UNIVERSIDAD APEC
UNAPEC

FACULTAD DE HUMANIDADES Y CIENCIAS
DECANATO DE INFORMÁTICA

"Análisis y Propuesta para la Implementación de una Infraestructura para Interconectar las Bibliotecas de las Universidades de Santo Domingo, utilizando Tecnología Inalámbrica"

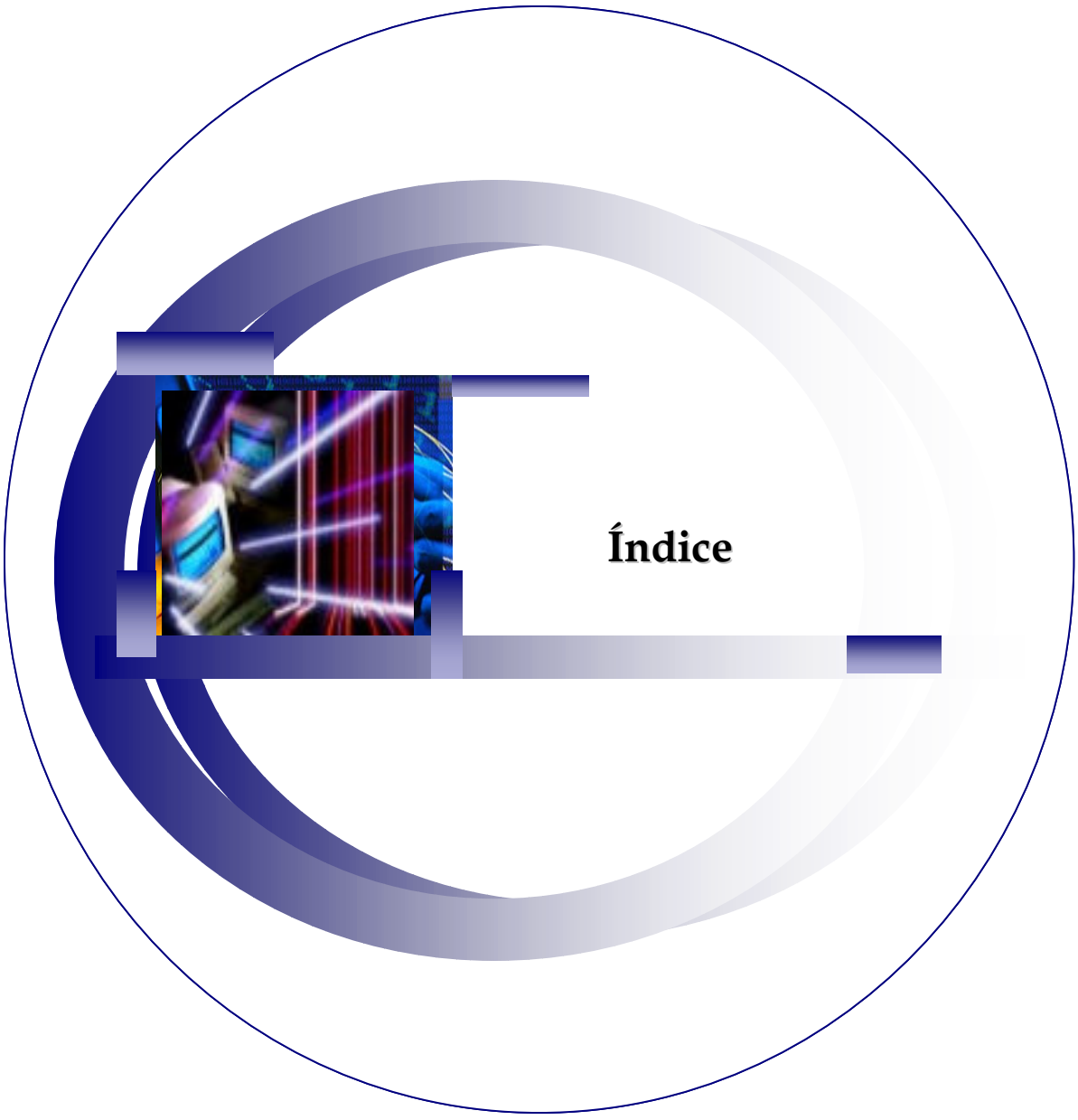
Sustentantes

Miledys Mercedes Taveras Medina **2000-0177**

Aleidania Lorenzo Bierd **2000-0361**

Monografía para Optar por el Título de:
Ingeniero en Sistemas de Computación

Santo Domingo, D. N.
2004



Índice

ÍNDICE

Dedicatorias

DEDICATORIA

A MIS PADRES

Rosmery Medina y Federico Taveras. Este monográfico más que para mí, es un triunfo para ustedes. A ustedes les debo el estar aquí y ser lo que soy el día de hoy. Les dedico especialmente mi último gran esfuerzo antes de graduarme.

A MIS HERMANOS

Kelvyn Alexander, Wascar y Junior Taveras. Son tan importantes para mí, los quiero mucho. Ustedes son una parte muy importante en mi vida y a ustedes también les dedico este triunfo.

A MI ABUELA

Miledys Santana. Lamento que te hayas ido y no lograras verme terminar. Este logro es para ti. Sé que donde quiera que estés vas conmigo y sé que te sientes orgullosa de mí. Que Dios te tenga en gloria.

Miledys Mercedes Taveras Medina

DEDICATORIA

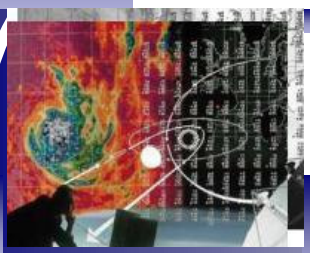
Dedico este trabajo de una manera muy especial a mis padres, **Milagros Bierd y Euribiades Lorenzo,** por ser ellos la fuente de todas las fuerzas para seguir adelante. Por ser los que siempre me han apoyado en todas las metas que me he trazado, por todos los momentos buenos que me han dado a lo largo de toda mi vida, por enseñarme a ser cada día mejor, por la confianza que en mi han depositado, por darme la inspiración de luchar y lograr todas mis metas, por ser mi fuente de vida.

A los seres más importantes de mi vida, mi Nenita querida, mi hermano Allen Manuel, mi sobrino Engel Alemnis, mi hermana del alma Nidia Ozuna (Leslie) y mi cuñada Yari. Además, mi querida hermanita Jahaira Rodríguez, aunque no estas presente en este momento para disfrutarlo juntas sé que desde el cielo me deseas lo mejor.

A mi compañera de monográfico Miledys Taveras, por haber puesto su mejor y mayor esfuerzo para hacer lo mejor.

A todos mis familiares, que de alguna manera contribuyeron con mi educación y formación académica a lo largo de toda mi vida. A mis mejores amigas(os), Johanna Ramírez, Rafaelina Rivas, Alejandro Bonilla, Ivelisse Ozuna, Leomary Franco, Lilliam Ozuna, todos mis amigos del colegio, Domingo Suárez.

Aleidania Lorenzo Bierd



Agradecimientos

AGRADECIMIENTOS

A DIOS

Porque estas presente en cada paso que damos tus hijos, por permitirme llegar a cumplir esta meta, por estar conmigo siempre y no dejarme vencer. Gracias Dios mío por esta oportunidad y espero seguir dando lo mejor de mí siempre.

A MI FAMILIA

Mami, gracias por tus atenciones, por preocuparte tanto por mí, por todas las veces que me ayudaste con tus consejos y por todas las veces que fuiste a buscarme cuando tenía que llegar tarde de la universidad para que no me pasara nada. **Papi,** sin ti no lo habría logrado, gracias por todo lo que hiciste por mí durante toda mi carrera y todavía en el final, gracias por tu preocupación y tu ayuda. **Alex,** sin tus locuras y sacándome de mis casillas de vez en cuando no habría logrado descargarme del estrés en que me sumergía por momentos, gracias hermanito querido por ser tan especial y por haber estado ahí cuando te necesite. Tía **Martha,** gracias por tu preocupación y por ayudarme. A mis abuelos, tíos, tías y primos que me dieron su apoyo incondicional.

A TI

Bernardo Hidalgo. Gracias amor por haberme comprendido, por brindarme tu apoyo y tu consuelo cuando me sentí desanimada. Gracias por ser quien eres y gracias a Dios por haber permitido que llegaras a mi vida. Te quiero mucho.

A MI COMPAÑERA DE MONOGRÁFICO

Aleidania Lorenzo, cuantas cosas, las malas noches, las vueltas y viajes que tuvimos que dar. Gracias por haber decidido emprender este viaje conmigo y por haber completado el camino juntas, te deseo muy buena suerte en el nuevo camino que emprendes.

A MIS COMPAÑEROS

Gleny Soto, aunque no trabajamos juntas ahora, compartimos muchas inquietudes y nos ayudamos mutuamente. **Sihara Mateo**, por fin, estamos del otro lado de la vía, gracias por ser mi amiga y por tu apoyo incondicional. **Diana Soriano**, aunque ahora estés en otro país, te llevo en mi corazón por ser una gran amiga y apoyarme siempre. Y a todos los demás con los que en algún momento compartí en mi trayectoria por la universidad.

A LOS PROFESORES

Ing. Jaime Peña Urbáez, gracias por su gran ayuda, le debemos mucho, usted es un excelente profesor y ser humano. Al **Ing. Freddy Jiménez** por la orientación que nos brindó cuando lo solicitamos. A **Huygens Brito, Domingo Martínez y Rubén Santana** por permitirnos estar en sus aulas y por todos los conocimientos que adquirimos junto a ustedes. A los profesores del monográfico por su empeño de seguir brindándonos sus conocimientos aún en la recta final.

A MI AMIGA

Dinelisse Rodríguez. Gracias por tolerar mi ausencia y por seguir a mi lado a pesar de tenerte tan descuidada. Eres una gran amiga. Te quiero mucho.

A TODOS

Al **Ing. Yván Mártinez** por su colaboración a nuestro proyecto, por habernos dedicado el tiempo necesario para que obtuviéramos el mejor resultado. Al **Sr. Julio César Peñaló** por su ingenio y por ayudarnos a ver ciertas consideraciones que no habíamos tomado en cuenta. Al **Lic. Generoso** por aportar sus conocimientos para la correcta organización de nuestro trabajo.

Gracias a todas las personas que de una forma u otra estuvieron conmigo y que siempre me desearon lo mejor. Gracias por apoyarme y por haber confiado en mí.

Siempre mirando al frente y con Dios delante llegaremos lejos.

Miledys Mercedes Taveras Medina

AGRADECIMIENTOS

Agradezco todo lo que soy hoy día a nuestro señor y padre celestial Dios, tanto por darme la oportunidad de realizar una de mis más grandes y anheladas metas, como también por darle la gran oportunidad a mis padres, en especial a mi mamá, de verme hecha una profesional.

Gracias a todos mis familiares mi Hermano, Sobrino, Cuñada, Abuela, Tíos(as), Primos(as) y a todas aquellas personas que pertenecen a mi familia, por haber sido piezas muy importantes en mi vida y apoyarme de la manera en que lo han hecho hasta hoy día. Un agradecimiento muy especial a todos mis amigos(as) que desde mi niñez y hasta el día de hoy no se han apartado de mi, que siempre han estado ahí en todos los momentos buenos y malos de mi vida.

Debo agradecer muy grandemente a las personas que nos ayudaron con el desarrollo de este proyecto, por ser las personas que más aportaron para que nuestro monográfico tenga la mejor calidad, ellos son: Yván A. Martínez, Julio Cesar Peñaló, Radhames Ortiz, Generoso y la persona de la cual he aprendido todos los mejores conocimientos en el área de redes Inalámbricas, además de ser la fuente motivadora del tema trabajado, el Señor Jaime Peña Urbáez.

A todos aquellos profesores que han formado parte de mi formación académica desde el colegio como el profesor Zacarías Medina, hasta la universidad como los profesores, José Antonio Rodríguez, Domingo Martínez, Freddy Jiménez, Rubén Santana, Héctor Abreu, Lenin Herrera, Huygens Brito, entre otros.

Muchas gracias a la mamá de mi compañera de monográfico Señora Rosmery Medina por todos los días que tubo que acogerme en su casa para poder estudiar y trabajar todos nuestros proyectos.

Mil gracias a todos...

Aleidania Lorenzo Bierd

Introducción

INTRODUCCIÓN

En Estos últimos años la comunicación inalámbrica ha evolucionado notablemente. El uso de dispositivos móviles ya es masivo y a éstos cada vez se le han ido agregando nuevas funcionalidades, sin embargo esto es sólo el inicio de la comunicación inalámbrica, ya que éstas continúan apostando a convertir el aire en el mejor medio de transporte de datos.

Las transmisiones inalámbricas constituyen una eficaz y poderosa herramienta que permite la transferencia de voz, datos y video, sin la necesidad de utilizar cables para establecer la conexión.

Esta transferencia de información es lograda a través de la emisión de ondas de radio, permitiendo así tener dos grandes ventajas las cuales son la movilidad y flexibilidad del sistema en general.

En este trabajo de grado se destaca la ventaja que nos ofrece tener interconectadas las bibliotecas de las universidades de Santo Domingo. Esta consideración se basa en el hecho de que el objetivo principal de la tecnología está orientado a facilitar la vida del ser humano, por lo que al unificar las fuentes bibliográficas de cada localidad, la búsqueda y posterior ubicación de los textos contribuye a dicho objetivo.

También es necesario identificar los elementos que hay que tomar en cuenta para crear una red inalámbrica para el transporte de datos, como son: la seguridad, antenas, puntos de acceso, zona de Freesnel, ubicación de los puntos conexión, etc.

A medida que se adentre en el contenido de este proyecto, el lector identificará las diferentes tecnologías de transmisión inalámbrica, como son: Radio Frecuencia, Microondas, Satélites, Infrarrojo, etc., así como también los conceptos básicos asociados a la comunidad inalámbrica.

Adelante.....

Capitulo I

Antecedentes de la Tecnología Inalámbrica

I. ANTECEDENTES DE LA TECNOLOGÍA INALÁMBRICA

1.1 Origen y Evolución de la Tecnología Inalámbrica

Antecedentes

Las comunicaciones inalámbricas comenzaron con:

- La postulación de las ondas electromagnéticas por James Cleck Maxwell durante el año de 1860 en Inglaterra.
- La demostración de la existencia de estas ondas por Heinrich Rudolf Hertz en 1880 en Inglaterra.
- La invención del telégrafo inalámbrico por Guglielmo Marconi.

Durante 1890 eminentes científicos como Jagdish Chandra Bose de India, Oliver Lodge en Inglaterra y Augusto Righi de la Universidad de Bologna, se encargaron del estudio de los fundamentos naturales de las ondas electromagnéticas.

La noción de la transmisión de información sin el uso de cables fue visto por nuestros ancestros como algo mágico.

En 1896 la primera patente de comunicaciones inalámbricas fue concedida a Guglielmo Marconi en el Reino Unido. Desde aquel momento, entonces el número de desarrollos en el campo de las comunicaciones inalámbricas tomaron ese sitio.

En 1980 comienza la era celular. Diferentes desarrollos y nuevas tecnologías tomaron lugar durante los años de 1990 al 2000.

Las comunicaciones avanzan sin parar y ponen al alcance de los usuarios el acceso a los datos desde cualquier punto y desde cualquier dispositivo. Las nuevas tecnologías de comunicación inalámbricas son el punto crucial de la tecnología de comunicación en este año.

Durante largo tiempo la gestión de la información digital dependía de grandes sistemas y de sus terminales. Luego, éstos se conectaron de forma remota mediante la línea telefónica. Más tarde, llegaron los ordenadores personales y con ellos el auge tanto de los sistemas aislados e individuales como de los conectados alrededor de una red local.

Sin embargo, en todos los casos había una clara dependencia del punto de enlace, el punto de conexión a los servidores en una LAN, o a una línea telefónica en el caso de terminales y PCs remotos. Luego los sistemas portátiles permitieron cortar con los puestos fijos. Pero la libertad se perdía a la hora de comunicarse con los servidores de la empresa o con Internet, ya que también dependían de nuevo de los cables.

1.2 Funcionamiento de la Tecnología Inalámbrica

El IEEE aprobó en 1996 un nuevo protocolo de comunicaciones llamado 80211b o también conocido como Wi-Fi (Wireless Fidelity). En este protocolo se define la forma de transmisión de información usando ondas radioeléctricas.

El espectro radioeléctrico es limitado, puesto que se destina para muchos usos: radioaficionados, televisión, radio, ... así que el mismo instituto definió una banda de frecuencia que en ese momento se encontraba en desuso y era aplicable a nivel mundial, la de los 2,4 Ghz.

Anteriormente fue una banda militar de alta frecuencia, pero con el tiempo las comunicaciones militares evolucionaron a frecuencias más elevadas y a comunicación por satélite, con lo que se decidió dedicar esa banda a comunicaciones médicas. El paso del tiempo ha querido que esta banda quede libre y se use para el estándar Wi-Fi.

Para comunicarse en esta banda son necesarios unos dispositivos formalmente son llamados Tarjetas Inalámbricas, pero que en realidad no son más que tarjetas de red que, en vez de funcionar con un cable convencional, realizan esta transmisión por radio. Son dispositivos que están bajando continuamente de precio en el mercado y cada vez son más asequibles para un usuario doméstico.

Incorporando una tarjeta de este tipo conectada a un PC, podemos realizar enlaces entre distintos ordenadores.

El problema que presentan estas tarjetas es su baja potencia, lo que repercute en un menor alcance. Afortunadamente, algunos fabricantes se han dado cuenta de las necesidades que los compradores demandan y han optado por ofrecer la posibilidad de conectar, mediante un conector que incluyen en la propia tarjeta, un cable ("pigtail") que une la tarjeta a una antena externa y así ampliar el radio de acción.

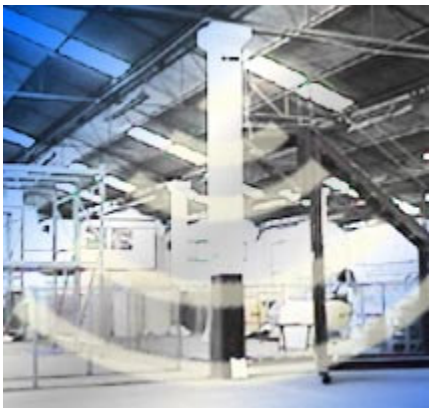
1.3 Tecnologías de Transmisión Inalámbricas

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

También es útil para hacer posibles sistemas basados en plumas. Pero la realidad es que esta tecnología está todavía en pañales y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

1.3.1 Radio Frecuencia RFID



Se le conoce así a las ondas aéreas electromagnéticas para comunicar información desde un punto a otro; son portadoras de radio porque desempeñan la función de entregar energía al receptor. Los datos que se transmiten son sobrepuestos sobre la portadora de radio para que pueda extraer de manera precisa por el receptor. Es a lo que se conoce como la modulación de la portadora por la información que se transmite. Después de que los datos son sobrepuestos (modulados) en el transportador de radio, la señal de radio ocupa más de una sola frecuencia, donde la frecuencia de la información modulada se agrega a la portadora. Múltiples portadoras de radio pueden coexistir en el mismo espacio a la vez, sin que haya interferencia, si las ondas de radio se transmiten sobre radiofrecuencias diferentes. Para extraer los datos, un receptor de radio se sintoniza en una radiofrecuencia mientras rechaza otras.

La identificación por radiofrecuencia (RFID) es una de las tecnologías que mayor progresión está alcanzando actualmente en el desarrollo de la gestión y el incremento de los beneficios en actividades de distribución de todo tipo.

Checkpoint, principal proveedor mundial de sistemas de protección electrónica de artículos por radiofrecuencia (RF-EAS), ofrece una gama completa de avanzadas soluciones de identificación para aplicaciones detallistas, logísticas, industriales, en bibliotecas, etc.

La alianza de Checkpoint con Mitsubishi Materials Corporation, denominada Diamond Checkpoint Development Group, ha venido a reforzar las posiciones de liderazgo que ambas empresas poseían, respectivamente, en las tecnologías de la radiofrecuencia y los circuitos integrados. El resultado es una gama completa de productos de identificación por radiofrecuencia que incluye las etiquetas de 13,56 MHz de bajo costo, los lectores fijos y portátiles y los programas informáticos de aplicación.

RFID - Historia

Años 40	Durante la Segunda Guerra Mundial, Inglaterra emplea transmisores de RF para distinguir sus aviones de regreso de los del enemigo.
Años 60	Identificación por radiofrecuencia de seguridad de los equipos y el personal involucrados en instalaciones nucleares.
Años 80	Seguimiento de ganado con receptores de identificación por radiofrecuencia en lugar del marcado. Las compañías de ferrocarril prefieren la identificación por radiofrecuencia a los códigos de barra para la señalización de la mercancía en ruta.
Años 90	La identificación por radiofrecuencia empieza a sustituir a las monedas o las fichas en las carreteras de peaje.
Febrero 1997	Checkpoint se une a Mitsubishi Materials Company con el objetivo de acabar con la barrera de 1 dólar por etiqueta.
1998	Creación de la etiqueta de RFID Performa 13,56 MHz.
Febrero 1999	Lanzamiento comercial de la serie Performa y de los sistemas de identificación por radiofrecuencia para bibliotecas, con lo que se crea una gama completa de etiquetas y lectores.
Octubre 2000	Presentación de los productos de lectura-escritura de Checkpoint, como la etiqueta de 1.024 bits y los lectores de corto y largo alcance.

- ✓ **Transmisión por radiofrecuencia**

La transmisión por radiofrecuencia puede ser útil para introducir los datos en el sistema de información contable sin necesidad de ningún tipo de cableado.

Algunas de las ventajas de utilizar esta tecnología son: facilitar el control de almacenes, llevar un control del inventario en tiempo real, optimizar el espacio físico de los almacenes, reducir movimientos de equipos y empleados, incrementar la productividad de la mano de obra al sincronizar movimientos de materiales, simplificar el surtido de materiales a producción y de productos a clientes, permitir la comunicación inmediata dentro de una planta, enlazar controladores de acceso, terminales portátiles, lectores de códigos de barras, impresoras, basculas, PCs sin necesidad de ningún tipo de cableado.

1.3.1.1 Bluetooth

Bluetooth es una iniciativa multidistribuidor que proporciona una norma mundial para conectividad inalámbrica de corto alcance entre una serie de dispositivos móviles o fijos.

Desarrollada inicialmente por Ericsson, Bluetooth permite a los teléfonos móviles y otros dispositivos inalámbricos comunicarse a velocidades de hasta 721 Kbits/seg por radio de corto alcance con ordenadores portátiles, impresoras, faxes y otros dispositivos equipados al efecto, evitando así la necesidad de instalar cables y conectores especiales. Bluetooth utiliza la banda de radio sin licencia y disponible en todo el mundo de 2,45 GHz.

Es un estándar que utiliza FHSS, capaz de transmitir a velocidades de 1 Mbps y es apoyado por más de 2000 empresas de tecnología. Bluetooth ha surgido últimamente como un posible substituto a todo tipo de cable anexado a una computadora, debido a su costo y el apoyo de cientos de instituciones empresariales.

En cuanto a su implementación Bluetooth utiliza el término *piconet*. Un *piconet* es un grupo de 2 u 8 aparatos que utilizan "Bluetooth",estos aparatos que forman parte del *piconet* comparten el mismo rango que es utilizado por un "Hopping Sequence", a su vez cada *piconet* contiene un aparato "Principal" que es el encargado de coordinar el "Hopping Pattern" del *piconet* para que los demás aparatos "Esclavos" sean capaces de recibir información.

Además éste es un estándar libre lo que simplifica su uso para diseñar y sacar al mercado nuevos productos innovadores que se beneficien de la conectividad inalámbrica.

Cada dispositivo Bluetooth esta equipado con un transceiver que transmite. Además de los canales de datos, están disponibles 3 canales de voz a 64 Kbs. Cada dispositivo tiene una dirección única de 48 bits basada en el estándar de la IEEE 802.11 para redes de área local inalámbricas, que le permite formar temporalmente parte de una piconet. Las conexiones son uno a uno, con un rango máximo de 10 metros, aunque mediante el uso de repetidores se puede lograr un alcance de hasta 100 metros con algo de distorsión.

- ✓ **Inmunidad a las interferencias**

En cuanto a interferencias con otros dispositivos, hay que tener cuidado con los que operan en la misma banda. Por ejemplo, lo mismo que está prohibido el uso de teléfonos móviles en los aviones, se puede prohibir el uso de cualquier otro dispositivo que incorpore un chip Bluetooth, ya que podría interferir con los elementos de navegación.

El protocolo banda base que utiliza Bluetooth combina las técnicas de conmutación de circuitos y de paquetes y para asegurar que los paquetes llegan en orden. La velocidad para un canal asimétrico de datos puede llegar a 721 Kbit/s en un sentido y 57,6 Kbit/s en el otro, o 432, 6 Kbit/s en ambos sentidos si el enlace es simétrico.

Un aspecto muy importante, dado lo reducido del chip, y que va a ir incorporado en dispositivos portátiles y alimentado con baterías, es que los dispositivos Bluetooth cuando no intercambian datos, entonces establecen el modo de "espera" para ahorrar energía, quedando a la espera de mensajes.

Bluetooth opera en una banda de frecuencia que está sujeta a considerables interferencias, por lo que el sistema ha sido optimizado para evitar éstas interferencias. En este caso La técnica de salto de frecuencia es aplicada a una alta velocidad y una corta longitud de los paquetes (1600 saltos / segundo, para slots-simples). Los paquetes de datos están protegidos por un esquema ARQ (repetición automática de consulta), en el cual los paquetes perdidos son automáticamente retransmitidos, aun así, con este sistema, si un paquete de datos no llegase a su destino, sólo una pequeña parte de la información se perdería.

La voz no se retransmite nunca, sin embargo, se utiliza un esquema de codificación muy robusto. Éste esquema, que está basado en una modulación variable de declive delta (CSVD), que sigue la forma de la onda de audio y es muy resistente a los errores de bits. Estos errores son percibidos como ruido de fondo, que se intensifica si los errores aumentan.

1.3.1.2 Celulares

- ✓ **Historia de la telefonía celular**

Martin Cooper fue el pionero en esta tecnología, a él se le considera como "el padre de la telefonía celular" al introducir el primer radioteléfono, en 1973, en Estados Unidos, mientras trabajaba para Motorola; pero no fue hasta 1979 cuando aparecieron los primeros sistemas comerciales en Tokio, Japón por la compañía NTT.

En 1981, los países nórdicos introdujeron un sistema celular similar a AMPS (Advanced Mobile Phone System). Por otro lado, en Estados Unidos, gracias a que la entidad reguladora de ese país adoptó reglas para la creación de un servicio comercial de telefonía celular, en 1983 se puso en operación el primer sistema comercial en la ciudad de Chicago.

Con ese punto de partida, en varios países se diseminó la telefonía celular como una alternativa a la telefonía convencional inalámbrica. La tecnología tuvo gran aceptación, por lo que a los pocos años de implantarse se empezó a saturar el servicio. En ese sentido, hubo la necesidad de desarrollar e implantar otras formas de acceso múltiple al canal y transformar los sistemas analógicos a digitales, con el objeto de darle cabida a más usuarios.

Para separar una etapa de la otra, la telefonía celular se ha caracterizado por contar con diferentes generaciones. Las generaciones de la telefonía inalámbrica.

--Primera generación (1G)

La 1G de la telefonía móvil hizo su aparición en 1979 y se caracterizó por se analógica y estrictamente para voz. La calidad de los enlaces era muy baja, tenían baja velocidad (2400 bauds). En cuanto a la transferencia entre celdas, era muy imprecisa ya que contaban con una baja capacidad (Basadas en FDMA, Frequency Division Multiple Access) y, además, la seguridad no existía. La tecnología predominante de esta generación es AMPS (Advanced Mobile Phone System).

--Segunda generación (2G)

La 2G arribó hasta 1990 y a diferencia de la primera se caracterizó por ser digital. EL sistema 2G utiliza protocolos de codificación más sofisticados y se emplea en los sistemas de telefonía celular actuales. Las tecnologías predominantes son: GSM (Global System por Mobile Communications); IS-136 (conocido también como TIA/EIA136 o ANSI-136) y CDMA (Code Division Multiple Access) y PDC (Personal Digital Communications), éste último utilizado en Japón.

Los protocolos empleados en los sistemas 2G soportan velocidades de información más altas por voz, pero limitados en comunicación de datos. Se pueden ofrecer servicios auxiliares, como datos, fax y SMS (Short Message Service). La mayoría de los protocolos de 2G ofrecen diferentes niveles de encripción. En Estados Unidos y otros países se le conoce a 2G como PCS (Personal Communication Services).

--Generación 2.5 G

La generación 2.5G ofrece características extendidas, ya que cuenta con más capacidades adicionales que los sistemas 2G, como: GPRS (General Packet Radio System), HSCSD (High Speed Circuit Switched), EDGE (Enhanced Data Rates for Global Evolution), IS-136B e IS-95Bm entre otros.

--Tercera generación 3G

La 3G se caracteriza por contener a la convergencia de voz y datos con acceso inalámbrico a Internet; en otras palabras, es apta para aplicaciones multimedia y altas transmisiones de datos. Los protocolos empleados en los sistemas 3G soportan altas velocidades de información y están enfocados para aplicaciones más allá de la voz como audio (mp3), video en movimiento, videoconferencia y acceso rápido a Internet, sólo por nombrar algunos.

En un futuro próximo los sistemas 3G alcanzarán velocidades de hasta 384 Kbps, permitiendo una movilidad total a usuarios, viajando a 120 kilómetros por hora en ambientes exteriores. También alcanzará una velocidad máxima de 2 Mbps, permitiendo una movilidad limitada a usuarios, caminando a menos de 10 kilómetros por hora en ambientes estacionarios de corto alcance o en interiores.

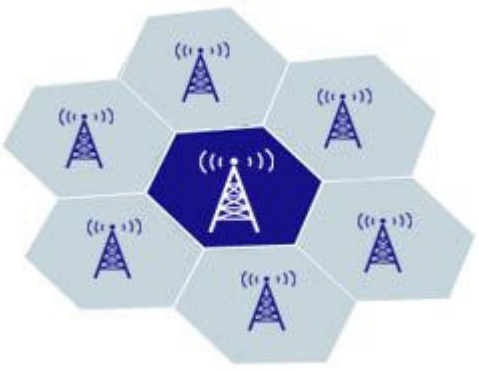
En relación a las predicciones sobre la cantidad de usuarios que podría albergar 3G, The Yanlee Group anticipa que en el 2004 habrá más de 1,150 millones en el mundo, comparados con los 700 millones que hubo en el 2000.

Dichas cifras nos anticipan un gran número de capital involucrado en la telefonía inalámbrica, lo que con mayor razón las compañías fabricantes de tecnología, así como los proveedores de servicios de telecomunicaciones estarán dispuestos a invertir su capital en esta nueva aventura llamada 3G.

- ✓ **Cómo funcionan los teléfonos celulares**

La gran idea del sistema celular es la división de la ciudad en pequeñas células o celdas. Esta idea permite la re-utilización de frecuencias a través de la ciudad, con lo que miles de personas pueden usar los teléfonos al mismo tiempo. En un sistema típico de telefonía análoga de los Estados Unidos, la compañía recibe alrededor de 800 frecuencias para usar en cada ciudad.

La compañía divide la ciudad en celdas. Cada celda generalmente tiene un tamaño de 26 kilómetros cuadrados. Las celdas son normalmente diseñadas como hexágonos (figuras de seis lados), en una gran rejilla de hexágonos.



Cada celda tiene una estación base que consiste de una torre y un pequeño edificio que contiene el equipo de radio.

Cada celda en un sistema análogo utiliza un séptimo de los canales de voz disponibles. Eso es, una celda, más las seis celdas que la rodean en un arreglo hexagonal, cada una utilizando un séptimo de los canales disponibles para que cada celda tenga un grupo único de frecuencias y no haya colisiones.

Un proveedor de servicio celular típicamente recibe 832 radio frecuencias para utilizar en una ciudad. Cada teléfono celular utiliza dos frecuencias por llamada, por lo que típicamente hay 395 canales de voz por portador de señal. (las 42 frecuencias restantes son utilizadas como canales de control). Por lo tanto, cada celda tiene alrededor de 56 canales de voz disponibles.

En otras palabras, en cualquier celda, pueden hablar 56 personas en sus teléfonos celulares al mismo tiempo. Con la transmisión digital, el número de canales disponibles aumenta. Por ejemplo el sistema digital TDMA puede acarrear el triple de llamadas en cada celda, alrededor de 168 canales disponibles simultáneamente.

La tecnología celular requiere un gran número de bases o estaciones en una ciudad de cualquier tamaño. Una ciudad grande puede llegar a tener cientos de torres. Cada ciudad necesita tener una oficina central la cual maneja todas las conexiones telefónicas a teléfonos convencionales, y controla todas las estaciones de la región.

- ✓ **¿Qué significa que un teléfono soporte "modo dual"?**

Un teléfono que soporta el modo dual puede utilizar una señal digital, o de ser necesario una análoga. Esta ventaja lo mantendrá conectado en algunas regiones remotas que no cuentan todavía con servicio digital.

- ✓ **Tecnología Wap**

WAP (Wireless Application Protocol o Protocolo de Aplicaciones Inalámbricas).

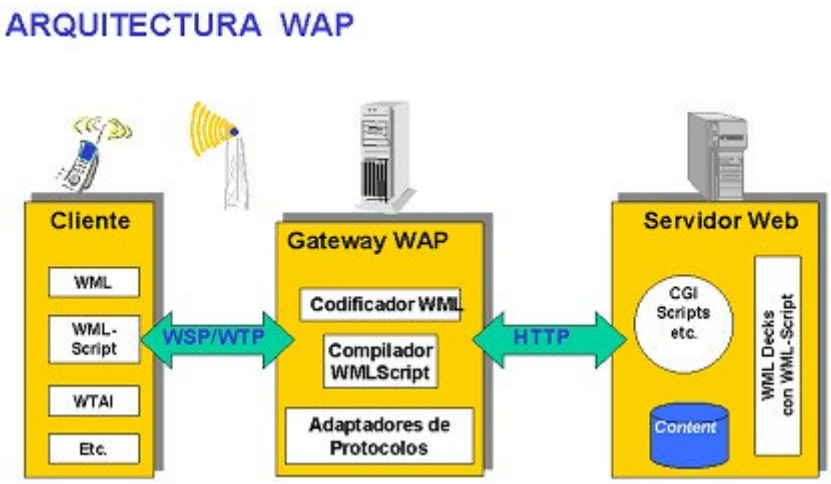
Es una solución unificada para los servicios de valor agregado existentes y futuros para la telefonía móvil. El protocolo incluye especificaciones para las capas de sesión y de transporte del modelo OSI, así como funcionalidades de seguridad. WAP también define un entorno de aplicaciones.

Es escalable, permitiendo así a las aplicaciones disponer de las capacidades de pantalla y recursos de red según su necesidad y en una gran variedad de tipos de terminales. Los servicios podrán ser aplicables a pantallas de una sola línea o a terminales mucho más complejos como las PDA´s.

Funcionamiento de WAP

El usuario solicita la página WAP que quiera ver.

- El micronavegador del móvil envía la petición con la dirección (URL) de la página solicitada y la información sobre el abonado al Gateway WAP (software capaz de conectarse a la red de telefonía móvil y a Internet) .
- El Gateway examina la petición y la envía al servidor donde se encuentra la información solicitada.
- El servidor añade la información http o HTTPS pertinente y envía la información de vuelta al Gateway.
- En el Gateway se examina la respuesta del servidor, se valida el código WML en busca de errores y se genera la respuesta que se envía al móvil.
- El micronavegador examina la información recibida y si el código es correcto lo muestra en pantalla.



Ámbitos De Aplicación

WAP ofrece infinitas posibilidades de cara tanto a empresas y profesionales como al consumidor:

De cara a empresas y profesionales:

- Agendas corporativas WAP
- Gestión de pedidos (fuerza de ventas)
- Servicios de localización
- Gestión de flotas
- Servicios de mensajería
- Tiendas virtuales
- Comercio electrónico móvil
- ...

De cara al consumidor:

- Servicios de banca on-line (mobile home-banking, bolsa, ...)
- Venta y reserva de billetes (transportes)
- Ticketing: espectáculos
- Información tiempo, tráfico, horarios, turística, ...
- Escenarios de compra
- ...

Ventajas e Inconvenientes

La tecnología WAP tiene importantes ventajas ya que permite acceder a Internet por medio de un dispositivo que podemos llevar con nosotros a cualquier parte.

Sin embargo la tecnología WAP está teniendo menos éxito del esperado debido a que también tiene algunos inconvenientes. En primer lugar la pequeña pantalla de un teléfono móvil no permite mostrar contenidos con gráficos atractivos.

También es difícil navegar y cuesta demasiado tiempo desplazarse por los menús para llegar a la opción que buscamos. Esto es debido a que en la pantalla caben pocas opciones para cada menú por lo que hay que dividirlos en varios pasos.

Cuando se trata de escribir un texto hay que tomárselo con paciencia porque al no disponer de un teclado completo cada tecla del teléfono móvil sirve para varias letras. Aunque una opción es adquirir un pequeño teclado que se conecta al teléfono móvil.

Con el agravante de que por mucho que intentemos aprender a manejarlo bien sólo podremos ir un poco más rápido ya que el sistema no lo permite. De todas formas algunos de estos inconvenientes pueden ir solucionándose poco a poco por lo que todavía el acceso a Internet por WAP no ha dicho su última palabra.

1.3.1.3 Beepers

Un radiolocalizador es un dispositivo de comunicación personal. Los radiolocalizadores se clasifican con base en la forma como se comunican:

a) Únicamente Tono:

El radiolocalizador de "Únicamente Tono" no es sólo un dispositivo de tonos. Este es el nombre común que se utiliza en la industria. El radiolocalizador hace más que solo generar un tono. Hay 6 formas en que el radiolocalizador de "Únicamente Tono" se puede comunicar: 4 tonos diferentes, una luz y una vibración.

b) Tono y Voz:

La radiolocalización con voz es todavía popular en algunas partes del mundo. No ha sido adoptada en áreas donde la radiolocalización tiene gran uso debido al número limitado de suscriptores que se pueden acomodar en un canal de radio. Un sistema de radiolocalización a gran escala con múltiples transmisores no sería económicamente factible con radiolocalizadores de voz.

c) Despliegue Numérico:

A los radiolocalizadores numéricos algunas veces el público en general les llama "beepers digitales". Este es un nombre incorrecto ya que existen dispositivos como los radiolocalizadores con despliegue numérico analógico, y un radiolocalizador generalmente no es analógico y digital a la vez.

Este es, hasta ahora, el radiolocalizador más usado en el mundo. El "contenido de información" del mensaje es bastante completo (más que un tono), y la capacidad del canal es mucho mayor que en el caso de mensajes de voz.

Los propietarios del sistema en muchas partes del mundo ofrecen este tipo de radiolocalizador y ha tenido una amplia aceptación por parte del público. Dado que muchos radiolocalizadores pueden operar en un canal de radio, y casi todos los sistemas numéricos están totalmente automatizados (sin operadores), el costo de su utilización es muy bajo.

d) Despliegue Alfanumérico:

Un mensaje alfanumérico enviado apropiadamente le dice al suscriptor: quién llamó, por qué, dónde debe ir, cuándo, la dirección, la hora, etc. Es importante observar que no se requiere contestar una llamada con un radiolocalizador alfanumérico. Esta sola característica puede ahorrarle al suscriptor mucho tiempo y esfuerzo. En aquellos lugares del mundo donde no se tienen disponibles teléfonos públicos (para contestar una llamada), la característica alfanumérica ofrece una gran ventaja sobre los otros tipos de radiolocalizadores.

Determinación De La Frecuencia Del Radio

Las frecuencias más comunes para radiolocalización son:

BANDA	FRECUENCIA
Banda alta de VHF	138 -174 MHz
Rango inferior de UHF	406 -420 MHz
Rango medio de UHF	435 – 480 MHz
Rango superior de UHF	495 -512 MHz
Banda de 900 MHz	929 – 932 MHz

1.3.1.4 Wi-Fi

Entre las predicciones tecnológicas, todas las grandes consultoras coinciden en señalar el desarrollo de las tecnologías Wi-Fi como una de las principales tendencias. Las ventas de aparatos con conexión inalámbrica se incrementaran gracias a factores como la extensión de los estándares, el aumento de la interoperabilidad, la creciente demanda de aparatos portátiles o la aparición de nuevas aplicaciones.

Esta tecnología está viviendo uno de sus momentos más dulces desde que allá por los años 80 los *Bulletin Board System*, redes previas al desarrollo de Internet mantenidas por los usuarios, se pusieran en funcionamiento. Las consultoras prevén un aumento considerable de este mercado en los próximos años y muchas empresas albergan en él sus esperanzas para salir definitivamente de la crisis.

WI-FI o Wireless Fidelity es el nombre que se le ha dado a la tecnología de transmisión de datos o acceso a Internet inalámbrico que utiliza el protocolo de Comunicación 802.11 y trabaja en la banda de 2,4 GHz y 5 GHz de uso libre.

El alcance de una conexión de este tipo puede llegar a los cien metros a la redonda, por lo que es posible implementarla en casas, empresas y sitios donde acude mucha gente.

Es denominado también como un protocolo de comunicación inalámbrica de área local que permite, tanto a los usuarios domésticos como corporativos, navegar a través de Internet por medio de ondas de radio, es decir, sin la utilización de cables, al menos en distancias cortas. De este modo, cualquier usuario con un computador portátil o computadora de bolsillo al entrar en lugar con tecnología WiFi puede conectarse a la red fácilmente.

WiFi funciona de la siguiente manera: se necesita una infraestructura primaria por donde transiten datos a altas velocidades, de allí la señal de Internet pasa mediante un punto de acceso (access point) que la distribuye en forma de señales de radio por medio de antenas. La computadora debe estar equipada con una tarjeta que recoja las señales. Equipos como los nuevos modelos de Palm y las computadoras equipadas con el procesador Centrino de Intel no necesitan la tarjeta, pues la tienen incorporada.

- ✓ **Utilizaciones del WI-FI**

La tecnología WiFi podrá ser utilizada en diferentes actividades comerciales que requieran la transmisión de datos a través de un medio inalámbrico.

• Ventas: las personas que trabajen en ventas y cobros podrán realizar y modificar los inventarios en el mismo momento en que sus clientes hagan el pedido.

• Facturación: si esta tecnología llega a su máximo punto de desarrollo, será posible realizar actividades como facturación de recibos y pago de estos mediante el sistema de banca virtual que funciona en el país.

• Envío de reportes y datos: desde un lugar con cobertura se podrá enviar cualquier tipo de datos utilizando su equipo portátil o agenda electrónica.

- ✓ **Compatibilidades del WI-FI**

Para acabar con los conflictos entre los diferentes WI-FI, los fabricantes de terminales están colocando en el mercado los «Puntos de Acceso Inalámbrico de Banda Dual», que se encargan de procesar la información que se emite tanto a 5 GHz como a 2,4 GHz.

Otra iniciativa es la que ha ideado la Wi-Fi Alliance (asociación que reúne a más de 130 fabricantes), quien ha creado la marca WI-FI Certificate para asegurar la compatibilidad entre las diferentes empresas.

Más complicada es su compatibilidad con el UMTS y el GPRS. Los expertos sostiene que estas tecnologías, aun siendo diferentes, están llamadas a entenderse de aquí a unos años. Por ejemplo, una empresa puede beneficiarse de las ventajas de tender una red WLAN en sus oficinas, pero posiblemente precise del UMTS para gestionar su flota de transporte.

No obstante, ya existe la tecnología y el hardware que garantiza que una portátil o una PDA, por ejemplo, puedan funcionar tanto en redes inalámbricas como en UMTS -aunque en fase experimental- y GPRS-GSM. Existen en el mercado tarjetas de acceso a redes WI-FI capaces de albergar la tarjeta SIM del móvil. Los expertos presumen que en los próximos años se producirá un carrera entre los fabricantes de hardware y operadores de telefonía para copar el mercado de compatibilidad entre ordenadores, PDA's y teléfonos móviles.

- ✓ **¿Cuán rápido es Wi-Fi?**

Wi-Fi está diseñado para transmitir datos en forma inalámbrica a velocidades muy altas –a niveles de Megabits. La velocidad final que se logra depende de varios factores; entre ellos: la cantidad de usuarios activos utilizando un punto de acceso, la distancia en que se encuentra del punto de acceso, cualquier obstrucción que interfiera con la señal, y la velocidad de la línea alámbrica que conecta al punto de acceso. Generalmente la señal Wi-Fi transmite razonablemente bien a través de cristal y muchos tipos de pared, pero no transmiten bien a través de metal, concreto o edificios.

- ✓ **¿Qué es un "HotSpot"?**

El término "HotSpot" se está utilizando para referirse a los puntos de acceso Wi-Fi en diferentes localidades públicas (fuera de su hogar u oficina). Generalmente los "HotSpots" y los puntos de acceso Wi-Fi tienen alcance limitado en el servicio, usualmente 300 pies o menos, sin obstrucciones. La nueva tecnología y la utilización de múltiples puntos de acceso harán posible que se extienda el alcance de la señal Wi-Fi en algunas localidades en el futuro.

1.3.1.5 Wi Max

Permite conectar hasta 1.552 personas por antena, cada 50 kilómetros. Imagínese que se encuentra en Isla Fuerte, en el Golfo de Morrosquillo, y puede transmitir las imágenes de un maravilloso atardecer, en vivo y en directo, a través de su cámara web conectada a un equipo portátil. Imagínese, además, que un indígena, que habita en las selvas colombianas, a miles de kilómetros, puede seguir por Internet inalámbrico la clase de geografía que se dicta en un colegio de Medellín.

Esto será posible a partir de 2006, cuando entre en funcionamiento Wi Max (Interoperabilidad Mundial para Acceso de Microondas), la tecnología inalámbrica de mayor ancho de banda y alcance, que cubre hasta 50 kilómetros de radio (Wi Fi llega hasta los 30 kilómetros).

La primera transmisión en Latinoamérica con Wi Max la realizó Intel, en Cartagena, cuando hizo una demostración con equipos portátiles, desde el Castillo de San Felipe de Barajas, en el Cerro de La Popa y el Hotel Cartagena Hilton, en el sector turístico del Laguito.

- ✓ **Directo a la casa**

Actualmente si se tiene acceso directo a Internet de banda ancha éste llega a la casa por medio del cable del teléfono, Wi Max traerá la señal a la casa a través de torres, que envían la señal de forma inalámbrica, sin necesidad de instalar cableado por las calles, como se hace tradicionalmente.

Cien compañías integran el Foro de Wi Max, que busca hoy encontrar un estar universal. "Lo importante es que los dispositivos tengan un estándar único, independiente de la marca, para que puedan comunicarse entre sí.

- ✓ **El complemento perfecto**

Wi Max, que traerá la señal de Internet al hogar, se complementará con Wi Fi, que se usará dentro de la casa para comunicar los equipos entre sí. Por ejemplo, el DVD portátil con el televisor o para pasar información de un dispositivo a otro.

Esta nueva tecnología, debido a su poder de cobertura, rapidez en la transmisión de datos y lo mejor de todo: habitar en un mundo libre de cables, donde se pueda llevar la oficina a todas partes, al igual que el entretenimiento, la cultura, la salud y la educación. Sin duda estas nuevas tecnologías cambiarán nuestra visión del mundo y la forma como lo vivimos.

1.3.2 Microondas

Se denomina así la porción del espectro electromagnético que cubre las frecuencias entre aproximadamente 3 Ghz y 300 Ghz (1 Ghz = 10^9 Hz), que corresponde a la longitud de onda en vacío entre 10 cm. y 1mm.

La propiedad fundamental que caracteriza a este rango de frecuencia es que el rango de ondas correspondientes es comparable con la dimensión físicas de los sistemas de laboratorio; debido a esta peculiaridad, las microondas exigen un tratamiento particular que no es extrapolable de ninguno de los métodos de trabajo utilizados en los márgenes de frecuencias con que limita.

Las líneas de baja frecuencia son usualmente ABIERTAS, con lo cual, si se intenta utilizar a frecuencias elevadas, automáticamente surgen problemas de radiación de la energía electromagnética; para superar este inconveniente es necesario confirmar los campos electromagnéticos, lo que normalmente se efectúa por medio de contornos metálicos; así, los sistemas de transmisión usuales a microondas son, o bien líneas coaxiales, o bien, en general, guías de onda continuadas por conductores abiertos o tuberías.

La utilización en microondas, de las válvulas de vacío convencionales, como amplificadores osciladores, esta limitada, por una parte, por el tiempo de tránsito de los electrones en el interior de la válvula y, por otra, por las inductancias y por las capacidades asociadas al cableado y los electrodos de la misma.

- ✓ **Propiedades de las microondas**

La energía electromagnética reacciona de diferentes formas según el objeto con el que interactúa en la superficie de la Tierra, esta energía puede tomar tres caminos: ser reflejada, transmitida o absorbida.

Las microondas no se excluyen a estos comportamientos, pero su respuesta en los censores del radar dependerá de factores como (Chuvieco, 1996):

- Naturaleza del sustrato (suelo, vegetación, agua)
- Orientación de características topográficas (ángulo de incidencia)
- Aspereza superficial (rugosidad)
- Espesor de la cubierta superficial
- Contenido de agua del cuerpo
- Propiedades dieléctricas del cuerpo (condiciones dieléctricas)

Es importante observar que las reflexiones de las microondas por la superficie de la Tierra no se comportan como otras longitudes de ondas del espectro electromagnético. Las superficies que transmiten una señal fuerte y brillante en una imagen del radar pueden comportarse como una señal débil en el rango del infrarrojo y ser oscuras en una fotografía o en el espectro visible para imágenes de los satélites Landsat o SPOT.

- ✓ **Rugosidad**

El concepto de rugosidad se refiere a cuan áspero es la superficie de un cuerpo respecto al tamaño de la longitud de onda. Cuando las longitudes de onda corta inciden en una superficie llana, la respuesta de ésta en el radar se comportará como rugosa; la misma superficie aparecerá como lisa cuando incidan longitudes de onda mas largas. Esto quiere decir que a igual rugosidad de terreno, un cuerpo se comportará como un cuerpo liso con longitudes de ondas mas largas (Chuvieco, 1996).

De acuerdo a la rugosidad del terreno para una señal dada, la reflectividad de la señal será alta sobre superficies rugosas, dispersando la energía en todas direcciones. Sobre superficies lisas, caso del agua calma, la reflexión es especular y la señal de retorno al radar puede ser prácticamente nula.

En imágenes generadas por radares, las superficies ásperas aparecerán más brillantes que superficies más lisas del mismo material. La aspereza superficial influencia la reflectividad de la energía de la microonda.

Las superficies lisas horizontales que reflejan casi toda la energía de la incidencia lejos del radar se llaman los reflectores especulares, ejemplos de estas superficies, son el agua tranquila o caminos pavimentados que aparecen oscuras en las imágenes de radar. En cambio las superficies ásperas dispersan la energía de la microonda incidente en muchas direcciones, esto se conoce como reflexión difusa. Las superficies vegetales causan reflexión difusa y generan imágenes con un tono más brillante.

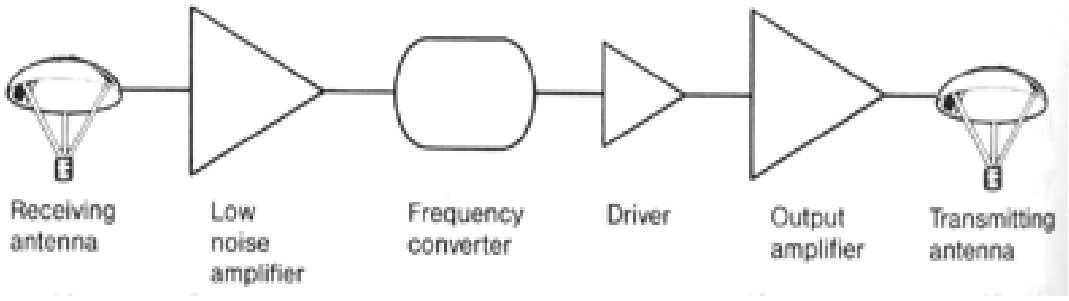
- ✓ **Comunicación Vía Microondas**

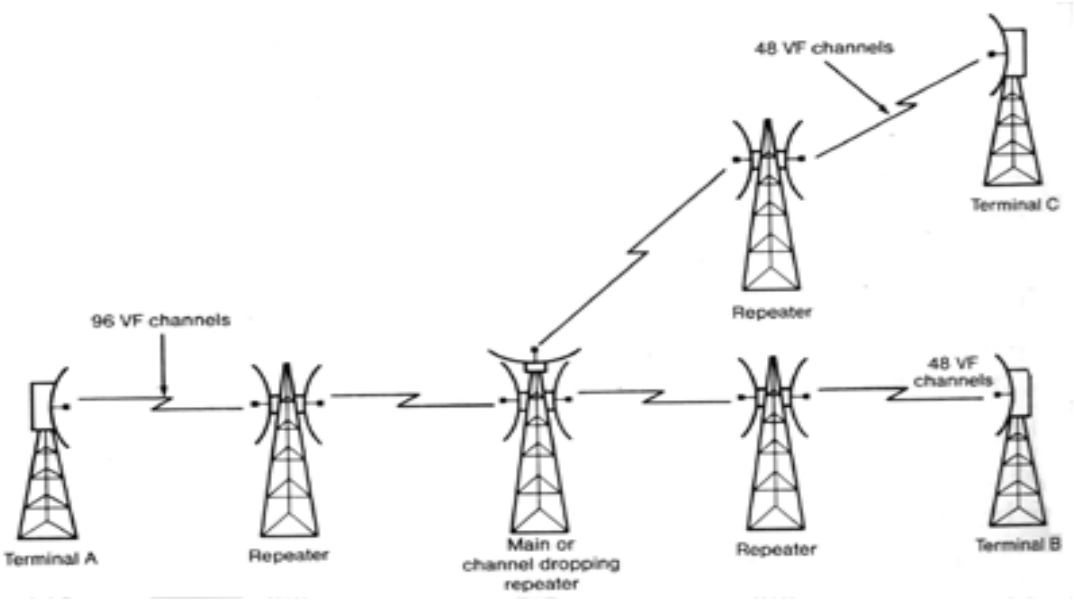
Básicamente un enlace vía microondas consiste en tres componentes fundamentales: El Transmisor, El receptor y El Canal Aéreo. El Transmisor es el responsable de modular una señal digital a la frecuencia utilizada para transmitir, El Canal Aéreo representa un camino abierto entre el transmisor y el receptor, y como es de esperarse el receptor es el encargado de capturar la señal transmitida y llevarla de nuevo a señal digital.

El factor limitante de la propagación de la señal en enlaces microondas es la distancia que se debe cubrir entre el transmisor y el receptor, además esta distancia debe ser libre de obstáculos. Otro aspecto que se debe señalar es que en estos enlaces, el camino entre el receptor y el transmisor debe tener una altura mínima sobre los obstáculos en la vía, para compensar este efecto se utilizan torres para ajustar dichas alturas.

- ✓ **Antenas Y Torres De Microondas**

La distancia cubierta por enlaces microondas puede ser incrementada por el uso de repetidoras, las cuales amplifican y redireccionan la señal, es importante destacar que los obstáculos de la señal pueden ser salvados a través de reflectores pasivos. Las siguientes figuras muestran como trabaja un repetidor y como se ven los reflectores pasivos.





La señal de microondas transmitidas es distorsionada y atenuada mientras viaja desde el transmisor hasta el receptor, estas atenuaciones y distorsiones son causadas por una perdida de poder dependiente a la distancia, reflexión y refracción debido a obstáculos y superficies reflectoras, y a pérdidas atmosféricas.

- ✓ **Generación De Microondas**

Quizás fue el MAGNETRON, como generador de m. De alta potencia, el dispositivo que dio pie al desarrollo a gran escala de las microondas, al abrir paso a la utilización de sistemas de radar durante la II Guerra Mundial; sin embargo, fueron KLYSTRONS, los que dieron una mayor versatilidad de utilización de las microondas, sobre todo en el campo de las comunicaciones, permitiendo además una mayor comprensión de los fenómenos que tiene en lugar los tubos de microondas.

El principio básico de funcionamiento de estos generadores es la modulación de velocidad de un haz electrónico que al atravesar una cavidad resonante, excita en ella oscilaciones electromagnéticas de la frecuencia de microondas deseada. El estudio de los KLYSTRONS obligó a un amplio desarrollo desde los fenómenos de carga espacial, la interpretación de la operación de los tubos.

Sin embargo, fue el desarrollo de otro tipo de válvulas, las de ONDA PROGRESIVA (TWT, Travelling-Wave Tube); siglas de ésta clase de tubos, las que dieron lugar a una mejor compresión de los fenómenos que tienen lugar en los haces electrónicos, sobre todo en lo que respecta a las ondas electromecánicas, daban lugar a amplificación o generación de microondas.

Para que este acoplamiento sea efectivo es preciso reducir la velocidad de fase de la onda electromagnética lo cual se hace mediante estructuras periódicas de entre las cuales la más utilizada es la hélice; de esta forma es posible mantener una iteración continuada entre la onda electromagnética y el haz electrónico, modulado en velocidad, y consecuentemente en densidad, que va cediendo su energía, digamos cinética, a la onda electromagnética. Posteriormente también se desarrollo el tubo de onda regresiva (BWO< Backward- wave oscillator), en el cual la velocidad de fase de la onda va en dirección opuesta al flujo de energía en el circuito.

Los dispositivos anteriores se basan en la conversión de energía de continuidad en la energía de microondas, mientras que los amplificadores paramétricos (AMPLIFICADOR, 8) utilizan como fuente de energía una de alterna que convierten, por un procedimiento de mezcla, en la de alta frecuencia deseada. En lugar de utilizar como elemento resistivo, utilizan un elemento reactivo, como puede ser un diodo de capacidad variable, y de aquí el bajo nivel de ruido que se puede lograr. Un fundamento análogo tienen los amplificadores cuánticos MASER. Son estos amplificadores de bajo nivel de ruido los que han abierto un gran campo de operación en radioastronomía, así como las intercontinentales vía satélite etc.

- ✓ **Transmisión De Microondas**

Un sistema en el que se utilizan localmente las microondas constará fundamentalmente de un generador y de un medio de transmisión de la onda hasta la carga; en caso contrario, tendremos necesidad de un sistema emisor y otro receptor, estando el emisor compuesto por los elementos anteriormente citados, donde la carga será una antena emisora, mientras que el receptor será otra antena, medio de transmisión y detector adecuado.

Además de estos elementos existirán otras componentes como pueden ser atenuadores, desfasadores, frecuencímetros, medidores de onda estacionaria, etc.

La guía de onda es esencia una tubería metálica, a través de la cual se propaga el campo electromagnético sin prácticamente atenuación, dependiendo esta del material de que la misma esté fabricada; así, a una frecuencia determinada, y para una geometría concreta, la atenuación será tanto menor cuanto mejor conductor sea el material.

A diferencia de lo que ocurre en el medio libre, en el que el haz de ondas electromagnéticas es mas o menos divergente y sus campos transversales electromagnéticos, en una guía el campo esta confinado en su interior, evitándose la radiación hacia el exterior, y sus campos ya no pueden ser TEM sino que han de hacer necesariamente del tipo TE (campo electrónico transversal a la dirección de propagación), o bien TM (campo magnético transversal) o bien híbridos, es decir, mezcla de TE y TM.

- ✓ **Microondas terrestres**

Suelen utilizarse antenas parabólicas. Para conexiones a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas.

Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.

La principal causa de pérdidas es la atenuación debido a que las pérdidas aumentan con el cuadrado de la distancia (con cable coaxial y par trenzado son logarítmicas). La atenuación aumenta con las lluvias.

Las interferencias es otro inconveniente de las microondas ya que al proliferar estos sistemas, pude haber más solapamientos de señales.

✓ **Microondas por satélite**

El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada.

Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario.

Se suele utilizar este sistema para:

- Difusión de televisión.
- Transmisión telefónica a larga distancia.
- Redes privadas.

El rango de frecuencias para la recepción del satélite debe ser diferente del rango al que este emite, para que no haya interferencias entre las señales que ascienden y las que descienden.

Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta que es devuelta al receptor o receptores, ha de tenerse cuidado con el control de errores y de flujo de la señal.

Las diferencias entre las ondas de radio y las microondas son:

- Las microondas son unidireccionales y las ondas de radio omnidireccionales.
- Las microondas son más sensibles a la atenuación producida por la lluvia.
- En las ondas de radio, al poder reflejarse estas ondas en el mar u otros objetos, pueden aparecer múltiples señales "hermanas".

1.3.3 Satélite

- ✓ **¿Que es un Satélite?**

El satélite de comunicaciones es un dispositivo que actúa principalmente como "reflector" de las emisiones terrenas. Es la extensión al espacio del concepto "torre de microondas". Al igual que éstas, los satélites reflejan un haz de microondas que transportan información codificada. Realmente, la función de reflexión se compone de un receptor y un emisor, que operan a diferentes frecuencias, recibe a 6 GHZ y envía a 4 GHZ, (por ejemplo).

Un satélite es un objeto lanzado a la órbita de los planetas. Hay satélites naturales como la luna, y satélites artificiales que hacen ciertos trabajos tales como enviar y recibir señales de televisión, de teléfono, de fax entre otros.

Se distinguen dos clases de satélites:

Satélites activos: Provistos de cámaras fotográficas y de televisión, detectores de radiaciones y de meteoritos, radio, fuentes de energía eléctrica, etc., equipo que depende de la función programada y del peso soportable.

Satélites pasivos: No llevan en su interior ningún instrumento de medida y sus movimientos son estudiados desde la tierra.

- ✓ **Sistemas satelitales**

Las comunicaciones vía satélite han sido una tecnología muy utilizada para proveer comunicaciones a áreas alejadas y de difícil acceso. Ante la escasa y en muchos casos nula infraestructura terrestre de comunicaciones en las zonas remotas, las comunicaciones vía satélite abren una ventana hacia al resto del mundo. Las comunicaciones satelitales permiten transmitir múltiples servicios de voz, datos y video a velocidades en el orden de Megabits por segundo. Las terminales satelitales hacen posible las comunicaciones donde otros medios no pueden penetrar por su alto costo.

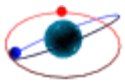
La introducción de pequeñas terminales conocidas como VSAT (Very Small Aperture Terminal) ha permitido que el costo de las comunicaciones vía satélite haya bajado drásticamente. VSAT es una tecnología de comunicaciones vía satélite que mediante el uso de antenas de satélite con diámetros pequeños, permiten comunicaciones altamente seguras entre una estación maestra y nodos dispersos geográficamente. Entre las aplicaciones típicas de este tipo de terminales se encuentra la telefonía rural, educación a distancia, redes privadas y acceso a Internet, entre otras.

Existen satélites de todo tipo, los hay geoestacionarios (GEO, Geostacionary Earth Orbit), aquellos que giran a una órbita natural a 36,000 Km. de la superficie de la tierra. Existen satélites en órbitas bajas (LEO, Low Earth Orbit)) y medias (MEO, Medium Earth Orbit) que dan varias vueltas a la tierra y que para cubrir casi toda la superficie están agrupados en constelaciones de satélites.

Los métodos de acceso al medio en comunicación trabajan de manera similar a la telefonía celular. Aunque en comunicaciones vía satélite SCPC / FDMA (Single Channel Per Carrier / FDMA) y TDMA son los métodos de acceso múltiple más populares para redes privadas con VSAT; otras variantes de TDMA como DAMA (Demand Asigment Multiple Access) y ALOHA son también utilizados en menos proporción. TDMA y CDMA son ampliamente usados para comunicaciones móviles por satélite por los satélites LEOs y MEOs.

- ✓ **Frecuencias De Bandas**

BANDAS DE FRECUENCIAS DE SATÉLITE			
Banda	**Rango de Frecuencias (GHz)**	**Servicio**	**Usos**
VHF	30-300 MHz	Fijo	Telemetría
UHF	300-1000 MHz	Móvil	Navegación, Militar
L	1 - 2	Móvil	Emisión de audio, radiolocalización.
S	2 - 4	Móvil	Navegación
C	4 - 8	Fijo	Voz, datos, video, Emisión de video
X	8 - 12	Fijo	Militar
Ku	12 - 18	Fijo	Voz, datos, video, Emisión de video.
K	18 - 27	Fijo	Emisión de video, com. Intersatélite
Ka	27 - 40	Fijo	Emisión de video, com. Intersatélite

✓ **Tipos De Órbitas Satelitales** 

Existen varios tipos de órbitas de los satélites artificiales los cuales se clasifican de acuerdo a:

Su distancia de la Tierra (geoestacionaria, geosíncrona, de baja altura, de media altura y excéntricas). Su plano orbital con respecto al Ecuador (ecuatorial, inclinada y polar). La trayectoria orbital que describen (circular y elíptica).

Órbita Geosincrona: Es una órbita circular con un periodo de un día sideral. Para tener este periodo la órbita debe tener un radio de 42,164.2 Km. (desde el centro de la tierra).

Órbita Geoestacionaria (GEO): Este tipo de órbita posee las mismas propiedades que la geosíncrona, pero debe de tener una inclinación de cero grados respecto al ecuador y viajar en la misma dirección en la cual rota la tierra. Un satélite geoestacionario aparenta estar en la misma posición relativa a algún punto sobre la superficie de la Tierra, lo que lo hace muy atractivo para las comunicaciones a gran distancia.

Órbita de Baja Altura (LEO): Estas órbitas se encuentran en el rango de 640 Km a 1,600 Km entre las llamadas región de densidad atmosférica constante y la región de los cinturones de Van Allen. Los satélites de órbita baja circular son muy usados en sistemas de comunicaciones móviles.

Órbitas de Media Altura: Son las que van desde 9,600 Km hasta la altura de los satélites geosíncronos. Los satélites de órbita media son muy usados también en las comunicaciones móviles.

Órbita Ecuatorial: En este tipo de órbita la trayectoria del satélite sigue un plano paralelo al ecuador, es decir tiene una inclinación de 0.

Órbitas Inclinada: En este curso la trayectoria del satélite sigue un plano con un cierto ángulo de inclinación respecto al ecuador.

Órbitas Polar: En esta órbita el satélite sigue un plano paralelo al eje de rotación de la tierra pasando sobre los polos y perpendicular la ecuador.

Órbitas circulares: Se dice que un satélite posee una órbita circular si su movimiento alrededor de la tierra es precisamente una trayectoria circular. Este tipo de órbita es la que usan los satélites geosíncronos.

Órbitas elípticas (Monlniya): Se dice que un satélite posee una órbita elíptica si su movimiento alrededor de la tierra es precisamente una trayectoria elíptica. Este tipo de órbita posee un perigeo y un apogeo.

- ✓ **Componentes De Un Satélite**

Los satélites de comunicaciones emplean antenas en la frecuencia de microondas para recibir señales de radio procedentes de las estaciones transmisoras; esas señales son repetidas de vuelta a otras estaciones en tierra. El satélite actúa como una estación repetidora. La estación A transmite señales de una frecuencia específica; (enlace ascendente) al satélite. El satélite, a su vez, recibe las señales y las retransmite hacia la estación terrestre B a la frecuencia del enlace descendente. La señal transmitida por el enlace descendente puede ser recibida por cualquier estación que esté dentro de la zona de cobertura. Las señales pueden ser: voz, imágenes, transmisiones de datos o señales de televisión. La capacidad de los satélites para transmitir y recibir se consigue gracias a un dispositivo denominado transpondedor. Los transpondedores de los satélites operan a frecuencias muy altas, generalmente del orden de Gigaherzios.

La mayoría de los satélites actuales emplean frecuencias en el rango de 6/4 gigaherzios. Otros satélites utilizan un ancho de banda mayor, y sus transpondedores operan en el rango de 14/12 gigaherzios.

- ✓ **Clasificación De Los Satélites Dependiendo De La Altura**

Satélites GEO

Los satélites GEO son útiles en comunicaciones locales. Ubicados sobre zona ecuatorial a una altura de 35.786 Km. Con la tecnología actual se pueden tener satélites espaciados cada 2 grados en los 360 totales del plano ecuatorial, sin presentar interferencia, por lo tanto pueden haber 360/2 = 180 satélites de comunicaciones geoestacionarios a la vez.

Tres de estos satélites pueden cubrir el globo con excepción a ciertas partes cerca de los polos norte y sur. Si se ponen estos satélites encima del ecuador y siguen la dirección de la rotación de la Tierra, parecen estar en la misma situación todo el tiempo.

Satélites MEO

Satélites de las comunicaciones encima del polo norte y polo sur están en órbita elemento. Los Receptores de la tierra rastrean estos satélites y desde sus órbitas son más grandes que LEO tienen que quedar dentro de rango de los receptores por un período del tiempo más largo.

MEO, satélites ubicados alrededor de los 10.000 Km sobre la tierra, empleados generalmente en funciones de ubicación como localización automática de móviles LAM.

Satélites LEO

LEO, satélites de muy baja órbita, del orden de cientos de Km, operando en la banda de 1 Ghz. El proyecto IRIDIUM (Motorola) pertenece a este grupo.

Un satélite en baja órbita de la Tierra rodea 100 a 300 millas sobre las Tierra. Desde está así cerca de la Tierra, el satélite debe viajar a velocidades muy rápidas, a veces a aproximadamente 17. 500 millas por hora. Toman sobre una hora y una mitad a órbita la tierra.

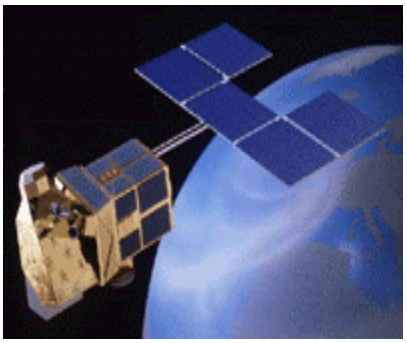
Satélites naturales

La Luna es el satélite de la Tierra, si bien la Luna y la Tierra tienen un tamaño tan similar que se las puede considerar en algunos momentos como un sistema de dos planetas.

El movimiento de la mayor parte de los satélites conocidos del Sistema Solar alrededor de sus planetas es directo, es decir, de oeste a este y en la misma dirección que giran sus planetas. Solamente ciertos satélites de grandes planetas

exteriores giran en sentido inverso, es decir, de este a oeste y en dirección contraria a la de sus planetas; probablemente fueron capturados por los campos gravitatorios de los planetas algún tiempo después de la formación del Sistema Solar.

- ✓ **¿Qué es un satélite artificial?**



El satélite artificial es una de las herramientas más útiles creadas por el hombre. Posibilita observar y controlar nuestro planeta y mirar al Cosmos sin la interposición de la atmósfera. Se entiende por satélite artificial a cualquiera de los objetos puestos en órbita alrededor de la Tierra. Los objetivos son variados y van desde los fines científicos, tecnológicos a los militares.

Un satélite artificial es un objeto no tripulado puesto en órbita alrededor de la Tierra, quedando fuera de esta definición los cohetes lanzadores como las cápsulas tripuladas o de carga, los transbordadores espaciales y las estaciones orbitales.

Tampoco son considerados satélites artificiales las sondas espaciales enviadas a cualquier otro destino del Sistema Solar.

- ✓ **En la actualidad hay satélites de:**

Observación. Para la recolección, procesamiento y transmisión de datos de y hacia la Tierra.

Comunicaciones: utilizados para la comunicación telefónica y la transmisión de datos digitales e imágenes de televisión. Para la transmisión, distribución y diseminación de la información desde diversas ubicaciones en la Tierra a otras distintas posiciones.

Navegación: permiten determinar posiciones en el mar con un error límite de menos de 10 m, y también ayudan a la navegación en la localización de hielos y trazado de corrientes oceánicas.

Meteorológicos: fotografían la Tierra y proporcionan datos a las estaciones meteorológicas para la predicción de las condiciones atmosféricas de todo el mundo.

Estudio de recursos terrestres y científicos: se utilizan para estudiar la alta atmósfera, el firmamento, o para probar alguna ley física.

Satélite militar

Militares. Son aquellos que apoyan las operaciones militares de ciertos países, bajo la premisa de su seguridad nacional. La magnitud de sus programas espaciales militares es tan grande y secreta que hasta hace poco sólo se podía valorar por el número de lanzamientos que suponía.

Alimentación de los Satélites Artificiales

Los satélites artificiales se alimentan mediante células solares por medio baterías que se cargan con ellas y, en algunos casos, reciben la energía de generadores nucleares, en los que el calor producido por la desintegración de los radioisótopos se convierte en energía eléctrica.

Los satélites están equipados con transmisores de radio para enviar datos, con radiorreceptores y circuitos electrónicos de almacenamiento de datos, y con equipos de control como sistemas de radar y de guía para el seguimiento de estrellas. Los satélites se colocan en órbita mediante cohetes de etapas múltiples denominados lanzadores.

Los satélites pueden dividirse de manera conveniente en dos elementos principales, la carga útil y la plataforma. La carga útil es la razón de ser del satélite, es aquella parte del satélite que recibe, amplifica y retransmite las señales con información útil; pero para que la carga útil realice su función, la plataforma debe proporcionar ciertos recursos:

- La carga útil debe estar orientada en la dirección correcta.
- La carga útil debe ser operable y confiable sobre cierto periodo de tiempo especificado.
- Los datos y estados de la carga útil y elementos que conforman la plataforma deben ser enviados a la estación terrestre para su análisis y mantenimiento.
- La órbita del satélite debe ser controlada en sus parámetros.
- La carga útil debe de mantenerse fija a la plataforma en la cual está montada.
- Una fuente de energía debe estar disponible, para permitir la realización de las funciones programadas.

- Cada uno de estos requerimientos es proporcionado por los siguientes conglomerados de elementos conocidos como subsistemas:

Subsistema de Estructura, misma que puede tener muy distintas formas, pero que siempre se construye con metales muy ligeros que a la vez tienen gran resistencia.

Subsistema de Propulsión, compuesto por múltiples motores o impulsores de bajo empuje, que sirven al satélite para realizar pequeñas correcciones y cambios de velocidad para controlar su orientación en el espacio y proporcionar el control adecuado de los parámetros de la órbita.

Subsistema de control de orientación, que trabaja contra las perturbaciones a las que está sometido el aparato, como el viento solar. Este sistema permite al satélite saber constantemente donde está y hacia donde debe orientarse para emisiones lleguen a la zona deseada, considerando su natural movimiento Norte-Sur y Este-Oeste alrededor de un punto. Además, orienta los paneles solares hacia el Sol, sin importar cómo esté posicionado el satélite. La computadora de a bordo, que lleva una serie de programas capaces de reaccionar ante una variada gama de problemas.

Subsistema de potencia. Como fuente de energía secundaria, las baterías proveen energía suficiente para alimentar a los sistemas e instrumentos cuando la energía proveniente del Sol no puede ser aprovechada, esto ocurre por ejemplo, durante eclipses; éstas son cargadas poco antes del lanzamiento y de ellas depende la vida del satélite. La fuente primaria de energía para el satélite lo constituyen las celdas solares que son colocadas en grupos para conformar lo que se conoce como panel solar Los paneles, por sus grandes dimensiones y su relativa fragilidad, deben permanecer plegados durante el despegue. Su apertura añade otro factor de incertidumbre durante la puesta en órbita del satélite. Una vez en posición y perfectamente orientados, empiezan a proporcionar energía a los sistemas, que hasta entonces han debido usar baterías.

Esta energía es administrada por un sistema especial que regula el voltaje y la distribuye de forma adecuada al resto de componentes. Cuanto mayor es el número de celdas agrupadas, más potencia puede generarse. Aunque es verdad que éstas suelen deteriorarse con el paso del tiempo, ahora los constructores de satélites colocan un número suplementario de ellas para garantizar que proporcionarán suficiente electricidad, incluso, durante el último periodo de su vida útil.

Subsistema de telemetría, seguimiento y órdenes es el encargado de hacer contacto con las estaciones terrenas con el fin de recibir órdenes de ellas y darles seguimiento. Esto permite el correcto mantenimiento de los subsistemas del satélite.

El módulo de carga útil es aquel en que están instalados los instrumentos que justifican la misión espacial. Algunos de ellos son muy sofisticados: podemos encontrar desde cámaras hasta telescopios, pasando por detectores sensibles a fenómenos atmosféricos, antenas y amplificadores para comunicaciones, entre otros. Para los satélites de comunicaciones, la carga útil esta conformada por los transpondedores.

Un transpondedor esta formado por un filtro de entrada que selecciona la frecuencia a amplificar, un controlador de ganancia para el amplificador y su respectiva fuente de alimentación, estos transpondedores reciben la señal desde la Tierra a través de antenas y receptores, la amplifican y la envían a su destinatario; si el satélite no hace esto, la señal llegará tan débil que no se percibirá en las estaciones receptoras.

Aunque el satélite es sometido a pruebas exhaustivas durante su construcción y antes de su lanzamiento, siempre es probable que algo falle y esto, entonces, significa afrontar pérdidas considerables; es por ello que desde hace algunos años los propietarios de los satélites suelen adquirir pólizas de seguro que cubran las principales eventualidades (lanzamiento fallido, menor eficiencia de la prevista en órbita, duración en activo inferior a la prevista, etcétera).

- ✓ **Como funcionan los satélites**

Dado que las microondas viajan en línea recta, como un fino rayo a la velocidad de la luz, no debe haber obstáculos entre las estaciones receptoras y emisoras. Por la curvatura de la Tierra, las estaciones localizadas en lados opuestos del globo no pueden conectarse directamente, sino que han de hacerlo vía satélite.

Un satélite situado en la órbita geoestacionaria (a una altitud de 36 mil Km) tarda aproximadamente 24 horas en dar la vuelta al planeta, lo mismo que tarda éste en dar una vuelta sobre su eje, de ahí que el satélite permanezca más o menos sobre la misma parte del mundo.

Como queda a su vista un tercio de la Tierra, pueden comunicarse con él las estaciones terrenas -receptoras y transmisoras de microondas- que se encuentran en ese tercio. Entonces, ¿cómo se conectan vía satélite dos lugares distantes?

Una estación terrena que está bajo la cobertura de un satélite le envía una señal de microondas, denominada enlace ascendente. Cuando la recibe, el transpondedor (*aparato emisor-receptor*) del satélite simplemente la retransmite a una frecuencia más baja para que la capture otra estación, esto es un enlace descendente. El camino que recorre esa comunicación, equiparándolo con la longitud que ocuparía un cable, es de unos 70 mil Km, lo cual equivale, más o menos, al doble de la circunferencia de la Tierra, y sólo le toma alrededor de 1/4 de segundo cubrir dicha distancia.

1.3.4 Infrarrojo

Los infrarrojos son ondas electromagnéticas que se propagan en línea recta, siendo susceptibles de ser interrumpidas por cuerpos opacos. Su uso no precisa licencias administrativas y no se ve afectado por interferencias radioeléctricas externas, pudiendo alcanzar distancias de hasta 200 metros entre cada emisor y receptor.

Los Infrarrojos son emisiones de energía en forma de ondas electromagnéticas en la zona del espectro situada inmediatamente después de la zona roja de la radiación visible. La longitud de onda de los rayos infrarrojos es menor que las ondas de radio y mayor que la luz visible, oscila entre aproximadamente 10-6 y 10-3 metros. la radiación infrarroja pude detectarse como calor, para lo que se emplean instrumentos como el bolómetro. Los rayos infrarrojos se utilizan para obtener imágenes de objetos lejanos ocultos por la bruma atmosférica.

En el campo de las comunicaciones infrarrojas (IR) el control esta basado en un par de microcontroladores cuyo algoritmo es capaz de crear una portadora respetando un protocolo de transmisión serial de datos todo al mismo tiempo con solo un par de Leds IR y un par de detectores.

Se maneja un protocolo el cual evita que sean alterados los datos mediante una encriptación, no interfiriendo a ser interferido por otros sistemas IR.

En los medios de comunicación infrarroja, se emplea la emisión infrarroja proveniente de alguna fuente, en este caso un diodo emisor infrarrojo, la cual por medios electrónicos es modulada, de una manera tal que permita viajar y ser recibida por un elemento sensible a esta radiación y ser nuevamente convertida en una señal electrónica inteligible.

- ✓ **Tecnología Infrarroja**

La Tecnología infrarroja opera en la banda de 300,000 GHz pero su uso es más limitado que *Spread Spectrum*, ya que una transmisión infrarroja requiere de una línea-visual directa entre los aparatos que están realizando la transmisión, este tipo de implementación es utilizado por controles de televisión y Videos.

- ✓ **Puerto Infrarrojo**

Los usuarios de ordenadores portátiles conocen bien el hecho de que el equipo siempre debe ir acompañado de una bolsa conteniendo cables, fuente de alimentación, periféricos diversos, etc. Conscientes de ello, los fabricantes de hardware han elaborado una serie de estándares y protocolos para la comunicación inalámbrica mediante dispositivos infrarrojos.

Es el conocido estándar IrDA (siglas de InfraRed Data Association). IrDA es un estándar para la conexión de equipos informáticos mediante dispositivos infrarrojos.

Por otro lado existen en el domicilio multitud de aparatos que van acompañados de su correspondiente control remoto. El usuario suele buscar la posibilidad de un control remoto único para todos los equipos, en lugar de tener que usar el adecuado para cada equipo. Por supuesto se plantea la posibilidad de controlar los equipos desde el ordenador, simulando el control remoto.

- ✓ **Características Del Infrarrojo**

La tecnología infrarroja tiene muchas aplicaciones interesantes y útiles. En el campo de la astronomía infrarroja se están realizando nuevos y fascinantes descubrimientos sobre el universo. En medicina, la radiación infrarroja es una herramienta de diagnóstico muy útil. Las cámaras fotográficas infrarrojas son utilizadas en actividades policiales y de seguridad, así como en aplicaciones militares y de lucha contra incendios. Las imágenes infrarrojas se emplean para detectar pérdidas de calor en edificios y probar sistemas electrónicos. Los satélites infrarrojos monitorean el clima terrestre, estudian modelos de vegetación, llevan a cabo en estudios geológicos y miden las temperaturas oceánicas.

Nuestros ojos son detectores que han ido evolucionando para detectar ondas de luz visible. La luz visible es uno de los pocos tipos de radiación que puede penetrar nuestra atmósfera y que es posible detectar desde la superficie de la Tierra. Existen otros tipos de luz (o radiación) que no podemos ver. De hecho, solamente se puede ver una parte muy pequeña de toda la gama de radiación llamada espectro electromagnético. El espectro electromagnético incluye los rayos gamma, los rayos X, los rayos ultravioletas, la luz visible, los rayos infrarrojos, las microondas y las ondas de radio. La única diferencia entre estos distintos tipos de radiación es su longitud de onda y su frecuencia.

A medida que pasamos de los rayos gamma a las ondas de radio, la longitud de onda aumenta y la frecuencia disminuye (también disminuyen la energía y la temperatura). Todos estos tipos de radiación viajan a la velocidad de la luz (300.000 Km/s en el espacio vacío). Además de la luz visible, también llegan a la superficie de la tierra desde el espacio ondas radio, una parte del espectro infrarrojo y una parte muy pequeña de radiación ultravioleta. Afortunadamente, nuestra atmósfera bloquea el resto de la radiación, la cual es muy peligrosa y hasta mortal para las formas de vida en la Tierra.

Dentro del espectro electromagnético, la radiación infrarroja se encuentra comprendida entre el espectro visible y las microondas. Las ondas infrarrojas tienen longitudes de onda más largas que la luz visible, pero más cortas que las microondas; sus frecuencias son menores que las frecuencias de la luz visible y mayores que las frecuencias de las microondas. El término infrarrojo cercano se refiere a la parte del espectro infrarrojo que se encuentra más próxima a la luz visible; el término infrarrojo lejano denomina la sección más cercana a la región de las microondas.

La fuente primaria de la radiación infrarroja es el calor o radiación térmica. Cualquier objeto que tenga una temperatura superior al cero absoluto (-273,15 °C, o 0 grados Kelvin), irradia ondas en la banda infrarroja. Incluso los objetos que consideramos muy fríos —por ejemplo, un trozo de hielo—, emiten en el infrarrojo.

Cuando un objeto no es suficientemente caliente para irradiar ondas en el espectro visible, emite la mayoría de su energía como ondas infrarrojas. A la temperatura normal del cuerpo, la mayoría de las personas irradian más intensamente en el infrarrojo, con una longitud de onda de 10 micrones.

Sentimos los efectos de la radiación infrarroja cada día. El calor de la luz del sol, del fuego, de un radiador de calefacción o de una acera caliente proviene del infrarrojo.

Aunque no podemos ver esta radiación, los nervios en nuestra piel pueden sentirla como calor. Las terminaciones nerviosas de la piel son sensibles a la temperatura y pueden detectar la diferencia entre la temperatura interior del cuerpo y la temperatura exterior de la piel. También utilizamos rayos infrarrojos cuando usamos una unidad de control remoto de un televisor.

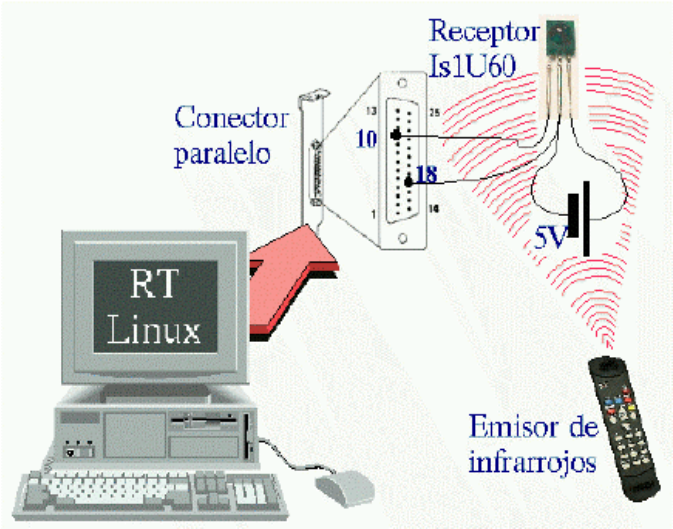
- ✓ **Redes Infrarrojas**

Las ondas infrarrojas se usan para comunicaciones de corto alcance no atraviesan los objetos sólidos lo cual ofrece una ventaja de no interferencia. Además, la seguridad de los sistemas infrarrojos contra espionaje es mejor que la de los sistemas de radio, no es necesario obtener licencia del gobierno para operar un sistema infrarrojo.

Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso, algunas compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores / emisores en las ventanas de los edificios.

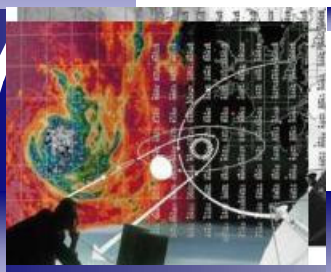
El principio de la comunicación de datos es una tecnología que se ha estudiado desde los 70´s, Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar.

El mismo principio se usa para la comunicación de Redes, se utiliza un "transreceptor" que envía un haz de Luz Infrarroja, hacia otro que la recibe. La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente. Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un "Transreceptor Infrarrojo". Los primeros transreceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transreceptor recibía la señal. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transreceptor.



InfraLAN es una red basada en infrarrojos compatible con las redes Token Ring a 4Mbps, pudiendo utilizarse independientemente o combinada con una red de área local convencional.

Capitulo II



Red Inalámbrica

II. RED INALÁMBRICA

✓ Que son las Redes inalámbricas.?

Una red de computadoras local inalámbrica es un sistema de comunicación de datos que utiliza tecnología de radiofrecuencia. En esta red se transmite y recibe datos sobre aire, minimizando la necesidad de conexiones alámbricas, es decir, combinan la conectividad de datos son la movilidad de usuarios.

Algunas ventajas productivas de su utilización son:

Instalación Flexible

Al reducir la necesidad de instalar cables, la red aumenta sus posibilidades de cobertura.

Movilidad

El usuario captura datos y accede a la información en tiempo real, lo cual apoya la productividad y posibilidades de respuesta inmediata en el proceso.

Escalabilidad

Pueden haber variedad en configuraciones para cubrir las necesidades de instalación y aplicaciones específicas.

Existen dos amplias categorías de Redes Inalámbricas:

De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN).

De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares.

La otra opción que existe en redes de larga distancia son las denominadas: *Red Pública De Conmutación De Paquetes Por Radio*. Estas redes no tienen problemas de pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en lugar de comunicaciones de voz.

Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radio frecuencia restringidas por la propia organización de sus sistemas de cómputo.

2.1 Equipos

2.1.1 Puntos de Acceso (Access Point)

Un Access Point (Punto de Acceso) es un Bridge a Nivel MAC (transparent media Access control -MAC-) que provee acceso a estaciones Inalámbricas hacia redes de área local cableadas. Por intermedio de estos dispositivos, las estaciones Inalámbricas pueden integrarse rápida y fácilmente a cualquier red cableada existente. Se puede denominar también como una Estación base o "base station" que conecta una red cableada con uno o más dispositivos inalámbricos.

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

El punto de acceso proporciona una "conexión" transparente a dispositivos los inalámbricos que estén dentro de su cobertura. Permite agregar fácilmente y de una manera rápida otros dispositivos inalámbricos que amplían su cobertura y su operabilidad. Permite que una red LAN convencional sea ampliada a zonas inaccesibles. Al evitar el cableado, los Puntos de Acceso (AP) ofrecen movilidad y diferenciación con respecto a las redes convencionales.

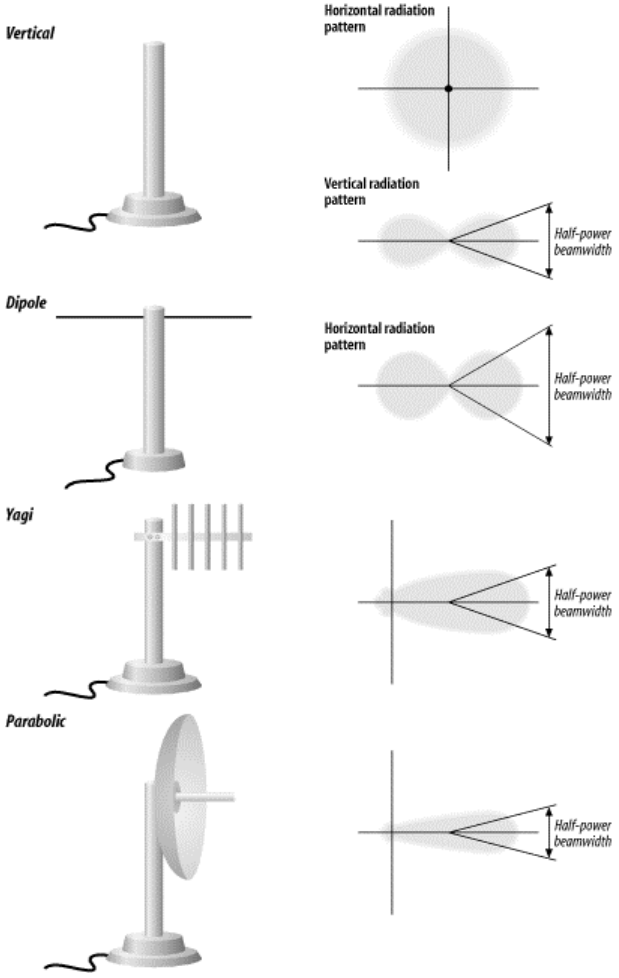
Para hacer una red inalámbrica no es preciso un punto de acceso, pues, al igual que en otro tipo de redes, se puede hacer una red inalámbrica del tipo "Peer-To-Peer", es decir, sin un acceso centralizado. Cuando una red inalámbrica 802.11 funciona en modo "Peer-to-peer", los usuarios inalámbricos se pueden ver entre si, pero no pueden ver a los usuarios conectados a la red alámbrica (si los hubiese). En una red "Peer-to-peer", al no ser centralizada, todo el tráfico de la red pasa por todas las tarjetas, en vez del propiamente destinado a la misma.

Los puntos de acceso tienen la ventaja exclusivas de actuar como repetidores, es decir, coger la señal de otro punto de acceso y repetirla, ampliando así el área de cobertura. Los puntos de acceso tienen otra importante propiedad, se les puede conectar una antena opcional para aumentar la cobertura inalámbrica hasta más de 5 Km

2.1.2 Antenas

Las antenas son dispositivos utilizados para recoger o radiar ondas electromagnéticas. Aumentan la zona de influencia / cobertura de nuestras tarjetas inalámbricas, de manera que en lugar de dar cobertura a unos pocos metros, podemos alcanzar cientos de metros sin problemas.

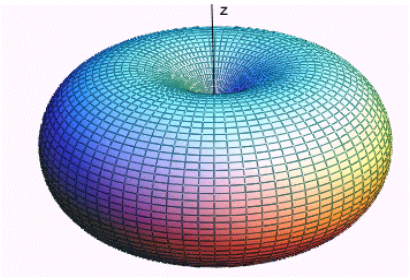
Se han realizado pruebas de campo y se han establecido comunicación entre dispositivos inalámbricos a más de 70 Km. (con antenas parabólicas de alta ganancia).

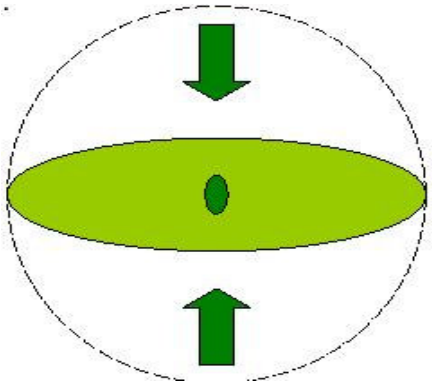


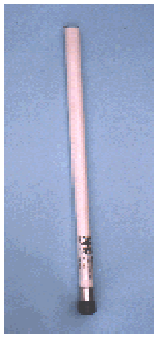
Básicamente disponemos de dos tipos:

- ✓ **Omnidireccionales:**

También llamadas sistemas basados en espectros dispersos o extendidos (spread spectrum), al contrario que las direccionales, el diagrama de radiación de la antena es disperso, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas. Se supone que dan servicio por igual independientemente de su colocación, pero debido a que las frecuencias en las que estamos trabajando son próximas a microondas, los diagramas no son circulares, son óvalos. Suelen ser una simple varilla vertical.

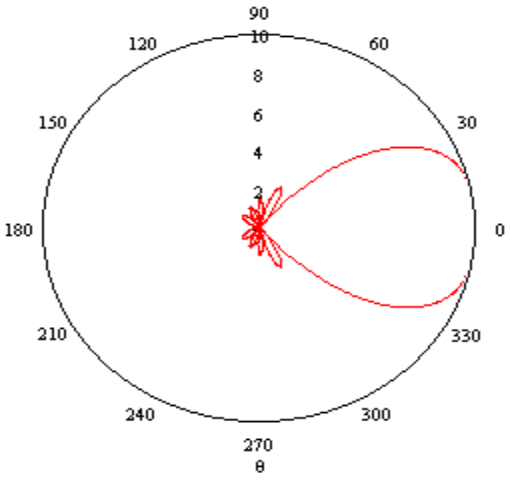






Antena Colineal

- ✓ **Direccionales:**



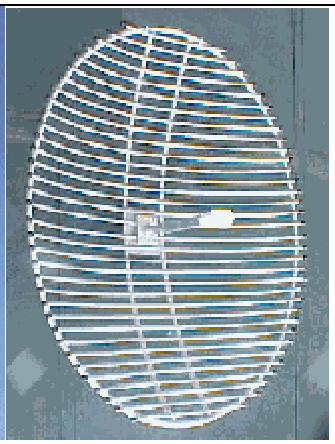
También llamada sistema de banda angosta (narrow band) o de frecuencia dedicada, Son directivas y solo emiten / reciben la energía electromagnética con un ancho de haz definido por la construcción de la antena, por tanto en este caso las antenas de emisión y recepción deben estar perfectamente alineadas. Las direccionales emiten la señal hacia un punto en concreto, con mayor o menor precisión. Dentro del grupo de antenas direccionales, existen las de Rejilla o Grid, las Yagi, las parabólicas, las "Pringles" y las de Panel.

Para que la transmisión pueda ser enviada en una dirección especifica, debemos tener en cuenta la frecuencia, la cual debe ser mucho mayor que la utilizada en transmisiones omnidireccionales.

Antena Direccional de rejilla o parabólica: Es la típica antena para establecer enlaces punto a punto o para conectar a un nodo. Se caracterizan por su alta ganancia, que va desde unos discretos 15dBi, llegando en los modelos superiores hasta los 24dBi. Cuanta más alta es la ganancia de este tipo de antenas, más alta es su direccionalidad, ya que se reduce muchísimo el ángulo en el que irradian la señal, llegando a ser tan estrechos como 8º de apertura.

Antena Direccional tipo Patch Panel: Con estas antenas se consigue crear pequeñas zonas de cobertura, tanto como recintos, estaciones de metro y similares, consiguiendo con varias de ellas establecer 'células' (como en telefonía móvil). Otra utilidad puede darse para sustituir una antena omnidireccional, tras la cual pudiera encontrarse un edificio u otra estructura que impidiera que la señal se propagase, poniendo varias de ellas para cubrir la zona deseada y no desperdiciar señal.

A esta unión de antenas se las llama 'Array'. Normalmente la anchura del haz que irradian estas antenas es de 25º tanto en vertical como en horizontal.

Yagui	Parábola
	 

Hay que decir que cuanta más alta sea la ganancia de la antena, mayores distancias podremos cubrir con una antena, y con mejor calidad podremos captar señales que pudieran llegarnos muy débilmente.

2.1.3 Tarjetas de Red

- ✓ **CPE**

(Customer Premise Equipment / Tarjeta de acceso a la red inalámbrica)

Es el dispositivo que se instala del lado del usuario inalámbrico de esa red (LAN). Así como las tradicionales placas de red que se instalan en un PC para acceder a una red LAN cableada, las Tarjetas dialogan con Access Point (AP) quien hace de punto de acceso a la red cableada.

Las más conocidas son las que vienen en formato PCMCIA, para portátiles, aunque también las hay en formato PCI (PC normal), en CompactFlash, Smart Card y similares. Son equivalentes a una tarjeta de red normal, sólo que sin cables. Su configuración a nivel de IP es EXACTAMENTE igual que una Ethernet.

Las diferencias más importantes entre una Red Inalámbrica y una Ethernet, (a parte de que las primeras no llevan cable...) son: El cifrado de datos, el ESSID, el Canal, y el ajuste de velocidad.

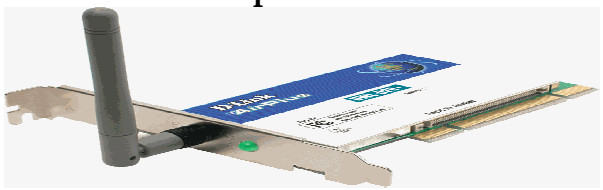
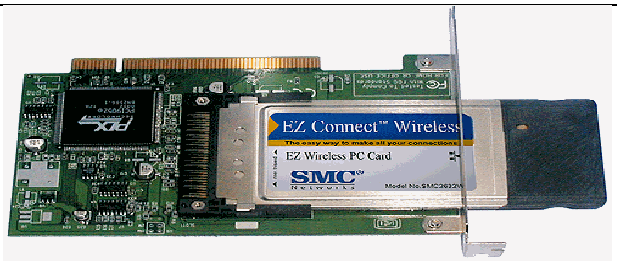
Las tarjetas de Red inalámbricas pueden ser de distintos modelos en función de la conexión necesaria a la computadora.

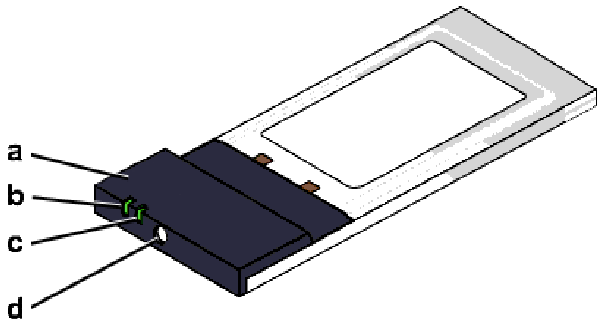
- **Tarjeta de Red inalámbrica USB**

Cuando la conexión a la computadora se realiza del puerto USB de la misma. Suelen utilizar estos adaptadores cuando se desea una conexión externa fácilmente desconectable o portable.

- **Tarjeta de Red inalámbrica PCI**

Cuando las conexiones a la computadora se realiza de su slot interno PCI. Suelen utilizarse estos adaptadores cuando se desea que la instalación dentro del PC. Cuando la conexión a la computadora se realiza a través de su slot PCMCIA. Suelen ser el caso más habitual en PC portátiles.

Tarjetas PCMCIA para portátiles:	**Tarjetas PCI para PCs de sobremesa:**
	**Con antena incorporada:** 
	 **PCMCIA con adaptador PCI: 13 dBm**



a – Antena integrada

b – Led de actividad

c – Led de power

d– Conector antena exterior *(utilizando un Pig Tail)*

2.1.4 Otros

- ✓ **El Pigtail**

El Pigtail, o rabo de cerdo (menudo nombre), no es más que un pequeño cable, que sirve de adaptación entre la tarjeta WIFI y la antena o el cable que vaya hacia la antena. Este Pigtail tiene 2 conectadores: 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 es una cosa estándar, aunque es verdad que el más conocido es el compatible con las tarjetas AVAYA y ORINOCO. El uso de este cable es imprescindible para conectar una antena a la tarjeta, salvo en algunos modelos de antenas diseñadas expresamente para usar en interiores, que ya vienen con ese conector de serie.

- ✓ **Lightning Arrestor**

Dispositivo que en caso de descarga electriza sobre la antena (por un rayo normalmente), desvía la descarga a una toma de tierra.

Es importante conectar uno de estos dispositivos en el cable de la antena para proteger a la tarjeta (y al equipo) de la posible descarga de un rayo (sobre todo en zonas donde son frecuentes tormentas eléctricas y no tengamos algún pararrayos cercano).

- ✓ **Amplificador [Amplifier]**

Un amplificador es un dispositivo electrónico que aumenta la fuerza de la señal, para lograr más alcance en una conexión. Los problemas se que tienen al conectar un amplificador para equipos inalámbricos:

- Las comunicaciones inalámbricas son Half Duplex, eso quiere decir que los dispositivos no emiten y reciben simultáneamente, sino que se van alternando. El Amplificador debe detectar cuando envía y cuando recibe la tarjeta o Punto de Acceso, y realizar el cambio automáticamente, un retraso en este cambio podría descompensar la comunicación e incluso dañar la tarjeta WiFi.

- El amplificador lo que hace es aumentar tanto la señal como el ruido que pueda tener, y sobre todo aumenta la fuerza de la señal al enviar, al recibir normalmente lo que se consigue es avivar un poco la recepción. De manera que si se quiere establecer una conexión punto a punto habría que colocar amplificadores en los dos extremos, de lo contrario, las emisiones de uno llegarían al otro pero no al revez.

- La ubicación del amplificador debe ser muy próxima a la antena, esto conlleva a tener que meter otro cable de alimentación para el amplificador, a no ser que se tenga una nota de corriente cerca.

Siempre es recomendable que para aumentar el alcance, que se empleen sobre todo antenas de mayor ganancia, cables y conectores con menor perdida de señal y usar antenas lo más direccionales posible. Es mejor invertir en un nodo intermedio antes que en un amplificador.

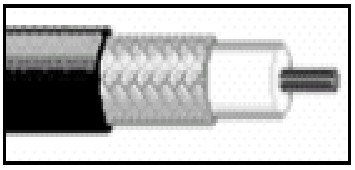
- ✓ **Sniffer**

Es un programa que permite almacenar el tráfico de una Red bajo TCP/IP. Identificando lo que sucede en las diversas actividades que manejan información como lo son aplicaciones internas de red o correo o navegación o FTP o chat, nombres de usuarios, contraseñas etc.

- ✓ **Spectrum Analyzer**

Un analizador de espectro que convierte una señal del dominio de tiempo en el dominio de frecuencias y el analizador TRF es el tipo más común el día de hoy.

- ✓ **Los cables**



Son un factor crítico a la hora de montar una estación cliente o un nodo. Los cables, todos, tienen pérdidas, sólo que unos tienen más que otros. Del cable depende que la señal llegue correctamente desde la tarjeta a la antena, y viceversa, y es recomendable usar siempre el mínimo cable posible, independientemente de que el cable sea muy bueno. ¿Por qué?, Evidentemente cuanto menos cable use, menores pérdidas de señal habrá.

- ✓ **Los Conectores**

Básicamente se van a usar los conectores N para las antenas (salvo marcas raras), tanto en macho como hembra. Son conectores relativamente fáciles de localizar, y de ellos depende la calidad de un buen enlace. Una mala soldadura, un conector de baja calidad, puede introducir una cantidad importante de pérdidas que hagan imposible establecer un enlace. Recuerda que los conectores también tienen pérdidas, no por el conector en sí, sino por el enlace entre el cable y el conector: el estaño, mala sujeción, mala calidad de ambos, etc.

2.2 Estándares de Comunicación

802.11

Hoy en día existen varias tecnologías y estándares para las comunicaciones de redes de área local inalámbricas. En este artículo nos centraremos en los estándares 802.11 liderados por el IEEE y que han sido muy exitosos en el ámbito comercial. Estos estándares, definen una red formada por un medio inalámbrico compartido y transmisión encriptada de la información.

¿Qué es 802.11?

802.11 es un estándar para comunicaciones transmitidas sobre ondas de radio. También conocido como Wi-Fi, 802.11b es el estándar en redes inalámbricas de la IEEE.

Este estándar desarrollado por el Instituto de Ingeniería Eléctrica y Electrónica IEEE 802.11, describe las normas a seguir por cualquier fabricante de dispositivos inalámbricos para que puedan ser compatibles entre sí.

Los más importantes estándares son:

- **IEEE802.11a:** hasta 54 Mbps (megabits por segundo) de ancho de banda disponible, trabajando en la frecuencia de 5GHz.

- **IEEE802.11b:** hasta 11 Mbps. Este es el más usual y el más utilizado, y sobre el que trabajaremos en nuestras pruebas trabajando en la frecuencia de 2,4GHz.
- **IEEE802.11g**: estándar hasta 54 Mbps, trabajando en la frecuencia de 2,4 GHz como 802.11a
- **IEEE802.11n:** estándar que permitirá alcanzar velocidades binarias por encima de los 100 Mbps, no estará listo hasta al menos el 2005 y trabajando en la frecuencia de 5 GHz.

Al ser un estándar mundial, muchos fabricantes de hardware están creando equipos inalámbricos para poder conectar ordenadores, y van mucho más allá, utilizando Wireless para otras aplicaciones como pueden ser: servidores de impresión o cámaras Web. Un mundo lleno de posibilidades.

Un poco de su historia

En 1990, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN. Pero no es hasta 1994 cuando aparece el primer borrador.

En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Personal Communications Systems). En ese mismo año, la ETSI (European Telecommunications Standards Institute), a través del comité ETSI-RES 10, inicia actuaciones para crear una norma a la que denomina HiperLAN (High Performance LAN) para, en 1993, asignar las bandas de 5,2 y 17,1 GHz. En 1993 también se constituye la IRDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos.

En 1996, finalmente, un grupo de empresas del sector de informática móvil (mobile computing) y de servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos.

Entre los miembros fundadores de WLI Forum se encuentran empresas como ALPS Electronic, AMP, Data General, Contron, Seiko Epson y Zenith Data Systems.

La alianza WI-FI (Wireless Fidelity) es una organización sin fines de lucro formada en 1999 para certificar la interoperabilidad de los productos 802.11 y para promocionarlos con un estándar global de WLAN en todos los segmentos.

802.11 aunque en un primer momento sólo se aplicaba al tipo b, ahora mismo engloba a los diferentes tipos de estándares utilizados en el mercado en este momento (802.11.b, 802.11,a y 802.11.g) los cuales, a pesar de su denominación, son en principio tecnologías incompatibles.

Cada tipo tiene sus ventajas e inconvenientes. La principal ventaja de la variante b es sin duda su popularidad, la capacidad de transmisión de datos a velocidades de 12 Mgbs a un precio más que razonable y su mayor cobertura. Su cruz, las quejas que recibe acerca de su seguridad.

El 802.11.a, en cambio, es más seguro y veloz (hasta cinco veces más rápido), soporta a más número de usuarios y su espectro de transferencia (5GHz) está libre de interferencias de móviles y de dispositivos Bluetooth. Los inconvenientes son la menor implantación entre las comunidades de usuarios y en que su precio es mucho más caro.

Ambas tecnologías cuentan con diferente alcance. El 802.11b cubre un máximo de 460 metros en espacio libre. En espacios cerrados, sin embargo, su alcance es sólo de 30 a 90 metros, dependiendo del tipo de construcción del edificio (si es de acero o cemento, o de un tipo de construcción más antiguo). Por su parte, el estándar 802.11.a dispone de menor cobertura (entre 30 y 300 metros, si no hay muros u otros obstáculos, mientras que en habitaciones cerradas, de 12 a 90 metros).

Clasificación de los Estándares 802.11

802.11a - Estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54 Mbps, apoyándose en la banda de los 5GHz. A su vez, elimina el problema de las interferencias múltiples que existen en la banda de los 2,4 GHz (hornos microondas, teléfonos digitales DECT, Bluetooth).

802.11b - Extensión de 802.11 para proporcionar 11 Mbps usando DSSS. También conocido comúnmente como Wi-Fi (Wireless Fidelity): Término registrado promulgado por la WECA para certificar productos IEEE 802.11b capaces de ínter operar con los de otros fabricantes. Es el estándar más utilizado en las comunidades inalámbricas.

802.11c - Estándar que define las características que necesitan los APs para actuar como puentes (bridges). Ya está aprobado y se implementa en algunos productos.

802.11e - Estándar sobre la introducción del QoS en la comunicación entre PAs y TRs. Actúa como árbitro de la comunicación. Esto permitirá el envío de vídeo y de voz sobre IP. Su único inconvenientes el encarecimiento de los equipos.

802.11f - Estándar que define una práctica recomendada de uso sobre el intercambio de información entre el AP y el TR en el momento del registro a la red y la información que intercambian los APs para permitir la interportabilidad. La adopción de esta práctica permitirá el Roamming entre diferentes redes.

802.11g - Utiliza la banda de 2,4 GHz, pero permite transmitir sobre ella a velocidades teóricas de 54 Mbps. Se consigue cambiando el modo de modulación de la señal, pasando de 'Complementary Code Keying' a 'Orthogonal Frequency Division Multiplexing'. Así, en vez de tener que adquirir tarjetas inalámbricas nuevas, bastaría con cambiar su firmware interno.

802.11h - Estándar que sobrepasa al 802.11a al permitir la asignación dinámica de canales para permitir la coexistencia de éste con el HyperLAN. Además define el TPC (Transmit Power Control) según el cual la potencia de transmisión se adecua a la distancia a la que se encuentra el destinatario de la comunicación.

802.11i - Conjunto de referencias en el que se apoyará el resto de los estándares, en especial el futuro 802.11a. El 802.11i supone la solución al problema de autenticación al nivel de la capa de acceso al medio, pues sin ésta, es posible crear ataques de denegación de servicio (DoS).

802.11j - Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.

802.11m - Estándar propuesto para el mantenimiento de las redes inalámbricas.

802.11n - Aunque el estándar que permitirá alcanzar velocidades binarias por encima de los 100 Mbps no estará listo hasta al menos el 2005, se ha anunciado el lanzamiento de los primeros chipsets basados en un pre-estándar a mediados del próximo año.

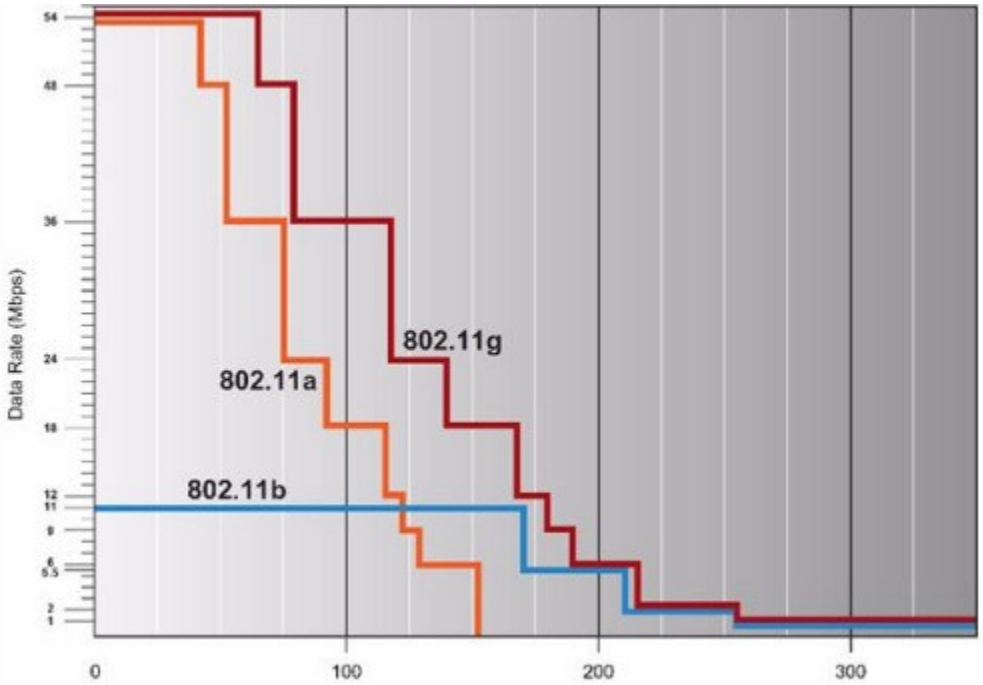
Este estándar usará la frecuencia de 5GHz tal y como viene usando el 802.11a con el cual será compatible. Esta noticia confirma que el estándar de 5GHz es el futuro de las redes inalámbricas y ya hoy en día el presente para la unión de nodos con el uso de 802.11a y en un futuro del 11n.

Esta es la tabla en la que podemos comparar los tres protocolos de IEEE que actualmente se comercializan dentro del estándar 802.11. Estos son el 802.11b, 802.11a y 802.11g en orden de aprobación por el **IEEE:**

Estándares Inalámbricos			
Estándar	**802.11b**	**802.11a**	**802.11g**
Aprobado IEEE	Julio 1999	Julio 1999	Junio del 2003
Popularidad	Adoptado masivamente	Nueva tecnología, crecimiento bajo	Nueva tecnología, con un rápido crecimiento
Velocidad	Hasta 11 Mbps	Hasta 54 Mbps	
Coste	Barato	Relativamente caro	Relativamente barato
Frecuencia	2.4 - 2.497 Ghz	5.15 - 5.35 Ghz 5.425 - 5.675 Ghz 5.725 - 5.875 Ghz	2.4 - 2.497 Ghz
Cobertura	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos	Cobertura baja, unos 150 metros, con mala conectividad con obstáculos	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos
Acceso Público	El número de Hotspots crece exponencialmente	Ninguno en este momento.	Compatible con los HotSpots actuales de 802.11b. El paso a 802.11g no es traumático para los usuarios.

Estándares Inalámbricos			
Estándar	**802.11b**	**802.11a**	**802.11g**
Modos de datos	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Modulación	CCK	OFDM	OFDM y CCK

Podemos ver una gráfica con la relación entre la distancia (medida en pies, un pie = 0.3048 metros) y el ancho de banda que podemos usar en cada caso. Por supuesto las distancias pueden variar dependiendo de la potencia y los dBm irradiados por la tarjeta de cada fabricante.



Como se ha comprobado la frecuencia más usada en este momento es la de 2.4Ghz. Dicha frecuencia es libre en prácticamente todos los países del mundo, ya que se trata de una frecuencia reservada para la investigación, educación o sanidad. Sin embargo en muchos países determinadas frecuencias dentro de los 2.4 Ghz están reservadas por el ejército o los gobiernos.

Bandas ISM

A mediados de los años 80, el FCC (Federal Communications Comission) asignó las bandas **ISM** (Industrial, Scientific and Medical) 902-928 MHz, 2,4-2,4835 GHz, 5,725-5,85 GHz a las redes inalámbricas. Las bandas ISM son bandas de frecuencias para uso comercial y sin licencia (son las utilizadas por los teléfonos inalámbricos domésticos DECT, los microondas, o los dispositivos Bluetooth, por ejemplo). En nuestro caso 802.11 utiliza el rango de frecuencias de 2,4 a 2,4835 GHz, y la divide en canales (11 para EE.UU. y 9 para Europa), definiendo unos anchos de banda de 11, 5, 2 y 1 Mbps por canal.

Número de Canal	Frec. EE.UU.	Frec. Europa
1	2412	No Disponible
2	2417	No Disponible
3	2422	2422
4	2427	2427
5	2432	2432
6	2437	2437

Número de Canal	Frec. EE.UU.	Frec. Europa
7	2442	2442
8	2447	2447
9	2452	2452
10	2457	2457
11	2462	2462
Frecuencia en MHz.		

En la siguiente tabla se puede ver la relación entre los canales y la frecuencia.

Relación entre canal y frecuencia	
Canal	**Frecuencia**
1	2.412 Ghz
2	2.417 Ghz
3	2.422 Ghz
4	2.427 Ghz
5	2.432 Ghz
6	2.437 Ghz
7	2.442 Ghz
8	2.447 Ghz
9	2.452 Ghz
10	2.457 Ghz
11	2.462 Ghz
12	2.467 Ghz
13	2.472 Ghz
14	2.484 Ghz

En la siguiente tabla podemos ver los canales disponibles (no olvides que están relacionados con la frecuencia) dependiendo de cada país:

Países y Canales	
Países	**Canales**
Europa (ETSI)	1 - 13
USA (FCC)	1 - 11
Francia	10 - 13
Japón	1 - 14

2.3 Seguridad

En primer lugar hay que situarse dentro de lo que seguridad significa en el mundo informático.

Se dice que una red es segura cuando casi nadie puede entrar la misma o los métodos de entrada son tan costosos que casi nadie puede llevarlos a cabo. Casi nadie puede significar que es segura en un 99.99%, por ello debemos desechar la idea de que los sistemas informáticos son seguros al 100%. No es cierto.

Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener.

Una vez situados vamos a ver los pasos que podemos seguir para introducir una seguridad razonablemente alta a nuestra red inalámbrica. Debemos tener en cuenta que cuando trabajamos con una red convencional cableada disponemos de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos de comunicación de la misma. En nuestro caso no, de hecho vamos a estar "desperdigando" la información hacia los cuatro vientos con todo lo que esto conlleva.

Una de las preguntas más frecuentes que se le hacen a los vendedores o integradores de redes Lan inalámbricas, es “¿Qué hay con la seguridad?”. Estos días, lo más inteligente que puede hacer cualquier administrador de redes, es preocuparse por la seguridad, entre otras cosas, debido a la atención que se le esta prestando en diferentes medios. Desdichadamente, empleados descontentos, hackers, virus, espionaje industrial, y otras formas de ataque no son poco comunes en nuestras redes.

Durante mucho tiempo la seguridad de las comunicaciones por teléfono estaba asegurada por el simple hecho de que no era fácil, al menos en la práctica, pinchar la línea de cobre que llevaba la señal desde la centralita a nuestra oficina o al hogar.

Con las redes locales ocurría otro tanto. Mientras nadie pudiera "pinchar" en el cable, la comunicación interna estaba asegurada y no podía salir al exterior. Pero Internet y el acceso de todos los equipos internos hacia el exterior cambiaron totalmente las reglas. La seguridad se ha convertido en uno de los aspectos claves para transferir información, no meramente para curiosear en varias páginas Web, que se ha convertido en uno de los principales motivos de empleo de la red.

Pero el problema se complica cuando basta con un receptor para captar la señal de otro equipo. Claro que esto sólo ocurriría si se comete la imprudencia de no activar mecanismos que impidan el acceso a cualquier intruso, o que codifican la señal para que no sea fácilmente descifrable y comprensible. En la tecnología inalámbrica el estándar WEP contempla la codificación de las transmisiones, así como sistemas de control y restricción de acceso.

Para distintos problemas, diferentes soluciones. No hay una única solución inalámbrica. De hecho se perfilan dos, a las que habría que sumar las utilizadas por los actuales servicios telefónicos. Pero como éstos se utilizan para otro tipo de información y de servicios, nos centraremos en las dos tecnologías más importantes, que ya comienzan a hacerse un hueco entre las instalaciones de hoy en día.

Con frecuencia la señal no se queda entre las cuatro paredes de la oficina, sino que puede ser detectada, utilizada y / o explotada por aquellos atacantes conocidos como hackers de redes inalámbricas (War Drivers) y hackers de señales inalámbricas (War Chalkers). Con la ayuda de un equipo sencillo y un software "rastreador" de los puntos de acceso inalámbrico que está listo para su descarga de Internet, estos individuos recorrerán ciudades y pueblos en busca de puntos inseguros de acceso inalámbrico.

2.3.1 Amenazas y/o Ataques

- **Amenazas**

La mayoría de las personas sienten seguridad cuando están utilizando una red alámbrica, pero tan pronto como los datos comienzan a viajar a través del "aire", se preocupan. Después de todo, lo que se piensa es, la red alámbrica se encuentra *dentro* de sus instalaciones, y eso hace pensar que ya tiene algún elemento extra de seguridad. La verdad, es que *cualquier* red, incluida una red alámbrica, esta sujeta a potenciales riesgos de seguridad:

- Ataques desde dentro del grupo de usuarios de la red.
- Acceso no autorizado.
- Fuga de información hacia fuera de la compañía.

Las buenas noticias son que hay formas de combatir estas amenazas para redes tanto alámbricas como inalámbricas y, de hecho, los segmentos de redes inalámbricas incluyen algunas funciones de seguridad incluidas que tal vez no tengamos consideradas.

- **Enemigos Amistosos? – El control del sitio**

Por siempre, una de las más grandes amenazas de las redes en cualquier compañía, viene desde dentro de la compañía misma. Sin las medidas de seguridad adecuada, cualquier usuario *registrado* de la red puede acceder a datos a los que el / ella no debe tener ningún acceso. Empleados y ex-empleados inconformes, pueden haber descubierto la forma de leer, distribuir e incluso, alterar archivos de datos de información crítica para la compañía.

Los administradores de red, independientemente de si tienen segmentos de redes alámbricas o inalámbricas, necesitan contar con las herramientas de seguridad para sus ambientes, los niveles de seguridad adecuados para cada usuario, y una forma eficiente de auditar constantemente la efectividad de la seguridad.

- **¡ FUERA DE AQUÍ! – Solo usuarios autorizados**

Otra área de preocupación en cuanto a la seguridad – si no es que la más grande en este momento - para cualquier administrador de red, es el crecimiento que está teniendo Internet. Si los usuarios de la red interna pueden *salir* a Internet, eso quiere decir, que los usuarios de afuera, pueden *entrar* a nuestra red si no tomamos las precauciones necesarias.

Y eso aplica no solo a la Internet, si no a cualquier medio con que contemos para permitir que cualquier usuario desde afuera pueda comunicarse hacia el interior de nuestra red. Los productos para Acceso Remoto que permiten al personal de ventas o de *marketing* acceder a la red por medio de dial-up para revisar sus correos o sincronizar archivos, las oficinas remotas que se pueden conectar a través de MODEM, los Websites y las "*Extranets* " que conectan a nuestros clientes y/o proveedores a nuestra red, todos estos medios, pueden dejar nuestra red vulnerable para ataques de hackers, virus o cualquier otro intruso.

Existen actualmente muchos productos y herramientas para permitir a los administradores de la red asegurar las redes en prevención de estas amenazas. La autenticación de usuarios y sus políticas, son administradas principalmente por el sistema operativo, y puede ser mejorada agregando productos de terceros. Los productos de *Firewall,* ofrecen una protección adicional.

- **Los Espías escuchando detrás de la puerta**

Quizás la mayor amenaza, o cuando menos la más difícil de proteger, es cuando *alguien* esta solamente husmeando entre los paquetes de datos. Actualmente, las redes alámbricas se encuentran "algo" vulnerables a estas fugas de información. La mayoría de las tarjetas de red que hay en el mercado actualmente, pueden trabajar en " *modo promiscuo* ", esto quiere decir, que con el software adecuado, les permite capturar todos los paquetes de datos que circulen en la red. ¿Qué administrador de red actualmente no posee algún tipo de "sniffer" para detectar problemas en la red?. Estos programas, lo que hacen es leer, capturar y organizar cualquier tipo de dato que haya cruzado por la red.

Ataques

Para detectar las principales formas en que se vulnera la seguridad de las redes inalámbricas se clasificó a los tipos de intrusión, causas, efectos y probables soluciones.

- ✓ **Ataques de Intromisión**

Los ataques de intromisión se caracterizan por aprovechar una de las características de las redes inalámbricas, la libertad de conectarse desde cualquier artefacto *wireless* (inalámbrico) siempre y cuando éste se encuentre iluminado por un punto de acceso.

Los perpetradores se aprovechan de no tener que pasar por ningún proceso de autenticación o filtro de acceso y acceden a la red en su totalidad.

- ✓ **Clientes no autorizados**

Cuando alguien desea conectarse a una red LAN haciéndose pasar por un usuario común, se puede hablar de un ataque de intromisión. Para evitar esto los puntos de acceso deben ser configurados con el objetivo de que solicite una clave a todo aquel que acceda a la red.

- ✓ **Puntos de Acceso piratas**

Es similar al caso anterior, con la diferencia que aquí es un AP el que se suma a una red sin ser autentificado.

- ✓ **Intercepción y Monitoreo no Autorizado de Tráfico Inalámbrico**

Como en las redes tradicionales, es posible monitorear e interceptar el tráfico de una red LAN inalámbrica. Sólo basta situarse dentro del rango de operaciones (91 metros aproximadamente para el estándar 802.11b) para entrar en cualquier sistema que viaje sobre Wi-Fi.

- ✓ **Análisis de paquetes inalámbricos**

Los atacantes utilizan técnicas similares a las que usarían en una red LAN tradicional, capturando los primeros paquetes transmitidos (donde generalmente se encuentra el nombre de usuario y la contraseña) e ingresando como un miembro legítimo de la red, para luego piratear los sistemas.

- ✓ **Clonación de un AP (gemelo malvado)**

De esta forma el atacante sustituye el AP original haciéndole creer al usuario que su acceso es legítimo solicitándole información esencial.

- ✓ **Jamming**

Generalmente, el Denial of Service (DoS) o servicio denegado se debe a que la frecuencia sobre la que se transmite está equivocada y fuera de rango. Esa es una de las fórmulas que utiliza el atacante para distorsionar la señal y captar la información que viaja vía radiofrecuencia.

- ✓ **Ataques Cliente a Cliente**

Este caso consiste en la defensa que debe poseer un usuario, incluso, de otro usuario. Cuando establecemos conexión con un usuario de una red inalámbrica debemos confirmar que éste no quiera atacarnos, ya que se utiliza a menudo el tráfico normal como Caballo de Troya a la hora de ingresar a sistemas ajenos.

- ✓ **Alteración de la Configuración del AP**

Cuando se opta por tener un AP más ágil y rápido para el bien de sus usuarios se corre el peligro de que este artefacto esencial de la transmisión de datos se vuelva vulnerable al ataque de especialistas.

Es por eso que una serie de fabricantes de soluciones de comunicación inalámbricas, como Nortel Networks, Cisco, Lucent y 3Com, entregan herramientas de software y hardware para evitar que sus productos sean vulnerables a ataques mediante la desconfiguración de sus AP.

Es precisamente en este punto donde se han volcado todos los esfuerzos con el propósito de fortalecer la seguridad en redes inalámbricas con el uso de técnicas de autenticación, encriptación y configuración; para de esta forma evitar ser presas de un intruso que vulnere los sistemas.

2.3.2 Técnicas de Seguridad Inalámbrica

- **Modos de modulación**

Las versiones de red local inalámbrica 802.11a y 802.11b se diferencian en sus modos de modulación. La técnica DSSS utilizada en 802.11b, codifica los datos al incorporar una secuencia aleatoria de bits a los datos originales y distribuir ésta a través del ancho de banda total. Resultados: la señal original desaparece prácticamente con el ruido de fondo del medio y resulta, por lo tanto, muy segura frente al riesgo de ser interceptada.

La técnica OFDM de la versión 802.11a funciona de una forma similar. Aquí la señal completa se divide en varias subseñales emitidas a través de todo el ancho de banda que se recompondrán en el receptor. De este modo, se permite una elevada velocidad de datos al tiempo que se garantiza una gran seguridad frente a la intercepción.

- **Control de acceso: codificación y autentificación**

Por sí sólo, el modo de modulación no garantiza una red local inalámbrica segura. Se necesitan varios requisitos para obtener una seguridad real:

- **Asignación de clave SSID:**

Cada usuario (cliente o punto de acceso) de una red LAN recibe su propia identificación SSID que ha sido asignada por el administrador al configurar la red inalámbrica.

Existen dos métodos de detección de SSID de puntos de acceso inalámbricos.

Activo: la mayor parte de los controladores de tarjetas inalámbricas permiten el rastreo de SSID mediante este método. Para comprobar si un punto de acceso está activo se puede enviar un paquete de prueba con el SSID correspondiente al principio, de forma que el AP adecuado responda. Si se omite el SSID todos los APs que estén por los alrededores responderán, en principio, con su SSID para indicar que están activos.

Pasivo: aunque la mayoría de los APs se comportan del modo descrito en el método activo, anterior hay algunos que se pueden configurar para no revelar su identificador de red cuando se le pregunte.

En estos casos el uso de herramientas especiales permite conocer de todos modos su existencia ya que pueden analizar los paquetes que circulan por las ondas de radio y revelar así qué SSID están disponibles (aunque ocultos) e incluso que nodos se están comunicando. La existencia de este método hace imposible ocultar una red inalámbrica.

La mayor parte de los controladores de los adaptadores de red inalámbricos permiten descubrir redes por el método activo (si el dispositivo soporta la configuración inalámbrica cero de Windows XP y 2003 también permite el uso de este método).

El Identificador del Conjunto de Servicios Extendidos (*Extended Service Set Identifier – ESS ID*).

Para que cualquier estación pueda tener acceso a algún AP, primero se debe determinar si la estación pertenece a su red o a su Conjunto Extendido de Servicios (*Extended Service Set* – **ESS)**. El AP primero revisa si el identificador de ESS de la estación (comúnmente de 32 caracteres) concuerda con el suyo.

Los que no son miembros, aún siendo el mismo fabricante y mismo modelo del AP, no podrán participar en la red y por lo tanto no podrán contar con el patrón de saltos y el *dwell time,* por lo que no podrán recibir ni enviar ningún paquete de datos.

Como medida adicional, este identificador, solo podrá ser cambiado al administrar el equipo en cuestión con privilegios de administrador y algunos fabricantes, solo permiten este cambio al estar conectados físicamente al equipo, nunca de manera remota.

Si hay la necesidad de tener dos segmentos de red separados en una sola red, como por ejemplo, un segmento para contabilidad y el resto para los demás, entonces basta con programar los ESS ID diferentes. Si la necesidad es de contar con diferentes AP en una sola zona, para cubrir un área con balanceo de carga, o para soportar el *overlapping* y permitir el roaming, entonces los AP se programan con el mismo ESS ID pero, con diferentes patrones de salto.

Con un ESS ID de 32 caracteres y una secuencia de salto de 3 dígitos, es posible darnos cuenta lo difícil que sería para cualquiera adivinar el ESS ID exacto y la secuencia de salto para poder obtener acceso a la Lan por medio de cualquiera de sus segmentos inalámbricos.

- **Direcciones MAC**

El fabricante asigna una única dirección MAC global a cada adaptador de una red WLAN.

Toda NIC (Network Interface Card, Tarjeta Adaptadora de Red), independientemente del medio que utilicemos (cable, aire, medio de la capa 1 – Física – del modelo OSI de 7 capas), dispone de un identificador llamado dirección MAC.

Este identificador "trabaja" en la capa 2 – Enlace de Datos – del modelo OSI, y es un identificador exclusivo para cada NIC.

Esta MAC está formada por 48 bits de los cuales los 24 primeros identifican al fabricante, y los 24 siguientes son el número de serie / referencia que el fabricante le ha asignado a la NIC.

Por ello se supone que no existen dos NIC con la misma MAC, o no deben de existir, aunque en el mercado existen tarjetas de red a las cuales se le pueden cambiar la MAC.

La forma de representar la dirección MAC es en hexadecimal:

3A-F5-CD-98-33-B1

O bien: 3AF5CD-9833B1, siendo la anterior la forma más común de representación.

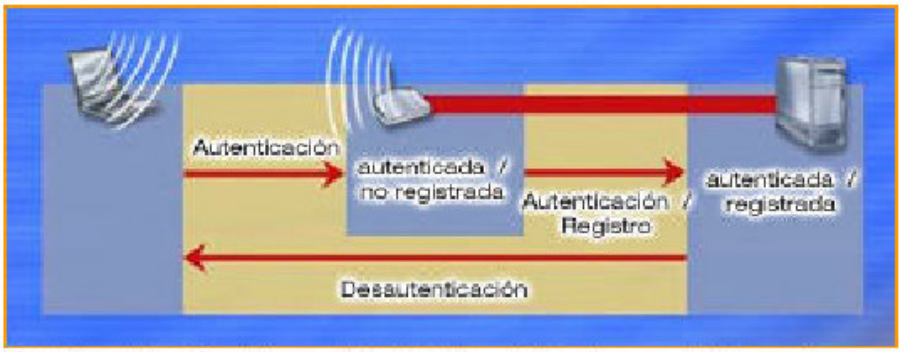
En toda trama de información que circula por una red, independientemente del medio sobre el que se transporte, habrá sido encapsulada en la capa de Enlace con una MAC destino y una MAC origen, lo que permite que esta trama llegue al dispositivo con la MAC destino coincidente.

Si disponemos de un programa que ponga la NIC en modo promiscuo, que acepte todas las tramas de información aunque no sea él la MAC destino, estaremos hablando de un Sniffer, un programa para buscar redes, capturar tramas y poderlas estudiar.

En resumen: cualquier dispositivo conectado a una red necesita disponer de una MAC para identificarse a nivel de la Capa de Enlace. En los dispositivos inalámbricos disponemos de esas MACs.

- **Autenticación (Registro e identificación).**

Cada estación debe probar que está autorizada para conectarse a la red WLAN correspondiente. Por este motivo, los productos para WLAN actuales utilizan el algoritmo WEP.



Cualquier sistema operativo cuenta con niveles de seguridad y administración de usuarios. Aquí es un poco más necesario, ya que en una red inalámbrica, es de suponerse que los usuarios se encuentran en movimiento y por lo tanto, moviendo sus equipos de una ubicación a otra, por lo que una política de contraseñas exigente agrega un nivel mas de seguridad al asegurar que la estación está siendo usada por la persona que se supone debe utilizarla.

- **Codificación WEP** (*Wired Equivalency Privacy)*

El comité de IEEE 802.11 es responsable por fijar los estándares para las redes inalámbricas y la mayoría de los productos que se encuentran en el mercado actualmente fueron diseñados y fabricados para cumplir con el estándar. Esta organización ha tocado los puntos respecto a la seguridad creando la *Wired Equivalency Privacy* – **WEP**.

Usuarios preocupados por el acceso no autorizado se preocupan porque algún intruso sea capaz de:

- ✓ Acceder a la red utilizando un equipo similar (o igual) al que utilizamos en nuestra Lan.
- ✓ Capturar el tráfico de red que viaja por nuestra Lan inalámbrica (*eavesdropping*).

802.11b – WEP de 64 y 128 bits.

802.11b+ - WEP de 64, 128 y 256 bits.

Ambos dispositivos (adaptador y Punto de Acceso) deben de soportar el mismo tipo de cifrado. El WEP de 64 bits puede ser desencriptado sin problemas, y no todos los dispositivos inalámbricos soportan encriptaciones mayores.

En las redes 802.11, el acceso a los recursos de la red, esta prohibido para cualquier usuario que no conozca o no pruebe conocer las "llaves" actuales. La mayoría de las marcas ofrecen este nivel extra de seguridad agregando una contraseña de autenticación. El usuario de la estación de hardware, primero debe proporcionar las "llaves" correctas antes de que la estación de acceso al AP y a toda la red.

El *eavesdropping* es prevenido por el algoritmo de *WEP* en donde un generador de números aleatorios es inicializado por medio de una llave secreta. Este simple algoritmo tiene las siguientes propiedades:

- ✓ **Razonablemente Fuerte**. Un ataque de fuerza bruta a este algoritmo es difícil debido a que cada *frame* es mandado con un vector de inicialización el cual reinicia el PRNG para cada *frame*.
- ✓ **Auto Sincronización**. Debido a que al igual que en cualquier Lan, las estaciones inalámbricas trabajan en un medio que puede perder la conexión por cualquier causa y los paquetes se pierden, el algoritmo de WEP re-sincroniza en cada mensaje que manda.

- **EAP (**Protocolo de autenticación extensible)

Para poder ofrecer un mecanismo de autenticación estándar para IEEE 802.1X, IEEE escogió el protocolo de autenticación extensible (EAP). EAP es un protocolo basado en la tecnología de autenticación del protocolo punto a punto (PPP)-que previamente se había adaptado para su uso en segmentos de redes LAN punto a punto.

En un principio los mensajes EAP se definieron para ser enviados como la carga de las tramas PPP, de ahí que el estándar IEEE 802.1X defina EAP sobre la red LAN (EAPOL). Este método se utiliza para encapsular los mensajes EAP y así poder enviarlos ya sea a través de segmentos de redes Ethernet o de redes LAN inalámbricas.

- **TKIP**

Protocolo de Integridad de Claves Temporales (TKIP) para reforzar la encriptación de los paquetes inalámbricos. TKIP incluye funciones de seguridad como; función de mezcla de claves por paquete, mensaje de chequeo de integridad (MIC), vector de inicialización (IV) y mecanismo de cambio de claves. Con todas estas funciones se elimina la vulnerabilidad de la simple encriptación WEP. La encriptación WEP también está incorporada, en 64 y 128 bits.

- **OSA vs SKA.**

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

- **CNAC.**

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

- **Utilizar el estándar 802.1x**

Nuevo estándar con el que permitimos autenticar al usuario entrante a nuestra WLAN. El autenticador no tiene por que ser una máquina inteligente, por lo que pequeños APs podrán utilizar este estándar 802.1x.

Para ofrecer una mayor seguridad de la que proporciona WEP, el equipo de conexiones de red de Windows XP trabajó con IEEE, distribuidores de red y otros colaboradores para definir IEEE 802.1X. El mismo es un borrador de estándar para el control de acceso a redes basado en puerto que se utiliza para proporcionar acceso a red autenticado para las redes Ethernet. Este control de acceso a red basado en puerto utiliza las características físicas de la infraestructura LAN conmutada para autenticar los dispositivos conectados a un puerto LAN. Si el proceso de autenticación no se realiza correctamente, se puede impedir el acceso al puerto. Aunque este estándar se ha diseñado para redes Ethernet con cable, se puede aplicar a las redes LAN inalámbricas 802.11.

Concretamente, en el caso de las conexiones inalámbricas, el punto de acceso actúa como autenticador para el acceso a la red y utiliza un servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) para autenticar las credenciales del cliente.

La comunicación es posible a través de un "puerto no controlado" lógico o canal en el punto de acceso con el fin de validar las credenciales y obtener claves para obtener acceso a la red a través de un "puerto controlado" lógico. Las claves de que dispone el punto de acceso y el cliente como resultado de este intercambio permiten cifrar los datos del cliente y que el punto de acceso lo identifique. De este modo, se ha agregado un protocolo de administración de claves a la seguridad de 802.11.

Los pasos siguientes describen el planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red.

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando una estación inalámbrica entra en el alcance del punto de acceso, éste envía un desafío a la estación.

- Cuando la estación recibe el desafío, responde con su identidad. El punto de acceso reenvía la identidad de la estación a un servidor RADIUS que realiza los servicios de autenticación.

- Posteriormente, el servidor RADIUS solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad. La estación envía sus credenciales al servidor RADIUS (a través del "puerto no controlado" del punto de acceso).

- El servidor RADIUS valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.

- El punto de acceso utiliza la clave de autenticación para transmitir de manera segura las claves correctas a la estación, incluida una clave de sesión de unidifusión para esa sesión y una clave de sesión global para las multidifusiones.

- Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.

- **Utilice la tecnología de red privada virtual (VPN):**

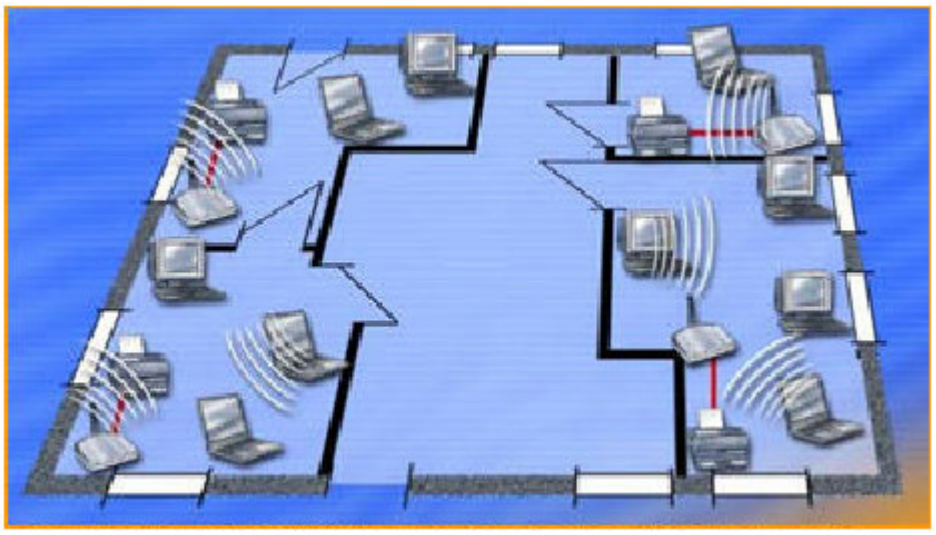
Montar una red privada virtual entre el origen y el destino. Utilizando una VPN se proporciona un túnel seguro independientemente del camino por el que circule la información, incluido Internet. Ya existen APs en el mercado que lo soportan.

Las redes privadas virtuales (VPN) llevan ya bastante tiempo operando y están consideradas como muy seguras. Se obtendrá una red local inalámbrica segura si se sabe sacar provecho de esta tecnología para redes inalámbricas.

Un escenario típico para muchos usuarios es una pequeña oficina (agencias, etc.) que se reparte en varias habitaciones de una misma planta. Hasta ahora, cada trabajador utilizaba su propia impresora; lo que se podría organizar de forma centralizada en el futuro (una impresora por habitación).

Cada habitación también debería disponer de acceso central a Internet (ADSL). Se prefiere la siguiente red (802.11b):

Ejemplo de una red completamente inalámbrica



- **La tecnología de Espectro Disperso de Salto de Frecuencia** (*frequency hopping spread spectrum* – **FHSS)**.

La tecnología de espectro disperso fue introducida hace aproximadamente 50 años por los militares como una forma segura de enviar y recibir comunicaciones. Desde el principio (y debido a su naturaleza) fue concebida para ser resistente al ruido, las interferencias, el bloqueo o la detección no autorizada.

Los transmisores de espectro disperso, envían sus señales a través de un rango de frecuencias a bajo poder, en contraste con otras tecnologías (como microondas) que concentran todo su poder en una sola frecuencia. Hay varias formas de implementar la transmisión por medio de espectro disperso, las dos más comunes, son la secuencia directa y el salto de frecuencia.

El rango de frecuencias que están utilizando actualmente los equipos para transmisión inalámbrica, se encuentra en el rango de las frecuencias disponibles para la banda ICM (Industrial Científica y Medica – ISM en inglés) que va de los 2.400 – 2.483 GHz, la cual dividen en series de hasta 79 canales distintos y separados. Las transmisiones son enviadas por cada canal en lo que parece ser una secuencia aleatoria (llamada "secuencia pseudo-aleatoria"). Los radios cambian de frecuencia varias veces en un segundo, transmitiendo en cada canal por un periodo específico de tiempo, y luego cambiando al siguiente canal en la secuencia y así, hasta cubrir todos los canales y después volver a repetir la secuencia. Sin conocer cuanto tiempo la señal permanecerá en un canal (llamado "*dwell time* ") y cual es el patrón de saltos?, es prácticamente imposible para una estación "no asociada" el recibir y descifrar los datos.

El uso de diferentes patrones de salto, *dwell times,* y/o el número de canales, es lo que permite a mas de dos redes inalámbricas independientes convivir una junto a la otra sin causarse interferencia y sin temor a que los datos de una red, puedan ser enviados a la otra.

- **Encriptación de Datos**

Si sus necesidades, son de mantener sus datos ultra secretos, como en el caso de las agencias militares y algunas financieras, entonces seguramente necesitaran tomar medidas extras. El último y más alto nivel de seguridad es agregando algún producto de encriptación de datos en toda la red como un todo. Ya sea por software o por hardware, el paquete de datos, será codificado antes de ser enviado hacia la Lan. Solo las estaciones que tengan la llave de desencriptación correcta, podrán decodificar el mensaje y leer los datos.

Si la seguridad total es necesaria, entonces la encriptación de datos es la mejor solución. Algunas de estas capacidades se encuentran ya en algunos sistemas operativos.

- **AES (Advanced Encryption Standard)**

AES (Advanced Encryption Standard) permite proteger la privacidad de todos los datos inalámbricos. AES ha sido elegido por el National Institute of Standards and Technology estadounidense como sistema de seguridad para las redes inalámbricas que transportan información gubernamental.

- **Firewall**

Uno de los sistemas básicos de seguridad, que debemos utilizar para nuestra conexión a una red, es la instalación de un Firewall o cortafuegos. Un Firewall es un sistema de defensa que se basa en la instalación de una "barrera" entre tu PC y la Red, por la que circulan todos los datos. Este tráfico entre la Red y tu PC es autorizado o denegado por el Firewall (la "barrera"), siguiendo las instrucciones que le hayamos configurado.

¿Cómo funciona un Firewall?

El funcionamiento de este tipo de programas se basa en el "filtrado de paquetes". Todo dato o información que circule entre nuestro PC y la Red es analizado por el programa (Firewall) con la misión de permitir o denegar su paso en ambas direcciones.

El comprender esto último es muy importante, ya que si autorizamos un determinado servicio o programa, el Firewall no va a decirnos que es correcto o incorrecto, o incluso, que siendo correctos los paquetes que están entrando o saliendo, éstos contienen datos perniciosos para nuestro sistema o la Red, por lo que hay que tener buen cuidado en las autorizaciones que otorguemos.

- **Otras consideraciones de las redes inalámbricas**

Las redes inalámbricas cuentan con otras características que las hace un poco menos preocupantes en cuanto a seguridad. Por ejemplo, algunos AP, filtran el tráfico de red que no va dirigido a las estaciones inalámbricas asociadas. Esto quiere decir que la mayoría del tráfico de red nunca saldrá al "aire". Por otro lado, los equipos inalámbricos tienen un rango de transmisión limitado, dependiendo del entorno, por lo que si alguien deseara "escuchar" algo de la señal, debiera estar relativamente cerca. Y por último, los usuarios de servicios inalámbricos pueden estarse moviendo de un AP a otro durante una misma sesión, y en este caso, el tráfico de red nunca será transmitido utilizando el mismo patrón de saltos que antes, haciendo que el "escuchar" (*eavesdropping, Proteger la transmisión de la fuga de información)* sea prácticamente imposible.

La mejor solución es utilizar varios de los anteriores para poner más trabas a los usuarios que no tienen autorización, si bien, el impedir el acceso por completo es muy difícil.

2.3.3. Pasos para asegurar una red inalámbrica

A continuación comentaremos los pasos necesarios para asegurar nuestra red inalámbrica.

Paso 1, debemos activar el WEP. Parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado. Esto viene a ser como si el/la cajero/a de nuestro banco se dedicase a difundir por la radio los datos de nuestras cuentas cuando vamos a hacer una operación en el mismo. WEP no es completamente seguro, pero es mejor que nada.

Paso 2, debemos seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No debemos usar fechas de cumpleaños ni números de teléfono.

Paso 3, uso de OSA. Esto es debido a que en la autenticación mediante el SKA, se puede comprometer la clave WEP, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.

Paso 4, desactivar el DHCP y activar el ACL. Debemos asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.

Paso 5, Cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial reconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar a la baja la frecuencia de broadcast del SSID, deteniendo su difusión a ser posible.

Paso 6, hacer uso de VPNs. Las Redes Privadas Virtuales nos dan un extra de seguridad que nos va a permitir la comunicación entre nuestros dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.

Paso 7, aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un Firewall que filtre el tráfico entre los dos segmentos de red.

2.3.4 Decálogo de la seguridad en Redes Inalámbricas

10 puntos para tener en cuenta.

Intentar reducir la seguridad de Redes inalámbricas nunca está de más.

Regla 1: Discreción

Evite anunciar innecesariamente la presencia de su instalación WiFi. Asegúrese de cambiar el SSID de sus equipos y no dejar el que viene de fábrica. También si es posible, deshabilite la baliza (beacon) SSID.

Procure instalar las antenas de punto de acceso (AP) y los niveles de potencia de los equipos para evitar la llegada de señal a áreas donde la cobertura no es deseada ni requerida.

Regla 2: Protéjase de la clonación

Hoy día es fácil "convertir" un dispositivo para que se presente como otro dispositivo (impersonation). Los dispositivos perdidos o robados son también una amenaza. El filtrado por direcciones de Control de Acceso de Medios (MAC) es un método de autenticación que no puede utilizarse en forma individual. Siempre debe ser acompañado de un método de autenticación independiente de los dispositivos, como los nombres de usuarios y contraseñas, directorios de red existentes u otros esquemas de autentificación.

Regla 3: Cifre los datos

Desear privacidad es algo normal. Para esto, los datos transmitidos inalámbricamente deben ser cifrados. El cifrado básico provisto por WiFi, conocido WEP, es relativamente débil en todas sus formas y su mantenimiento es costoso e ineficiente. En forma complementaria a este método es aconsejable utilizar tecnologías probadamente eficaces en redes como IPSec con cifrado 3DES. Siempre procure utilizar esquemas de seguridad estándar que faciliten la interoperabilidad.

Regla 4: Filtre los datos

Esta regla en realidad no es exclusiva de las redes inalámbricas, pero es útil recordarla aquí: Limite y controle a donde puede ir el tráfico de la red inalámbrica. Un Firewall es la herramienta ideal para esta tarea. Si la red inalámbrica va a ser usada para un propósito determinado, como el acceso a recursos empresariales específicos, entonces configure filtros de paquetes para que los datos que provienen de la red inalámbrica no puedan llegar a lugares indeseados.

Regla 5: Limite el acceso físico a los puntos de acceso

Evite emplazar APs en escritorios u otros lugares que pueden ser fácilmente accedidos. Visitantes curiosos, inescrupulosos o empleados descuidados pueden fácilmente mover, reemplazar o resetear los APs. La seguridad no puede garantizarse si no se cuida este punto.

Regla 6: Mantenga los ojos abiertos

Monitoree activamente las configuraciones de los AP. No es suficiente con configurar un AP correctamente. Una vez configurado, el AP debe permanecer apropiadamente configurado. Considere que es fácil para alguien ejecutar un reseteo de hardware en un AP que está colocado en un escritorio o el techo.

Al monitorear activamente la configuración del AP, puede asegurar que el AP es automáticamente reconfigurado ante eventos de ese tipo que pudiesen ocurrir.

Regla 7: Controle los equipos clandestinos

En muchos lugares los APs pueden ser fácilmente instalados por empleados e intrusos y atentar contra las políticas de seguridad de la red. Mantener una política activa de detección de transmisiones WiFi con software de tipo sniffer es un requerimiento operacional crítico para la seguridad.

Regla 8: Extreme la atención si no usa puntos de acceso

En una red inalámbrica operando en modo Ad Hoc (o peer to peer), un intruso puede filtrarse y obtener acceso a la red simplemente usando un cliente legítimo cono un punto de entrada. Los productos conocidos como personal Firewall o software Firewall complementados con otras herramientas de administración de red que activamente rastreen y administren al cliente antes de permitirle el acceso mediante la LAN inalámbrica son una buena prevención.

Regla 9: Controle el uso de ancho de banda

El no cumplir esta regla lo expone a ataques de negación de servicio (DoS) o una ineficiente utilización del ancho de banda en el mejor de los casos. Hay varias maneras de regular la utilización del ancho de banda pero debe tener en cuenta que los equipos WiFi más básicos no dan ninguna solución en este punto. Esto en realidad no es un problema si ubica esta funcionalidad en otra parte adecuada de su red.

Regla 10: El tiempo es oro

Siempre que sea posible, implemente políticas de administración en tiempo real. En muchas ocasiones las redes WiFi están ampliamente distribuidas. Por ejemplo abarcan campus enteros e incorporan múltiples sitios globales. Las políticas de seguridad (por Ej. Listas de usuarios validados o derechos de acceso) naturalmente cambiaran. Estos cambios deben verse reflejados en tiempo real a través de la red inalámbrica para reducir la ventana de oportunidades para la intrusión, y más importante aún, facilitar el inmediato cierre de las brechas de seguridad detectadas.

Capitulo III

Conceptos Básicos

III. CONCEPTOS BÁSICOS

3.1 Arquitecturas de la red Inalámbrica

802.11 Arquitecturas - Topologías

La topología de IEEE 802,11 consiste en los componentes, llamados "sets" o "conjuntos", para proporcionar un WLAN que permite movilidad transparente de la estación. Los 802,11 estándares apoyan los tres sistemas siguientes de la topología-arquitectura:

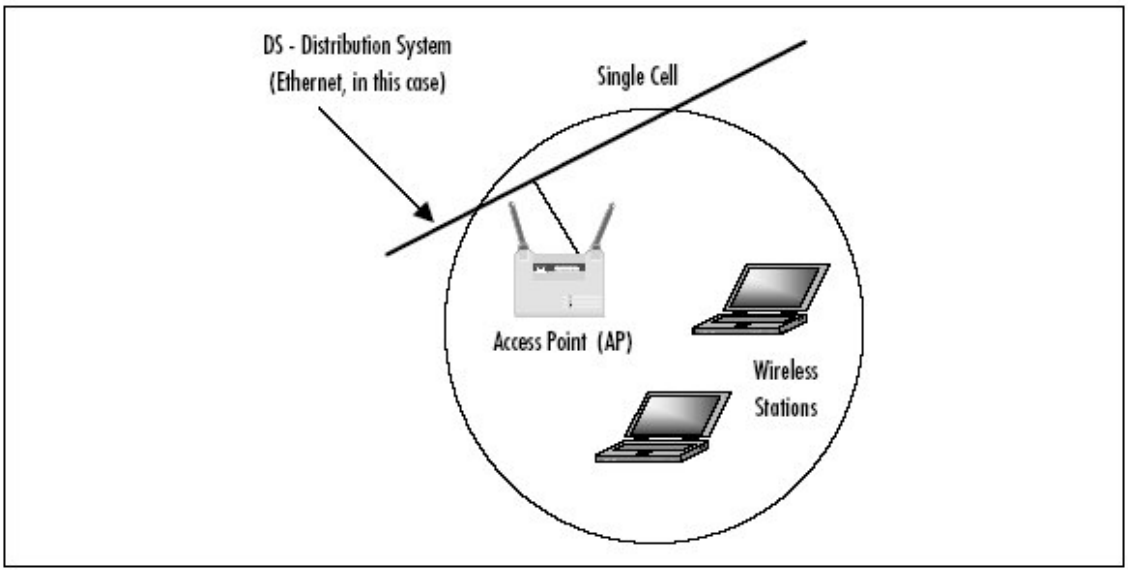
Basic Service Set (BSS) (Conjunto de Servicio Básico)

Un "Basic Service Set" (BSS) consiste en un grupo de usuarios de PC inalámbricos, y un punto de acceso que está directamente conectado a la LAN por cable. Cada PC inalámbrico en este BSS puede hablar con cualquier ordenador en su grupo inalámbrico vía enlace de radio, o acceder a otros ordenadores o recursos de red en la infraestructura LAN por cable vía el punto de acceso.

Es un grupo de estaciones que sé intercomunican entre ellas, en la cual se definen dos tipos:

- ✓ **Independientes:** cuando las estaciones, sé intercomunican directamente.
- ✓ **Infraestructura:** Cuando se comunican todas a través de un punto de acceso.

Conjunto de Servicio Básico (BSS)

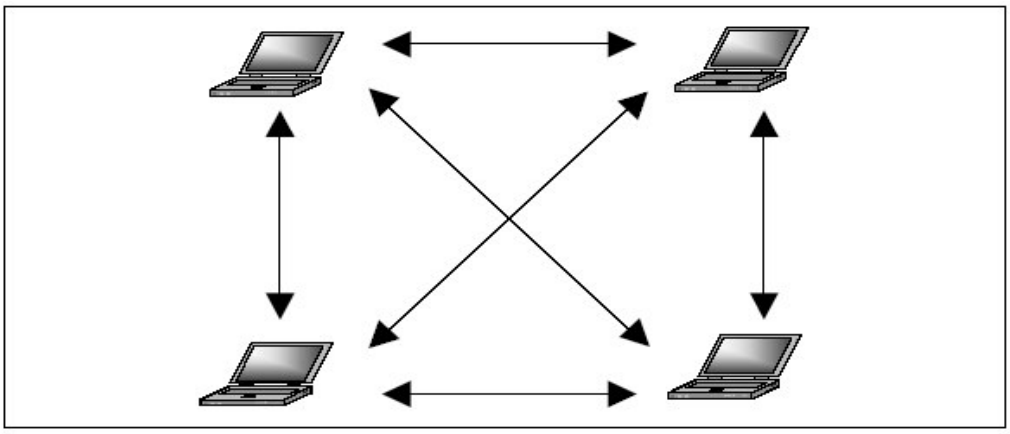


Independent Basic Service Set (IBSS) (Conjunto de Servicio Básico Independiente).

Las redes de IBSS también se refieren a una configuración independiente o red ad-hoc. Lógicamente, una configuración de IBSS es muy similar a una red punto a punto en el hogar o en la oficina, en la cual no se requiera ningún nodo para funcionar como un servidor. Los sistemas de la topología-arquitectura IBSS incluyen un número de estaciones o terminales inalámbricas que se comunican directamente una con otra, sin que el AP intervenga o cualquier conexión a una red alámbrica.

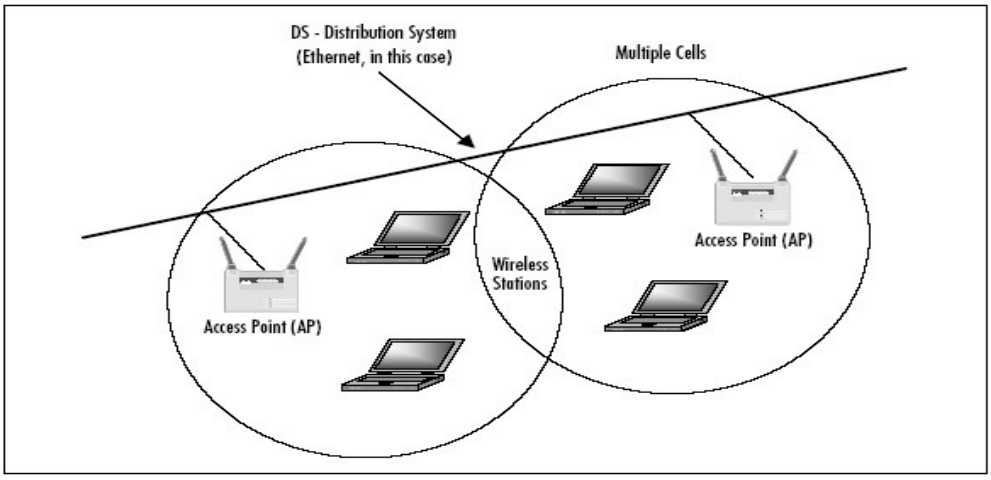
Es útil para rápida y fácilmente instalar un red inalámbrica en cualquier lugar donde no exista una infraestructura inalámbrica, ni se requiere para los servicios, tales como salas de conferencia en hoteles, los aeropuertos, o las demostraciones comerciales. Generalmente, las puestas en práctica ad hoc cubren un área pequeña (limitada) y no están conectadas con ninguna red.

Red del Conjunto Básico de Servicios Independiente (IBSS)



Extended Service Set (ESS) (Conjunto de Servicio Extendido)

Un Conjunto de Servicio Extendido, es un conjunto de dos o más redes BSS que forman una subred sencilla, Si existe más de un punto de acceso en la red, cada uno de ellos puede actuar como repetidor o puente entre redes inalámbricas y de esta forma obtenemos una red ESS.



3.2 Topologías de redes Inalámbricas

Con topología nos referimos a la disposición lógica de los dispositivos.

Podemos encontrar varios términos para estas topologías, los términos más usados son administrados y no administradas, alojadas y par, e infraestructura y "Ad-Hoc".

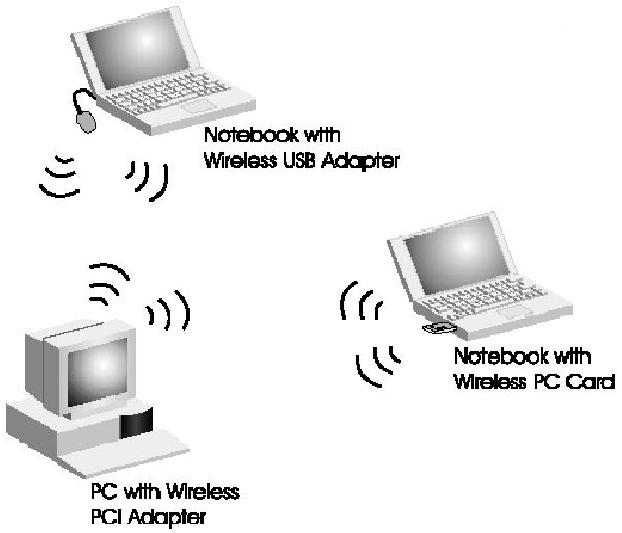
En este trabajo utilizamos el término infraestructura y "Ad-Hoc".

Estos términos están básicamente relacionados con las mismas distinciones básicas de topología.

- **Topología Ad-Hoc.**

Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red Peer to Peer o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento, como máximo puede soportar 256 usuarios.

Esta opción conecta dispositivos entre sí, sin necesidad de un Punto de Acceso. Podemos interconectar varios dispositivos entre sí. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre si. Modo Ad-Hoc:



En el caso de las redes Ad-Hoc, el número MAC es generado por el adaptador inalámbrico que crea "la conversación", y es un identificador MAC aleatorio. Cuando un adaptador inalambrico es activado, primero pasa a un estado de "escucha", en el cual, durante unos 6 segundos está buscando por todos los canales alguna "conversación" activa. Si encuentra alguno, le indicará al usuario a cual se quiere conectar. En el supuesto de que no se pueda conectar a otro Host que ya estuviera activo, pasa a "crear la conversación", para que otros equipos se puedan conectar a él.

Para una determinada WLAN con topología Ad-Hoc, todos los equipos conectados a ella (Host) deben de ser configurados con el mismo identificador de servicio básico (Basic Service Set, BSSID)

Descripción general del funcionamiento de la modalidad Ad-Hoc

Este modo no tiene punto de acceso. Podemos decir que en este tipo de estructura solo hay dispositivos inalámbricos presentes, las tareas de señalización y la sincronización son controladas por una estación.

La red Ad-Hoc tiene varios inconvenientes comparada con las redes infraestructura , uno de ellos es que este tipo de red no permite la posibilidad de trasmitir tramas entre dos estaciones que no se oyen mutuamente.

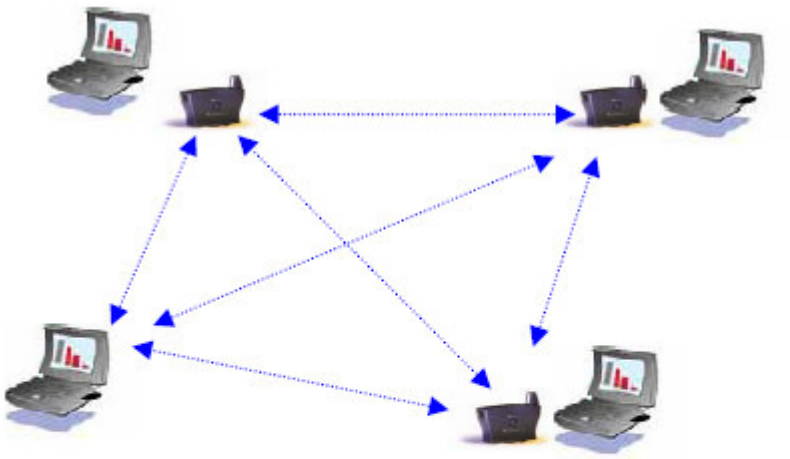
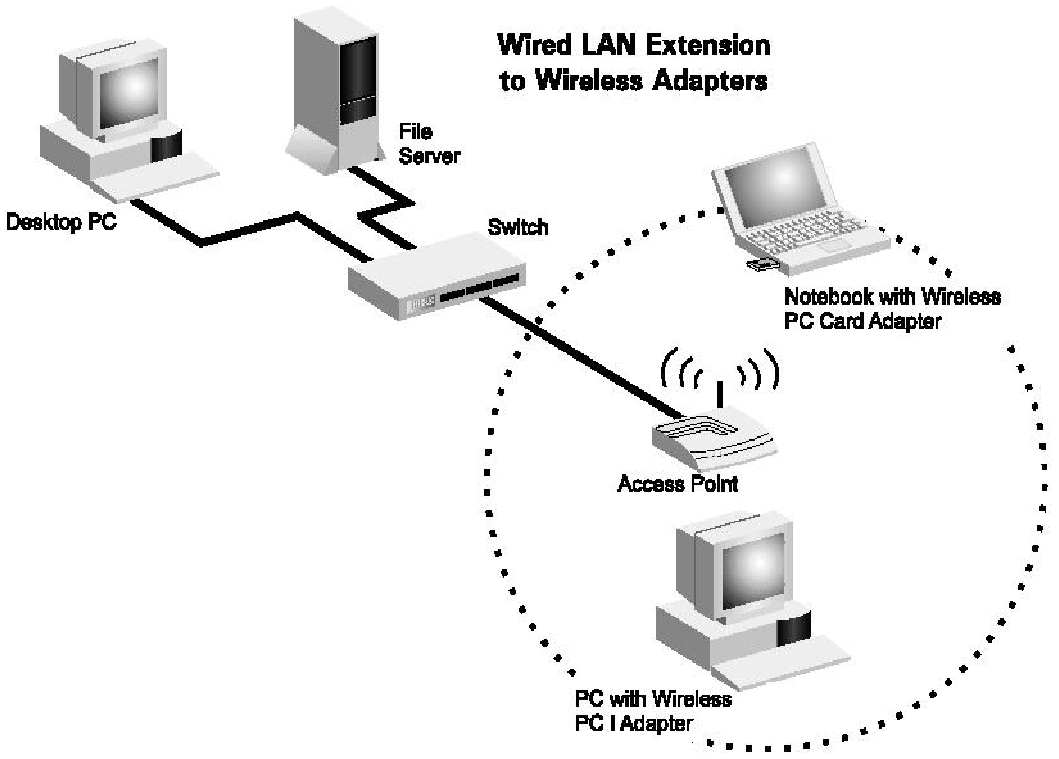


Figura 3: Modo Ad Hoc

- **Topología Infraestructura**

En el cual existe un nodo central (Punto de Acceso) que sirve de enlace para todos los demás (Tarjetas de Red). El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión especifica. 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. La extensión y el número de dispositivos dependen del estándar de conexión inalámbrico que se utilice y del producto.



Del mismo modo, como en las redes Ethernet, en las cuales se dispone de un Hub o concentrador para "unir" todos los Host, ahora disponemos de los Puntos de Acceso (AP), los cuales se encargan de "crear esa conversación" para que se puedan conectar el resto de Host inalámbricos que están dentro de su área de cobertura. Ahora la MAC que identifica a esta "conversación" es la MAC del AP (MAC real).

Esta opción de las redes inalámbricas que sólo puede ser activada por Puntos de Acceso, y utilizada por tarjetas inalámbricas. Permite el enlace con más puntos de acceso y la agrupación de clientes. Admite el Roaming entre Puntos de Acceso.

Si la zona es grande por lo general hay varios puntos de acceso lo que significa que hay varias estaciones base, en cambio si la zona es pequeña como puede ser un hogar o un edificio con un solo punto de acceso bastaría.

Existen en el mercado muchos tipos de APs, con mayores o menores prestaciones:

- Firewall integrado.
- Switch incorporado.
- Función de Bridge entre edificios.
- Función de repetidor.
- Potencia de emisión recepción.

Modo Infraestructura: como máximo puede soportar 2048 nodos/usuarios.

Pero si se hace un uso del ancho de banda "intensivo", como con juegos o multimedia, de 6 a 8 usuarios es el máximo recomendable.

Funcionamiento de la modalidad Infraestructura

El dispositivo inteligente, denominado ESTACIÓN en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a si mismo o mediante el sondeo activo de una red especifica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

Esta asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para distribuir la información de la ubicación actual de la estación en la red.

La estación solo puede trasmitir o recibir datos una vez terminada la asociación.

Esta modalidad obliga a que todo el trafico que proceda de dispositivos inalámbricos pase por un punto de acceso antes de llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones tienen un periodo de tiempo en el cual solo se limita a la escucha de las trasmisiones, en esta parte del protocolo se detectan las portadoras.

Antes de trasmitir, la estación debe esperar durante un periodo de tiempo especifico después de que la red esta despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones.

En este tipo de modalidad (Infraestructura) el emisor o el receptor es siempre el punto de acceso.

Es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones.

Entre ellas, se incluye un intercambio de reserva, que puede tener lugar antes de trasmitir un paquete, mediante un intercambio de tramas " petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir " desde el punto de acceso y puede evitar trasmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no esta completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso proporciona una transición fluida.

La sincronización entres las estaciones de la red se controlan mediante las tramas de señalización periódicas enviadas por el punto de acceso.

Estas tramas contienen el valor de reloj del punto de acceso en el momento de las trasmisiones, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

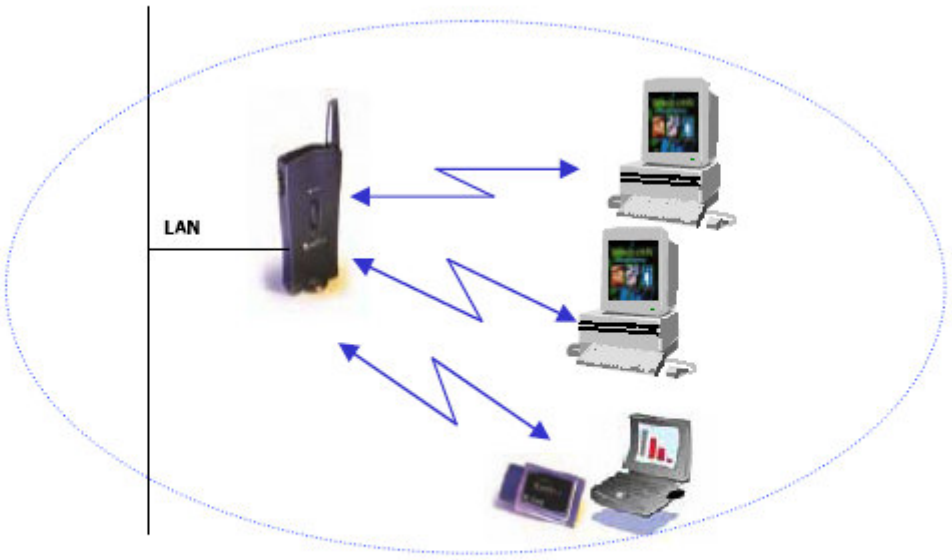


Figura 2: Modo Infraestructura

Las redes inalámbricas pueden construirse con o sin Punto de Acceso (AP), esto es lo que nos determina si es una "Ad-Hoc" o una "Infraestructura".

3.3 Organizaciones que trabajan con la tecnología inalámbrica.

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

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

Asociaciones de la industria: estas organizaciones son creadas para promover el crecimiento de la industria a través de educación y promoción, proveyendo información objetiva sobre la industria en general, tecnologías, tendencias, organizaciones, oportunidades independientemente de la tecnología. La organización más importante en esta categoría es la WLANA (Wireless LAN Association) cuya misión es ayudar y fomentar el crecimiento de la industria a través de la educación que puede ser caracterizada por asociaciones industriales y comerciales.

WECA (Wireless Ethernet Compatibility Alliance)

Alianza de fabricantes formada para mantener la compatibilidad entre dispositivos inalámbricos. La WECA creo el estándar de dispositivos inalámbricos Wifi, que cumplen la norma IEEE 802.11b.

La alianza constituida para fomentar la compatibilidad entre tecnologías Ethernet inalámbricas WECA (Wireless Ethernet Compatibility Alliance) ha decidido cambiar su nombre por el de Wi-Fi Alliance.

El estándar de networking inalámbrico IEEE 802.11b es conocido por una diversidad de nombres dependiendo del contexto: AirPort, si se trata de usuarios Apple, Wireless Ethernet, de una forma más genérica, y Wi-Fi, quizá la denominación más extendida. Lo cierto, es que todos estas denominaciones hacen referencia a la misma tecnología y WECA ha decidido tomar partido reduciendo la confusión al reconocer la amplia aceptación de Wi-Fi como denominación de la principal tecnología que centra sus esfuerzos en la actualidad, se trata, sin lugar a dudas, de un nombre más fácil de recordar. Creada en 1999, Wi-Fi Alliance está abierta a todas aquellas compañías que soporten estándares Wi-Fi (802.11b o Ethernet inalámbrica a 2,4 GHz y 11 Mbps) y Wi-Fi5 (802.11a o Ethernet inalámbrica a 5 GHz y 54 Mbps).

En estos momentos está integrada por más de 140 miembros, incluida Apple Computer, y ha reconocido ya más de 300 productos compatibles con WiFi. La WECA ha definido un conjunto de pruebas que certifican que los productos que las superan pueden funcionar conjuntamente con los de otros fabricantes. Un laboratorio de pruebas independiente, el Silicon Valley Networking Lab, Inc. realiza estas pruebas. Cuando un producto supera las pruebas con éxito, la compañía es autorizada a usar el sello de compatibilidad Wi-Fi en su producto y material accesorio correspondiente. Los consumidores tienen la garantía de que cualquier producto con el logotipo Wi-Fi funcionará con otros productos Wi-Fi.

NEMA (Asociación Nacional de Manufactureros Eléctricos)

Es la mayor asociación en los Estados Unidos representando compañías que fabrican productos para la industria eléctrica. Sus compañías miembros caen en una o más de nueve divisiones de NEMA, cada una hecha de secciones cuyas compañías fabrican los mismos productos u otros relacionados. Juntas, ellas fabrican una amplia esfera de productos para la generación, transmisión, distribución, control, y uso final de la electricidad.

ETSI European Telecommunications Standards Institute

En la Organización ETSI se proporciona información sobre la Asamblea General, la Asamblea Técnica y cada uno de los Comités Técnicos. Se trabaja en la estandarización de las telecomunicaciones y se ofrece respuesta a las múltiples dudas que puedan aparecer.

FCC (Federal Communications Comisión, Comisión Federal de Comunicaciones)

Organismo gubernamental independiente encargado del control y regulación del sector de las Telecomunicaciones (comunicaciones por radio, televisión, teléfono, satélite y cable) en los Estados Unidos.

IEEE

La IEEE ("i" triple "e") es una asociación profesional técnica sin fines de lucro con más de 380,000 miembros individuales en 150 países. El nombre completo es Instituto de Ingenieros en Eléctrica y Electrónica (Institute of Electrical and Electronics Engineers, Inc.)

A través de sus miembros la IEEE es la autoridad principal en áreas técnicas que abarca desde la ingeniería computacional, tecnología biomédica y telecomunicaciones, hasta energía eléctrica, aeroespacial y electrónica para los consumidores, entre otras.

Con su publicar técnico, conferencias y actividades de los estándares basadas en consensos, la IEEE produce el 30% de la literatura mundial en ingeniería eléctrica y de la tencología de computadoras y control; anualmente tiene más de 300 conferencias magistrales y casi 900 estándares activos.

WLANA (Wireless LAN Association)

Es una asociación de industrias y empresas cuya misión es ayudar y fomentar el crecimiento de la industria WLAN a través de la educación y promoción.

IANA (Internet Assigned Numbers Authority).

Es el organismo de la ISOC (Internet Society) de la administración de las direcciones Internet (direcciones IP) así como de la creación de nuevos dominios (DNS). La IANA delega la asignación de dominios ya creados a la InterNIC. IANA es el acrónimo de INTERNET ASSIGNED NUMBER AUTHORITY.

La Agencia de Asignación de Números Internet era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por ICANN.

Bluetooth SIG

Basado en la especificación BluetoothTM especificación que utiliza la tecnología de radio para proveer conectividad a Internet a bajo costo a computadoras portátiles, teléfonos móviles o otros dispositivos portátiles.

HiperLAN1, HiperLAN Alliance e HiperLAN2 Global Forum

Organizaciones europeas que utilizan enlaces de radio de alto desempeño a frecuencias en el rango de 5 GHz.

HomeRF

Basada en una especificación para comunicaciones inalámbricas en hogares conocida por sus siglas en inglés SWAP (shared wireless access protocol). El HRFWG (homeRF Working Group) fue fundado para proveer los cimientos para un amplio rango de dispositivos al establecer una especificación abierta a la industria para comunicaciones digitales inalámbricas entre PCs y dispositivos domésticos alrededor de los hogares.

OFDM

Esta organización está basada básicamente en una tecnología patentada conocida como W-OFDM (Wide-band orthogonal frecuency división multiplexing)

WLI forum

WLIF estableció un estándar interoperable en 1996 conocido como OpenAir, el estándar está disponible a cualquier compañía que se une al Forum. OpenAir es una tecnología de espectro extendio con salto en frecuencia a 2.4 GHz.

Referencias	
Organización	**URL**
IEEE	http://www.ieee.org/
WLANA	http://www.wlana.org/
WECA	http://www.wirelessethernet.org/
HomeRF	http://www.homerf.org/
HiperLAN/2	http://www.hiperlan2.com/
Bluetooth	http://www.bluetooth.com/

3.4 Tecnologías de transmisión de acceso múltiple

3.4.1 FDMA (Acceso Múltiple por División de Frecuencia)

La **tecnología FDMA** separa el espectro en distintos canales de voz, al separar el ancho de banda en pedazos (frecuencias) uniformes. La tecnología FDMA es mayormente utilizada para la transmisión analógica. Esta tecnología no es recomendada para transmisiones digitales, aun cuando es capaz de llevar información digital.

FDMA, es la manera más común de acceso truncado. Con FDMA, se asigna a los usuarios un canal de un conjunto limitado de canales ordenados en el dominio de la frecuencia. Los canales de frecuencia son muy preciados, y son asignados a los sistemas por los cuerpos reguladores de los gobiernos de acuerdo con las necesidades comunes de la sociedad.

Cuando hay más usuarios que el suministro de canales de frecuencia puede soportar, se bloquea el acceso de los usuarios al sistema. Cuantas más frecuencias se disponen, hay más usuarios, y esto significa que tiene que pasar más señalización a través del canal de control.

Los sistemas muy grandes FDMA frecuentemente tienen más de un canal de control para manejar todas las tareas de control de acceso. Una característica importante de los sistemas FDMA es que una vez que se asigna una frecuencia a un usuario, ésta es usada exclusivamente por ese usuario hasta que éste no necesite el recurso.

3.4.2 TDMA (Acceso Múltiple por División de Tiempo)

La **tecnología TDMA** comprime las conversaciones (digitales), y las envía cada una utilizando la señal de radio por un tercio de tiempo solamente. La compresión de la señal de voz es posible debido a que la información digital puede ser reducida de tamaño por ser información binaria (unos y ceros). Debido a esta compresión, la tecnología TDMA tiene tres veces la capacidad de un sistema analógico que utilice el mismo número de canales.

TDMA, es común en los sistemas de telefonía fija. Las últimas tecnologías en los sistemas de radio son la codificación de la voz y la compresión de datos, que eliminan redundancia y periodos de silencio y decrementan el tiempo necesario en representar un periodo de voz. Los usuarios acceden a un canal de acuerdo con un esquema temporal.

Aunque no hay ningún requerimiento técnico para ello, los sistemas celulares, que emplean técnicas TDMA, siempre usan TDMA sobre una estructura FDMA. Un sistema puro TDMA tendría sólo una frecuencia de operación, y no sería un sistema útil. TDMA es un concepto bastante antiguo en los sistemas de radio.

En los sistemas modernos celulares y digitales, TDMA implica el uso de técnicas de compresión de voz digitales, que permite a múltiples usuarios compartir un canal común utilizando un orden temporal. La codificación de voz moderna, reduce mucho el tiempo que se lleva en transmitir mensajes de voz, eliminando la mayoría de la redundancia y periodos de silencio en las comunicaciones de voz. Otros usuarios pueden compartir el mismo canal durante los periodos en que éste no se utiliza.

3.4.3 CDMA (Acceso Múltiple por División de Código)

Es un término genérico que describe una interfaz inalámbrica basada en la tecnología de acceso múltiple por división de código o de espectro expandido.

CDMA. Pasado, presente y futuro

La tecnología CDMA constituyó un fuerte elemento impulsor de los sistemas 2G en el momento de su aparición a principios de la década de los 90. Actualmente, en el marco de las actividades de desarrollo de los sistemas 3G, CDMA vuelve a presentar un papel preponderante, esta vez en versión de banda ancha o W-CDMA (Wideband CDMA) De hecho, esta tecnología aparece en la mayor parte de las propuestas presentadas a la UIT relativas a interfaz de radio para la tercera generación.

Los sistemas CDMA convencionales están basados en técnicas de espectro esparcido (spread-spectrum), que constituyen un legado del ámbito de la defensa en aplicaciones relativas a la eliminación de interferencias (anti-jamping), medidas de distancias (ranging) o encriptación. Estas técnicas se basan en esparcir el espectro de frecuencias de una señal en un ancho de banda mayor que el mínimo requerido para la transmisión, una situación que se mantiene a lo largo de todo el proceso de transmisión. Posteriormente, al llegar al receptor, la señal se recompone para obtener la señal inicial que se deseaba transmitir.

De esta forma, se puede obtener una serie de enlaces que utilizan la misma banda de frecuencia simultáneamente sin que se generen interferencias. CDMA es una tecnología de acceso múltiple, lo que significa que puede dar soporte a varios usuarios de forma simultánea; como puede ser, por ejemplo, una llamada telefónica. De esta manera el acceso múltiple significa que un número de usuarios suficientemente elevado comparte un mismo conjunto de canales de modo que cualquier usuario puede acceder a cualquier canal sin que existan asignaciones predeterminadas entre usuarios y canales.

CDMAOneTM

Es un nombre comercial de marca registrada, reservado para uso exclusivo de las empresas que son miembros de CDG. El mismo describe un sistema inalámbrico completo que incorpora la interfaz aérea IS-95 CDMA y la norma de la red ANSI-41 para la interconexión por conmutación, además de muchas otras normas que integran el sistema inalámbrico completo.

CDMA2000

Identifica la norma TIA para tecnología de tercera generación, que es un resultado evolutivo de CDMAOne, el cual ofrece a los operadores que han desplegado un sistema CDMAOne de segunda generación, una migración transparente que respalda económicamente la actualización a las características y servicios 3G, dentro de las asignaciones del espectro actual, tanto para los operadores celulares como los de PCS.

La interfaz de red definida para CDMA2000 apoya la red de segunda generación de todos los operadores actuales, independientemente de la tecnología: CDMAOne, IS-136 TDMA o GSM). La TIA ha presentado esta norma ante la ITU como parte del proceso IMT-2000 3G.

CDMA y el Internet Móvil

Los servicios móviles basados en el estándar CDMA permiten a centenares de millones de usuarios disfrutar de contenido multimedia, en todo momento y en cualquier lugar. Según un estudio publicado por la firma Datacomm Research Company, cuya sede se encuentra en Chesterfield, Missouri, el mercado de Internet Móvil estallará una vez que los operadores comiencen a ofrecer recursos multimedia a precios razonables.

Estándar para celulares CDMA (IS95)

Con CDMA, para diferenciar a los distintos usuarios, en lugar de frecuencias separadas se usan códigos digitales únicos. Los códigos son conocidos tanto por la estación móvil (teléfono celular) como por la estación base, y se llaman "Secuencias de Código Pseudo-Aleatorio". Por lo tanto todos los usuarios comparten el mismo rango del espectro radioeléctrico.

En telefonía celular, CDMA es una técnica de acceso múltiple digital especificada por la Asociación de Industria de Telecomunicaciones (TIA) como "IS-95." La TIA aprobó el estándar para celulares CDMA IS-95 en julio de 1993.

Los sistemas IS-95 dividen el espectro radioeléctrico en portadoras de 1.25 MHz de ancho de banda.

Tecnología CDMA

CDMA usa una tecnología de Espectro Ensanchado, es decir la información se extiende sobre un ancho de banda muyo mayor que el original, conteniendo una señal (código) identificativa. Una llamada CDMA empieza con una transmisión a 9600 bits por segundo. Entonces la señal es ensanchada para ser transmitida a 1.23 Megabits por segundo aproximadamente.

El ensanchamiento implica que un código digital concreto se aplica a la señal generada por un usuario en una célula. Posteriormente la señal ensanchada es transmitida junto con el resto de señales generadas por otros usuarios, usando el mismo ancho de banda. Cuando las señales se reciben, las señales de los distintos usuarios se separan haciendo uso de los códigos distintivos y se devuelven las distintas llamadas a una velocidad de 9600 bps.

Los usos tradicionales del espectro ensanchado son militares debido a que una señal ensanchada es muy difícil de bloquear, de interferir y de identificar. Esto es así porque la potencia de estas señales esta distribuida en un gran ancho de banda y solo aparece como un ruido ligero. Lo contrario ocurre con el resto de tecnologías que concentran la potencia de la señal en un ancho de banda estrecho, fácilmente detectable.

Sincronización

En la fase final del radio-enlace, sentido estación base - móvil nuestra llamada no se transmite de forma continua. Cada cierto tiempo se conmuta entre los distintos usuarios y se transmite parte de su llamada con el pseudo-código correspondiente. Este proceso se debe repetir continuamente para que un usuario no pierda la llamada al no reconocer su código concreto.

Por ello las estaciones base deben estar sincronizadas con una referencia de tiempo común.

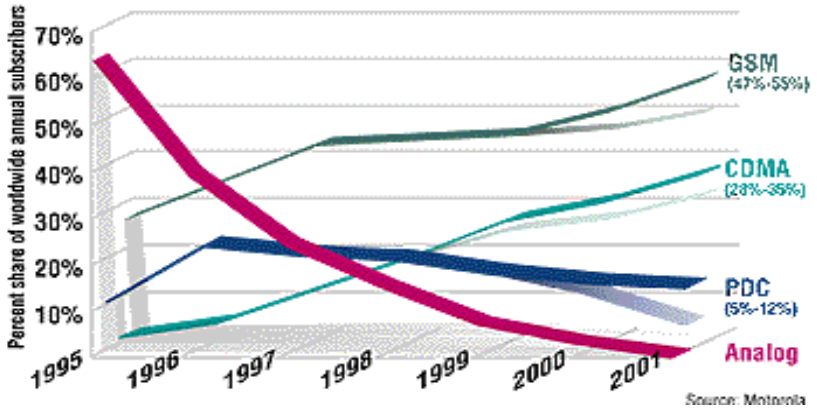
El Sistema del Posicionamiento Global (GPS) usa esta técnica de sincronización. GPS es un satélite basado en un sistema de radionavegación capaz de proporcionar mediante medios prácticos y económicos la posición, velocidad, y tiempo a un número ilimitado de usuarios, de forma continua.

Ventajas de CDMA

Las ventajas que ofrece CDMA son:

- La capacidad aumenta de 8 a 10 veces respecto al sistema AMPS y de 4 a 5 veces respecto de GSM.
- Mejor calidad de llamada con sonido más claro.
- Sistema simplificado que usa la misma frecuencia en cada sector de cada célula.
- Mejora las características de cobertura, etc.

Gráfica sobre la evolución de las distintas tecnologías:



3.4.3.1 W-CDMA. (Wideband Code División Multiple Access)

W-CDMA es una tecnología CDMA extendida en términos de ancho de banda en un entorno de frecuencias de entre 5 y 20 MHz. Actualmente, la mayor parte de actuaciones en W-CDMA se están desarrollando para 5 MHz, aunque se espera que próximamente aparezcan de una manera regular los desarrollos en ancho de banda de 10, 15 y 20 MHz.

Un aspecto crucial relativo a W-CDMA viene dado por las cuestiones de planificación de red, puesto que, al tratarse de un sistema de 3G, ha de proporcionar servicios multimedia. En este contexto, es necesario identificar los aspectos clave analizando su impacto en el esquema de negocio de los operadores: en particular, la modelización del canal W-CDMA presenta un importante papel en la planificación de red, así como la estimación del impacto del tráfico.

Otro aspecto de especial importancia para la planificación viene dado por el proceso de asignación de licencias.

W-CDMA Se refiere a las normas ETSI y NTT DoCoMo (filial móvil de la japonesa NT&T) para tecnología de tercera generación sometida ante la ITU, como parte del proceso IMT-2000 3G. Esta norma incorpora una interfaz aérea que utiliza la técnica CDMA, pero que no es compatible en la forma en que está definida para las interfaces inalámbricas y de red con CDMAOne, CDMA2000 o IS-136. La especificación de interfaz aérea no es compatible con GSM y, por lo tanto, no apoya la migración evolutiva.

Diferencias principales entre cdma2000 y W-CDMA

	CDMA2000	W-CDMA
Sincronización de la estación base	Sincronizado	*No sincronizado*
Adquisición y detección de la estación base	Correlación PN de tiempo desplazado	Búsqueda de códigos paralelos en tres pasos para la detección de la estación base y la sincronización de ranuras / tramas
Longitud de la trama	20 ms	10 ms
Velocidad de la plaqueta	3.6864 Mcps	4.096 Mcps *
Piloto de enlace delantero para el calculo del canal	Piloto común CDM	Piloto dedicado TDM
Formación de haz de antena y haces cerrados	Piloto auxiliar dedicado CDM	Piloto dedicado TDM

3.5 Hand Off

Hand Off es el proceso de transferir la llamada de un usuario de un satélite a otro. En Globalstar puede ser de dos tipos:

Soft Hand Off:

Dos o más señales recibidas a través de distintos enlaces son demoduladas simultáneamente, combinadas, y descodificadas por la misma entidad. Se caracteriza por iniciar las comunicaciones utilizando un nuevo piloto para la misma frecuencia CDMA antes de terminar la comunicación con el antiguo piloto sin interrumpir por tanto la llamada. Este hand off tiene lugar cuando el terminal de usuario opera en el canal de tráfico.

Hard Hand Off:

La entidad receptora deja de demodular y descodificar la información transmitida en un enlace y comienza a demodular y descodificar la información transmitida en otro enlace con posible pérdida de información. Se caracteriza por una desconexión temporal del canal de tráfico al cambiar el terminal de usuario de frecuencia.

3.6 Tecnologías de Modulación de Frecuencia

- ✓ **FHSS (Frequency Hopping Spread Spectrum) (Salto de Frecuencia del Espectro Disperso)**

Sistema de transmisión de datos en la capa física que modula en diferentes frecuencias los datos que se envían, cambiando de una frecuencia a otra durante la transmisión, siempre dentro de la banda de los 2,4GHz. Se reservan 83MHz para FHSS.

La señal 802.11 ocupa un ancho de banda de 1MHz y espera aleatoriamente entre 79 canales diferentes (estándar Europeo).

La secuencia "hopping" del transmisor es conocida por el receptor, que sincroniza con el transmisor. La interferencia puede ocurrir solamente si dos transmisores utilizan el mismo canal simultáneamente.

Frequency Hopping es el tipo de comunicación original Spread Spectrum. En las WLANs 802.11, la velocidad de "hopping" es alrededor de 2.5 hops/segundo.

Frequency-hopping spread-spectrum (FHSS) utiliza una señal portadora que cambia de frecuencia en un patrón que es conocido por el transmisor y el receptor. Apropiadamente sincronizada, la red efectúa este cambio para mantener un único canal lógico de operación.

Esta tecnología utiliza una forma de salto que le permite al paquete de datos (voz, datos o video) que brinque a través de los 104 canales que existen en la frecuencia 2.4Ghz o otras. Esto permite que el paquete tenga mejor porcentaje de llegar a su destinatario. El radio es ideal para largas distancias y aplicaciones punto a punto pero son muy costosos.

DSSS (Direct-sequence spread-spectrum) (Secuencia Directa del Espectro Disperso)

Genera un patrón de bit (Secuancia Barker de 11 bits) redundante por cada bit a ser transmitido. Este proceso extiende la energía de RF por un ancho de banda más extenso que el que se requeriría para transmitir los datos en bruto. Este bit patrón es llamado un chip (o chipping code). La longitud del chip, tiene una probabilidad mayor de que los datos puedan ser recuperados, porque el receptor agrupa la entrada del RF para recuperar los datos originales.

Si uno o más bits en el chip son "dañados" durante la transmisión, se pueden recuperar los datos originales a través de técnicas estadísticas aplicadas sobre las señales de radio, sin necesidad de retransmisiones. Para un receptor no atendido, DSSS aparece como una señal de ruido con un ancho de banda de bajo poder que es ignorada por el resto de los receptores.

La mayoría de los fabricantes de productos para LAN inalámbricas han adoptado la tecnología DSSS después de considerar los beneficios vs. los costos y rendimiento que se obtienen con ella.

La ventaja de esta técnica es que reduce el efecto de fuentes de interferencia de banda estrecha. Esta secuencia proporciona 10.4dB de aumento del proceso, el cual reúne los requisitos mínimos para las reglas fijadas por la FCC.

Esta tecnología salta pero dentro de un canal. Esta es la razón por la que los radios DSSS requieren que existan 6 canales de separación para que no se intervenga entre ella misma. Es por eso que el canal 1, 6, 11 se debe de utilizar para prevenir interferencia entre la frecuencia 2.4Ghz. Ideal porque es muy económico y es fácil de integrar. Desventaja es que es sujeto a interferencia más que los radios de FHSS.

Tabla A-1 Frecuencias DSSS para operar en diferentes regiones

Nº Canal	Frecuencias Norteamericanas	Frecuencias Europeas	Frecuencias Japonesas
1	2412 MHz	N/A	N/A
2	2417 MHz	N/A	N/A
3	2422 MHz	2422 MHz	N/A
4	2427 MHz	2427 MHz	N/A
5	2432 MHz	2432 MHz	N/A
6	2437 MHz	2437 MHz	N/A
7	2442 MHz	2442 MHz	N/A
8	2447 MHz	2447 MHz	N/A
9	2452 MHz	2452 MHz	N/A
10	2457 MHz	2457 MHz	N/A
11	2462 MHz	2462 MHz	N/A
12	N/A	N/A	2484 MHz

- ✓ **Modulación PSK, BPSK** (Binary Phase Shift Keying)

Con un sistema BPSK son posibles dos salidas de fase diferentes con una sola portadora. Si la señal de entrada cambia de estado, la fase de la señal de salida se recorre entre dos ángulos de 180°, la frecuencia se mantiene.

- ✓ **OFDM: Orthogonal Frecuency Division Multiplexing**

Esta tecnología tiene mas de 3 años en el mercado y sigue su curso en desarollo. El protocolo de 802.11a funciona bajo esta tecnologia que tecnicamente no require Linea de Vista. Esto es ideal porque hay zonas dificiles de conectar y esta tecnologia lo hace facil. Desventaja: Es que no existe forma de incrementar la distancias de estas. No existen amplificadores y la realidad es que los "actual thruputs" desminullen mas abajo de 1Mbps cuando son distancias a mas de 2-3km en enlaces punto a punto, haciendo la tecnologia solo util para el interior.

- ✓ **Qpsk (Quaternary Phase Shift Keying)**

Técnica de modulación de frecuencia digital utilizada para enviar datos sobre redes de cable coaxial. Como es fácil de implementar y bastante resistente al ruido, se utiliza principalmente para enviar datos desde el abonado de cable hacia Internet.

- ✓ **Modulación FSK (Frecuency Shift Keying)**

FSK es la más simple de las modulaciones digitales y por lo tanto es de bajo desempeño. Es similar a la modulación en frecuencia excepto que la señal moduladora es un tren de pulsos binarios que varía entre dos voltajes discretos.

3.7 mW y dBm

dBm es la potencia de radio expresada en dB referida a 1mW. En España la potencia máxima permitida de emisión para la banda ISM (2,4GHz) es de **100mW**.

Esta potencia de emisión es el resultado de sumar la potencia de salida de la tarjeta WIFI, con la ganancia de la antena y teniendo en cuenta las perdidas del cable y conectores.

Para convertir mW a dBm, tenemos que multiplicar por 10 el logaritmo de la potencia expresada en mW. Por ejemplo, si la potencia máxima son 100mW:

$$10 \times \log 100mW = 20\ dBm$$

La potencia máxima legal de emisión es de 100mW o 20 dBm.

La mayoría de los dispositivos inalámbricos emiten en un rango de 20 a 50mW:

10 x log 50mW = 17 dBm

Lo que quiere decir que podemos utilizar una antena de hasta 3 dBm máximo para estar dentro de la legalidad.

Por ejemplo, el adaptador PCI de SMC indica que emite a +13 dBm (20 mW), si suponemos que utilizamos una antena de +8 dBm de ganancia y tenemos unas pérdidas en el cable de –3 dBm, estaremos emitiendo:

+13 + 8 – 3 = 18 dBm (63 mW)

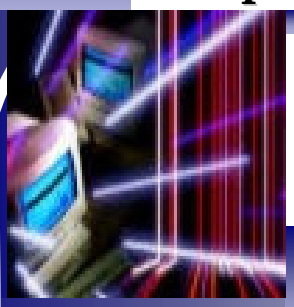
Inferior al máximo establecido legalmente.

Tabla de conversión rápida de dB a mW.

DBm	mw		DBm	mw
0dBm	1mW		16dBm	40mW
1dBm	1.25mW		17dBm	50mW
2dBm	1.56mW		18dBm	64mW
3dBm	2mW		19dBm	80mW
4dBm	2.5mW		20dBm	100mW
5dBm	3.12mW		21dBm	128mW
6dBm	4mW		22dBm	160mW
7dBm	5mW		23dBm	200mW
8dBm	6.25mW		24dBm	256mW
9dBm	8mW		25dBm	320mW
10dBm	10mW		26dBm	400mW

DBm	mw		DBm	mw
11dBm	12.5mW		27dBm	512mW
12dBm	16mW		28dBm	640mW
13dBm	20mW		29dBm	800mW
14dBm	25mW		30dBm	1000mW
15dBm	32mW			

Capitulo IV



Análisis y Propuesta para la Implementación de la Infraestructura para Interconectar las Bibliotecas de las Universidades de Santo Domingo

IV. ANÁLISIS Y PROPUESTA PARA LA IMPLEMENTACIÓN DE LA INFRAESTRUCTURA PARA INTERCONECTAR LAS BIBLIOTECAS DE LAS UNIVERSIDADES DE SANTO DOMINGO

4.1 Caso de Estudio: Bibliotecas Universitarias

En este estudio se plantea una solución para que los estudiantes universitarios tengan la facilidad de acceder a los datos de bibliografías existentes en las bibliotecas de las universidades del territorio de Santo Domingo, sobre todo que puedan obtener la información necesaria en el menor tiempo posible, ya que la interconexión planteada es inalámbrica, la cual proporciona una mayor velocidad de transmisión de la data.

La mayoría de las universidades en cuestión tienen en sus Web Sites las consultas a las bibliotecas, lo que facilita y agiliza el manejo de informaciones. Todo esto es indicio de lo importante que sería el proceso de implementación de esta propuesta.

Las bibliotecas universitarias que hemos tomado en consideración para este proyecto son:

- ✓ UNAPEC (Universidad Acción Pro-Educación y Cultura)

  Biblioteca: Lic. Fidel Méndez Núñez.

- ✓ UNIBE (Universidad Iberoamericana)
- ✓ UTESA (Universidad Tecnológica de Santiago, Recinto Santo Domingo de Guzmán)
- ✓ UASD (Universidad Autónoma de Santo Domingo)
- ✓ PUCMM (Pontificia Universidad Católica Madre y Maestra, Recinto Santo Tomas de Aquino)

  Biblioteca: Rafael Herrera Cabral
- ✓ O & M (Universidad Dominicana Organización & Método)

  Biblioteca: Dr. Luis Scheker
- ✓ INTEC (Instituto Tecnológico de Santo Domingo)

  Biblioteca: Emilio Rodríguez Demorizi
- ✓ UNPHU (Universidad Nacional Pedro Henríquez Ureña)

  Biblioteca: UNPHU

4.2 Distancia entre cada punto de conexión

Informe de distancia y elevación entre la central y las localidades aliadas.

Proyecto :
Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

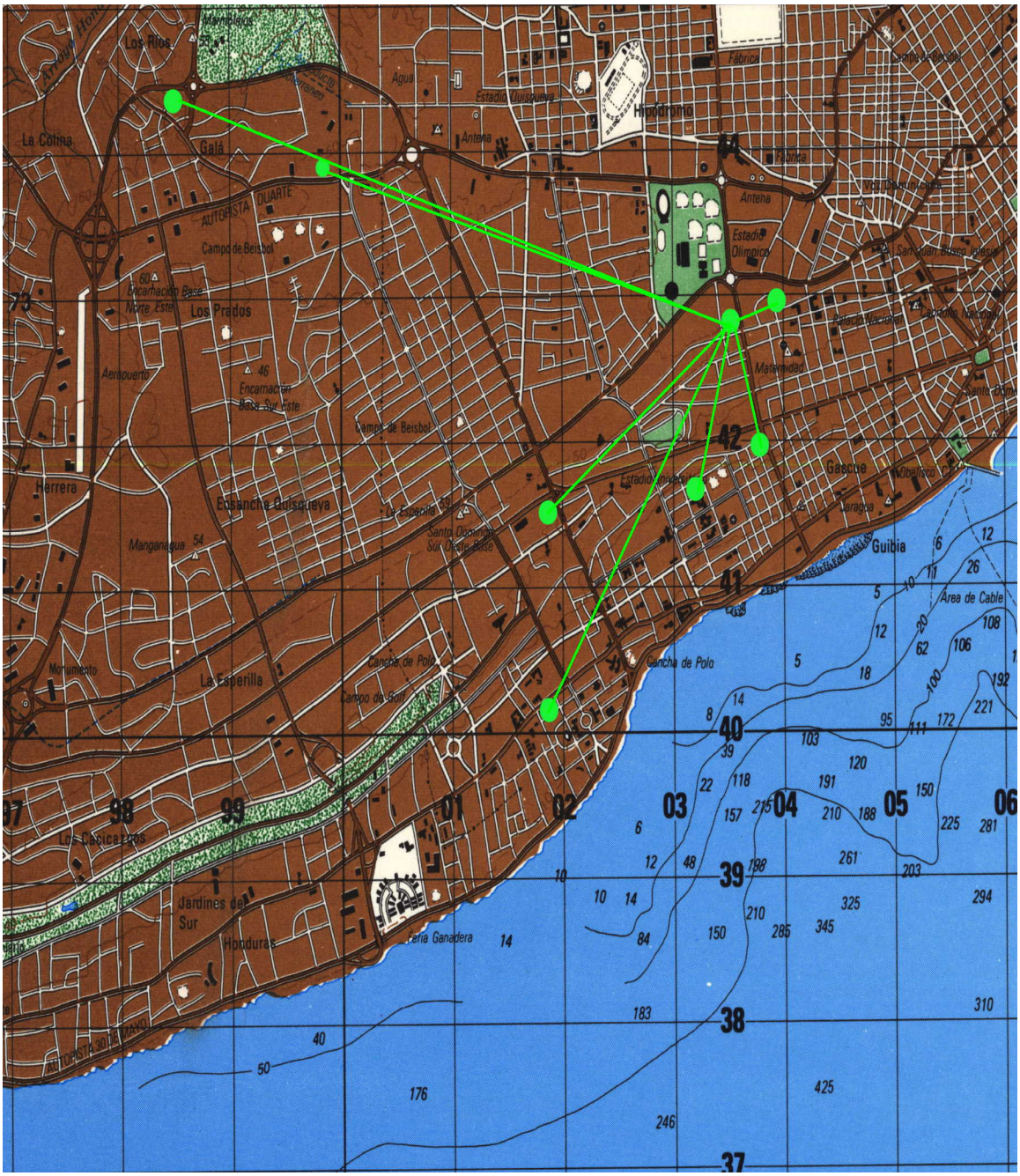
Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Desde	A	Acimut cuadrícula	Distancia cuadrícula (millas)	Distancia cuadrícula (metros)	Incremento elevación
UNAPEC	INTEC	288°48'14"	3.508mi	5646.364m	2.000m
UNAPEC	UNPHU	287°03'31"	2.372mi	3817.971m	3.050m
UNAPEC	UNIBE	64°05'37"	0.242mi	389.102m	-4.950m
UNAPEC	PUCMM	236°16'18"	1.293mi	2080.126m	-3.750m
UNAPEC	O&M	213°14'53"	1.898mi	3055.102m	-37.450m
UNAPEC	UASD	205°17'50"	0.691mi	1111.598m	-31.550m
UNAPEC	UTESA	178°28'57"	0.469mi	755.265m	-21.450m

Informe extraído del sistema TGO.

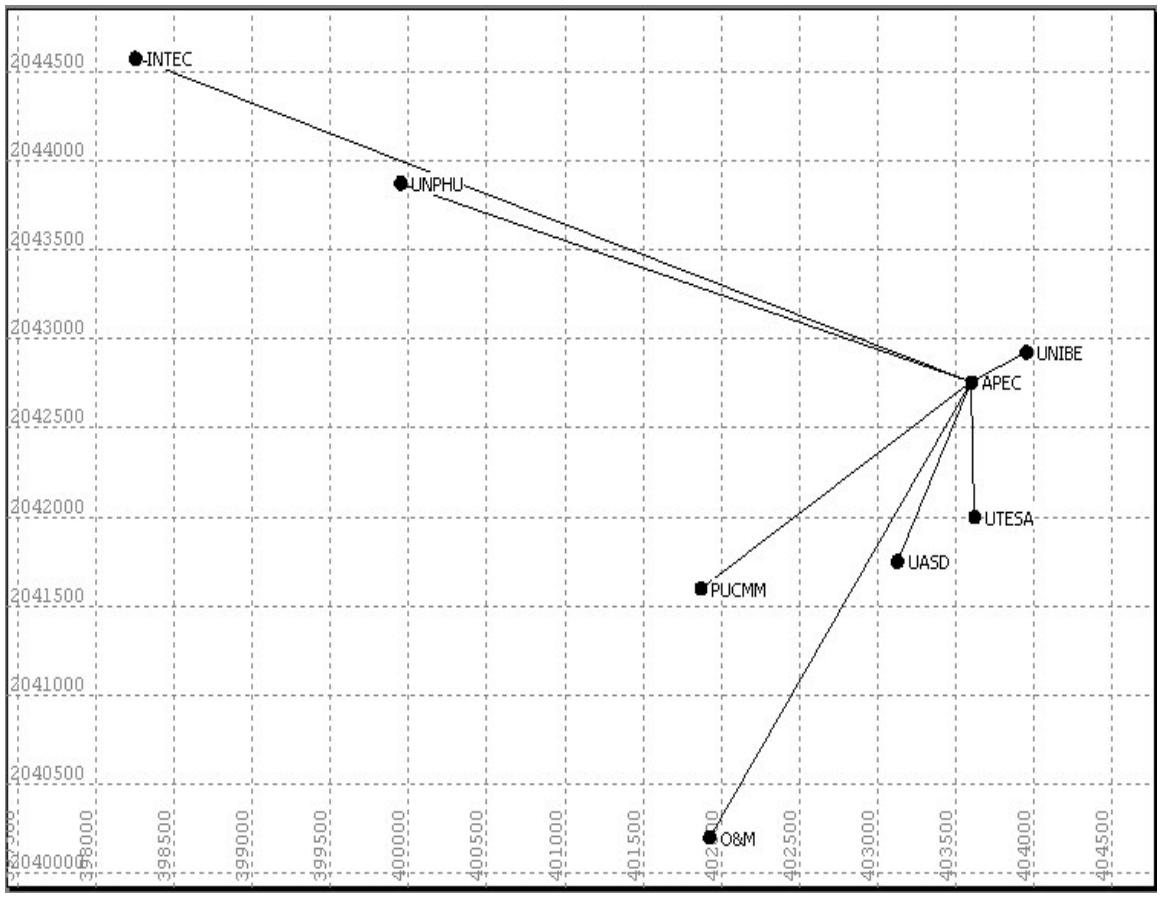
Este informe muestra la distancia aérea en millas y metros, así como también la diferencia de elevación con relación al nivel del mar existentes entre las localidades y la sede central.

4.3 Distribución Geográfica de la Red



Mapa Topográfico

El mapa de topográfico nos ofrece bajo la forma de curvas de nivel[1] el relieve del terreno y la ubicación geográfica de cada uno de los puntos que conforman la red. Dichos puntos han sido marcados en color verde.



Esta imagen fue construida por el sistema Trimble Geomatics Office (TGO) a partir de la extracción de las coordenadas UTM (Universal Transverse Mercato)[2] del mapa topográfico visto anteriormente.

[1] Curvas de Nivel: muestran el contorno hipotético que tendría la línea de intersección entre el suelo y un plano horizontal colocado a determinadas alturas.
[2] UTM: Este sistema permite localizar la posición geográfica con una precisión de hasta un metro.

La imagen referenciada permite visualizar las coordenadas aproximadas de cada una de las universidades. La conexión entre cada punto fue hecha en base al tipo de red que se propone utilizar, la cual es la red punto-multipunto, cada punto fue conectado desde su origen (las diferentes universidades) a la central (UNAPEC).

4.4 Estándar a utilizar

El Standard 802.11g fue elegido luego de haber depurado las características de los demás estándares de frecuencia libre que están actualmente en el mercado, por las siguientes razones:

1- Su capacidad de transmisión hasta 54 Mbps, que es en la actualidad la capacidad mas alta en transmisión inalámbrica de datos, hasta que entre en vigencia el estándar 802.11n.
2- Utiliza la frecuencia de 2.4 Ghz, la cual es libre en la mayoría de los países.
3- Compatible con los HotSpots actuales de 802.11b.
4- Las tasas de transferencia de datos que permite este estándar es de:

   1, 2, 5.5, 11 Mbps

   6, 9, 12, 18, 24, 36, 48, 54 Mbps
5- Este estándar es relativamente barato.

4.5 Topología y Arquitectura

Sugerimos utilizar la topología de Infraestructura, ya que el tipo de red que se esta proponiendo es punto-multipunto, la cual utiliza AP (Puntos de Acceso) y estos necesariamente se auxilian de esta topología.

La arquitectura que mejor se adapta a la topología que se va a utilizar es la BSS (Conjunto Básico de Servicios), porque la misma permite conectar nuestra red inalámbrica con las redes alámbricas que existe en cada una de las bibliotecas universitarias, dejando claro que no estamos conectando terminales, sino redes alámbricas con inalámbrica.

4.6 Seguridad

La seguridad o los niveles de seguridad, es una de las partes fundamentales que hay que considerar al momento de instalar una red ya sea alámbrica o inalámbrica. La escala de seguridad, dependerá básicamente de lo critica que sea la información que se esté transmitiendo.

En la red que proponemos, la seguridad dependerá en gran medida de la utilización que se le de a dicha red. Dicho esto, porque si se utiliza solo para verificación de existencia de textos, la información no seria tan critica como en el caso de que hubiese que transmitir datos personales (claves, matriculas, nombres, etc.) de los estudiantes o personas registradas.

Según el enfoque que le damos a la red que proponemos, la cual se limita solo al intercambio de informaciones bibliográficas, sugerimos la utilización de:

6- **Estándar de seguridad 802.1x,** se usa para gestionar el proceso de autenticación entre la sede central y las demás localidades, así como la gestión y reparto de claves de cifrado de cada una de ellas. Permite el uso del protocolo extendido de autorización (EAP) para integrarse con sistemas externos de autenticación y autorización que pudiesen tener las distintas universidades.

7- **SSID, asignación de clave.** Cada universidad que integre la red, recibe su propia identificación SSID que le será asignada por el administrador al configurar la red inalámbrica, de esta forma podrán identificarse las diferentes localidades cada vez que transmitan o reciban datos. El método de SSID que se recomienda utilizar el "activo", porque la mayor parte de los controladores de tarjetas inalámbricas permiten el rastreo de SSID mediante este método.

8- **Direcciones MAC.** Es muy importante que todas las localidades registren sus direcciones MAC para que la red pueda reconocer los equipos y asi evitar la intromisión de dispositivos no autorizados.

9- **Servicio de Autenticacion WEP.** Cada estación debe probar que está autorizada para conectarse a la red. Como sabemos la autenticacion WEP requiere que tanto el AP como las estaciones que se conectan a él tengan el mismo tipo de cifrado para que se puedan entender. Recomendamos que se utilize la autenticación WEP que tenga la capacidad de llegar hasta los 512 bits porque actualmente es el cifrado más avanzado.

10- **Uso del OSA.** Consideramos necesario utilizar también el sistema abierto de autenticación OSA, porque este nos permite cambiar la clave de los dispositivos que pertenecen a la red cada cierto tiempo de forma automática. Esto además nos brinda mayor seguridad, pues los intrusos no tendrían tiempo para obtener información suficiente de la clave como para exponer la seguridad del sistema.

11- **Encriptación AES.** Sin importar lo crítico de la información que se transmita a través de cualquier tipo red, es necesario que los datos esten cifrados o encriptados. Por esto, sugerimos la utilización del estándar de encriptación AES, ya que este el sistema de encriptación de mayor renombre a nivel mundial.

12- **FireWall.** La utilización de un cortafuegos o Firewall es de suma importancia en cualquier tipo de red, debido a que este es un sistema de defensa que coloca una barrea lógica entre la red y los posibles intrusos. Es por ello, que consideramos conveniente la instalación de Firewall para evitar el acceso directo tanto a la red inalámbrica porpuesta como a las redes alámbricas que existen en las diferentes universidades.

13- **Seguridad Física**. El nivel de seguridad que aplique dependerá de cada una de las universidades. Cada una de ellas debe velar de que el acceso a los equipos sea sólo por parte del personal autorizado y de brindarle a los equipos la seguridad apropiada para su mantenimiento.

Nota:

Además de las sugerencias dadas anteriormente, exhortamos a quien decida implementar este proyecto, referirse al tema de "Seguridad" que se encuentra en el Capítulo II de esta monografía.

4.7 Descripción de los Componentes WLAN

4.7.1 Descripción del Punto de Acceso (Access Point)

Como ya sabemos un punto de acceso es simplemente "Guardar y Repetir", son dispositivos que validan y retransmiten los mensajes recibidos. Estos deben ser colacados en un lugar donde puedan abarcar toda el área donde se encuentran las localidades. Debido a que la red que proponemos es de tipo punto-multipunto, se debe colocar solo un punto de acceso, el cual estará ubicado en la sede central.

Dicho AP debe contar con las siguientes características:

- ✓ La antena del repetidor debe de estar a la altura requerida, esto producirá una mejor cobertura.
- ✓ La antena receptora debe de ser más compleja que la repetidora, así aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.
- ✓ El punto de acceso debe funcionar en la banda de 2.4 Ghz, porque esta es la banda que utiliza el estándar 802.11g que proponemos utilizar.
- ✓ Sistema de seguridad inteligente capaz de detectar la presencia en la red de puntos de acceso no autorizados que intenten infringir la seguridad del sistema, así como la presencia de hackers y puntos de acceso cercanos a la red.

- ✓ Calidad de servicio.
- ✓ Administración de energía.
- ✓ Rendimiento de procesamiento de datos graduable.

4.7.2 Antenas

4.7.2.1 Descripción física de Antenas

Como la red planteada de del tipo punto-multipunto, es de recomendar que las antenas a utilizar son de dos tipos, distribuidas de la siguiente manera:

Para la Central:

La localidad central (UNAPEC) debe poseer una antena Omnidireccional, ya que en esta el diagrama de radiación es disperso, emitiendo en todas direcciones, pudiendo la señal ser recibida por las demás antenas.

Para las Terminales:

Las demás localidades deberán tener una antena Direccional, esto así porque estas emiten la señal hacia un punto en concreto, dichos puntos transmitirán hacia la cede central.

4.7.1.2 Zona de Freesnel

La Zona de Fresnel (FZ) es un elemento que hay que tomar en consideración cuando se está planificando la instalación de las antenas y así evitar que ocurran errores con la Radio Frecuencia (RF). La FZ ocupa una serie de áreas concéntricas tipo hélice, alrededor de la ruta de la línea de Vista (LOS).

Esto es importante para conservar la integridad de la RF porque define el área que se encuentra alrededor de la LOS y que puede introducir interferencia en la señal cuando es bloqueada.

Algunos objetos en la FZ tales como árboles, montañas y edificios pueden desviar o reflejar la señal principal lejos de la recta, cambiando la LOS de la señal. Estos mismos objetos pueden absorber o desaparecer la señal principal de la RF, causando una degradación o perdida total de la señal.

El radio de la FZ puede ser calculada con la siguiente formula:

$$r = 43.3 \times \sqrt{d / 4f}$$

Donde:

d: es la distancia en millas de un punto a otro.

f: es la frecuencia en Ghz que se va a utilizar en la transmisión.

r: es el resultado, el cual se representa en pies.

Estos son los resultados de los cálculos hechos a la red propuesta.

Desde	Hasta	Distancia (Millas)	f (¿?)	r (pies)	r (metros)
APEC	INTEC	3.508mi	2.497 Ghz	25.46078	7.645879
APEC	UNPHU	2.372mi	2.497 Ghz	20.93626	6.287166
APEC	UNIBE	0.242mi	2.497 Ghz	6.68728	2.008192
APEC	PUCMM	1.293mi	2.497 Ghz	15.45757	4.641912
APEC	O&M	1.898mi	2.497 Ghz	18.72794	5.624005
APEC	UASD	0.691mi	2.497 Ghz	11.30006	3.393412
APEC	UTESA	0.469mi	2.497 Ghz	9.573763	2.875004

4.8 Reglamento para las concesiones de licencias para prestar servicios de telecomunicaciones en la Republica Dominicana

Estos son los puntos principales de la resolución aprobada el día veinticuatro (24) de enero del año dos mil dos (2002) por el INDOTEL, autoridad dominicana encargada de regir las leyes para las concesiones, licencias y permisos de servicios de telecomunicaciones. El proyecto propuesto se debe regir por estos reglamentos, que otorgan el permiso para la utilización del espacio aéreo en la transmisión de datos. Al mismo tiempo protege dicho espacio para que no sea utilizado o interferido por otros.

INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL)

RESOLUCIÓN NO. 007-02

QUE APRUEBA LAS ENMIENDAS EFECTUADAS AL "REGLAMENTO DE CONCESIONES, INSCRIPCIONES EN REGISTROS ESPECIALES Y LICENCIAS PARA PRESTAR SERVICIOS DE TELECOMUNICACIONES EN LA REPÚBLICA DOMINICANA "

El Instituto Dominicano de las Telecomunicaciones (INDOTEL), por órgano de su Consejo Directivo, en ejercicio de las facultades conferidas por la Ley General de Telecomunicaciones, No. 153-98, promulgada en fecha 27 de mayo de 1998, ha dictado la siguiente RESOLUCIÓN:

CONSIDERANDO: Que en virtud de todo lo anterior, en fecha dos (2) de junio del año dos mil (2000), el Consejo Directivo de esta entidad dictó la Resolución 4-00, mediante la cual aprobó el Reglamento de Concesiones, Inscripciones en Registros Especiales y Licencias para prestar Servicios de Telecomunicaciones en la República Dominicana, con el objeto fundamental de desarrollar una reglamentación comprensiva, que complementara las disposiciones de la Ley No. 153-98 antes citada en lo referente al otorgamiento de las Autorizaciones previstas en la Ley No. 153-98 para prestar u operar servicios públicos o privados de telecomunicaciones, usar frecuencias del espectro radioeléctrico y para poder efectuar operaciones jurídicas y comerciales con dichas Autorizaciones, luego de su otorgamiento por el INDOTEL.

EL CONSEJO DIRECTIVO DEL INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL), EN EJERCICIO DE SUS FACULTADES LEGALES Y REGLAMENTARIAS, RESUELVE:

PRIMERO: APROBAR, en todas sus partes, las enmiendas efectuadas por el INDOTEL sobre el Reglamento de Concesiones, Inscripciones en Registros Especiales y Licencias para prestar Servicios de Telecomunicaciones en la República Dominicana, cuyo texto íntegro se transcribe a continuación, constituyendo la versión vigente y unificada del Reglamento de Concesiones, Inscripciones en Registros Especiales y Licencias para prestar Servicios de Telecomunicaciones en la República Dominicana.

"REGLAMENTO DE CONCESIONES, INSCRIPCIONES EN REGISTROS ESPECIALES Y LICENCIAS PARA PRESTAR SERVICIOS DE TELECOMUNICACIONES EN LA REPUBLICA DOMINICANA".

CAPITULO II. ALCANCE Y OBJETIVOS.

CAPITULO III. DISPOSICIONES GENERALES PARA LAS SOLICITUDES.

CAPITULO IV. CONCESIONES.

(B.1) En el caso de una asociación sin fines de lucro, organizada según la ley No. 520 de 1920 (incluyendo organización religiosa no católica).

(B.2) Documentación adicional aplicable en todos los casos previstos por el literal B.

(C) Información Técnica.

(D) Información Económica y Financiera.

Art. 21. Procedimiento para Obtener una Concesión.

Art. 22. Otorgamiento de la Concesión.

Art. 23. Contenido del Contrato de Concesión.

Art. 24. Plazo para Inicio del Servicio.

Art. 25. Derechos Generales del Titular de la Concesión.

Art. 26. Obligaciones Generales del Titular de la Concesión.

Art. 27. Duración de la Concesión.

Art. 28. Renovación de la Concesión.

CAPITULO V. INSCRIPCIONES EN REGISTROS ESPECIALES

Art. 29. Aspectos Generales para las Inscripciones en Registros Especiales.

Art. 30. Requisitos para las solicitudes de Inscripción en los Registros Especiales.

(A) Información General.

(B) Si el solicitante es una persona jurídica, necesitará presentar la siguiente información legal: documentación constitutiva.

(B.1) Si se han modificado los estatutos, será necesario presentar.

(B.2) En el caso de una Compañía Extranjera.

(B.3) En el caso de una asociación sin fines de lucro, organizada según la Ley No. 520 de 1920 (incluyendo organización religiosa no católica).

(C) Información Técnica.

Art. 31. Procedimiento para Obtener una Inscripción en un Registro Especial.

Art. 32. Emisión de un Certificado de Inscripción en el Registro Especial Correspondiente.

Art. 33. Plazo para Inicio del Servicio.

Art. 34. Derechos del Titular de la Inscripción en un Registro Especial.

Art. 35. Obligaciones del Titular de la Inscripción en un Registro Especial.

Art. 36. Duración de la Inscripción en un Registro Especial.

Art. 37. Renovación de la Inscripción en un Registro Especial.

CAPÍTULO VI. LICENCIAS

Art. 38. Aspectos Generales de la Licencia.

Art. 39. Licencias para Servicios Públicos de Radiocomunicaciones.

Art. 40. Requisitos para obtener una Licencia para Servicios Privados de Radiocomunicaciones, enlaces radioeléctricos, Asociaciones sin Fines de Lucro, Instituciones del Estado, Instituciones Religiosas reconocidas por el Estado, Misiones Diplomáticas y casos de emergencia justificados ante el INDOTEL.

(A) Información General

(B) Información Técnica

Art. 58. Adjudicación.

Art. 59. Pago.

Art. 60. Consecuencias del Incumplimiento en el Pago.

Art. 61. Emisión de Licencias vinculadas a una Concesión y/o Inscripción en Registro Especial.

CAPÍTULO VIII. TRANSFERENCIA, CESIÓN, ARRENDAMIENTO, OTORGAMIENTO DEL DERECHO DE USO, CONSTITUCIÓN DE UN GRAVAMEN O TRANSFERENCIA DE CONTROL.

Art. 62. Aspectos Generales Relativos a una Transferencia, Cesión.

Arrendamiento, Otorgamiento del Derecho de Uso, Constitución de un Gravamen o Transferencia de Control.

Art. 63. Requisitos para obtener una Autorización para una Transferencia, Cesión, Arrendamiento, Otorgamiento del Derecho de Uso, Constitución de un Gravamen o Transferencia de Control.

- En el caso de una compañía constituida en la República Dominicana.
- En el caso de una Compañía Extranjera.
- En el caso de una asociación sin fines de lucro, organizada según la Ley No. 20 de 1920 (incluyendo organización religiosa no católica).

Art. 64. Procedimiento para obtener la Autorización de una Transferencia, Cesión, Arrendamiento, Otorgamiento del Derecho de Uso, Constitución de

Gravamen, o Transferencia de Control de una Concesión y/o Licencia, o Inscripción vinculada a una Licencia.

Art. 65. Procedimiento para obtener una Autorización para una Transferencia, Cesión, Arrendamiento, Otorgamiento del Derecho de Uso, Constitución de un Gravamen, o Transferencia de Control de una Inscripción que no se encuentre vinculada a una Licencia.

Art. 66 Rechazo de una Solicitud de Autorización de Transferencia, Cesión, Arrendamiento, Otorgamiento del Derecho de Uso, Constitución de un Gravamen, o Transferencia de Control.

Art. 67 Notificación de la Finalización de la Operación.

CAPITULO IX. ESTABLECIMIENTO DE UN REGISTRO NACIONAL Y CREACIÓN DE UN BOLETÍN PUBLICO

Art. 68. Naturaleza y Objeto del Registro Nacional.

Art. 69. Organización del Registro Nacional.

Art. 70. Alcance del Registro Nacional.

Art. 71. Contenido del Registro Nacional.

(a) En relación con la persona natural o jurídica autorizada.

(b) En relación con la Concesión, Inscripción en Registro Especial o Licencia.

(c) En relación con la renovación de Concesión, Inscripción y Licencia.

(d) En relación con la expansión de área geográfica.

(e) En relación con la transferencia, cesión, arrendamiento, otorgamiento de un derecho de uso, constitución de un gravamen y transferencia de control de una Concesión, Inscripción en Registro Especial o Licencia.

(f) En relación con las modificaciones a Autorizaciones que han sido aprobada por el INDOTEL.

(g) En relación con las sanciones.

(h) En relación con las revocaciones o cancelaciones.

(i) En relación con las decisiones arbitrales homologadas por el INDOTEL y las emitidas por los Cuerpos Colegiados, en virtud del Artículo 79 de la Ley.

(j) Cualquier otra información pertinente, determinada por el Director Ejecutivo del INDOTEL.

Art. 72. Acceso Público a las Solicitudes.

Art. 73. Creación de un Boletín Público.

Art. 74. Publicaciones de Decisiones Emitidas en el Boletín Público.

CAPITULO X. COSTOS Y DERECHOS.

Art. 75. Clases de Costos y Derechos.

Art. 76. Costos de Procesamiento.

Art. 77. Autorización Obtenida a Través de un Llamado a Concurso Público.

Art. 78. Pago de Costos y Derechos.

CAPITULO XI. DISPOSICIONES TRANSITORIAS.

Art. 79. Autorizaciones Pendientes.

Art. 80. Autorizaciones Vigentes.

Art. 81. Adecuación de los Contratos de Concesión para la prestación de Servicios Portadores y Finales de Telecomunicaciones.

Art. 82. Autorizaciones para Proyectos de Desarrollo.

CAPITULO XII. DISPOSICIONES FINALES.

Art. 83. Ejecutoriedad.

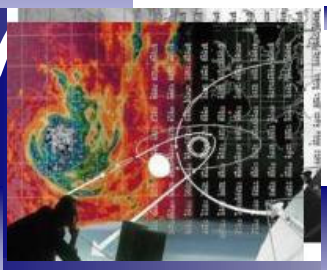
Art. 84. Entrada en Vigencia.

Art. 85. Disposición Derogatoria.

Si desea conocer el reglamento en detalle solo debe acceder a la siguiente dirección electrónica:

http://www.indotel.org.do/Site/Marco_Legal/consejo/Resoluciones_2002/Resolucion_007-02.pdf

Capitulo V



Ventajas de la Implementación de una Red Inalámbrica para la Interconexión de las Bibliotecas Universitarias

V. VENTAJAS DE LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA PARA LA INTERCONEXIÓN DE LAS BIBLIOTECAS UNIVERSITARIAS

La tecnología nos obliga a mantenernos actualizados ya que cada día surge algo nuevo. La propuesta más reciente en términos de comunicación que está en el mercado es la tecnología inalámbrica "Wireless". Cada tecnología nueva trae con ella un sin número de ventajas que debemos tomar en suma consideración cuando tomemos la decisión de incursionar en ella, porque estas nos servirán de apoyo a la hora de defender nuestros proyectos.

Las ventajas más atractivas en las redes inalámbricas, a nuestro parecer, se pueden estructurar de la siguiente forma:

Simplicidad y Flexibilidad

1. Los enlaces inalámbricos pueden desplegarse más rápidamente.
2. Es más sencillo, rápido y económico reconfigurar o modificar una red inalámbrica cuando las necesidades de mercado demandan cambios.
3. Las localidades se agregan o eliminan con más facilidad.
4. Las tecnologías inalámbricas son más fáciles de instalar y retirar.

Velocidad y Alcance

1. El despliegue de la red puede alcanzar áreas remotas que carecen de infraestructura sin tener que albergar redes complejas.
2. Rápida instalación.

Confiabilidad y Seguridad

1. Tan confiable como cualquier tipo de enlace tradicional, pero proveyendo anchos de banda significativamente mayores.

Economía y Precio

1. Reducción en los costos de infraestructura. La implementación de la tecnología inalámbrica es menos costosa en comparación con las redes cableadas. La inversión inicial se puede escalar a medida que el proyecto se expande.
2. Reducción en los costos de asistencia al usuario.
3. La infraestructura inalámbrica es menos propensa a fallas y requiere de menos mantenimiento que una línea tradicional.
4. Posee el más bajo costo de operación.

Ventajas de Implementar una Red Inalámbrica Punto-Multipunto

- **Conexión entre localidades Múltiples**

✓ Estación Base.

✓ Localidades Remotas.

✓ Estaciones Repetidoras.

- **Utiliza Antenas Sectoriales en la Estación Base para conectarse con las localidades remotas.**

❖ **Wireless-LAN diseña una verdadera arquitectura de red multipunto:**

- ✓ Cero Colisión de Paquetes.
- ✓ Punto-a-Multipunto facilita que los Repetidores extiendan el alcance y sirvan a más usuarios.
- ✓ Co-localización de las Estaciones Base brinda mayor flexibilidad de despliegue y mayor capacidad de servicios.
- ✓ La facilidad para Reuso de Frecuencia permite un despliegue de redes similares a las Celulares.
- ✓ Los Códigos de Adquisición facilitan las estrategias de colocalización de Repetidoras y por ende, mayor eficiencia en la Red.

❖ **Seguridades:**

- ✓ El Sistema Cerrado (Propietario) brinda una seguridad extremadamente alta en la Red.
- ✓ Filtraje de TCP/IP.
- ✓ Filtraje de Direcciones IP.
- ✓ Códigos de Acceso y Encriptación.

Principales Hallazgos

PRINCIPALES HALLAZGOS

En el levantamiento de las informaciones que realizamos, encontramos algunas situaciones que presentamos a continuación:

1. Algunas universidades aún no tienen publicadas en sus páginas Web las fuentes bibliográficas de sus bibliotecas.

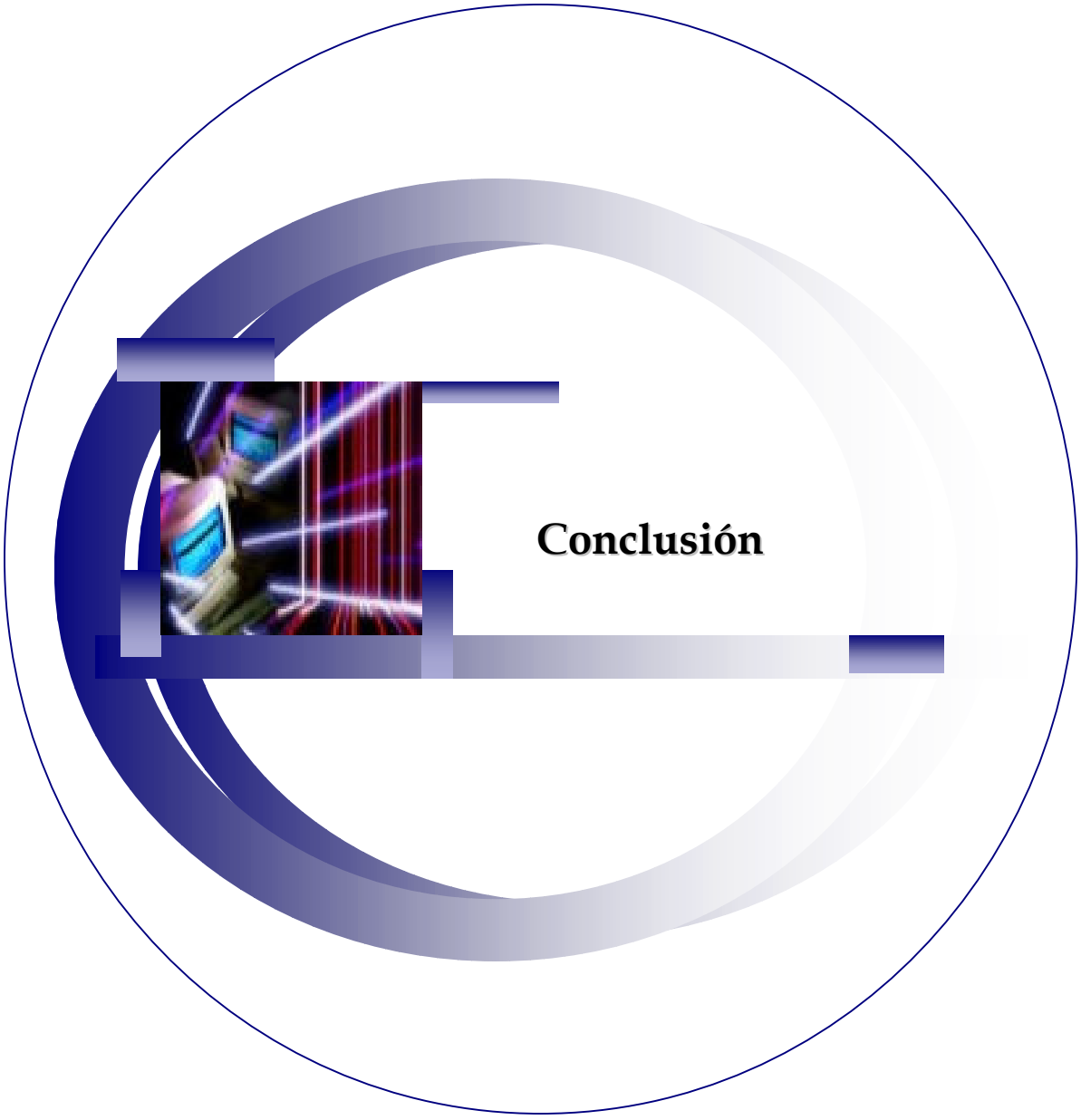
2. Cuando buscamos las coordenadas y la elevación de cada institución, constatamos que tenemos una gran variedad de elevaciones al nivel de la superficie de la provincia de Santo Domingo.

3. Encontramos que la Universidad Apec (propuesta como Sede Central en el proyecto) cuenta con conexión inalámbrica[1] a Nivel Administrativo.

4. En nuestro país la compañía telefónica VERIZON esta implementando en numerosos establecimientos comerciales puntos de acceso para comunicación inalámbrica, demostrando una vez más que la tecnología inalámbrica está revolucionando el mercado de las comunicaciones.

5. Se ha comprobado que en términos de costos y flexibilidad es preferible la tecnología inalámbrica, por poseer una infraestructura más fácil de implementar en cualquier tipo de localidad.

[1] Información suministrada por la Sra. Larissa Bonilla (Escuela de Informática UNAPEC)



Conclusión

CONCLUSIÓN

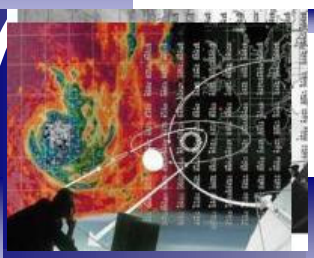
Las redes inalámbricas, como nueva tecnología, ha llegado al mercado a revolucionar nuestra forma tradicional de comunicarnos. Gracias a las innumerables ventajas que nos ofrecen frente a las demás tecnologías, pueden convertirse en poco tiempo en la principal vía de comunicación en nuestras universidades debido a la necesidad imperante de consultar o requerir data en el menor tiempo posible.

El proyecto que proponemos hace uso de la tecnología inalámbrica, esto así, porque la cantidad de información que necesitamos manejar y la periodicidad con la que será requerida, se necesita de una conexión a la red permanente y la garantía de un ancho de banda potente y estable. Estas características que mostramos pueden ser cubiertas plenamente por una red inalámbrica, siempre y cuando cuente con el mantenimiento necesario.

Es bueno recalcar que además de lo que representa en sí el proyecto en su fase inicial el mismo permite la posibilidad de expansión y de reutilización. Esto es posible gracias a la flexibilidad que caracteriza a la tecnología inalámbrica.

La ampliación del proyecto, además de factible es sumamente fácil y menos costosa que si se desarrollara con una red tradicional. Además de que la red propuesta se podría utilizar para otras funciones que las universidades requieran y que no han sido planteadas aún.

Finalmente, deseamos que nuestro proyecto y las consideraciones que hemos planteado en él, cumplan con los requerimientos de lugar que son necesarios para llevarlo acabo. Por lo mismo esperamos que sea considerado como una de las mejores vías y/o alternativas para comunicar de una forma más adecuada los recursos que son manejados por las instituciones universitarias y que nosotros los estudiantes utilizamos tan frecuentemente.



Recomendaciones

RECOMENDACIONES

Las recomendaciones o consideraciones que ofrecemos sobre la propuesta que presentamos son las siguientes:

- ✓ Es necesario establecer una Sede Central, porque el tipo de red que se plantea es de Red Punto-Multipunto y en dicha sede es donde estará ubicado el Punto de Acceso (AP) que servirá de comunicación entre las localidades.

- ✓ Se recomienda a las universidades que aún no han publicado en sus Páginas Web las bibliografías que tienen en existencia, que deben realizar esta operación para que sea más rápido el proceso de combinación de búsquedas y así puedan estar incluidas en el proyecto.

- ✓ Es muy importante que las personas responsables de administrar el proyecto y de implementarlo revisen el "REGLAMENTO DE CONCESIONES, INSCRIPCIONES EN REGISTROS ESPECIALES Y LICENCIAS PARA PRESTAR SERVICIOS DE TELECOMUNICACIONES EN LA REPÚBLICA DOMINICANA " Resolución No. 007-02 de INDOTEL (Instituto Dominicano de Telecomunicaciones) – referenciado en el Capítulo IV de este trabajo de grado – para evitar cualquier tipo de infracción a la ley.

- ✓ La seguridad es una de las partes más delicadas en cualquier proyecto. En la propuesta que realizamos, mostramos los niveles más importantes que se deben tomar en cuenta, pero sabemos que cada institución tiene algunos márgenes extras de seguridad, así que les exhortamos a verificar cualquier otra medida adicional que les sirva de ayuda para mantener la seguridad de la red bajo su control.

- ✓ Por lo general la implementación de una red, aunque es para un fin específico; siempre pueden ampliarse las ideas y hacer un proyecto más complejo y cubrir otras áreas con él. Recomendamos ver cualquier posibilidad que contribuya a mejorar o ampliar la propuesta que presentamos.

Glosario

GLOSARIO

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

Ad-Hoc. Es un sistema de red inalámbrica (802.11) que permite a los clientes que están situados en un rango determinado puedan conectarse entre ellos sin necesidad de la presencia de un Punto de Acceso. En este tipo de red, cualquier cliente puede hacer las veces de punto de acceso proporcionando a los demás acceso a Internet o cualquier otro servicio. También se le denomina Punto a Punto, o IBSS (referido al estándar 802.11). El otro sistema de red inalámbrica que emplea Puntos de Acceso se le denomina Infraestructura.

Ancho de Banda. Técnicamente es la diferencia en hertzios (Hz) entre la frecuencia más alta y la más baja de un canal de transmisión. Sin embargo, este término se usa mucho mas a menudo para definir la cantidad de datos que puede ser enviada en un período de tiempo determinado a través de un circuito de comunicación dado.

Apogeo. Punto de una órbita en torno a la Tierra más separado del centro de esta. También se describe como, punto de una órbita, en el cual es máxima la distancia entre el objeto que la describe y su centro de atracción.

Bluethoot. Tecnología y protocolo de conexión entre dispositivos inalámbricos que integran un chip específico para comunicarse en la banda de frecuencias 2,402-2,480 GHz con un alcance máximo de 10 metros y tasas de transmisión de datos de hasta 721 Kbps (en la segunda generación de BlueTooth). Cada dispositivo posee una dirección única de 48 bits que lo identifica de manera inequívoca, siguiendo el estándar IEEE 802.

Bolómetro. Instrumento utilizado para medir pequeñas cantidades de energía radiante en el rango del espectro comprendido entre las ondas luminosas y las microondas. Lo inventó en 1860 el ingeniero y científico estadounidense Samuel Pierpont Langley, y en la actualidad se utiliza principalmente, para detectar la energía que irradian fuentes lejanas en forma de calor.

Bridge (Puente). Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.

BSSID (Basic Service Set Identification). Suele identificar una red creada a través del Punto a Punto.

Canal. Un canal es una frecuencia de uso único y exclusivo dentro de su cobertura, por los mismos clientes.

Célula solar: Es una célula fotoeléctrica constituida esencialmente por una pequeña pastilla de silicio o de otra materia semiconductora que, al ser tocada por los rayos solares, genera una débil corriente eléctrica. Los vehículos espaciales las emplean en gran cantidad, formando enormes paneles o recubriendo su superficie exterior.

Cliente. Un cliente es un equipo en una red.

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

Cobertura. Área geográfica próxima a un nodo o estación base que recibe suficiente señal para mantener una conexión. Depende de diversos factores como tipo de antena, ubicación, topografía del terreno, potencia de la señal, etc.

Datagrama. Agrupamiento lógico de información enviada como unidad de la capa de red en un medio de transmisión, sin el establecimiento de un circuito virtual.

DBi. Decibelios por encima (o por debajo) de la señal ideal de una antena.

Dirección Ethernet. Una dirección Ethernet es una dirección única y programada previamente, a veces llamada dirección de control de acceso al medio (MAC). Cada sistema con una red Ethernet tiene su propia dirección Ethernet. Esta dirección hexadecimal de 12 dígitos está codificada en el circuito del adaptador de red del sistema cuando se fabrica. Otros dispositivos de la red utilizan esta dirección para identificar el equipo. Esta dirección no es la misma que la dirección IP que se asigna a los equipos en las redes TCP/IP. En estas redes, la dirección IP está asociada con la dirección MAC para permitir la comunicación en la red. Suelen aparecer con el siguiente formato:

XX:XX:XX:XX ó XXXX:XXXX:XXXX

Donde la X puede ser cualquier dígito hexadecimal (0-F)

Dirección IP. Una dirección IP proporciona una identificación única para cada equipo en Internet o en una red local. Las direcciones IP, por lo general, son un grupo de cuatro números separados por puntos, por ejemplo, 169.254.10.2.

Ninguno de los números puede ser mayor que 255. Cada interfaz Ethernet tiene una dirección IP. Para algunas estaciones base inalámbricas (puntos de acceso) como la Dell® TrueMobile™ 1170, existe una interfaz Ethernet LAN y una interfaz Ethernet WAN; por lo tanto, hay una dirección IP LAN y una dirección IP WAN.

DHCP (Protocolo de configuración de direccionamiento dinámico). DHCP es el proceso de establecer automáticamente las configuraciones TCP/IP para cada equipo en la red. Protocolo disponible en muchos sistemas operativos que genera automáticamente direcciones IP en un límite especificado para los dispositivos de una red. Los dispositivos retienen la dirección asignada durante un periodo de tiempo específico definido por el administrador, una vez expirado, la dirección asignada vuelve a estar disponible para ser asignada de nuevo a otro equipo. Además de la Dirección IP, el servidor DHCP puede proveer otros datos de configuración de red, comoson la Puerta de Enlace, Servidores DNS, Servidores WINS, Nombre del Dominio, etc...

Enlace Punto a Punto. Enlace en el que las comunicaciones están dirigidas entre dos puntos de conexión concretos. En Redes Wireless suelen ser las conexiones que enlazan dos nodos para ampliar el alcance de la red, o para conectar dos redes remotas. Se suelen emplear antenas directivas de gran ganancia (dependiendo de la distancia que separe los nodos).

Ethernet. Ethernet es la tecnología de red de área local más ampliamente utilizada. Es un estándar de la industria muy extendido desarrollado originalmente por Xerox y formalizado en 1980 por DEC, Intel y Xerox. Las redes Ethernet transmiten datos a 10/100/1000 MBps utilizando un protocolo especificado. Los usuarios deben estar conectados físicamente a la red en todo momento para poder acceder a la misma.

GPS. Es un satélite basado en un sistema de radionavegación capaz de proporcionar mediante medios prácticos y económicos la posición, velocidad, y tiempo a un número ilimitado de usuarios, de forma continua.

Hot Spot. Lugar donde existe un punto de acceso en una WLAN que ofrece servicio de banda ancha a usuarios móviles.

IEEE802.X. Conjunto de especificaciones de la redes LAN dictadas por el IEEE (the Institute of Electrical and Electronic Engineers). La mayor parte de las redes cableadas cumplen la norma 802.3, especificación para las redes ethernet basadas en CSMA/CD, o la norma 802.5, especificación para las redes Token Ring. Existe un comité 802.11 trabajando en una normativa para redes inalámbricas de 1 y 2 Mbps.

La norma tendrá una única capa MAC para las siguientes tecnologías: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) e infrarrojos. Se están desarrollando borradores de las normas.

IEEE. Instituto de Ingenieros Eléctricos y Electrónicos. (Institute of Electrical and Electronics Engineers.)

IRMAU. Unidad adaptadora al medio infrarrojo. (Infrarroja Medium Adapter Unit.)

ISM. Bandas de aplicaciones industriales, científicas y medicas. (Bands Industrial, Scientific and Medical.)

Infraestructura de red. Red inalámbrica centrada en un punto de acceso. En este entorno los puntos de acceso no solo proporcionan comunicación con la red cableada sino que también median el tráfico de red en la vecindad inmediata.

Intranet. Red de área amplia con gran infraestructura y acceso privado.

Kbps. Kilo bits por segundo.

Lan (Red de Área Local). La red LAN es un grupo de computadores equipados con las tarjetas adaptadoras de red apropiadas, conectadas por cable o por aire, que comparten aplicaciones, datos y periféricos. Todas las conexiones se realizan a través de medios alámbricos o inalámbricos, pero las redes LAN no utilizan servicios telefónicos. En general, abarcan un establecimiento o un edificio.

LLC. Control de enlace lógico. (Logic Link Control.)

MAC. Control de acceso al medio. (Medium Access Control.)

Mbps. Mega bits por segundo.

Micrones. El micrón o micrómetro es una unidad comúnmente utilizada en astronomía y equivale a una millonésima de metro.

Mw (Miliwatio). Un milésimo de watt, es la base para medir los niveles de intensidad de la señal en los circuitos de telecomunicaciones.

Nodo. Estación de trabajo con identificación propia que puede ser fuente y destino en la red. En redes inalámbricas se denomina Nodo a un ordenador o dispositivo conectado a una antena a través de un adaptador inalámbrico que sirve como "punto de acceso" a la red (también suelen estar conectado a redes cableadas).

Nodo inalámbrico. Ordenador de usuario con una tarjeta de red inalámbrica (adaptador).

PAN, Personal Area Network. Red de área personal. Red local de corto alcance. La transmisión de datos se realiza por contacto físico. También se le llama así a la red de área personal, un conjunto de dispositivos que normalmente son de uso personal, ej micrófono, teclado, impresora conectados con un computador.

Paneles solares. Especie de alas que llevan algunos satélites y vehículos astronáuticos, las cuales están recubiertas de pequeñas pastillas de silicio o de otra materia idónea. Estas pastillas o láminas, denominadas células solares, tienen la propiedad de transformar la luz del Sol en corriente eléctrica para el funcionamiento de los instrumentos y equipos que transportan.

Perigeo. Punto más próximo a la Tierra de la órbita de un astro o un satélite artificial.

Piconet. Una red de dispositivos que se conectan utilizando Bluetooth. Una piconet puede constar de dos a ocho dispositivos. En una piconet, habrá siempre un master y los demás serán esclavos.

Polarización. Angulo del campo eléctrico de la onda radiada con respecto al suelo. La polarización puede ser vertical, horizontal y circular. El campo magnético de la onda está polarizado 90 grados con respecto al campo eléctrico. La polarización de la onda radiada depende del tipo y la posición de la antena. Para que se puedan comunicar dos equipos sus antenas deben tener la misma polarización. Las antenas omnidireccionales suelen usar polarización vertical, las direccionales suelen usar polarización horizontal (las parabólicas pueden usar tanto horizontal como vertical) y las helicoidales usan polarización circular (o helicoidal).

Protocolo. El protocolo se refiere a un conjunto de reglas para enviar y recibir información en una red. Las reglas determinan el formato de los datos que se transmiten y otros aspectos de la conexión a la red, tales como la manera de detectar y corregir errores. El controlador de protocolo en cada equipo es un software que respeta dichas reglas cuando envía y recibe información. Estos controladores también se llaman frecuentemente protocolos.

Protocolo de Internet. El IP es el protocolo utilizado para enviar datos de un sistema a otro por medio de Internet. El protocolo IP describe cómo los equipos de Internet llevan un control de la dirección IP de cada equipo en la red y encaminan paquetes de datos de una dirección IP a otra.

Proveedor de Internet. Un ISP es una empresa que proporciona acceso a Internet y otros servicios relacionados tales como creación de sitios Web y host virtual a personas y a otras empresas. Un ISP dispone del equipo y el acceso a la línea de telecomunicación requeridos para establecer el protocolo POP en Internet dentro del área geográfica a la que presta servicio. Los ISP más grandes tienen sus propias líneas de alta velocidad alquiladas, porque así son menos dependientes de los proveedores de telecomunicación y pueden proporcionar un mejor servicio a sus clientes.

Punto de acceso. Dispositivo que permite comunicar a varios clientes inalámbricos entre ellos e incluso con otras redes inalámbricas o de cable. Los puntos de acceso hacen las funciones de "Bridges" (puente) y algunos incluso de "Routers" (encaminadores).

Red Independiente. Red que proporciona (normalmente en forma temporal) conectividad de igual a igual sin depender de una infraestructura completa de red.

Roaming. Cuando cualquier área del complejo se encuentra dentro del rango de recepción de uno o más AP, la cobertura de la célula se encuentra encimada, o como se le llama comúnmente " *overlap* ". Cada una de las estaciones inalámbricas establece automáticamente cual es la mejor conexión con alguno de los AP. Las áreas de cobertura encimadas son un atributo importante de las redes inalámbricas, pues permiten el *roaming* sin siquiera ser notado entre las células que se encuentran encimadas. El *Roaming* permite a los usuarios móviles con estaciones portátiles moverse libremente entre células, manteniendo constantemente su conexión a la red. El *roaming* es imperceptible, por lo que una sesión puede ser mantenida mientras se mueve de una celda a otra. Múltiples AP pueden proveer de una cobertura inalámbrica para un edificio o un campus completo. Cuando el área de cobertura de dos o mas AP se enciman, las estaciones en el área encimada, pueden decidir cual de los dos AP les provee una mejor conexión. En aras de mantener al mínimo la perdida de paquetes durante el cambio, el AP "viejo" así como el "nuevo" se comunican entre ellos para coordinar el proceso.

Router (Encaminador). Dispositivo hardware (o software) para redes informáticas dotado de capacidad para conmutación y con la principal finalidad de proporcionar un encaminamiento de paquetes ip.

SSID. Significa Service Set IDentifier, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TRs deben conocer el nombre de la red para poder unirse a ella. El primer paso para poder autenticar un cliente en una red wireless es el conocimiento del SSID. Para obtener acceso al sistema es necesario conocer el SSID.

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

Transpondedor. Receptor / transmisor en un satélite de comunicaciones. Recibe una señal de microondas transmitida desde la tierra (enlace ascendente), la amplifica y la retransmite de regreso a la tierra a una frecuencia diferente (enlace descendente).

Vpn (Red Privada Virtual). Configuración lógica de una serie de componentes hardware, que permite la utilización de redes públicas para establecer canales de comunicaciones privados a los que sólo pueden acceder usuarios autorizados.

WAN, Wide Area Network. Red de comunicaciones extendida. Redes con alcance mundial. Las redes WAN consisten en redes locales múltiples conectadas entre sí a través de servicios telefónicos, cables de fibra óptica, satélite, etc. Las WAN pueden abarcar una ciudad, una provincia, un país o incluso todo el mundo.

WECA (Alianza para la Compatibilidad de Ethernet Inalámbrica). Alianza de fabricantes formada para mantener la compatibilidad entre dispositivos wireless. La WECA creo el estándar de dispositivos inalámbricos Wi-Fi, que cumplen la norma IEEE 802.11b.

WEP. Wired Equivalent Privacy. Equivalencia de privacidad con cables. Normas y sistemas de cifrado en comunicaciones inalámbricas. Sistema de cifrado concebido inicialmente para dotar al mundo wireless de un nivel de privacidad equivalente, al menos, al de una red de cable. Se le han encontrado problemas como: seguridad insuficiente, partiendo de cifrado de 40 bits e incluso con las nuevas claves de 128 bits.

Wi-Fi (Wireless Fidelity). Sinónimo del estándar IEEE "802.11b", protocolo de transmisión inalámbrica que logra alcanzar desde 2 Mbps hasta un máximo teórico de 11 Mbps. Este estándar fue creado por un grupo de fabricantes de dispositivos inalámbricos para mantener la compatibilidad entre sus productos. Permite crear redes de ordenadores sin que exista un cable de por medio, usando para ello ondas de radio.

WLAN (Red de Área Local Inalámbrica). Una WLAN es un tipo de red de área local (LAN) que utiliza ondas de radio de alta frecuencia en lugar de cable para comunicar y transmitir datos entre los clientes de red y los dispositivos. Es un sistema de comunicación de datos flexible implementado como una extensión, o como una alternativa para una LAN conectada. Al igual que una LAN, la red permite que los usuarios de esa ubicación compartan archivos, impresoras y otros servicios. La mayoría de las redes WLAN utilizan tecnología de espectro distribuido. Su ancho de banda es limitado (generalmente inferior a 11 Mbps) y los usuarios comparten el ancho de banda con otros dispositivos del espectro; no obstante, los usuarios pueden operar dispositivos de espectro distribuido sin autorización de la FCC (Comisión Federal de Comunicaciones).

WIRELESS, (Inalámbrico, sin cables). Tecnologías de transmisión de datos sin enlace físico, el cable, entre los equipos. Es un sistema de comunicación que utiliza ondas de radiofrecuencia, ultrasonido o rayos infrarrojos (IR) para intercambiar datos entre dispositivos. Cada vez se está popularizando más el uso de este sistema para transferencia de datos entre cámaras digitales, PDAs, calculadoras, etc. con la computador.

En Internet, este término es utilizado para indicar que la transmisión de información se efectúa prescindiendo de cables. Es el caso de los celulares con sistema WAP, o las conexiones a Internet.

WPAN (Red Inalámbrica de Área Personal). Redes locales-personales que utilizan tecnología Bluetooth.

Bibliografía

BIBLIOGRAFÍA

Libros On-Line

- ✓ Cisco Wireless Lan

Publicado por: Syngress (http://www.eicage.org/eicage.asp)

- ✓ Design Wireless Network

Publicado por: Syngress (http://www.eicage.org/eicage.asp)

- ✓ Enciclopedia Microsoft Encarta 2004

Publicado por: Microsoft Corporation

WebGrafía (Direcciones Internet)

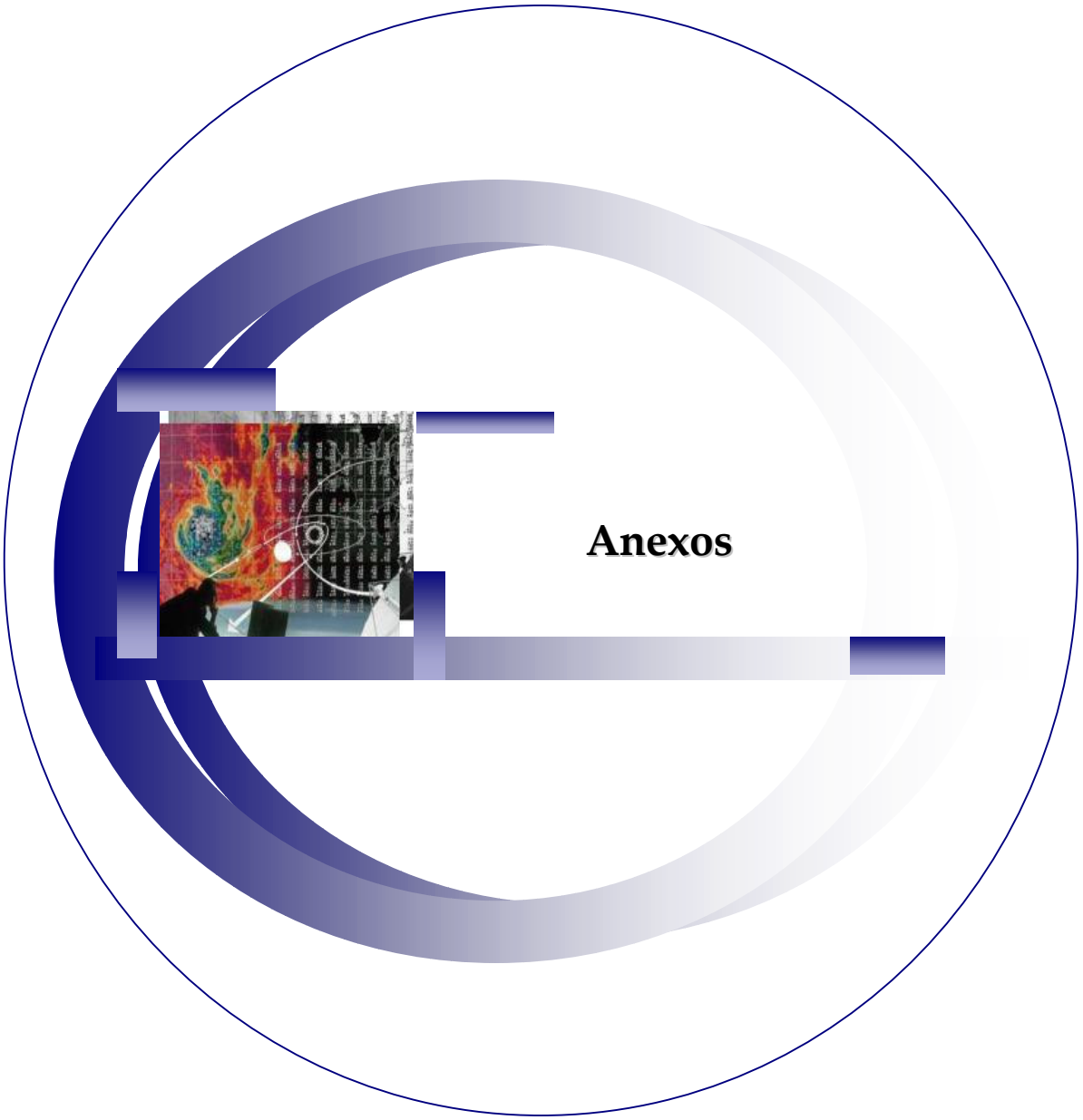
- http://www.upv.es/satelite/trabajos/Grupo3_99.00/GlobalStar8.htm
- http://www.monografias.com/trabajos13/modu/modu.shtml
- http://www.monografias.com/trabajos14/celularhist/celularhist.shtml
- http://ceres.ugr.es/~alumnos/c_avila/gsm24.htm.
- http://www.lared.com.ve/archivo/hardware11-06-04.html.
- http://www.casadomo.com/revista_domotica_news.asp?type=1&id=2524.
- http://www.baquia.com/com/20040227/not00002.html
- http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml.

- http://www.rediris.es/rediris/boletin/66-67/ponencia22.pdf.
- http://terra.es/personal/tamarit1/redes/introduccion.htm.
- http://www.unincca.edu.co/boletin/indice.htm.
- http://www.monografias.com/trabajos14/wi-fi/wi-fi.shtml.
- http://www.sandisk.com/consumer/download/connectplus/Spa_Information/WirelessNetwork.htm
- http://www.monografias.com/trabajos14/segur-wlan/segur-wlan.shtml.
- http://entomologia.rediris.es/gtli/espa/cuatro/B/utm.htm
- http://157.92.29.203/aula-gea/glosario.html.
- http://www.smc-europe.com/english/support/driver_manual/wirel/download/2652/manual_SMC2652W_SP.pdf
- http://www.conecsion.es/Soporte.asp?tab=Faqs.
- http://www.eveliux.com/articulos/wlans.html.
- http://www.enetchile.cl/productos/productoslinux/firewall.php
- http://www.gerencia.cl/noticia.mv?id=20040614x11.
- http://www.quasar.com.pe/html/4131_access_point.html.
- http://es.checkpointsystems.com/rfid/index.asp.
- http://es.checkpointsystems.com/rfid/timeline.asp
- http://ciberconta.unizar.es/LECCION/INTRODUC/435.HTM.

- http://www.symbol.com.mx/radiofrecuencia.htm.
- http://www.symbol.com.mx/red%20inalambrica.htm
- http://mssimplex.com/redinalambrica.htm.
- http://www.terra.es/tecnologia/glosario/ficha.cfm?id_termino=501.
- http://www.mailxmail.com/curso/informatica/wifi/capitulo6.htm
- http://www.mailxmail.com/curso/informatica/wifi/capitulo7.htm
- http://www.mailxmail.com/curso/informatica/wifi/capitulo8.htm
- http://www.mailxmail.com/curso/informatica/wifi/capitulo11.htm
- http://www.mailxmail.com/curso/informatica/wifi/capitulo13.htm
- http://www.mailxmail.com/curso/informatica/wifi/capitulo14.htm
- http://www.mailxmail.com/curso/informatica/wifi/capitulo15.htm
- http://www.mailxmail.com/curso/informatica/wifi/capitulo18.htm
- http://www.jegsworks.com/Lessons-sp/lesson10/lesson10-5.htm+%22Surge+Protector%22&hl=es&lr=lang_es
- http://www.redlibre.net/modules.php?name=Encyclopedia&op=content&tid=202
- http://www.redlibre.net/modules.php?name=Encyclopedia&op=content&tid=170
- http://www.redlibre.net/modules.php?name=Encyclopedia&op=content&tid=193

- http://www.dliengineering.com/vibman-spanish/analizadordeespectro1.htm
- http://support.jp.dell.com/docs/network/p44970/sp/glossary.htm
- http://www.upv.es/satelite/trabajos/Grupo2_98.99/glosnofr.html
- http://www.landatel.com/html/hotspot.html
- http://www.proxim.com/spanish/products/lynx/index.html
- http://linksys.com/
- http://www.wifi.com.ar/antenas.html.
- http://www.wifind.com.ar/modules.php?name=Content&pa=showpage&pid=3
- http://www.zaragozawireless.org/zgzwl/wk/index.php/Listado%20de%20tarjetas%20WI-FI
- http://lwwa175.servidoresdns.net:9000/proyectos_wireless/index.htm
- http://www.udec.cl/~lepino/recursos/Tarea1psi.pdf.
- http://www.intel.com/espanol/unwire/making_the_case.htm
- http://www.symantec.com/region/mx/enterprisesecurity/content/risks/LAM_2344.html#1
- http://www.eluniversal.com/2004/06/20/eco_art_20125D.shtml.
- http://www.cotopaxi.com.mx/paginas/soporte/articulos/redes/wireless1.htm

- http://www.cotopaxi.com.mx/paginas/soporte/articulos/redes/wireless2.htm
- http://www.cotopaxi.com.mx/paginas/soporte/articulos/redes/wireless3.htm
- http://www.electrica.frba.utn.edu.ar/redesinal.htm.
- http://www.swisswireless.org/wlan_calc_en.html
- http://www.nextec.com.ar/redes_Inalambricas/redes_inalambricas.html .
- http://www.indotel.org.do/Site/Marco_Legal/consejo/Resoluciones_2002/Resolucion_007-02.pdf
- http://www.glosarium.com/term/1457,14,xhtml.
- http://www.cientec.com/analisis/seguridad_redesb.asp.
- http://www.geocities.com/v.iniestra/apuntes/telefonia/.



Anexos

ANEXOS

Coordenadas de todos los puntos conectados a la red propuesta.

Coordenadas Geográficas de cada Punto

Proyecto :

Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Lista de puntos

Nombre	Latitud	Longitud
APEC	18°28'22.60142"N	69°54'46.97305"W
UNIBE	18°28'28.18949"N	69°54'35.06930"W
INTEC	18°29'20.90876"N	69°57'49.53513"W
UNPHU	18°28'58.42740"N	69°56'51.61581"W
PUCMM	18°27'44.73880"N	69°55'45.75324"W
UTESA	18°27'58.04202"N	69°54'46.16124"W
O&M	18°26'59.20143"N	69°55'43.63323"W
UASD	18°27'49.82721"N	69°55'02.99388"W

Ubicación Geográfica de cada Punto

Proyecto :

Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Lista de puntos

Nombre	Norte	Este	Elevación
APEC	2042755.000	403600.000	50.050
UNIBE	2042925.000	403950.000	45.100
INTEC	2044575.000	398255.000	52.050
UNPHU	2043875.000	399950.000	53.100
PUCMM	2041600.000	401870.000	46.300
UTESA	2042000.000	403620.000	28.600
O&M	2040200.000	401925.000	12.600
UASD	2041750.000	403125.000	18.500

Informe de Distancia y Elevación (O&M)

Proyecto :

Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Desde	A	Acimut cuadrícula	Distancia cuadrícula	Incremento elevación
O&M	PUCMM	357°45'01"	1401.080m	33.700m
O&M	INTEC	320°00'29"	5710.475m	39.450m
O&M	UNPHU	331°44'45"	4172.080m	40.500m
O&M	APEC	33°14'53"	3055.102m	37.450m
O&M	UASD	37°44'48"	1960.230m	5.900m
O&M	UTESA	43°16'45"	2472.453m	16.000m
O&M	UNIBE	36°37'00"	3395.033m	32.500m

Informe de Distancia y Elevación (PUCMM)

Proyecto :

Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Desde	A	Acimut cuadrícula	Distancia cuadrícula	Incremento elevación
PUCMM	INTEC	309°27'11"	4681.757m	5.750m
PUCMM	UNPHU	319°50'14"	2976.915m	6.800m
PUCMM	APEC	56°16'18"	2080.126m	3.750m
PUCMM	UNIBE	57°30'07"	2466.176m	-1.200m
PUCMM	UTESA	77°07'30"	1795.132m	-17.700m
PUCMM	O&M	177°45'01"	1401.080m	-33.700m
PUCMM	UASD	263°11'03"	1263.932m	-27.800m

Informe de Distancia y Elevación (UASD)

Proyecto :

Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Desde	A	Acimut cuadrícula	Distancia cuadrícula	Incremento elevación
UASD	INTEC	300°07'02"	5630.056m	33.550m
UASD	UNPHU	303°47'39"	3820.504m	34.600m
UASD	APEC	25°17'50"	1111.598m	31.550m
UASD	UNIBE	35°04'26"	1435.705m	26.600m
UASD	UTESA	63°12'14"	554.549m	10.100m
UASD	PUCMM	263°11'03"	1263.932m	27.800m
UASD	O&M	217°44'48"	1960.230m	-5.900m

Informe de Distancia y Elevación
(UNIBE)

Proyecto :

Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Desde	A	Acimut cuadrícula	Distancia cuadrícula	Incremento elevación
UNIBE	APEC	244°05'37"	389.102m	4.950m
UNIBE	INTEC	286°09'28"	5929.209m	6.950m
UNIBE	UNPHU	283°21'37"	4111.265m	8.000m
UNIBE	PUCMM	237°30'07"	2466.176m	1.200m
UNIBE	UASD	215°04'26"	1435.705m	-26.600m
UNIBE	UTESA	199°38'03"	982.102m	-16.500m
UNIBE	O&M	216°37'00"	3395.033m	-32.500m

Informe de Distancia y Elevación (UNPHU)

Proyecto :

Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Desde	A	Acimut cuadrícula	Distancia cuadrícula	Incremento elevación
UNPHU	INTEC	292°26'23"	1833.855m	-1.050m
UNPHU	PUCMM	139°50'14"	2976.915m	-6.800m
UNPHU	UNIBE	103°21'37"	4111.265m	-8.000m
UNPHU	APEC	107°03'31"	3817.971m	-3.050m
UNPHU	UASD	123°47'39"	3820.504m	-34.600m
UNPHU	UTESA	117°03'45"	4121.229m	-24.500m
UNPHU	O&M	151°44'45"	4172.080m	-40.500m

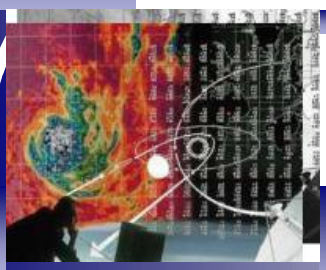
Informe de Distancia y Elevación
(UTESA)

Proyecto :

Análisis y propuesta para la implementación de una infraestructura para interconectar las bibliotecas de las universidades de Santo Domingo, utilizando tecnología inalámbrica

Nombre del usuario	Ing. Yván Martínez	**Zona**	19 North
Sistema de coordenadas	UTM	**Datum del proyecto**	ITRF
Modelo geoidal	CARIB97 (Caribbean)	**Unidades coordenadas**	Metros
Unidades de distancia	Metros	**Unidades de altura**	Metros

Desde	A	Acimut cuadrícula	Distancia cuadrícula	Incremento elevación
UTESA	UNIBE	19°38'03"	982.102m	16.500m
UTESA	APEC	358°28'57"	755.265m	21.450m
UTESA	UASD	243°12'14"	554.549m	-10.100m
UTESA	O&M	223°16'45"	2472.453m	-16.000m
UTESA	PUCMM	257°07'30"	1795.132m	17.700m
UTESA	UNPHU	297°03'45"	4121.229m	24.500m
UTESA	INTEC	295°38'21"	5950.954m	23.450m



Adendum

UNIVERSIDAD APEC

UNAPEC

ADENDUM DE MONOGRAFÍA PARA OPTAR POR EL TITULO DE:
INGENIERO EN SISTEMAS DE COMPUTACIÓN

"Análisis y Propuesta para la Implementación de una Infraestructura para Interconectar las Bibliotecas de las Universidades de Santo Domingo, utilizando Tecnología Inalámbrica"

Sustentantes

Miledys Mercedes Taveras Medina **2000-0177**

Aleidania Lorenzo Bierd **2000-0361**

Santo Domingo, D. N.
Agosto, 2004

ADENDUM

PRIMERA PARTE

Este trabajo de grado, trata sobre la proposición de implementar una red inalámbrica para interconectar las bibliotecas de Santo Domingo. En él mostramos las facilidades que nos ofrecen las tecnologías inalámbricas, debido a que cada día el uso de dispositivos móviles es mayor y la tecnología inalámbrica está en pos de convertirse en el mejor medio de transporte de datos.

La tecnología inalámbrica es un medio de comunicación que se encuentra en pleno apogeo, por lo que se considera actualmente como la tecnología más joven y más recomendable en el mercado para interconectar dispositivos o redes que pueden estar tanto a nivel local como a nivel remoto.

La red que proponemos está enmarcada en conectar las bibliotecas de las principales universidades de la provincia de Santo Domingo, lo cual indica que gracias a la flexibilidad que ofrece la tecnología inalámbrica se pueden incluir en un futuro no muy lejano otras universidades que lograran cumplir con los requisitos técnicos que se requieren para poder ser agregados a la red. De esta forma se podrá brindar a los estudiantes una mayor cantidad de opciones al momento de buscar la bibliografía que necesita.

Este proyecto puede servir no solo para interconectar las bibliotecas sino para que las instituciones universitarias se pueden unificar y alcanzar o lograr mayores objetivos en beneficio de los estudiantes y de las mismas instituciones. Esto así, porque empezando por compartir recursos mas adelante se puede llegar a que el proyecto no sea solo consultas, sino que pueda proporcionar otras utilidades, como pueden ser: reserva de libros en línea, virtualización de algunas publicaciones y de cualquier fuente que se pueda consultar.

Este planteamiento colaborará en gran proporción al mejoramiento de los medios que se utilizan para comunicar los campus universitarios, las dependencias y oficinas con las que cuentan las instituciones.

Un aporte muy importante que nos brinda la oportunidad de tener una red inalámbrica de este tipo es que se le puede permitir acceso a los estudiantes (con un profesor calificado para ello) a que puedan ver más de cerca los equipos y la forma en que se realizan las conexiones inalámbricas. Esto contribuye al fortalecimiento académico, básicamente en materias de telecomunicaciones.

ESTRATEGIA METODOLÓGICA

La metodología de estudio que utilizamos es la inductiva. La utilización de ella se debe a que actualmente existen ya redes inalámbricas en muchos lugares del mundo, por tanto lo que proponemos no es nada nuevo sino más bien lo mejor de lo que ya tenemos.

Entre las informaciones recaudadas para el proyecto está un mapa de relieve de la ciudad de Santo Domingo proporcionado por el Instituto Cartográfico Militar de la Rep. Dom. y con él obtuvimos las coordenadas geográficas necesarias para realizar todos los cálculos para la ubicación de las localidades.

Tomamos además en consideración la revisión de todas y cada una de las paginas Web de las universidades integradas en el proyecto para verificar que ya cada universidad cuenta con un Sitio en Internet y además que en su mayoría ya incluyen un área para la consulta de sus fuentes bibliográficas.

SEGUNDA PARTE
ASPECTOS CONCEPTUALES

La evolución de la tecnología inalámbrica viene desde siglos pasados cuando se descubrió que existían las ondas electromagnéticas hasta nuestros días. Sus modos de funcionamiento, dependen básicamente del tipo de transmisión que se utilice (Radio Frecuencia, Microondas, Satélite, Infrarrojo, etc.), así como de los estándares que fueron creados para regirlas.

Las redes de comunicación inalámbricas son sistemas de comunicación de datos que utilizan tecnología de radio frecuencia minimizando la necesidad de tener conexiones alámbricas. Para tener una red inalámbrica es necesario tener los equipos necesarios, entre ellos están: los radios, antenas, tarjetas de red, entre otros componentes.

Otros aspectos muy importantes que se deben tomar en consideración son los estatutos por los que se deben regir las comunicaciones inalámbricas y la seguridad que debe imperar en ella, ya que la comunicación por aire es sumamente delicada de manejar y se debe evitar la intromisión de dispositivos que no pertenecen a la red.

Siempre existen ciertos términos y especificaciones asociadas a determinadas áreas que se deben recalcar, como son: las topologías y arquitecturas propias de las redes inalámbricas. También se deben mencionar las diferentes instituciones que trabajan con este tipo de tecnología. Estas se clasifican de acuerdo a sus objetivos, por ellos están las organizaciones de los estándares, que son las que se encargan de las regulaciones correspondientes y las asociaciones de la industria, que son aquellas que se encargan de promover el crecimiento de la industria inalámbrica, a través de educación y promoción.

El punto central de esta monografía es la propuesta que se plantea en él. Se destacan los elementos claves que hay que considerar cuando se elabora un proyecto de esta magnitud. Entre esos elementos están:

- ✓ El caso de estudio, plantea una descripción de la red que se propone y de las localidades que la conformarán.
- ✓ La distribución geográfica de las diferentes localidades, engloba las coordenadas geográficas de cada una de las universidades integradas en el proyecto.
- ✓ La descripción de los componentes. Aquí encontramos los principales equipos que se necesitan para este tipo de implementación, así como las características que deben tener.

- ✓ La seguridad que se debe establecer para velar por un buen funcionamiento y cuidado de la red.

Finalmente, las ventajas que trae consigo un proyecto deben siempre estar enmarcadas de forma tal que incentiven a quien desee implementarlo y/o rediseñarlo para un nuevo fin.

PRINCIPALES HALLAZGOS

En el levantamiento de las informaciones que realizamos, encontramos algunas situaciones que consideramos necesarias presentar.

- ✓ Encontramos que la Universidad Apec (propuesta como Sede Central en el proyecto) cuenta con conexión inalámbrica a Nivel Administrativo.

- ✓ Algunas universidades aún no tienen publicadas en sus páginas Web las fuentes bibliográficas de sus bibliotecas.

- ✓ En nuestro país la compañía telefónica VERIZON esta implementando en numerosos establecimientos comerciales puntos de acceso para comunicación inalámbrica, demostrando una vez más que la tecnología inalámbrica está revolucionando el mercado de las comunicaciones.

- ✓ Cuando buscamos las coordenadas y la elevación de cada institución, constatamos que tenemos una gran variedad de elevaciones al nivel de la superficie de la provincia de Santo Domingo.

- ✓ Se ha comprobado que en términos de costos y flexibilidad es preferible la tecnología inalámbrica, por poseer una infraestructura más fácil de implementar en cualquier tipo de localidad.

CONCLUSIONES

Las redes inalámbricas, como nueva tecnología, ha llegado al mercado a revolucionar nuestra forma tradicional de comunicarnos. Gracias a las innumerables ventajas que nos ofrecen frente a las demás tecnologías, pueden convertirse en poco tiempo en la principal vía de comunicación en nuestras universidades debido a la necesidad imperante de consultar o requerir data en el menor tiempo posible.

Es bueno recalcar que además de lo que representa en sí el proyecto en su fase inicial el mismo permite la posibilidad de expansión y de reutilización. Esto es posible gracias a la flexibilidad que caracteriza a la tecnología inalámbrica.

La ampliación del proyecto, además de factible es sumamente fácil y menos costosa que si se desarrollara con una red tradicional. Además de que la red propuesta se podría utilizar para otras funciones que las universidades requieran y que no han sido planteadas aún.

Finalmente, deseamos que nuestro proyecto y las consideraciones que hemos planteado en él, cumplan con los requerimientos de lugar que son necesarios para llevarlo acabo. Por lo mismo esperamos que sea considerado como una de las mejores vías y/o alternativas para comunicar de una forma más adecuada los recursos que son manejados por las instituciones universitarias y que nosotros los estudiantes utilizamos tan frecuentemente.

RECOMENDACIONES

Las recomendaciones o consideraciones siempre es necesario hacerlas porque hay ciertas cosas que no consideramos cuando se realiza un proyecto.

- ✓ Es necesario establecer una Sede Central, porque el tipo de red que se plantea es de Red Punto-Multipunto y en dicha sede es donde estará ubicado el Punto de Acceso (AP) que servirá de comunicación entre las localidades.

- ✓ Se recomienda a las universidades que aún no han publicado en sus Páginas Web las bibliografías que tienen en existencia, que deben realizar esta operación para que sea más rápido el proceso de combinación de búsquedas y así puedan estar incluidas en el proyecto.

- ✓ Es muy importante que las personas responsables de administrar el proyecto y de implementarlo revisen el "REGLAMENTO DE CONCESIONES, INSCRIPCIONES EN REGISTROS ESPECIALES Y LICENCIAS PARA PRESTAR SERVICIOS DE TELECOMUNICACIONES EN LA REPÚBLICA DOMINICANA " Resolución No. 007-02 de INDOTEL (Instituto Dominicano de Telecomunicaciones) – referenciado en el Capítulo IV de este trabajo de grado – para evitar cualquier tipo de infracción a la ley.

- ✓ La seguridad es una de las partes más delicadas en cualquier proyecto. En la propuesta que realizamos, mostramos los niveles más importantes que se deben tomar en cuenta, pero sabemos que cada institución tiene algunos márgenes extras de seguridad, así que les exhortamos a verificar cualquier otra medida adicional que les sirva de ayuda para mantener la seguridad de la red bajo su control.

- ✓ Por lo general la implementación de una red, aunque es para un fin específico; siempre pueden ampliarse las ideas y hacer un proyecto más complejo y cubrir otras áreas con él. Recomendamos ver cualquier posibilidad que contribuya a mejorar o ampliar la propuesta que presentamos.