telecomunicación. La situación de las Tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes ("Wi-Fi"). Documento PDF

Telefónica. Guía del Usuario – Zona ADSL Wi-Fi. Documento PDF.

John Hammond, Bart Kessler, Greg Meyer, Juan Rivero ,Chad Skinner, Tim Sweeney. Wireless Hotspot Deployment Guide. Septiembre 2004. Documento PDF.

B. Anton – Gemtek Systems, Inc., B. Bullock – iPass, Inc.. J. Short – Nomadix, Inc. Wi-Fi Alliance – Wireless ISP Roaming (WISPr). Febrero 2003. Documento PDF.

http://www.coit.es

http://www.wi-fi.org/

http://canariaswireless.net

http://www.20minutos.es/barcelona/?noti=576

http://www.acri.ws/Wi-Fi.cfm

http://www.idg.es

http://www.infoguia.net/foros/index.php/act/ST/f/233/t/34967/view/getlastpost?act=ST&f=233&t=34967&st=0&

http://www.gvsoft.com

http://www.mipcdebolsillo.com/reportajes/com/iniciacion_Wi-Fi.php

http://www.monografias.com

http://www.wi-fi.org

http://www.wirelessmundi.com/Dealer_01.shtml

http://www.supertel.gov.ec

http://www.34telecom.com/box-docs.asp?area=76&suba=08&doc=716

http://www.monografiass.com/monografiass/EpZEppulVEYWGIEotS.php

http://www.d-link.com

http://www1.euro.dell.com/content/topics/global.aspx/solutions/truemobile?c=es&l=es&s=gen&~page=4&~tab=2

http://www.34t.com/box-docs.asp?doc=720

http://www.monografias.com/trabajos16/wimax/wimax.shtml

http://www.monografiass.com/monografiass/EpZEppulVEYWGIEotS.php

http://www.wifind.com.ar

http://www.intel.com

http://www.microsoft.com/latam/technet/articulos/wireless/pgch05.mspx

http://www.microsoft.com/latam/technet/articulos/wireless/pgch06.mspx

http://www.microsoft.com/latam/technet/articulos/wireless/bgch08.mspx

http://www.microsoft.com/latam/technet/articulos/wireless/ogch12.mspx

http://www.windowstimag.com/atrasados/2003/79_sep03/articulos/seguridad_3.asp

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx

http://www.itconsult2000.com

http://firstwave.ch/grundlagen/outdoor_anwendungen.es.html

http://www.chilewireless.cl/modules/sections/index.php?op=viewarticle&artid=6

ANEXOS

ANEXO A

Nomenclatura

ACL:	Listas de Control de Acceso
AES:	Advanced Encriptation Standard - Estándar Avanzado de Encriptación
AP:	Access Point – Punto de Acceso
ATM:	Asynchronous Transfer Mode – Modo de Transferencia Asincrónico
BSS:	Basic Service Set - Grupo de Servicio Básico
ESS:	Extended Service Set - BSS Extendido
CCK:	Complementary Code Keying – Código de Llaves Complementarias
CLI	Command Line Interface – Línea de Interface de Comandos
COR:	Central Office Router – Router de Oficina Central
CPE:	Customer Premise Equipment ó Tarjeta de acceso a la red inalámbrica
CSMA/CA:	Carrier Sense Multiple Access / Collision Avoidance – Sentido Portador de Múltiple Acceso / Evitar Colisión
DECT:	Digital Enhanced Cordless Telecommunications – Telecomunicaciones Digitales Realizadas sin Cordones
DRS:	Dynamic Rate Shifting – Cambio de Transferencia Dinámico
DS:	Distribution System - Sistema de Distribución
DSSS:	Direct Sequence Spread Spectrum – Propagación de Espectro por Secuencia Directa
EAP:	Extensible Address Protocol - Protocolo Extensible de Dirección
ETSI:	European Telecommunications Standards Institute – Instituto de Estándares Europeo de Telecomunicaciones
FCC:	Federal Communications Comisión – Comisión Federal de Comunicaciones de Estados Unidos
FHSS:	Frequency Hopped Spread Spectrum – Propagación de Espectro por Salto de Frecuencia
GATEWAY:	Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas
GSM:	Global System for Mobile Communications – Sistema Global para Comunicaciones Móviles
Home RF:	Home Radio Frecuency - Radio Frecuencia para el Hogar
HotSpot:	Lugar público donde está disponible una conexión inalámbrica de red
HPBW:	Half Power Beam Width – Ancho del haz a mitad de Potencia
IBSS:	Independent BSS - BSS Independiente
IEEE:	Institute of Electrical and Electronics Engineers – Instituto de Ingenieros Eléctricos y Electrónicos
ISM:	Industry, Scientific and Medical – Industrial Científica y Médica
MAC:	Médium Access Control – Control de Acceso al Medio
MD5:	Message Digest 5 - Resumen de Mensaje 5
NAS:	Network Attached Storage – Almacenamiento Agregado a la Red
NIC:	Network Interface Card – Tarjeta de Interfase de Red
LEAP:	Lightweight EAP - EAP Ligero
LoS:	Line of Sight - Línea de Vista
OFDM:	Ortogonal Frequency Division Multiplexing – Multiplexación Ortogonal por División de Frecuencia
PC Card Radio:	Tarjeta Inalámbrica para equipo portátil

PDA:	Personal Digital Assistants – Asistente personal digital
PEAP:	Protected EAP - EAP Protegido
PoE:	Power over Ethernet - Energía sobre Ethernet
PWLAN:	Public Wireless LAN – Redes LAN Públicas Inalámbricas
QoS:	Quality of Service – Calidad de Servicio
RADIUS:	Remote Authenticated Dial-In User Service – Servicio de autenticación remota por discado
ROR:	Remote Office Router – Router de Oficina Remoto
ROUTER:	Dispositivo que transmite paquetes de datos a través de una red
RSN:	Robust Security Network – Red de Seguridad Robusta
SOHO:	Small Office Home Office – Pequeña Oficina Pequeño Hogar
SSID:	Service Set ID - Identificador de conjunto de servicios
SUPERTEL:	Superintendencia de Telecomunicaciones
SWAP:	Shared Wireless Access Protocol – Protocolo de Acceso Inalámbrico Compartido
TIC:	Tecnologías de la Información y las Comunicaciones
TKIP:	Temorary Key Integrity Protocol - Protocolo de Integridad Temporal de Claves
TLS:	Transport Level Security - Nivel de Seguridad de Transporte
TTLS:	Tunneled TLS - Túnelado TLS
UMTS:	Universal Mobile Telecommunications System – Sistema Universal de Telecomunicaciones Móviles
VPN:	Virtual Private Network - Red Privada Virtual
WC:	Wireless Client – Cliente Inalámbrico
WECA:	Wireless Ethernet Compatibility Alliance
WEP:	Wired Equivalent Privacy - Privacidad Equivalente Cableada
Wi-Fi:	Wireless Fidelity – Fidelidad Inalámbrica
Wi-Fi Alliance:	Alianza Wi-Fi
WiMAX:	Worldwide Interoperability for Microwave Access – Interoperabilidad a lo Largo del Mundo para el Acceso Microonda
WISP:	Wireless Internet Service Provider – Proveedor de Servicios de Internet Inalámbrica
WLAN:	Red de área local inalámbrica
WPA:	Wi-Fi Protected Access - Acceso Protegido Wi-Fi
WPA2:	Wi-Fi Protected Access 2 - Acceso Protegido 2 Wi-Fi
WPAN:	Red de área personal inalámbrica

ANEXO B

Encuesta

Objetivo: Determinar las necesidades de los usuarios con respecto al uso de la tecnología inalámbrica que utiliza nodos Wi-Fi como alternativa para el acceso a Internet.

Instrucciones

Por favor responda a las preguntas planteadas en el siguiente cuestionario con la respuesta que más se aproxime a su realidad marcándolas con una (x).
Al llenar este cuestionario, usted contribuirá con el avance del proyecto de tesis: "Análisis y diseño para implementar un ISP inalámbrico utilizando un nodo Wi-Fi", de un egresado de la ESPE.

INTERNET

1. ¿Utiliza ud. Internet?	□ Siempre □ Frecuentemente □ Ocasionalmente □ Nunca
2. ¿Su cuenta de Internet es: ?	□ Ilimitada □ Por horas durante el día □ Por horas durante la noche □ Prepago □ Desconoce □ Otros (Especifique): _____ _____
3.- ¿Cuántas horas de Internet consume ud. diariamente?	□ Entre 0 y 2 horas □ Entre 2 y 4 horas □ Entre 4 y 6 horas □ Entre 6 y 10 horas □ Más de 10 horas
4. ¿Cómo considera ud. los costos de acceso a Internet en la ciudad de Quito?	□ Extremadamente costosos □ Costosos □ Normales □ Baratos □ Desconoce
5. ¿Qué tipo de tecnología utiliza su conexión a Internet?	□ Dial Up □ Banda Ancha □ Línea dedicada □ Desconoce □ Otros (Especifique): _____ _____
6. ¿Para qué utiliza Internet?	□ Enviar/recibir e-mail □ Navegación en el Web □ Recibir información □ Por trabajo netamente □ Ocio y entretenimiento □ Otros (Especifique): _____ _____
7. ¿Desde dónde accede a Internet?	□ Lugar de trabajo □ Lugar de estudio

	□ Casa □ Café net □ Dispositivo móvil o inalámbrico
8. ¿Cuánto paga ud. mensualmente por un servicio de acceso a Internet?	□ Menos de 20 usd. □ Entre 20 y 40 usd. □ Entre 40 y 60 usd. □ Más de 60 usd □ Desconoce

ACCESO Y TECNOLOGÍA INALÁMBRICA

9. ¿Le gustaría tener un acceso inalámbrico a Internet cuando se encuentra en un lugar como: ?	□ Aeropuerto □ Lugar de trabajo □ Universidad □ Hotel
10. ¿Dispone ud. de algún dispositivo con tecnología inalámbrica como: ?	□ Laptop □ PDA (Asistente personal digital) □ Palm □ Pc Pocket □ Ninguno de los anteriores □ Otros (Especifique): _____ _____
11. ¿Cómo calificaría ud., el hecho de disponer en la ESPE de un acceso inalámbrico a Internet para su uso cotidiano?	□ Muy beneficioso □ Beneficioso □ Ligeramente beneficioso □ No es beneficioso □ No opina
12. ¿Estaría dispuesto a contratar un servicio inalámbrico de acceso a Internet?	□ Si □ No
13. ¿Conoce ud. de alguna empresa o proveedor de servicios de Internet que proporcione acceso inalámbrico a Internet?	□ Si □ No Empresa(s): _____ _____
14. ¿Por qué razón ud. decidiría adquirir un servicio de acceso inalámbrico a Internet?	□ Por movilidad □ Por velocidad de acceso □ Por andar a la par con la tecnología □ Por librarse de utilizar cables □ Otros (Especifique): _____ _____

_____

14. ¿Por qué razón ud. decidiría adquirir un servicio de acceso inalámbrico a Internet?	□ Por movilidad □ Por velocidad de acceso □ Por andar a la par con la tecnología □ Por librarse de utilizar cables □ Otros (Especifique): _____ _____

Wi-Fi

15. ¿Ha leído o escuchado acerca de la tecnología Wi-Fi?	□ Si □ No
16. ¿Sus conocimientos acerca de la	□ Experto

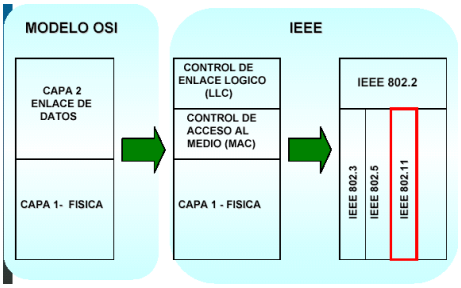
tecnología Wi-Fi, están en un nivel: ?	□ Intermedio □ Básico □ Nada
 *Wi-Fi o Wíreless Fidelity, es una tecnología que permite a empresas y particulares entrar al mundo de las conexiones de Internet inalámbricas de alta velocidad.* 17. ¿La conceptualización de Wi-Fi, le parece: ?	□ Extremadamente interesante □ Muy interesante □ Interesante □ No muy interesante □ Nada interesante
Los costos aproximados de tarjetas prepagadas mensuales para acceso inalámbrico a Internet serían: 1hr. → 4,00 usd 2hr. → 7,00 usd 4hr. → 12,00 usd Ilimitado → 50 usd 18. ¿Considera ud. que estos costos son: ?	□ Extremadamente caros □ Caros □ Justos □ Baratos □ Extremadamente baratos

Muchas gracias por su tiempo.

ANEXO C

Modelo OSI

El estándar IEEE 802.11 en su edición de 1999 define a la capa física (PHY – Physical Layer) y la capa de control de acceso al medio (MAC – Médium Access Control) para las WLAN's. Define capas físicas PHY para tasas de transmisión de 1 y 2 Mbps en la banda de radiofrecuencia (RF) sin licencia de 2.4 GHz y en la infrarroja (IR). El estándar 802.11 es un miembro de la familia de los estándares 802 emitidos por la IEEE que incluye el 802.3 (Ethernet) y 802.5 (Token ring). Se amplió dos veces en, 1999 por el 802.11a, que definía la PHY para la banda de 5 GHz a velocidades de 6 hasta 54 Mbps, y 802.11b, que definió la PHY para la banda de 2.4 GHz a 5.5 GHz y 11 Mbps.



Esquema de referencia del modelo OSI aplicado a WLAN según IEEE

La Capa Física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos, se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse. Los dos métodos para remplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

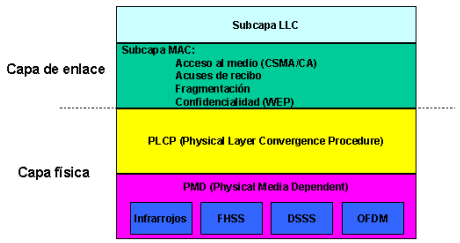
Capa Física (PHY)

La capa física (Physical Layer) de los estándares IEEE 802.11 se diseñó para cumplir con la regulación de radio frecuencia del FCC (Organismo Federal USA). Las mismas bandas de frecuencia, con algunas variantes, se utilizan en el resto del mundo. Los

canales (de 22 MHz cada uno) utilizados por 802.11b son los impares (canales 1,3,5,7,9,11 y13).

La capa física de servicios consiste en dos protocolos:

- Una función de convergencia de capa física, que adapta las capacidades del sistema físico dependiente del medio (PMD). Esta función es implementada por el protocolo PLCP o procedimiento de convergencia de capa física, que define una forma de mapear MPDUs o unidades de datos MAC en un formato de tramas susceptibles de ser transmitidas o recibidas entre diferentes estaciones a través de la capa PMD.
- Un sistema PMD, cuya función define las características y un medio de transmitir y recibir a través de un medio sin cables entre dos o más estaciones.



Esquema de las subcapas físicas PMD y PLCP

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos. En la capa física, se definen dos métodos de transmisión RF y un infrarrojo. El funcionamiento de la WLAN en bandas RF ilícitas, requiere la modulación en banda ancha para reunir los requisitos del funcionamiento en la mayoría de los países. Los estándares de transmisión RF son:

- La Frecuencia de Saltos (FHSS : Frecuency Hopping Spread Spectrum)
- La Secuencia Directa (DSSS : Direct Sequense Spread Spectrum).

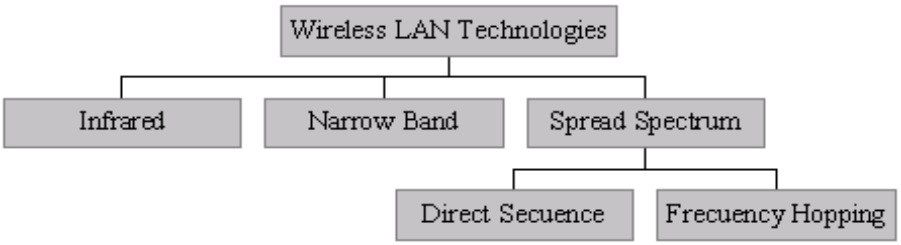
Ambas arquitecturas se definen para operar en la banda de frecuencia de 2.4 GHz, ocupando típicamente los 83,5 MHz de ancho de banda desde los 2.400 GHz hasta 2.483 GHz.

El método de transmisión por infrarrojos utiliza altísimas frecuencias para transportar los datos y es muy poco ocupada en aplicaciones comerciales de WLAN. Tienen un gran inconveniente, y es que al igual que la luz, los infrarrojos no pueden traspasar los objetos opacos. Por lo que emisor y receptor deben tener visión directa. Por lo que habitualmente permiten unas distancias muy pequeñas (máximas típicas de 90 cm. a 1 metro). Por lo que su funcionalidad se ve reducida drásticamente, siendo invisibles para usuarios móviles. Se suelen utilizar para montar alguna subred inalámbrica pero fija.

Método de Canalización

Como se mencionó anteriormente los dos métodos para remplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

Técnicas de Canalización Wireless



Los sistemas por infrarrojos, según el ángulo de apertura con que se emite la información, pueden clasificarse en:

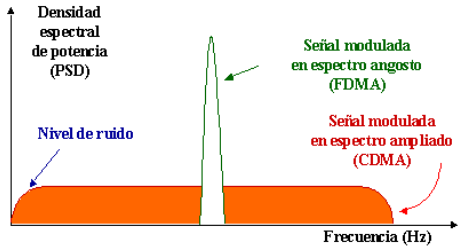
- ***Sistemas de corta apertura***, también denominados de rayo dirigido o de línea de visión (LOS, line of sight).
- ***Sistemas de gran apertura***, también denominados reflejados o difusos.

Por otra parte, las comunicaciones inalámbricas que utilizan radiofrecuencia pueden clasificarse en:

- ***Sistemas de banda estrecha (narrow band) o de frecuencia dedicada***. Este tipo trabaja de una forma similar a las ondas de una estación de radio. Esta señal puede atravesar paredes por lo que puede alcanzar una red bastante amplia, sin embargo

tienen problemas con las reflexiones que sufren las ondas de radio, para establecer esto hay que evitar las posibles interferencias.

- ***Sistemas basados en espectro disperso o extendido (spread spectrum)***. La FCC (Comisión Federal de Comunicaciones) a partir de 1985 permitió la operación sin licencia de dispositivos que utilicen 1 watio de energía o menos, en tres bandas de frecuencias: 902 a 928 MHz, 2.400 a 2.483,5 MHz y 5.725 a 5.850 MHz.



Esquema de Spread Spectrum vs. Banda Angosta

Espectro extendido (Spread Spectrum)

La gran mayoría de los sistemas inalámbricos, emplean la tecnología de Espectro Extendido (Spread Spectrum), una tecnología de banda amplia desarrollada por los militares estadounidenses, que provee comunicaciones seguras, confiables y de misión critica. La tecnología de Espectro Extendido está diseñada para intercambiar eficiencia en ancho de banda por confiabilidad, integridad y seguridad. Es decir, más ancho de banda es consumida con respecto al caso de la transmisión en banda angosta, pero el 'trueque' [ancho de banda/potencia] produce una señal que es en efecto más fuerte y así más fácil de detectar por el receptor que conoce los parámetros de la señal de espectro extendido que está siendo difundida. Si el receptor no está sintonizado a la frecuencia correcta, una señal de espectro extendido se miraría como ruido en el fondo. Otra característica del espectro disperso, es la reducción de interferencia entre la señal procesada y otras señales no esenciales o ajenas al sistema de comunicación.

Conviene tener presente que existen equipos que utilizan estas mismas frecuencias y que producen una energía de radiofrecuencia, pero que no transmiten información. Estos

equipos tienen aplicaciones Industriales, Científicas y Médicas (ICM) y en particular dichos equipos operan en otras bandas de frecuencia [902-908 MHz; 2,400-2,500 MHz y 5,525-5,875 MHz]. Ejemplos de estos equipos son: limpiadores domésticos de joyería, humidificadores ultrasónicos, calefacción industrial, hornos de microondas, etc.

Existen dos tipos de modulación de Espectro Extendido:

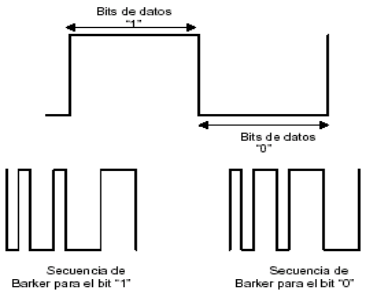
- Direct Sequence Spread Spectrum (DSSS)
- Frequency Hopped Spread Spectrum (FHSS)

Espectro extendido en secuencia directa (DSSS)

Esta técnica consiste en la generación de un patrón de bits redundante llamado *señal de chip* para cada uno de los bits que componen la señal de información y la posterior modulación de la señal resultante mediante una portadora de RF. En recepción es necesario realizar el proceso inverso para obtener la señal de información original.

Si uno o más bits son dañados durante la transmisión, técnicas estadísticas embebidas dentro del radio transmisor, podrán recuperar la señal original sin necesidad de retransmisión. DSSS se utilizará comúnmente en aplicaciones punto a punto.

La secuencia de bits utilizada para modular cada uno de los bits de información es la llamada secuencia de Barker y tiene la siguiente forma:



Secuencia de Barker

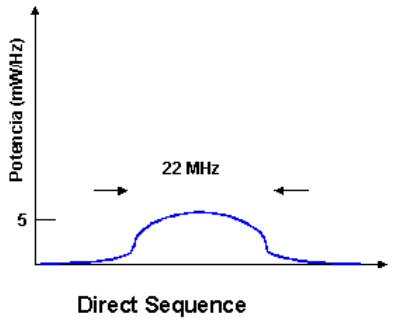
En la figura anterior se muestra el aspecto de una señal de dos bits a la cual se le ha aplicado la secuencia de Barker. DSSS tiene definidos tres tipos de modulaciones a aplicar

a la señal de información una vez se sobrepone la señal de *chip* tal y como especifica el estándar IEEE 802.11:

- La modulación DBPSK, Differential Binary Phase Shift Keying que proporciona una tasa de transferencia de 1 Mbps.
- La modulación DQPSK, Differential Quadrature Phase Shift Keying que proporciona una tasa de transferencia de 2 Mbps.
- La modulación CCK (Complementary Code Keying) que consiste en un conjunto de 64 palabras código de 8 bits proporcionando velocidades de transferencia de 5,5 y 11 Mbps.

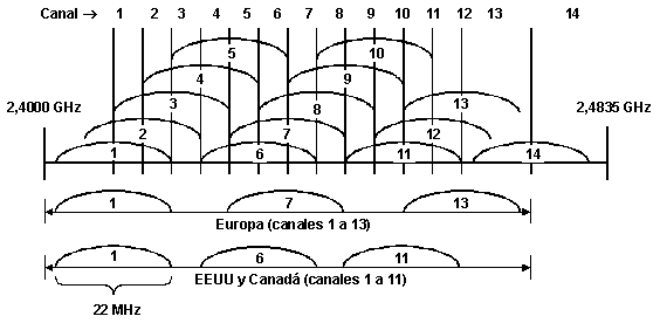
El estándar 802.11b estandariza el soporte a nivel físico de 5,5 y 11 Mbps. Para ello, DSSS fue seleccionada como la única técnica de nivel físico para evitar problemas regulatorios. Por tanto, 802.11b sólo interopera con los sistemas 802.11 basados en DSSS, pero no con los que trabajan en FHSS. La norma 802.11 original recoge ambas opciones.

La técnica de modulación sigue siendo la misma de 802.11 para 2 Mbps, QPSK (Quadrature Phase Shift Keying). Para soportar entornos con niveles de ruido elevados, así como distancias amplias, 802.11b utiliza Dynamic Rate Shifting, que permite que las velocidades se ajusten automáticamente a fin de compensar la naturaleza cambiante de los canales de radio.



En el caso de Estados Unidos y de Europa la tecnología de espectro ensanchado por secuencia directa, DSSS, opera en el rango que va desde los 2.4 GHz hasta los 2.4835 GHz, es decir, con un ancho de banda total disponible de 83.5 MHz. Este ancho de banda

total se divide en un total de 11 canales con un ancho de banda por canal de 22 MHz de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular.



Esquema de DSSS para EEUU y Europa

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema si la separación entre las frecuencias centrales es como mínimo de 30 MHz.

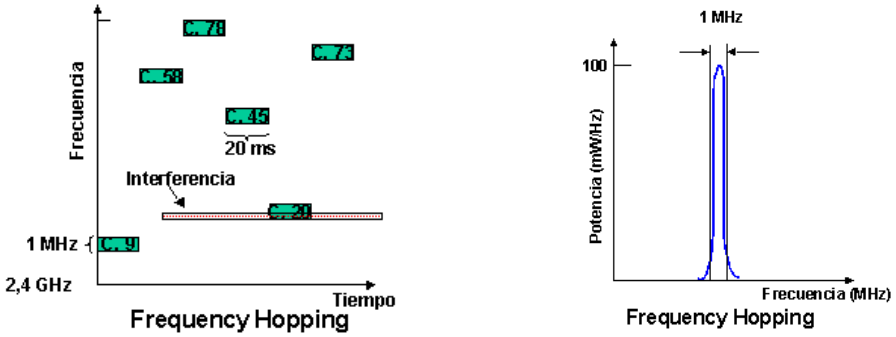
La banda de 5 GHz (IEEE 802.11a) permite la utilización de hasta ocho (8) Puntos de Acceso coexistiendo en la misma celda. La utilización de dispositivos de banda dual 802.11a + 802.11b permitiría la instalación de hasta once (11) Puntos de Acceso en la misma celda sin solape de frecuencia.

El dimensionado del número de Puntos de Acceso de una red debe garantizar el tráfico en el área considerada pero también la cobertura radioeléctrica. En muchas ocasiones la presencia de obstáculos obliga al despliegue de entornos multicelda para garantizar la cobertura del área deseada.

Espectro extendido con salto de frecuencia (FHSS)

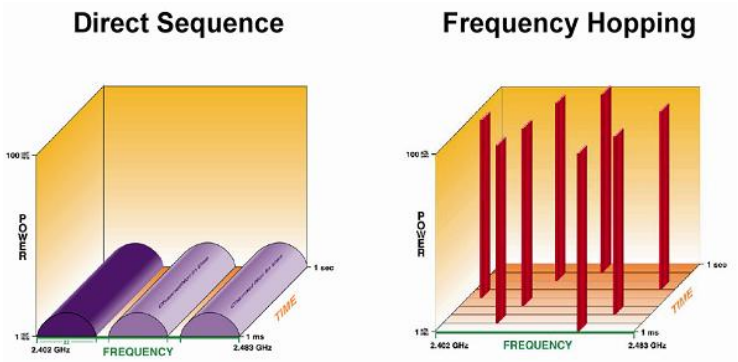
FHSS consiste básicamente, en utilizar una portadora de radio que no es fija en el tiempo, es decir el sistema cambia de forma seudo-aleatoria de portadora bajo una secuencia conocida por el emisor y el receptor. Igualmente, este sistema de transmisión expande el espectro de la señal en banda base y es, en cierta medida, muy resistente frente a interferencias.

FHSS es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto, donde se tiene menor ancho de banda y una cantidad de receptores (hasta 15 dispositivos) diseminados en un área relativamente cercana al punto de acceso.



La capa física Frecuencia de Saltos se exige para saltar por la banda ISM 5.8GHz cubriendo 79 canales. Cada canal ocupa un ancho de banda de 1Mhz y debe brincar a la tasa mínima especificada por los cuerpos reguladores del país pretendido. Los saltos consecutivos están separados 6 Mhz y tienen tres sets de secuencias donde cada set tiene 26 secuencias.

Cada una de las capas físicas utiliza su propio encabezado único para sincronizar al receptor y determinar el formato de la señal de modulación y la longitud del paquete de datos. Los encabezamientos de las capas físicas siempre se transmiten a 1Mbps. Los campos predefinidos en los títulos proporcionan la opción para aumentar la tasa de datos a 2 Mbps para el paquete de los datos existente.



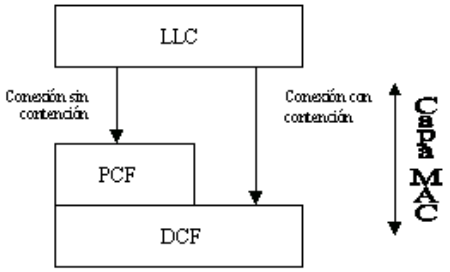
Esquema Direct Secuence Vs. Frecuency Hopping en 3D

Capa de enlace de datos (MAC)

Los diferentes métodos de acceso de IEEE 802 están diseñados según el modelo OSI y se encuentran ubicados en el nivel físico y en la parte inferior del nivel de enlace o subnivel MAC. Además, la capa de gestión MAC controlará aspectos tales como las funciones de entrega segura de datos con la reserva del canal (por ser este un medio compartido), se encarga de la privacidad de los datos transmitidos, sincronización y los algoritmos del sistema de distribución, que se define como el conjunto de servicios que precisa o propone el modo infraestructura.

La arquitectura MAC del estándar 802.11 se compone de dos funcionalidades Básicas que son:

- La Función de Coordinación Distribuida (DFC), que gestiona el acceso al medio mediante un proceso de contención (acceso contienda).
- La Función de Coordinación Puntual (PCF), que gestiona el acceso al medio mediante un proceso centralizado en el AP.



Esquema de la subcapa MAC según la IEEE

DCF (Distributed Coordination Function)

El tráfico que se transmite bajo esta funcionalidad, es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles no tolerados por los servicios síncronos.

Las características de DFC se las puede resumir en los siguientes puntos:

- Utiliza MACA (CSMA/CA con RTS/CTS) como protocolo de acceso al medio.

- Necesario reconocimientos ACKs (ACKnowledged), provocando retransmisiones si no se recibe.
- Usa campo Duration/ID que contiene el tiempo de reserva para transmisión y ACK. Esto quiere decir que todos los nodos conocerán al escuchar cuando el canal volverá a quedar libre.
- Implementa fragmentación de datos.
- Concede prioridad a tramas mediante el espaciado entre tramas (IFS).
- Soporta Broadcast y Multicast sin ACKs.

PCF (Point Coordination Function)

Por encima de la funcionalidad DCF se sitúa la función de coordinación puntual, PCF, asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas. El estándar IEEE 802.11, define una técnica de testeo circular desde el punto de acceso para este nivel. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio. Los métodos de acceso PCF y DCF pueden operar conjuntamente dentro de una misma celda o conjunto básico de servicios dentro de una estructura llamada supertrama. Una parte de esta supertrama se asigna al periodo de contienda permitiendo al subconjunto de estaciones que lo requieran transmitir bajo mecanismos aleatorios. Una vez finalizado este periodo el punto de acceso toma el medio y se inicia un periodo libre de contienda en el que pueden transmitir el resto de estaciones de la celda que utilizan técnicas deterministas.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

En las redes inalámbricas, no es posible escuchar el canal y transmitir la información de manera simultanea, por lo que no es posible percatarse de la existencia de colisiones, pudiendo entonces saturar al receptor de la información. Esto obliga a buscar mecanismos explícitos que lo eviten, así como a minimizare al máximo el número de

colisiones existentes. CSMA/CA (Carrier Sense Multiple Access/Collision Advoidance) es el algoritmo básico de acceso de las WLAN IEEE. Es muy similar al implementado en el estándar IEEE 802.3. El algoritmo funciona como se describe a continuación:

1.- Antes de transmitir información una estación debe testear el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).

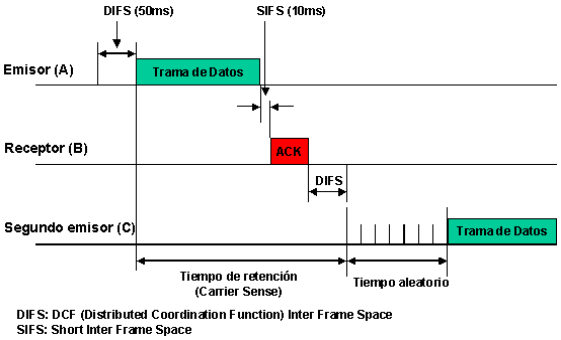
2.- Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada *espaciado entre tramas* (IFS).

3.- Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.

4.- Una vez finaliza esta espera debida a la ocupación del medio la estación ejecuta el llamado algoritmo de Backoff, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado *ventana de contienda* (CW). El algoritmo de Backoff da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

5.- Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición.

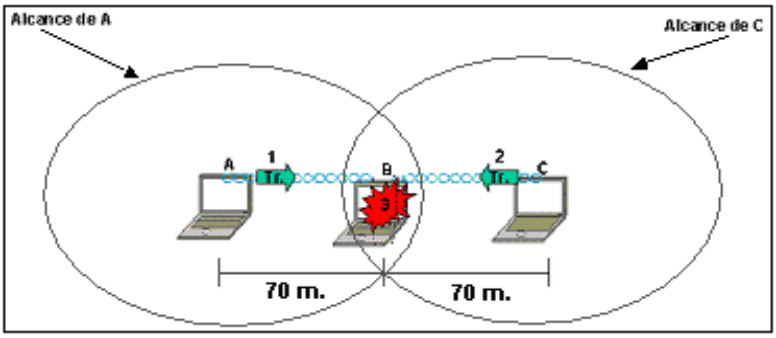
Cada retransmisión provocará que el valor de CW, que se encontrará entre Cwmin y CWmax se duplique hasta llegar al valor máximo. Por otra parte, el valor del slot time es 20µseg.



Esquema del algoritmo CSMA/CA

El algoritmo funciona bien si todas las estaciones son capaces de oír a todas las demás. Sin embargo, CSMA/CA en un entorno inalámbrico y celular, presenta algunos problemas de los cuales los más importantes son:

- Nodos ocultos. Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye.



1. A quiere transmitir una trama a B. Detecta el medio libre y transmite.	3. Se produce una colisión en la intersección por lo que B no recibe ninguna de las dos tramas.	2. Mientras A está transmitiendo C quiere enviar una trama a B. Detecta el medio libre (pues no capta la emisión de A) y transmite.

Esquema representativo del problema del Nodo Oculto

- Nodos expuestos. Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

La solución que propone 802.11 es MACA o MultiAccess Collision Avoidance.

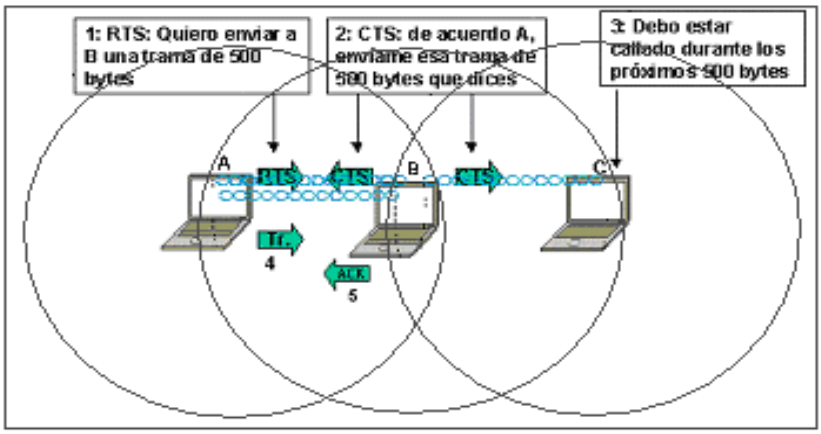
MACA (MultiAccess Collision Avoidance)

Según MACA, antes de transmitir el emisor envía una trama RTS (Request to Send), indicando la longitud de datos que quiere enviar, es decir el tiempo que ocupara el

medio. El receptor le contesta con una trama CTS (Clear to Send), repitiendo la longitud o el tiempo enviado. Al recibir el CTS, el emisor envía sus datos. Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS, si este no llega, la estación que lo espera podrá transmitir.
- Al escuchar un CTS, hay que esperar según la longitud enviada. La solución final de 802.11 utiliza MACA con CSMA/CA para enviar los RTS y CTS.

Después de que se recibe la trama de los datos, se devuelve una trama ACK (datos y tramas de transmisión de reconocimientos), que verifica una transmisión de datos exitosa.



1. Antes de transmitir la trama A envía un mensaje RTS	2. B responde al RTS con un CTS	3. C no capta el RTS, pero sÍ el CTS. Sabe que no debe transmitir durante el tiempo equivalente a 500 bytes	4. A envía su trama seguro de no colisionar con otras estaciones	5. B envía un ACK a A que indica transmisión exitosa

Esquema representativo del algoritmo MACA

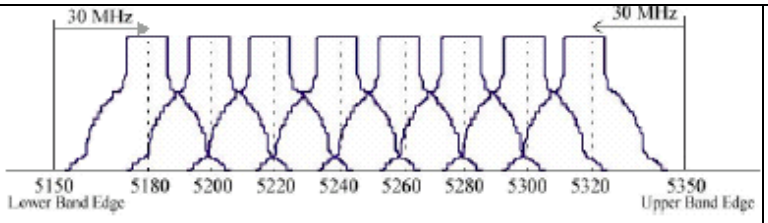
ANEXO D

Bandas de operación (802.11a y 802.11g)

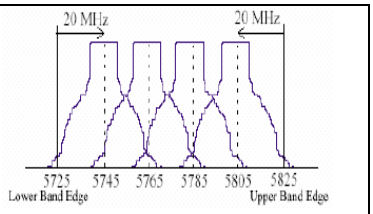
La banda de 5 GHz (banda U-NII) está formada por tres sub-bandas:

- 5,150 a 5,250 GHz, denominada U-NII Lower Band.
- 5,250 - 5,350 GHz, denominada U-NII Middle Band.
- 5,725 - 5,825 GHz, denominada U-NII Upper Band.

Cuando se utilizan tanto U-NII Lower Band como U-NII Middle Band, hay 8 canales no solapados disponibles; mientras que con la banda de 2,4 GHz sólo hay 3. El ancho de banda total disponible en la banda de 5 GHz también es mayor que en la banda de 2,4 GHz (300 MHz por 83,5 MHz). Así pues, una WLAN basada en el 802.11a puede admitir un mayor número de usuarios de alta velocidad simultáneos sin peligro de que surjan conflictos.



Esquema de Bandas U-NII baja y media



Esquema de Bandas U-NII alta

La frecuencia de funcionamiento más alta del estándar 802.11a tiene como consecuencia un alcance relativamente más corto. Se necesitarán más puntos de acceso 802.11a para cubrir la misma zona. Pero incluso con estos inconvenientes, las pruebas iniciales demuestran que los productos 802.11a ofrecen un rendimiento casi tres veces superior al de los 802.11b en cuanto a alcances en interiores.

En comparación con el estándar IEEE 802.11a, el 802.11g tiene un ancho de banda utilizable más bajo, lo que redunda en un menor número de usuarios WLAN de alta velocidad. Aunque las modulaciones OFDM permiten una velocidad más alta, el ancho de

banda disponible total en la banda de frecuencia de 2,4 GHz no varía. El motivo es que el IEEE 802.11g todavía está restringido a tres canales en la banda de 2,4 GHz.

Los equipos IEEE 802.11a alcanzan velocidades de datos más altas en alcances cortos o, no obstante, la velocidad de los datos disminuye rápidamente cuando la señal debe atravesar paredes y otros obstáculos.

Los productos IEEE 802.11g son capaces de conseguir velocidades de datos más elevadas y con mayor alcance que los productos con tecnología 802.11a. La combinación de OFDM y la mejor capacidad para atravesar paredes de sus 2,4 GHz confieren a los productos 802.11g una ventaja clara sobre otras tecnologías WLAN de alta velocidad. La capacidad para proporcionar una cobertura de gran rendimiento en un área comparativamente grande desde un único punto de acceso supone un factor importante de coste.

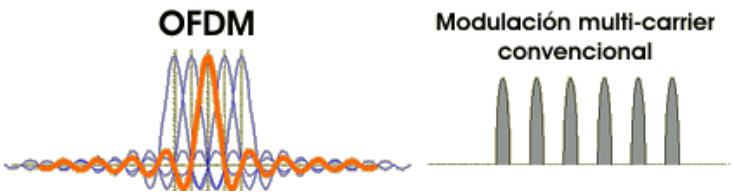
Un punto de acceso 802.11b de 2,4 GHz, por ejemplo, no podrá trabajar con una tarjeta de interfaz de red 802.11a de 5 GHz. No obstante, estos estándares pueden coexistir perfectamente.

ANEXO E

Multicanalización por división de frecuencias ortogonales (OFDM)

La tecnología OFDM (*Orthogonal Frecuency División Multiplexing*) parte una señal de alta velocidad en decenas o centenas de señales de menor velocidad, que son transmitidas en paralelo. Esto crea un sistema altamente tolerante al ruido, al mismo tiempo es muy eficiente en el uso del ancho de banda y por lo tanto permite una amplia cobertura de área punto a punto y multipunto. Además, utiliza hasta 12 canales sin solapamiento, con lo cual genera un aumento en la capacidad para las comunicaciones simultáneas. OFDM es la base para los estándares 802.11a, 802.11g, 802.16.

OFDM es una tecnología de modulación digital, una forma especial de modulación multi-carrier considerada la piedra angular de la próxima generación de productos y servicios de radio frecuencia de alta velocidad para uso tanto personal como corporativo. La técnica de espectro disperso de OFDM distribuye los datos en un gran número de carriers que están espaciados entre sí en distintas frecuencias precisas. Ese espaciado evita que los demoduladores vean frecuencias distintas a las suyas propias.



Modulación OFDM

OFDM tiene una alta eficiencia de espectro y menor distorsión multi-ruta. Actualmente OFDM no sólo se usa en las redes inalámbricas LAN 802.11a y 802.11g, sino en comunicaciones de alta velocidad por vía telefónica como las ADSL y en difusión de señales de televisión digital terrestre en Europa, Japón y Australia.

Actualmente existen equipos con la capacidad de transmitir desde 1.5Mbps hasta 30Mbps en 25MHz de ancho de banda y pronto se estarán produciendo equipos que

superaran velocidades de 100Mbps. Adicionalmente a la velocidad, se cuenta con opciones de seguridad que hacen virtualmente imposible descifrar la señal que se transmite.

Aunque OFDM sea una tecnología excelente para las aplicaciones WLAN de interior, las leyes de la física indican que el alcance de la comunicación es proporcional a la longitud de onda. En otras palabras, los objetos dispersan y atenúan la energía de radiofrecuencia de un modo más eficaz cuanto más alta sea la frecuencia utilizada.

FHSS	DSSS	OFDM
➢ Transmite los datos en portadoras que cambian o saltan de frecuencia en función del tiempo.	➢ Banda angosta dispersa sobre un amplio espectro. ➢ Baja amplitud.	➢ Transmite señales simultáneas de alta velocidad. ➢ Divide el espectro en varias subportadoras.
Ventajas		
➢ Alta tolerancia a interferencia. ➢ Alta seguridad contra intercepción de señal.	➢ Alta velocidad ➢ Más resistente contra interferencia que Banda Angosta.	➢ Alta eficiencia de espectro. ➢ Alta velocidad de transmisión. ➢ No requiere retrasmisión de datos.
Desventajas		
➢ Baja/media velocidad ➢ Dificultad en PMP ➢ Difícil de sincronizar en larga distancia.	➢ Ciertas falencias por ruido y multitrayectoria. ➢ Próximo a su límite de velocidad	➢ Costos ➢ Requiere mayor capacidad de procesamiento.

Cuadro comparativo de las modulaciones que utiliza 802.11

ANEXO F

Cuadro comparativo de las tres variantes más importantes de 802.11

	802.11b	**802.11g**	**802.11a**
Compatibilidad	IEEE 802.11b Wi-Fi Certificado	IEEE 802.11b y 802.11g Wi-Fi Certificado	IEEE 802.11a Wi-Fi Certificado
Número de canales	3 canales no solapados	3 canales no solapados	8 canales no solapados (4 en algunos países)
Rango típico Ambientes Indoor	100 ft (30 m) a 11 MBps; 300 ft (91 m) a 1 Mbps	100 ft (30 m) a 54 MBps; 300 ft (91 m) a 1 Mbps	40 ft (12 m) a 54 Mbps; 300 ft (91 m) a 6 Mbps
Rango típico Ambientes Outdoor (Linea de Vista)	400 ft (120 m) a 11 Mbps; 1500 ft (460 m) a 1 Mbps	400 ft (120 m) a 54 Mbps; 1500 ft (460 m) a 1 Mbps	100 ft (30m) a 54 Mbps; 1000 ft (305m) a 6 Mbps
Tasas de transferencia	11, 5.5, 2 y 1 Mbps	54, 48, 36, 24, 18, 12, 9 y 6 Mbps	54, 48, 36, 24, 18, 12, 8 y 6 Mbps
Medio Wireless	Direct Sequence Spread (DSSS), 2.4 GHz	Orthogonal Frequency Division Multiplexing (OFDM), 2.4 GHz	Orthogonal Frequency Division Multiplexing (OFDM), 5 GHz

HOJA DE LEGALIZACION DE FIRMAS

ELABORADA(O) POR

JASSON RAUL BOADA ORTIZ

_____

JASSON RAUL BOADA ORTÍZ

DECANO DE LA FACULTAD DE INGENIERIA

_____

MAYOR DE E. M. MARCO QUINTANA

Quito, 11 de Octubre del 2005