UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

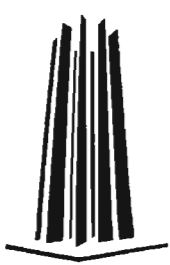
ANÁLISIS DE REDES INALÁMBRICAS DE ÁREA LOCAL DE 1994 - 2004, PARA SU IMPLEMENTACIÓN EN LA ESCUELA NORMAL No. 4 DE CIUDAD NEZAHUALCÓYOTL

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

DULCE MARÍA CARMONA LUGO
MIRIAM ISABEL LEAL MIJARES

ASESOR: ING. ADRIÁN PAREDES ROMERO



SAN JUAN DE ARAGÓN, EDO. DE MÉXICO 2005.

AGRADECIMIENTOS

A mi madre:
Por ser el pilar de mi vida,
estar conmigo siempre,
apoyarme
y sobre todo creer en mí.

A mi padre:
Por ser un ejemplo de superación,
quien me brindo la oportunidad de estudiar
y ser alguien en la vida.

Gracias a ambos.

A alguien especial:
Por soportar los problemas,
servirme de apoyo,
escuchar mis locuras,
y ser una parte fundamental en
éste proyecto.
Gracias Andrés.

Miriam.

Quiero agradecer a las personas que han dado forma y han influido profundamente en mi vida con su amor, con su ejemplo y con su apoyo incondicional.

A mis padres:

Por haberme dado lo mejor de ellos para que pudiera salir adelante, por la confianza que han depositado en mi y por todo el apoyo y cariño que siempre he recibido de su parte, muchas gracias.

A mi hermano:

Por todo el cariño y sobre todo la confianza que me brindó para que terminara mi carrera.

A la universidad:

Por la puerta abierta a la cultura que me permitió entrar al camino del conocimiento.

A mi escuela:

Por brindarme todas las herramientas necesarias que hicieron posible que alcanzara la primera meta del camino.

A mis maestros:

Que me abrieron las puertas del conocimiento y compartieron conmigo su sabiduría.

A mi amigo:

Quien confió en mi, me brindó su apoyo y cariño y me enseñó el verdadero concepto de la amistad.

Gracias a todos:

Dulce Maria Carmona Lugo

ÍNDICE

CAPÍTULO V PROPUESTA

BIBLIOGRAFÍA

INTRODUCCIÓN

La comunicación inalámbrica es aquella que se lleva a cabo sin el uso de cables de interconexión entre los usuarios.

Las redes inalámbricas han ganado muchos adeptos y popularidad en lugares como hospitales, fábricas, bodegas, tiendas de autoservicio, pequeños negocios y áreas académicas. Permiten a los usuarios accesar a la información y recursos en tiempo real sin necesidad de estar físicamente en un solo lugar. La red por si misma es móvil y elimina la necesidad de usar cables, establece nuevas aplicaciones añadiendo flexibilidad a la red y lo más importante, incrementa la productividad y eficiencia de las actividades diarias. Un usuario dentro de una red inalámbrica puede transmitir y recibir voz, datos y vídeo, entre edificios, dentro de ellos, en campus universitarios e inclusive sobre áreas metropolitanas a velocidades de hasta 11 Mbps.

Las nuevas posibilidades que ofrecen las redes inalámbricas son: permite una fácil incorporación de nuevos usuarios a la red, ofrecen una alternativa de bajo costo a los sistemas cableados, además de la posibilidad de accesar a cualquier base de datos o aplicación localizada dentro de la red.

En el presente trabajo se encuentra el desarrollo de los temas que fueron necesarios para proponer la implementación de una red inalámbrica dentro de la Escuela Normal No. 4 de Ciudad Nezahualcóyotl.

Capítulo 1 "Introducción a las redes Inalámbricas". En este capítulo se presentan los conceptos básicos requeridos para la comprensión y apreciación de las redes inalámbricas, su clasificación, configuración y características.

Capítulo 2 "Estándares y Protocolos". En este capítulo se analizan las características de los diferentes estándares para redes inalámbricas más utilizados y el funcionamiento de los protocolos de comunicación.

Capítulo 3 "Seguridad". En este capítulo el objetivo es conocer los diferentes mecanismos de seguridad que se puede tener dentro de una red inalámbrica.

Capítulo 4 "Análisis y diseño". En este capítulo se mencionan los dispositivos necesarios para montar una red, así como las características que se deben tomar en cuenta para su implementación.

Capítulo 5 "Propuesta". En este capítulo se muestra como montar una red inalámbrica dentro de la Escuela Normal No. 4 de Ciudad Nezahualcóyotl, así como la configuración a seguir.

Al final del proyecto podrá encontrar un glosario de términos más utilizados y las fuentes de información que han sido utilizadas para la sustentación del presente trabajo.

Esperando que este breve panorama del contenido del trabajo que conjunta el aspecto teórico y práctico, sea útil en la consulta acerca del tema de las Redes Inalámbricas de Área Local.

OBJETIVO GENERAL

Proponer una solución inalámbrica para acceder en tiempo y espacio a la información requerida de acuerdo a las necesidades definidas en la Escuela Normal No. 4 de Ciudad Nezahualcóyotl.

OBJETIVOS PARTICULARES

- Analizar la necesidad y conocer los beneficios de contar con una red inalámbrica para obtener información de forma móvil dentro de la Escuela, para mejorar el control de las partes de que se compone.

- Realizar una propuesta de redes inalámbricas utilizando los avances tecnológicos.

- Establecer los parámetros necesarios para la implementación de una red inalámbrica en la Escuela Normal No. 4 de Ciudad Nezahualcóyotl.

CAPÍTULO 1
INTRODUCCIÓN A LAS REDES INALÁMBRICAS

I.I Red inalámbrica

Una red inalámbrica es un conjunto de computadoras, o de cualquier otro dispositivo informático, comunicados entre sí mediante soluciones que no requieren el uso de cables de interconexión.

Para disponer de una red inalámbrica es necesario instalar tarjetas de red inalámbricas en las computadoras involucradas, así como de equipos llamados puntos de acceso (AP), los cuales dan cobertura a las áreas deseadas cuando se requiere de mayor cobertura; y hacer una pequeña configuración. Esto quiere decir que instalar una red inalámbrica es un proceso mucho más rápido y flexible que instalar una red cableada. Las redes inalámbricas le permiten a los usuarios moverse libremente sin perder la comunicación.

Las computadoras que forman parte de la red pueden comunicarse entre sí y compartir toda clase de recursos. Se pueden compartir archivos, directorios, impresoras, disqueteras o, incluso el acceso a otras redes, como Internet.

El origen de las redes inalámbricas se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica.

Estos resultados, publicados en el volumen 67 de los Procedimientos de IEEE, puede considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del espectro expandido, siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, la FCC permitió la operación sin licencia de dispositivos que utilizaran 1 Watt de energía o menos y asignó las bandas ICM de uso Industrial, Científico y Médico, las frecuencias de 902-928 Mhz, 2.4-2.484 Ghz, 5.725-5.850 Ghz a las redes inalámbricas basadas en espectro expandido. (ICM es una banda para uso comercial sin licencia).

La asignación de una banda de frecuencias propició una mayor actividad, hizo que las redes inalámbricas empezaran a dejar el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando más en la fase de desarrollo comercial, hasta que en mayo de 1991 se publicaron varios trabajos referentes a LAN inalámbricas operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por la norma IEEE 802.11 para que la red sea considerada realmente un segmento de LAN.

Hasta entonces, estas redes habían tenido una aceptación marginal en el mercado. Las razones eran las siguientes:

♦ Gran cantidad de técnicas, tecnologías y normas existentes en el ámbito de las comunicaciones móviles, debido a que los diferentes fabricantes estaban desarrollando sus propias soluciones, utilizando frecuencias y tecnologías muy distintas y normalmente incompatibles.

♦ Altos precios que reflejan los costos de investigación para desarrollar soluciones tecnológicas propietarias.

♦ Reducidas prestaciones, las redes inalámbricas únicamente permiten el soporte de datos, y velocidades de transmisión significativamente menores.

I.2 Clasificación de redes inalámbricas de acuerdo a su alcance

Se llama alcance a la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica.

Las comunicaciones inalámbricas se dividen en los siguientes grupos de acuerdo con su alcance:

◊ Redes inalámbricas de área personal, WPAN (Wireless Personal Area Network), cubre áreas de menos de 10 metros de distancia.

◊ Redes inalámbricas de área local, WLAN (Wireless Local Area Network), cubre áreas desde varios hasta cientos de metros.

◊ Redes inalámbricas de área metropolitana, WMAN (Wireless Metropolitan Area Network), cubre áreas que van desde cientos de metros hasta miles de kilómetros.

◊ Redes inalámbricas de área amplia, WWAN (Wireless Wide Area Network), cubren áreas dispersas desde miles hasta millones de kilómetros, a diferencia de WMAN que abarca ciudades, esta red abarca regiones y hasta países.

◊ Redes globales, WGAN (Wireless Global Area Network), cubren miles de kilómetros, abarcan varios países del mundo.

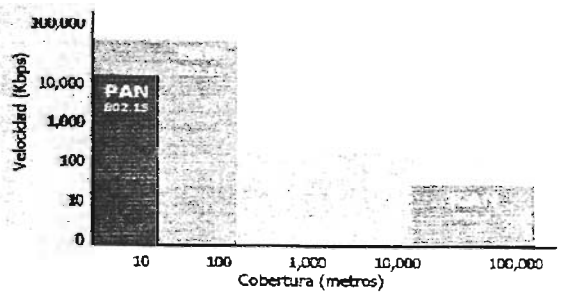


Figura 1. Barras

I.2.I Redes inalámbricas de área personal (WPAN)

Se llaman redes inalámbricas de área personal, WPAN, aquellas redes que tienen un área de cobertura a distancias inferiores a los 10 metros. La finalidad de estas redes es comunicar cualquier dispositivo personal con sus periféricos, así como permitir la comunicación directa a corta distancia entre estos dispositivos.

Impresoras, auriculares, módems, escáners, micrófonos, teclados, etc., pueden intercomunicarse con su terminal vía radio evitando tener que conectar cables para cada uno de ellos.

Las redes tipo WPAN son una nueva categoría en redes que cubren distancias cortas y cerradas. Algunos estándares usados para este tipo de redes son Bluetooth, 802.15 de IEEE y DECT, de los cuales se habla en este trabajo más adelante.

I.2.2 Redes inalámbricas de área local (WLAN)

Se llaman redes inalámbricas de área local, WLAN, a aquellas redes que tienen una cobertura de unos cientos de metros. Estas redes están pensadas para crear un entorno de red local entre computadoras situadas en el mismo edificio o grupo de edificios, para ello se utilizan dispositivos como puntos de acceso y antenas para enviar y recibir señales, con los que se puede crear una red con mayor cobertura.

La mayoría de las redes WLAN utilizan tecnología de espectro expandido, la cual ofrece un ancho de banda limitado, generalmente menor o igual a 11 Mbps, el cual es compartido con otros equipos o dispositivos que accesan al espectro, aunque existen en la actualidad redes que llegan a alcanzar los 54 Mbps con otro tipo de tecnologías.

Este tipo de redes inalámbricas es en las que se basa la realización de este trabajo.

I.2.3 Redes inalámbricas de área metropolitana (WMAN)

Se llaman redes inalámbricas de área metropolitana, WMAN, a las redes que tienen una cobertura desde unos cientos de metros hasta varios kilómetros. El objetivo es poder cubrir el área de una ciudad o entorno metropolitano.

Al igual que las WLAN, este tipo de redes utilizan puntos de acceso que pueden estar conectados para ampliar su cobertura, además de antenas bidireccionales.

Este tipo de redes utilizan estándares como el 802.16 de IEEE.

I.2.4 Redes inalámbricas de área amplia (WWAN)

Una red inalámbrica de área amplia, WWAN, es una red de computadoras que abarcan un área geográfica relativamente extensa, por medio de ella se pueden comunicar diferentes localidades utilizando conexiones satelitales, o por antenas de radio microondas.

La forma más común de implantación de una WWAN es por medio de satélites, los cuales enlazan una o más estaciones bases, para la emisión y recepción, conocidas como estaciones terrestres. Los satélites utilizan una banda de frecuencias para recibir la información, luego amplifican y repiten la señal para enviarla en otra frecuencia.

Para que la comunicación satelital sea efectiva genieralmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en tierra los perderían de vista. Para mantenerse estacionario, el satélite debe tener un periodo de rotación igual que el de la tierra, y esto sucede cuando el satélite se encuentra a una altura de 35.784 kilómetros.

I.2.5 Redes globales (WGAN)

Los sistemas inalámbricos de cobertura global que existen son los sistemas de telefonía móvil. Los primeros fueron sistemas analógicos con muy pocas prestaciones para trasmitir datos. Hasta finales de los años ochenta no aparecieron los primeros sistemas digitales con posibilidades de transmitir datos. A éstos se les ha conocido como sistemas de telefonía celular de segunda generación (2G). Éste es el caso de la tecnología europea GSM y de la norteamericana CDMA.

A diferencia de las WWAN que manejan cantidades superiores de información, las redes globales o de telefonía móvil sólo pueden manejar pequeñas cantidades de datos e imágenes.

I.3 Instalar una red inalámbrica

Las redes cableadas son un problema en aquellas empresas donde existe la posibilidad de cambiar la disposición de los puestos de trabajo. Sin embargo, para una red inalámbrica no supone ningún problema al cambiar una computadora de sitio.

El hecho de instalar una red inalámbrica no quiere decir que toda la red sea igual; la parte inalámbrica puede ser un complemento de la parte cableada, algunos usuarios pueden disponer de una red cableada y una red inalámbrica paralela para aquellos que por la labor que desempeñan necesitan disfrutar de la ventaja de la movilidad. Las redes inalámbricas son ideales si se necesita disponer de conexión en lugares abiertos, en sitios públicos o sitios cerrados pero disponiendo de movilidad.

La inquietud de disponer de la tecnología más moderna es loable y no cabe duda de que las redes inalámbricas ofrecen una mayor comodidad de uso o una mayor facilidad de instalación.

I.3.I Ventajas

Las principales ventajas que ofrecen las redes inalámbricas frente a las redes cableadas son las siguientes:

- Movilidad. La libertad de movimientos es uno de los beneficios más evidentes de las redes inalámbricas. Una computadora o cualquier otro dispositivo pueden situarse en cualquier punto dentro del área de cobertura de la red, sin tener que depender si es posible o no hacer llegar un cable hasta ese sitio. Ya no es necesario estar atado a un cable para navegar por Internet, imprimir un documento o acceder a la información de la red local corporativa o familiar.

- Desplazamiento. Una computadora portátil se puede desplazar sin perder la comunicación. Esto no sólo da cierta comodidad, sino que facilita el trabajo en determinadas tareas.

- Flexibilidad. Las redes inalámbricas permiten colocar una computadora de escritorio en cualquier lugar sin tener que hacer el más mínimo cambio en la configuración de la red. Resulta especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conectan a la red, la conexión inalámbrica evita llenar el suelo de cables. En sitios donde pueda haber invitados que necesiten conexión a Internet, las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

- Reducción de costos. El costo inicialmente más alto de la red inalámbrica es significativamente más bajo cuando se dan cambios frecuentes o el entorno es muy dinámico, además de tener mayor tiempo de vida y menor gasto de instalación. También permite ahorrar costos al permitir compartir recursos: acceso a Internet, impresoras, etc.

- Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo.

- Poca planificación. Con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo se tiene que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.

I.3.2 Desventajas

Los principales inconvenientes de las redes inalámbricas son los siguientes:

- Menor ancho de banda. Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas lo hacen a 11 Mbps. Existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tienen un precio superior.

- Seguridad. Cualquier persona con una computadora portátil sólo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Actualmente una red inalámbrica tiene diversos mecanismos y soluciones para que la seguridad ya no sea un problema.

- Interferencias. Las redes inalámbricas funcionan utilizando el medio radioeléctrico en la banda de 2.4 Ghz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado utilizan esta misma banda de frecuencias. Cuanto mayores sean las interferencias producidas por otros equipos, menor será el rendimiento.

- Incertidumbre tecnológica. Como la estandarización está siendo bastante lenta, ciertos fabricantes han sacado al mercado algunas soluciones propietarias que sólo funcionan en un mismo entorno y por lo tanto están atados a ellos. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones como para la recuperación ante posibles fallos. Cualquier empresa o particular que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de acceso, etc.

I.4 Operación de las redes inalámbricas

Este tipo de redes se diferencia de las convencionales principalmente en la capa física y en la capa de enlace de datos, la cual se divide en dos, según el modelo de referencia del IEEE.

> PHY. Es la capa que se ocupa de definir los métodos por los que se difunde la señal o como son enviados los bits de una estación a otra.

> MAC y LLC. Ambas forman la capa de enlace que se encarga de describir como se empaquetan nuevamente los datos y el modo de verificación de los bits para que no contengan errores.

Los dos métodos de transmisión para remplazar la capa física en una red inalámbrica son: Radio Frecuencia y Luz Infrarroja. Dentro de estos dos medios de transmisión inalámbricos se pueden establecer diversas clasificaciones.

I.4.I Sistema Infrarrojo

La luz infrarroja es un tipo de radiación electromagnética invisible para el ojo humano, los sistemas de comunicaciones con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja, los cuales utilizan muy altas frecuencias debajo del espectro de la luz para transportar datos, (opera en la banda de 300 a 428 Ghz, con una potencia máxima de 2 watts). La mayoría de los controles remotos de los aparatos domésticos utilizan este tipo de comunicaciones. La mayoría de las PDA's, algunos modelos de celulares y muchas computadoras portátiles incluyen un dispositivo infrarrojo como medio de comunicación entre ellos.

Los sistemas de comunicaciones de infrarrojo pueden ser divididos en dos categorías:

- Infrarrojo de haz directo. Esta comunicación necesita visibilidad directa sin obstáculos entre ambas terminales.

- Infrarrojo de haz difuso. En este caso el haz de luz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. En este caso no se necesita visibilidad directa entre terminales.

Las ventajas que ofrecen es que no están reguladas, son de bajo costo e inmunes a interferencias de los sistemas de radio de alta frecuencia. Sus principales inconvenientes son que están limitadas por el espacio y generalmente se utilizan cuando las estaciones se encuentran en un solo cuarto o piso, es sumamente sensible a objetos móviles que interfieran y perturban la comunicación entre el emisor y el receptor, la luz solar directa, las lámparas incandescentes y otras fuentes de luz brillante, así como la lluvia o la niebla.

Los sistemas infrarrojos son los más eficaces sistemas de comunicaciones punto a punto para corta distancia.

La IrDA (Infrared Data Association) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo, además ofrece la ventaja adicional de la seguridad, ya que las emisiones de haces infrarrojos se quedan en un entorno mucho más privado que las propagaciones de ondas de radio.

I.4.2 Sistemas de Radio Frecuencia

Existen distintas tecnologías aplicables al sistema de radio frecuencia. El empleo de cada una depende mucho de la aplicación. Se clasifican en:

- Sistemas de banda angosta (Narrow band).
- Sistemas de espectro expandido (Spread spectrum).
- Multiplexación ortogonal por división de frecuencias.

Al igual se cuenta con un método de modulación en cada sistema de radio frecuencia.

I.4.2.1 Sistema de banda angosta

Un sistema de radio de banda angosta trasmite y recibe información en un radio de frecuencia específica. Utiliza el ancho de banda de 901 - 902, 930 - 931 y 940 - 941 Mhz que está asignada a los servicios de comunicación personal de banda angosta.

En toda la banda se mantiene la frecuencia de la señal de radio tan angosta como es posible para pasar la información. El cruzamiento no deseado entre canales es evitado al coordinar cuidadosamente diferentes usuarios en diferente canal de frecuencia. En un sistema de radio, la privacidad y la no interferencia se incrementa por el uso de frecuencias separadas de radio. El radio receptor filtra todas aquellas frecuencias que no son de su competencia. La desventaja de esta tecnología es el uso amplio de frecuencias, uno para cada usuario, lo cual no es práctico si se tienen muchos.

I.4.2.2 Sistema de espectro expandido

La tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro expandido, el cual trabaja en tres bandas de frecuencias: 902 a 928 Mhz, 2.4 a 2.484 y 5.725 a 5.850 Ghz, llamadas bandas ICM, anteriormente limitadas a su implementación en dispositivos para fines industriales, científicos y médicos. (Por tanto las redes inalámbricas que trabajan dentro de estas bandas de frecuencias deben estar diseñadas para trabajar bajo interferencias considerables).

Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario para la transmisión de la información. Lo que consigue con esto es un sistema muy resistente a las interferencias de otras fuentes de radio, resistente a los efectos de eco y que puede coexistir con otros sistemas de radio frecuencia sin verse afectado y sin influir en su actividad. Esto hace que la tecnología de espectro expandido sea la más adecuada en las bandas de frecuencia para las que no se necesita licencia, además de ser compatible con redes cableadas, de trabajar a una velocidad de 11 Mbps y conectar sitios a una distancia de hasta 40 kilómetros.

Los sistemas de espectro expandido deben satisfacer criterios como:

- El ancho de banda de la señal transmitida debe ser mayor que la señal de información.

- El ancho de banda transmitido debe ser determinado por alguna función que sea independiente del mensaje y conocida en el receptor, ya que si el receptor no está sintonizado a la frecuencia correcta, la señal se miraría como ruido en el fondo.

La NOM-121-SCT1-1994, se refiere al proyecto de Norma Oficial Mexicana de Sistemas de Radio Comunicación que emplean la técnica de espectro expandido. Esta norma dice que los sistemas de radio frecuencia que utilicen esta técnica, podrán operar en estas bandas y están condicionados a no causar interferencia a los equipos ICM,

estaciones de radio comunicación de voz y datos con frecuencia específica asignada. Además estarán expuestos a recibir las interferencias que aquellas les puedan causar sin que tales sistemas reclamen protección.

Las técnicas de transmisión de espectro expandido para distribuir la señal son:

- FHSS, que trabaja en la banda de frecuencias de 2.4 Ghz.
- DSSS, que al igual trabaja en la banda de frecuencias de 2.4 Ghz.

I.4.2.2.1 Espectro expandido por salto de frecuencia (FHSS)

La técnica FHSS consiste en dividir la banda de frecuencias en una serie de canales e ir transmitiendo la información saltando de un canal a otro de acuerdo con un patrón de saltos (spreading code o hopping code) conocido tanto por el emisor como por el receptor. El tiempo máximo que se debe permanecer en cada frecuencia está regulado en 400 milisegundos. Cada canal tiene un ancho de banda de 1 Mhz dentro de la banda de frecuencia de 2.4 Ghz. El ancho de banda y el número total de canales disponibles varía de acuerdo al marco regulatorio de cada país o área geográfica.

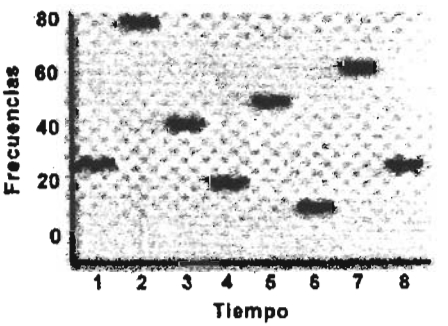


Figura 2. Sistema FHSS

Una de las ventajas de FHSS es que reduce las interferencias porque, en el peor de los casos, la interferencia afectará exclusivamente a uno de los saltos de frecuencia, liberándose a continuación, al saltar a otra distinta. El resultado es que el número de bits erróneos es extremadamente bajo.

Otra de las ventajas de FHSS es que permite que coexistan varias comunicaciones en la misma banda de frecuencias. Para ello, cada comunicación debe tener un patrón de saltos con distinta secuencia.

FHSS es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto, donde se tiene un cantidad de receptores diseminados en un área relativamente cercana al punto de acceso, la razón es que la velocidad máxima alcanzada con esta técnica es de 3 Mbps (aunque sólo está normalizada la velocidad de 1 Mbps).

I.4.2.2.2 Espectro expandido por frecuencia directa (DSSS)

La técnica DSSS se basa en sustituir cada bit de información por una secuencia de bits conocida como chip o código de chips (chipping code), el cual consta de 10 bits redundantes por cada bit transmitido. Estos códigos de chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits. Entre las señales que son eliminadas se encuentran el ruido y las interferencias.

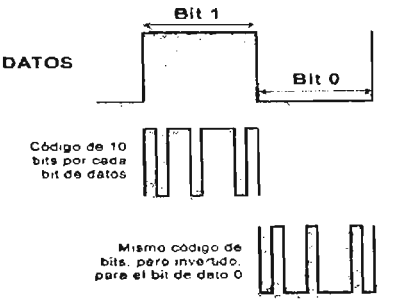


Figura 3. Sistema DSSS

El código de chips permite al receptor identificar los datos como pertenecientes a un emisor determinado. El emisor genera el código de chips y, sólo los receptores que conocen dicho código pueden descifrar los datos, cada receptor filtrará exclusivamente los datos que corresponden con su código de chips. Por otro lado, cuanto más largo es el código, más resistente será el sistema a las interferencias y mayor número de sistemas podrán coexistir simultáneamente; si uno o más bits son dañados durante la transmisión, se podrá recuperar la señal original sin necesidad de retransmisión.

DSSS tiene una velocidad de transmisión de 1, 2, 5.5 y 11 Mbps, por lo tanto es la más utilizada en la tecnología inalámbrica, ya que es más práctica. Un sistema DSSS de 11 Mbps permite que coexistan hasta tres señales en el mismo lugar.

La elección entre FHSS y DSSS dependerá de diversos factores relacionados con la aplicación de los usuarios y el entorno en el que el sistema esté operando.

I.4.2.3 Multiplexación ortogonal por división de frecuencias (OFDM)

Es una técnica de modulación donde la señal de radio se divide en varias bandas de frecuencia angosta para transmitir grandes cantidades de datos. Esta técnica divide el ancho de banda de los 5 Ghz, (5.15 - 5.25 Ghz, que es en la cual trabaja), en subcanales más pequeños que operan en paralelo. De esta forma se consigue llegar a velocidades de transmisión de hasta 54 Mbps.

La técnica OFDM fue patentada por laboratorios Bell en 1970. Esta técnica divide la frecuencia portadora en 52 subportadoras solapadas, 48 de estas subportadoras son

utilizadas para transmitir datos y otras cuatro para poder alinear las frecuencias en el receptor. Este sistema consigue un uso muy eficiente del espectro radio eléctrico.

Puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite son 6, 9, 12, 18, 24, 48 y 54 Mbps.

Una de las ventajas de OFDM es que consigue una alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno (eco). Estas ondas llegan al receptor con distinta amplitud y a distinto tiempo que la señal principal produciendo interferencias.

I.4.2.4 Modulación de la señal

Para poder transmitir la señal vía radio, hace falta definir un método de difusión de la señal y un método de modulación. La modulación consiste en modificar la señal pura de radio para incorporarle la información a transmitir. La señal base a modular recibe el nombre de portadora. Lo que se le cambia a la portadora para modularla es su amplitud, frecuencia, fase o una combinación de éstas. Mientras mayor es la velocidad de transmisión, más complejo es el sistema de modulación. Las técnicas de modulación utilizadas son las siguientes:

* BPSK.
* QPSK.
* GFSP.
* CCK.

Una vez emitida la señal modulada, el receptor tiene que recibir la señal, sincronizar el código de difusión y demodular la información. Los sistemas FHSS son más complicados de sincronizar que los sistemas DSSS. En el primer caso hay que sincronizar tiempo y frecuencia y en el segundo, sólo el tiempo.

I.5 Configuraciones de WLAN

La mayor parte de las redes inalámbricas de área local puede configurarse de las siguientes formas:

) IBSS. Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre las distintas terminales que forman la red. En este caso no existe ninguna terminal que coordine el grupo (servidor), no existe punto de acceso. Todas las comunicaciones son directas entre dos o más terminales del grupo. A esta modalidad se le conoce también como ad hoc, independiente.

Es una configuración en la cual sólo se necesita disponer de tarjetas o dispositivos inalámbricos.

Las comunicaciones ad hoc son muy fáciles de configurar y resultan muy interesantes cuando se necesita establecer una comunicación temporal entre dos equipos.

Permite compartir archivos, impresoras, juegos, etc. Este modo de comunicación es posible sin problemas para un máximo de 10 computadoras.

Figura 4. Configuración ad hoc

) BSS. En este caso se añade un punto de acceso que realiza las funciones de coordinación centralizada de la comunicación entre las distintas terminales de la red; es de mayor alcance que la configuración ad hoc. Los puntos de acceso tienen funciones de buffer y de gateway con otras redes. A la modalidad BSS también se le conoce como modo infraestructura.

Con esta configuración las terminales no tienen porque estar dentro del área de cobertura el uno del otro; al tener un punto de acceso intermedio pueden, al menos, duplicar su distancia. Otra característica es que el punto de acceso permite compartir la conexión a Internet entre todas las terminales, además de permitir crear redes con un mayor número de equipos, los cuales comparten recursos con los demás.

Figura 5. Configuración infraestructura

) ESS. Esta configuración permite crear una red inalámbrica formada por más de un punto de acceso. De esta forma se puede extender el área de cobertura, quedando constituida por un conjunto de celdas pegadas unas a otras. Una red ESS está formada por múltiples redes BSS.

Permite crear una red local inalámbrica con una extensa área de cobertura. Para cubrir toda el área se disponen de redes BSS, cada una de las cuales cuenta con su punto de

acceso. En esta configuración, las terminales pueden desplazarse por toda el área de cobertura sin perder la comunicación.

Los distintos puntos de acceso que forman una red ESS se interconectan entre sí a través de una red que, generalmente, suele ser una red cableada Ethernet. Esta conexión sirve también para que las terminales inalámbricas puedan comunicarse con las terminales de la red cableada.

En las redes ESS, deben configurarse los distintos puntos de acceso como miembros de una misma red. Esto implica que todos deben tener el mismo nombre de red y la misma configuración de seguridad, aunque funcionando en distintos canales de radio, ya que de otro modo, los puntos de acceso interferirían unos con otros impidiendo la comunicación con sus terminales.

Cuando un equipo se mueve fuera del alcance del punto de acceso con el que está asociado originalmente, automáticamente se reasocia con un nuevo punto de acceso con el que tenga cobertura. Esta reasociación la hace la terminal automáticamente, sin que el usuario tenga que hacer nada.

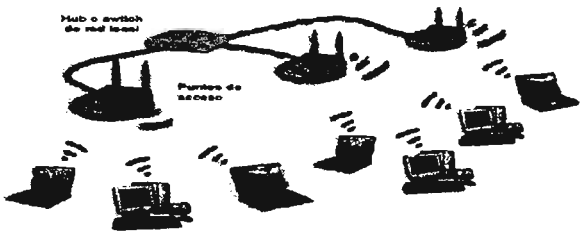


Figura 6. Configuración ESS

En las modalidades BSS y ESS todas las comunicaciones pasan por los puntos de acceso. Aunque dos equipos estén situados uno junto a otro, la comunicación entre ellos pasará por el punto de acceso al que estén asociados. Esto quiere decir que un equipo no puede estar configurado para funcionar en una red ad hoc (IBSS) y de infraestructura (BSS) a la vez.

Todos los dispositivos involucrados dentro de una red inalámbrica deben contener aspectos como:

≈ Estándares, los cuales permiten a éstos tener una comunicación basándose en sus características, para ser utilizados aunque no sean del mismo fabricante.

≈ Protocolos, son las reglas que se emplean en los equipos para que compartan información.

Los cuales se detallan dentro del siguiente capítulo.

CAPÍTULO 2
ESTÁNDARES Y PROTOCOLOS

II.1 Estándares para redes inalámbricas.

Un estándar es un conjunto de reglas y especificaciones, que describen las características de diseño u operación de un programa o dispositivo, que se publica y se ofrece a la comunidad técnica. Los estándares pueden contribuir a un rápido crecimiento del mercado si fomentan la interoperabilidad (la capacidad de un dispositivo creado por un fabricante para funcionar con dispositivos hechos por otros fabricantes).

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso del IEEE y el ETSI.

Los estándares ofrecen ciertas ventajas para el mercado de fabricantes y usuarios tales como:

◊ Manejan un conjunto limitado y preciso de términos.
◊ Incrementan la compatibilidad y conectividad.
◊ Facilitan el intercambio de información.
◊ Aumentan la productividad y la eficiencia.
◊ Crean una base para sustentar nuevas tecnologías.
◊ Permiten mantener un control mundialmente ideal de tecnología.

Algunos de los más conocidos para redes inalámbricas son:

Bluetooth

Bluetooth fue desarrollado en 1994 por Ericsson para conseguir la interconectividad de dispositivos inalámbricos, de una forma sencilla y sincronizada, con otras redes e Internet utilizando las ondas de radio como medio de transporte de la información.

HomeRF

En 1998 se creó un grupo de trabajo bajo el nombre HomeRF con el objetivo de desarrollar y promover un sistema de red inalámbrica para el hogar.

DECT

El estándar DECT fue concebido a finales de 1980 como estándar europeo para teléfonos inalámbricos en aplicaciones domésticas. Su objetivo es facilitar las comunicaciones inalámbricas entre terminales telefónicos.

HiperLAN

HiperLAN fue creado por el ETSI. La primera versión de este estándar, HiperLAN/1, publicada en 1996, HiperLAN/2 se creó en el 2000. En una red de HiperLAN/2 los datos se transmiten en conexiones entre la terminal móvil y el punto de acceso. *

II.1.1 Estándares IEEE

En 1997 el IEEE creó la norma 802.11 que se ocupa de definir las redes de área local inalámbricas.

Después se crearon otros basados en el uso de radio frecuencia en la banda de 2.4 Ghz y se diferenciaban por el método de transmisión de radio utilizado (FHSS y DSSS), los cuales no tuvieron gran auge por el problema del costo y la baja velocidad de 1 y 2 Mbps que manejaban. Hasta 1999 cuando se abarataron los costos, fue cuando se desarrollaron, creando nuevas normas.

Una red inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales cableadas.

Estándar 802.11

Fue creado en 1997. Es la especificación original que utiliza medio de transmisión infrarroja y radio eléctrico en la banda de 2.4 Ghz, con velocidades de 1 ó 2 Mbps, utilizando técnicas de transmisión de salto de frecuencia (FHSS) o de secuencia directa (DSSS).

Otra característica es el uso de WEP como medio de seguridad.

De éste estándar parten las demás versiones.

Estándar 802.11 a

Fue creado en 1999. Esta implementación utiliza la banda de los 5 Ghz, utiliza la técnica de transmisión OFDM para evitar interferencias.

Ofrece velocidades de 54 Mbps, llegándose a alcanzar los 72 y 108 Mbps con versiones propietarias. Cubre entre 30 y 300 metros si no hay muros y otros obstáculos.

* Las características de éstos estándares se encuentran en el anexo "Estándares".

Estándar 802.11 b

Creado en 1999. Permite operar a la velocidad de 1 hasta 11 Mbps en la banda de 2.4 Ghz. Utiliza la técnica de transmisión DSSS.

La mayoría de las redes de este tipo pueden alcanzar distancias hasta 100 metros en interiores y 460 metros en espacio libre.

Los productos basados en este estándar tiene garantizada la interoperatividad entre fabricantes, consiguiendo una reducción de costos y abaratamiento de los dispositivos para el usuario final.

Estándar 802.11 g

Surgió en 2001 con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2.4 Ghz. Esta norma permite transmitir datos a 54 Mbps y llegando hasta 100 Mbps en versiones propietarias.

Utiliza la técnica OFDM; la característica que lo hace especialmente interesante es su compatibilidad con 802.11 b.

La siguiente tabla contiene un resumen de las características de los tres estándares anteriores.

CARACTERÍSTICAS	802.11a	802.11b	802.11g
Regulador	IEEE (USA)	IEEE (USA)	IEEE (USA)
Banda de frecuencia	5 Ghz	2.4 Ghz	2.4 Ghz
Modulación	OFDM	DSSS	OFDM
Velocidad máxima	54 Mbps	11 Mbps	54 Mbps
Rango de velocidades (Mbps)	54, 48, 36, 24, 18, 12, 9 y 6	11, 5.5, 2 y 1	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2 y 1
Número de canales sin sobreposición	8	3	3
Ancho de banda en un área	432 Mbps (8x54)	33 Mbps (3x11)	162 Mbps (3x54)
Usuarios en un área	512	192	192
Eficiencia por canal	18 Mbps	6 Mbps	12 Mbps
Compatibilidad	Wi-Fi5	Wi-Fi	Wi-Fi
A destacar	Alta velocidad y número de usuarios	Buen alcance y consumo de potencia	Compatible con 802.11b y más alcance que 802.11a

Estándar 802.11 c

Este estándar habla sobre la pasarela MAC entre redes.

La capa MAC define los procedimientos que hacen posible que los distintos dispositivos compartan el uso del espectro radioeléctrico para las distintas versiones del estándar 802.11.

Estándar 802.11 e

Trabaja en los aspectos relacionados con la calidad de servicio (QoS).

Este estándar es usado para la transmisión de voz, vídeo, datos, imágenes, etc.

La calidad de servicio significa poder dar más prioridad de transmisión a unos paquetes que a otros, dependiendo de la naturaleza de la información. Por ejemplo, la información de voz necesita ser transmitida en tiempo real, mientras que la información de datos originada por una transferencia de archivo da igual que llegue medio segundo antes o después.

Estándar 802.11 h

Este estándar pretende conseguir una mejora del estándar 802.11a en cuanto a la gestión del espectro radioeléctrico.

Considera las compatibilidades entre HiperLAN y 802.11a para promover un nuevo estándar en la banda de 5 Ghz que sea compatible con los estándares anteriores y con otros existentes en otras partes del mundo como Japón.

Estándar 802.11 i

Este estándar aún no esta totalmente terminado, esta dirigido a combatir la inseguridad de las redes inalámbricas.

Pretende sacar un nuevo sistema mucho más seguro que sustituya a WEP.

Estándar 802.15

Este estándar es compatible con Bluetooth versión 1.1 que tiene una velocidad de 721 Kbps. Fue creado en 2002, se definen las especificaciones de la capa física y de enlace para redes tipo PAN.

Estándar 802.16

Se creó en 2002, con la idea de desarrollar un estándar de una red inalámbrica de área metropolitana (WMAN). Existen dos versiones, una opera en la banda de frecuencias de 10 a 66 Ghz y la otra de 2 a 11 Ghz.

Puede alcanzar distintas velocidades que van desde los 45, 90 y 150 Mbps y ofrece una cobertura que puede alcanzar hasta 50 kilómetros, sino hay obstáculos.

La siguiente tabla contiene un resumen de las variantes relacionadas al estándar 802.11:

Estándar	Descripción
802.11	Estándar WLAN original, utiliza medios de transmisión infrarrojo y radio frecuencia en la banda de los 2.4 Ghz. Soporta velocidades de 1 y 2 Mbps.
802.11 a	Estándar de alta velocidad que soporta hasta 54 Mbps y trabaja en la banda de frecuencias de los 5 Ghz.
802.11 b	Estándar que trabaja en la banda de frecuencias de 2.4 Ghz y soporta velocidades de 5.5 a 11 Mbps.
802.11 c	Pasarela MAC entre redes.
802.11 e	Esta dirigido a los requerimientos de calidad de servicio (QoS) para todas las interfaces IEEE WLAN de radio frecuencia.
802.11 f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11 g	Estándar de alta velocidad que proporciona hasta 54Mbps y que trabaja en la banda de frecuencias de 2.4 Ghz.
802.11 h	Define la administración del espectro de la banda de los 5 Ghz para su uso en Europa y en Asia.
802.11 i	Esta dirigido a combatir la vulnerabilidad actual en la seguridad para protocolos de autentificación y de codificación.
802.15	Este estándar maneja las especificaciones para las redes WPAN con compatibilidad con Bluetooth.
802.16	Maneja las especificaciones para redes de banda ancha de WMAN.

II.2 Protocolos

Un protocolo es un conjunto de reglas que emplean dos equipos informáticos para dialogar entre sí, de forma que puedan establecer y mantener una comunicación sin errores.

Para que los protocolos puedan llevar a cabo sus objetivos, añaden ciertos datos de control a la información original a transmitir. Estos datos adicionales son incluidos por la terminal emisora y suprimidos por la terminal receptora antes de entregar la información al destino.

A lo largo de los años han ido apareciendo distintos protocolos normalizados, cada uno de ellos dedicados a distintas aplicaciones o cubriendo distintas necesidades. Muchos de éstos han surgido a partir de los protocolos desarrollados por empresas u organismos concretos (caso de TCP/IP para interconexión de redes Internet), mientras que otros han sido desarrollados por los organismos de normalización.

Los protocolos de comunicaciones son programas que se instalan tanto en la terminal origen, como en el destino de la comunicación. Parte de estos programas residen en el propio hardware del equipo, otra parte viene incorporada en el Sistema Operativo y la restante es instalada por el usuario en el momento de configurar el equipo.

Las funciones de los protocolos se pueden resumir en las siguientes:

a) Identifican cada dispositivo en la ruta de las comunicaciones para asegurar la atención del otro dispositivo.
b) Verifican la correcta recepción del mensaje transmitido.
c) Verifican que el mensaje requiera retransmisión porque no puede ser correctamente interpretado.
d) Realizan la recuperación cuando hay errores.

II.2.1 Protocolo de Aplicaciones Inalámbricas (WAP)

WAP es utilizado para filtrar el contenido de Internet para las comunicaciones móviles. Este protocolo provee la posibilidad de acceder a los servicios de información contenidos en Internet además de otros servicios adicionales como el desvió de llamadas inteligentes, en donde, se realizan acciones como aceptar llamadas, desviarlas a otras personas o a un buzón vocal, etc., y ponerla a disposición de las terminales móviles.

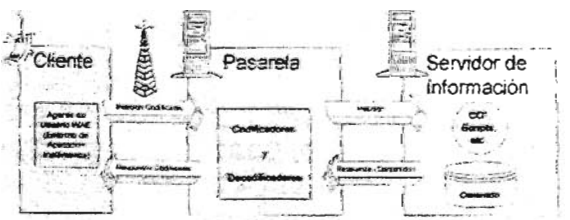


Figura 7. Modelo de funcionamiento del WAP

En la terminal inalámbrica existe un micro-navegador encargado de la coordinación con la pasarela, a la cual realiza peticiones de información que son tratadas y redirigidas al servidor de información adecuado. Una vez procesada la petición de información en el servidor, se envía esta información a la pasarela que de nuevo procesa para enviarlo a la terminal inalámbrica.

La arquitectura de WAP está definida en una estructura de capas[8], en donde cada capa es accesible por la capa superior así como por otros servicios y aplicaciones a través de un conjunto de interfaces muy bien definidos y especificados.

Figura 8. Arquitectura de WAP

II.2.2 Protocolo de Acceso Compartido (SWAP)

SWAP define una interfaz inalámbrica que está diseñada para soportar el tráfico de voz y los servicios de datos en redes WLAN dentro de los entornos domésticos e interoperar con las redes públicas de telefonía e Internet.

Esta normativa asegura la interoperatividad de una numerosa cantidad de productos con capacidades de comunicación inalámbrica que se desarrollan para computadoras destinadas al mercado doméstico. Esta especificación permite que las computadoras, periféricos, teléfonos y electrodomésticos se comuniquen con otros dispositivos de similar naturaleza.

La base radioeléctrica de este protocolo opera en la banda ICM de los 2.4 Ghz, combinando elementos de los estándares DECT para voz e IEEE 802.11para datos.

II.2.4 Protocolo TCP/IP

TCP/IP es el protocolo común utilizado por todas las computadoras conectadas e Internet, de manera que éstos puedan comunicarse entre sí. En Internet se encuentran conectadas computadoras de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Este protocolo se encargará de que la comunicación entre todos sea posible. Es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP es un conjunto de protocolos que cubren los distintos niveles del modelo OSI[9]. Los protocolos más importantes son el TCP y el IP.

---

[8] La descripción de cada una de ellas se encuentra en el anexo "Capas WAP".

[9] Ver anexo "Modelo OSI".

En la siguiente figura se observan los cuatro niveles o capas en las que se agrupan los protocolos de TCP/IP y en que se relacionan con los niveles OSI.

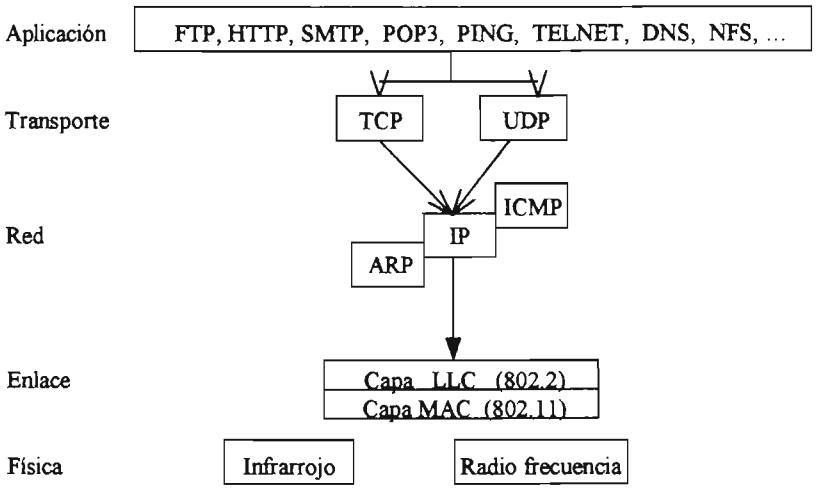


Figura 9. Niveles del protocolo TCP/IP

* La capa de aplicación corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios.
* La capa de transporte coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
* La capa de red concuerda con el modelo OSI. Se encarga de enviar los paquetes de información a sus destinos correspondientes.
* La capa de enlace y física se encargan de los métodos de acceso y de la transmisión a través del medio físico, coinciden con el modelo OSI.

TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet.

Su ventaja principal es: proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información está debe ser dividida en unidades de menor tamaño, cada una de estas unidades de información reciben el nombre de "segmentos", que son conjuntos de datos que se envían como mensajes independientes.

TCP es el encargado de dividir el mensaje original en segmentos de menor tamaño, y por lo tanto, mucho más manejables.

IP tiene únicamente la misión de encaminar el segmento, sin comprobar la integridad de la información que contiene. Identifica a cada terminal que se encuentre conectada a la red mediante su correspondiente dirección, esta dirección es la que identifica a la terminal para todas sus comunicaciones.

A las direcciones IP que utilizan los equipos de una red local se les conoce como dirección IP privada, mientras que a las direcciones IP de Internet se les conoce como públicas. Las direcciones IP privadas son asignadas arbitrariamente por el administrador o usuario de la red local, y las IP públicas son asignadas por las autoridades de Internet.

Las tareas de las que se encarga IP son:

- Ruteo de datagramas (los guía desde el equipo fuente hasta el equipo destino).
- Esquema de direccionamiento.
- Fragmentar o desfragmentar segmetos.

IPv4 (IP versión 4)

En la versión 4 de IP la dirección de Internet se utiliza tanto en la terminal como en la red a la que pertenece, la cual consta de 32 bits, de manera que sea posible distinguir a las terminales que se encuentran conectadas en la misma red. Con este propósito y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, que se representan mediante tres rangos de valores:

Clase	Primer byte	Identificación de red	Identificación de host	Número de redes	Número de host
A	1 ... 126	1 byte	3 byte	126	16.387.064
B	128 ... 191	2 byte	2 byte	16.256	64.516
C	192 ... 223	3 byte	1 byte	2.064.512	254

IPv6 (IP versión 6)

Una de las características importantes es el sistema de direcciones, en el cual se pasa de los 32 a los 128 bits, eliminando todas las restricciones del sistema de IPv4.

Las ventajas que tiene la versión 6 ante la versión 4 son:

γ Autoconfiguración. Cualquier dispositivo puede tener una dirección con sólo conectarse a la red. El dispositivo crea una dirección propia automáticamente y busca en

la red que no haya direcciones duplicadas. Para mayor privacidad, el dispositivo puede cambiar su dirección para cada sesión y mantener una dirección privada interna en la red y otra pública fija.

γ IP Móvil. Permite transmitir de una red a otra mientras mantiene una sola conexión. Da a cada dispositivo una dirección interna permanente y otra que cambia cuando el usuario sale de una red y entra a otra. IPv6 puentea los primeros paquetes de cada sesión y envía actualizaciones de unión directamente a cada tercer corresponsal, de modo que los demás paquetes se puedan enviar al dispositivo. IPv6 ofrece seguridad integrada de extremo a extremo, incorpora autenticación IPsec y codificación en el nivel de paquetes.

γ Calidad de servicio. IPv6 también ofrece calidad de servicio integrada y soporte para distribuciones múltiples. QoS permite establecer prioridades entre ciertos tipos de flujos sensibles al tiempo, y la distribución múltiple conserva el ancho de banda cuando los flujos se envían a varios usuarios en distintos lugares.

Una vez que se conocen las reglas esenciales para la comunicación entre equipos inalámbricos, se debe tener en cuenta otros aspectos que al igual son importantes, como lo es la seguridad.

Se llega a pensar que una red inalámbrica por si sola es insegura, pero gracias a diversos mecanismos que se han implementado, éste ya no es un problema que impide el pensar en la tecnología inalámbrica como una solución en redes.

Por tratarse de un aspecto sobresaliente, en siguiente capítulo, se encuentran desglosados los mecanismos indispensables para la seguridad.

CAPÍTULO 3
SEGURIDAD

III.1 Riesgos

La seguridad en redes inalámbricas, es un factor muy importante, debido a que el medio de transmisión es el aire. Estas redes emiten señales que pueden ser fácilmente recogidas en el exterior de la red, es por ello que para protegerla hay que empezar desde su planeación.

Los mayores riesgos que tienen estas redes son:

♦ Pérdida de equipo. Perder una computadora se convierte en un gran problema, si cae en manos equivocadas, por la información que pueda contener y además que puede tener acceso a la red con sólo estar dentro de la zona de cobertura de la señal. Para que no exista este problema hay que tomar las precauciones para evitar en lo posible la pérdida o robo del equipo (sea portátil o de escritorio). No dejar grabados los nombres de usuario y contraseña, ni dejar estos datos escritos en papeles que se mantengan pegados en el equipo.

♦ Infección por virus. Este problema se presenta tanto en redes cableadas, como inalámbricas, en donde todos o alguno de los equipos puede ser infectado y es interrumpido el trabajo. Para evitar la infección por este medio se debe contar con un antivirus actualizado, en cada equipo dentro de la red.

♦ Uso equivocado por personas autorizadas. Puede ser intencional o accidental, sea que el usuario borre información, la modifique o la copie para hacer uso malintencionado de ella. Una forma de prevenirlo es creando copias de seguridad de la información.

♦ Uso fraudulento por personas no autorizadas. Cualquier usuario puede conectarse a la red desde cualquier sitio sin necesidad de conectarse físicamente a ningún medio. Los usos fraudulentos de que pueden ser víctimas las redes inalámbricas son:

⇒ Escuchar. Con un receptor adecuado, los datos emitidos por un usuario pueden ser recogidos por otras personas.

⇒ Acceder. Se trata de configurar un dispositivo para acceder a una red en donde no se tiene autorización. Se puede hacer de dos formas: configurando una estación para que pueda acceder a un punto de acceso existente o instalando un nuevo punto de acceso.

⇒ Romper la clave. Consiste en intentar adivinar la clave de acceso de un usuario autorizado mediante intentos sucesivos.

⇒ Saturar. Se trata de dejar fuera de servicio a una red. La red no podrá ser utilizada por los usuarios; para dejarla inhabilitada bastará con saturar el medio

radioeléctrico con el suficiente ruido para que sea imposible llevar a cabo cualquier comunicación. A este ataque se le conoce como obstrucción de servicio.

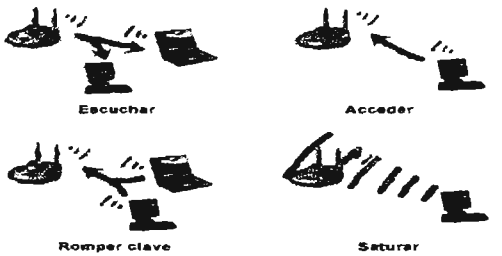


Figura 10. Usos fraudulentos de las redes inalámbricas

Para prevenir este tipo de problema se recomienda cambiar las claves de acceso y activar las medidas de seguridad no habilitadas por defecto, como lo es WEP, cambiar la identificación SSID.

III.2 Claves de acceso

Existe un gran riesgo en las redes inalámbricas debido al manejo de claves de acceso. Ya que los hackers utilizan técnicas para entrar a una red, la más utilizada se basa en averiguar dichas claves. Las claves más utilizadas por los usuarios de una red son muy predecibles por lo simples y cortas que suelen ser, debido a esto, existen diccionarios de claves que contienen una relación de las palabras que tienen una mayor probabilidad de ser utilizadas, y a los cuales tienen acceso los hackers.

Otra técnica utilizada por ellos es lo que se conoce como ingeniería social, la cual consiste en hacer una llamada por teléfono a un usuario haciéndose pasar por un técnico que tiene una situación que resolver por lo que necesita comprobar los datos.

Una de las formas más simples de mantener la seguridad es por las claves de acceso; para que éstas sean una buena protección sólo hay que tener en cuenta lo siguiente:

a) Tener una longitud mínima de seis caracteres.

b) Que no sea una palabra con significado.

c) Que no corresponda con las iniciales del nombre del usuario o de la empresa.

d) No ser una letra repetida.

e) No estar formada por letras contiguas del alfabeto.

f) No estar formada por letras contiguas del teclado.

g) Mezclar letras mayúsculas, minúsculas y números.

h) Cambiar periódicamente las claves de acceso.

Hay que tomar precauciones para que los intrusos no puedan hacer uso de los equipos, de las cuales algunas son:

◊ Nunca decirle a nadie la clave y asegurarse de que empleados no lo hagan.

◊ Evitar el uso de claves estáticas, hay que modificarlas constantemente.

◊ Utilizar un firewall.

◊ Examinar frecuentemente la red para comprobar que no hay conexiones no autorizadas.

III.3 Mecanismos básicos de seguridad IEEE 802.11

El estándar IEEE 802.11 contempla tres mecanismos de seguridad básicos:

- SSID. Es un código alfanumérico que se configura en cada equipo y punto de acceso que forma parte de la red. Puede ser utilizado como una simple contraseña entre la terminal y el punto de acceso o como un identificador del emplazamiento del emisor de una red pública. Existen puntos de acceso que permiten que se les deshabilite el SSID. Este sistema no garantiza la seguridad, ya que los códigos son emitidos en forma de texto sin codificar, y se envía de forma libre por el aire alrededor de 10 veces por segundo.

- Filtrado de direcciones MAC. Se puede generar una lista de direcciones MAC, creada para cada punto de acceso en la red y limitar el acceso a aquellos equipos contemplados en la lista. Las direcciones están formadas por doce caracteres alfanuméricos e identifican a la tarjeta de red, de fábrica. No son modificables por el usuario, se transmiten en forma de texto sin codificar y son fácilmente leíbles con un receptor adecuado.

Nota: (La dirección MAC es diferente a la capa MAC del modelo OSI).

- WEP. Con este sistema se cifran todos los datos que se intercambian entre los equipos y los puntos de acceso.

III.3.1 Privacidad equivalente a cable (WEP)

En 1999 el IEEE propuso un sistema de cifrado de datos que se incorpora a las redes con el estándar 802.11b, conocidas como Wi-Fi, llamado WEP, el cual surgió para

ofrecer a las redes inalámbricas un estado de seguridad similar a las cableadas. Su uso es opcional; y se convirtió en el sistema básico de seguridad para redes de este tipo.

WEP utiliza una clave generada de forma pseudoaleatoria por el algoritmo RC4, aplicada a una clave secreta definida por el usuario y un IV.

La clave secreta es única y deberá estar configurada en cada terminal y punto de acceso que se desee conectar a la red inalámbrica. La clave que genera el usuario puede ser de 40 o 104 bits; un inconveniente de esta clave es que es estática ya que una vez configurada permanece invariable, sólo puede cambiarse manualmente realizando la configuración de una nueva clave en cada equipo de la red.

El IV es de 24 bits, se transmite abiertamente a todos los equipos en forma de texto y cambia periódicamente.

Por lo tanto WEP sólo maneja dos tipos de claves de 64 y 128 bits. El cifrado de datos que maneja este sistema se representa en la siguiente figura.

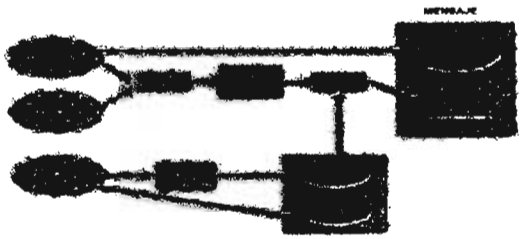


Figura 11. Cifrado WEP

De forma más simplificada el cifrado se puede ver de la siguiente forma:

Datos (abiertos)	CRC	XOR	RC4 (vector, clave)	=	Vector	Datos cifrados

En donde se tiene la clave pseudoaleatoria por una parte, por la otra los datos a transmitir y el algoritmo CRC que tiene la tarea de añadir el ICV (Valor de comprobación) el cual consta de cuatro caracteres que se adjuntan al final de la información y se utilizan para que el receptor pueda comprobar la integridad de la información recibida. A todo se le aplica la operación OR exclusiva (XOR), obteniendo el mensaje cifrado y el IV que se ha enviado a todos los equipos.

Una vez que llegan al destino los datos cifrados, se combina el IV con la clave secreta (que esta configurada en cada equipo) para generar la semilla que permita descifrar los datos mediante el algoritmo RC4. Aplicando nuevamente la operación OR exclusiva, se obtiene la información descifrada al igual que el ICV y mediante el algoritmo CRC comprobar que no hubo errores en la transmisión.

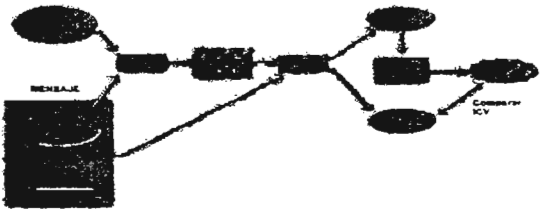


Figura 12. Descifrado WEP

El sistema WEP es vulnerable a los ataques, es por ello que no se puede asegurar la confidencialidad de la información. Algunos ejemplos de ataques contra él son:

- Descifrar un mensaje basado en la fragilidad del IV y en la utilización de códigos estáticos, es decir, si un hacker obtiene la clave secreta espiando la red puede descifrar la información interceptándola.

- Crear una tabla de IV´s y claves secretas permitiendo descifrar fácilmente todos los mensajes interceptados.

- Descifrar la información contenida en las cabeceras de los paquetes para poder reenviarlas a otro equipo y descifrar allí su contenido.

III.4 Estándar 802.1x

En 2001 el IEEE aprobó el estándar 802.1x para abordar el problema de la administración de claves, es por ello que con este estándar las claves rotan constantemente y utiliza llaves únicas por conexión. Se creó para contrarrestar los defectos de la seguridad de WEP.

Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos. Emplea llaves dinámicas en lugar de estáticas, hace uso de un protocolo de autentificación para su reconocimiento mutuo conocido como EAP (Protocolo de autentificación extensible). También utiliza un servidor que proporcione servicios de autentificación remota de usuarios entrantes conocido como RADIUS.

Este estándar se caracteriza porque la baja potencia de transmisión obtenida en el proceso de dispersión del espectro permite que la información viaje en niveles cercanos al ruido. En este caso la codificación y dispersión del espectro trabajan en conjunto para proteger la información y que el receptor inteligente distinga que es ruido y que es información válida. Con 802.1x es posible tener una transmisión de información difícil de interferir.

Protocolo de Autentificación Extensible (EAP)

Este protocolo se utiliza para controlar el acceso de los usuarios a los puntos de acceso y autentificar sus comunicaciones, también se utiliza para poder hacer una entrega segura de las claves de la sesión.

Con EAP se puede generar y distribuir automáticamente las claves WEP, para evitar hacerlo manualmente.

Servicio remoto de autentificación de usuarios entrantes (RADIUS)

Es un sistema de autentificación y contabilidad que verifica las credenciales de los usuarios y otorga el acceso a los recursos solicitados. Es ampliamente usado en ambientes de red en donde no se puede lidiar con un gran número de usuarios con información de autentificación distinta; se utiliza este sistema para facilitar la administración centralizada, sobre todo en donde se agregan y eliminan usuarios durante el dia y la información de la autentificación del usuario cambia constantemente.

RADIUS proporciona cierto nivel de protección contra ataques activos y pasivos, y se utiliza para administración remota.

III.5 Acceso Wi-Fi protegido (WPA)

En 2002 alianza Wi-Fi y el IEEE sacaron al mercado un sistema de seguridad conocido como WPA basado en el estándar 802.11i, por lo tanto se puede decir que WPA es un subconjunto de éste y es totalmente compatible con él.

Mejora fuertemente el nivel de protección de datos y el control de acceso a las redes inalámbricas Wi-Fi, es decir, se realizó para solucionar todas las debilidades de WEP. La ventaja que tiene WPA es que puede aplicarse a las redes Wi-Fi existentes, es compatible con el futuro sistema de seguridad del IEEE 802.11i y todas las características que incluye pueden ser actualizadas en los equipos por medio de software.

Una vez instalado el nivel de seguridad adquirido es extremadamente alto, asegurándose que sólo los usuarios autorizados pueden acceder a la red y que los datos transmitidos permanecen completamente inaccesibles para cualquier usuario que no sea el destinatario.

Las ventajas que aporta WPA frente a WEP son:

* Mejoras en el cifrado de datos mediante TKIP (Protocolo temporal de integridad de clave), este sistema asegura la confidencialidad de los datos.

* Autentificación de los usuarios mediante el estándar 802.1x y EAP, este sistema permite controlar a todos los usuarios que se conectan a la red ya que genera y distribuye las claves; si se desea permite el acceso de usuarios anónimos.

Protocolo temporal de integridad de clave (TKIP)

Es un protocolo abierto creado como parte del estándar 802.11i para corregir errores de seguridad en WEP. Ofrece una mezcla de claves por paquete, revisión de la integridad de los mensajes y mecanismo de recodificación para WEP.

III.4 Estándar 802.11i

Estándar del IEEE que aún no esta totalmente terminado, el primer borrador salió en 2002. Tiene como objetivo mejorar la seguridad de las redes inalámbricas.

Algunas mejoras son el control de acceso y la autentificación, además incluye temas como una metodología de cifrado mejor que WEP, un mejor uso del IV, protección contra los paquetes falsos, ataques de respuestas, entre otros.

Sus componentes principales son AES (Estándar de encriptación avanzada), autentificación 802.1x, TKIP y sistema de administración de claves para codificación.

Estándar de encriptación avanzada (AES)

Es un protocolo de codificación de información federal que garantiza la privacidad mediante claves de 128, 192 y 256 bits.

El AES requiere de actualizaciones de hardware para clientes y puntos de acceso.

Este estándar está aún en proceso de definición.

III.7 Firewall

El firewall o cortafuegos es una medida de seguridad que se puede implementar en las redes inalámbricas. No protege las comunicaciones sino que protege a la computadora individualmente para que ninguna persona ajena pueda hacer uso de información contenida en el disco duro o de cualquier otro recurso con que se cuente. Los puntos de acceso pueden tener algunas propiedades de firewall para proteger los recursos de la red. Su aplicación puede ser por medio de hardware específico, o software instalado en el equipo.

Figura 13. Formas de firewall

El firewall lleva a cabo su protección analizando los datos de petición de acceso a distintos recursos y bloqueando los que no estén permitidos, toma la decisión de que datos deja pasar y cuales no, analizando los paquetes de información.

Las reglas de las que dependen los filtros de los firewall se basan en distintos factores, condiciones o características de los paquetes de datos.

Parámetro	Significado
Protocolo	Dependiendo del tipo de protocolo que utiliza el paquete (TCP, HTTP, FTP, etc.), se puede permitir el acceso.
Dirección IP del destinatario	Identifica al equipo que va a recibir el paquete, puede realizar bloqueo de comunicación con otros equipos con los cuales no esta permitido el intercambio de información.
Puerto IP del destinatario	Identifica a la aplicación que va a recibir el paquete, filtra los servicios que pueden ser accedidos.
Dirección IP del remitente	Identifica al equipo que envío el paquete, además de bloquear comunicaciones también lo puede hacer para el acceso a Internet de algunos usuarios.
Puerto IP de remitente	Identifica a la aplicación que envió el paquete, filtra los servicios a los que puede acceder.
Contenido	Identifica el contenido de la información transmitida, ya que pueden filtrar los datos que contienen determinadas palabras o frases, analizando todo el contenido de los paquetes en busca de las palabras o frases prohibidas.

Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información de la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

III.8 Red privada virtual (VPN)

Una VPN se crea mediante el uso de protocolos especiales que permiten conectar una computadora a una red de una forma segura, debe instalarse en cada equipo que forma la

red. Algunos de estos protocolos son PPTP, L2TP e IPSec. La única particularidad de VPN es que un equipo debe hacer las funciones de servidor.

Las ventajas que ofrece crear una VPN son:

φ La gestión de la VPN es centralizada, escalable y eficiente.

φ Ofrece seguridad a las comunicaciones inalámbricas.

φ El software de VPN no tiene ningún costo adicional si se utiliza Windows.

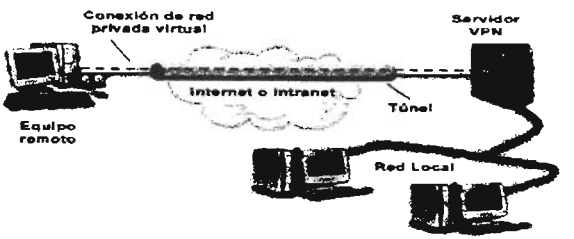


Figura 14. Conexión de red privada virtual

La red privada virtual cifra las comunicaciones entre el equipo del usuario y un servidor VPN mediante un sistema que se conoce como tunelado. No importa que la comunicación se realicé de forma inalámbrica, ya que la información transmitida tendrá la garantía de no poder ser cifrada hasta que no llegue a su destino.

El inconveniente de las redes privadas virtuales es que parte del caudal transmitido tiene que dedicarse al cifrado de los datos, es por ello que son redes un poco menos eficientes.

Si se configura una VPN ya no es necesario otro sistema como WEP, mientras que un firewall puede impedir las comunicaciones de este tipo de redes a menos que se configure para permitirlas.

III.9 Resumen de medidas de seguridad aplicables

Como un resumen, se pueden tomar algunas medidas de seguridad para que las redes inalámbricas sean confiables para los usuarios o empresas que las implementen.

1. Siempre informar a los usuarios de aquellas medidas mínimas de seguridad que se deben tener en cuenta, nombradas en el apartado III.1.

2. Cambiar los parámetros de seguridad que vienen configurados por el fabricante en el equipo, también cambiar el nombre de red (SSID).

3. Deshabilitar la configuración remota del punto de acceso.

4. Activar el cifrado WEP, es recomendable cambiar las claves periódicamente y que no sean fáciles.

5. Configurar los puntos de acceso para que no envíen el SSID.

6. Utilizar las características de un firewall, ya sea las que están en los puntos de acceso o instalándolo.

7. Deshabilitar la asignación dinámica de números IP (DHCP), cuando se tiene un servidor en la red.

8. Compartir sólo los recursos necesarios, sean archivos o impresoras, pero nunca compartir todo el disco duro y si es posible protegerlos con claves.

9. Instalar el WPA, o en su defecto manejar la seguridad con el estándar 802.1x.

10. Si es posible configurar una red privada virtual si se busca un mayor grado de seguridad.

11. Si la red inalámbrica pertenece a una empresa en donde se necesita de mayor seguridad por la información que maneja, contar con un software para el monitoreo de puntos de acceso no autorizados.

CAPÍTULO 4
ANÁLISIS Y DISEÑO

IV.1 Consideraciones generales

Resulta fácil deducir que la red inalámbrica local es un perfecto sustituto del cableado tradicional, en lugar de transmitir la información por medio de cable se hace por medio de ondas de radio con lo que se elimina una costosa y problemática instalación.

Existen elementos a considerar en la cobertura de una red inalámbrica como los inconvenientes atmosféricos (aire, agua, lluvia, etc.) y materiales que se encuentran en el lugar de la implementación.

Hay que analizar que tipo de red es la que conviene mejor a las necesidades, ya que se puede comunicar desde varios hasta cientos de usuarios, que pueden estar concentrados en una pequeña zona o en una gran área, sea en uno, varios edificios o en el exterior.

Las decisiones que hay que tomar al respecto son las siguientes:

⇒ Cuál será la configuración de la red, si se necesita instalar puntos de acceso y cuántos serán necesarios.

⇒ Qué tarjeta inalámbrica se instalará en cada equipo.

⇒ Qué tipo de antenas se necesitan para cubrir el área en la que se requiere disponer de servicio.

⇒ Como se conectará la red inalámbrica a una red cableada o a Internet.

Para este proyecto se utilizan productos basados en el estándar 802.11b debido a la compatibilidad que tiene y a que la velocidad es adecuada a los requerimientos que se hacen nombran más adelante.

Los equipos basados en este estándar llegan a tener cobertura de 100 hasta 400 metros en espacio abierto con visibilidad directa entre equipos y sin interferencias de otros que trabajen a 2.4 Ghz. Mientras que si alguno se instala en el interior, su alcance se reduce dependiendo de los obstáculos.

La mayoria vienen equipados con un sistema que baja automáticamente la velocidad de transmisión conforme la señal se va debilitando. Significa que conforme se aumenta la distancia entre emisor y receptor se puede ir disminuyendo la velocidad de transmisión de datos.

Debido a que las interferencias representan un gran problema hay que evitarlas para que no se corte la comunicación, cuando un equipo detecta la presencia de una señal de

interferencia automáticamente entra en un periodo de espera, esto hace que el servicio se degrade pero no se interrumpe.

Las redes inalámbricas de área local funcionan a base de puntos de acceso que cóordinan las comunicaciones y adaptadores de red (tarjetas de red) que se instalan en las computadoras y les permite formar parte de la red. Adicionalmente existen antenas para aumentar el alcance de los equipos. Los puntos de acceso controlan la asignación del tiempo de transmisión, también funcionan para tener comunicación con redes cableadas.

Al diseñar una red local inalámbrica se deberán instalar tantos puntos de acceso que garanticen la cobertura total de área, lo cual se logra colocando estos dispositivos de tal manera que las señales se superpongan una con otra para eliminar las zonas muertas o sin señal que pudiera haber; ya que según se mueva el usuario la señal que recibe el adaptador de red se puede cambiar de un punto de acceso a otro para continuar con la transmisión, a esto se le llama "Roaming".

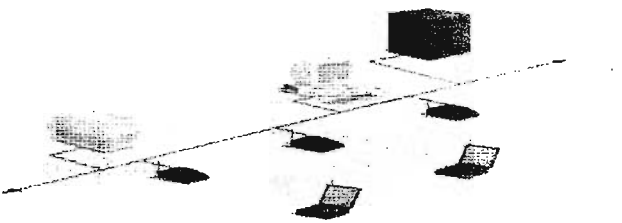


Figura 15. Roaming

En algunos casos puede convenir utilizar bridges como puntos de extensión para aumentar el número de puntos de acceso a la red, los cuales no tienen que estar conectados por un cable.

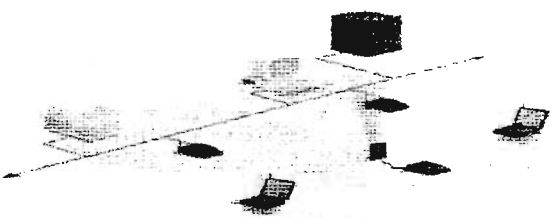


Figura 16. Punto de extensión

Además de todo esto hay que considerar varios factores para adquirir un sistema inalámbrico.

Cobertura

Los equipos basados en el estándar 802.11b llegan a tener una cobertura de cientos de metros en espacio abierto sin interferencias como hornos de microondas, etc.

Rendimiento

Depende de los modelos que implementen los fabricantes, el número de usuarios con que cuente y del tipo de sistema inalámbrico.

Compatibilidad con otras redes

La mayoría de redes inalámbricas proporcionan interconexión con redes cableadas como Ethernet, además el estándar 802.11b es compatible con el 802.11g que tiene una mayor velocidad de transmisión de datos.

Las redes que utilizan distintas bandas de frecuencias no pueden comunicarse entre sí. Igualmente si se basan en distintas técnicas de transmisión.

Escalabilidad

Estas redes pueden soportar un amplio número de equipos añadiendo puntos de acceso para dar energía a la señal y extender la cobertura.

También se puede ampliar mediante antenas para tener un mayor alcance o por puntos de extensión.

Seguridad

La seguridad para redes inalámbricas se basa en el sistema WEP, entre otros, a los cuales se hizo referencia en el capítulo anterior del proyecto; y varían de acuerdo al equipo, al fabricante y al software que se implemente.

Costos

El costo de implementar una red inalámbrica varía de acuerdo a la extensión que va a tener por el número de puntos de acceso que se requieran, adaptadores de red, antenas (si se requiere). Además que depende de la marca o fabricante.

Un punto a favor es que en comparación con las redes cableadas es menor el gasto de instalación y mantenimiento.

IV.2 Dispositivos

Como se mencionó los dispositivos que intervienen en la implementación de una red inalámbrica son varios y a continuación se describen sus principales características.

IV.2.1 Adaptadores de red (tarjetas de red)

Los adaptadores de red son las tarjetas o dispositivos que se conectan a los equipos para que funcionen dentro de una red inalámbrica. Son fundamentalmente estaciones de radio que se encargan de comunicarse con otros adaptadores o con puntos de acceso para mantener al equipo al que están conectados dentro de la red.

Los adaptadores necesitan una antena, la cual viene integrada dentro del propio adaptador sin que se note externamente; aunque existen algunos en los cuales si se puede identificar la antena claramente. En cualquier caso pueden incluir un conector para disponer de una antena externa y aumentar su alcance.

Existen varios tipos de adaptadores inalámbricos de red.

Adaptadores PCMCIA

Estas tarjetas fueron creadas en 1989, están hechas para ser utilizadas en computadoras portátiles. Se insertan en puertos con el mismo nombre que ya están incorporados en los equipos.

Todas las tarjetas tienen un ancho de 54 milímetros, el largo es variable pero como mínimo tienen 85.6 milímetros, esto se da porque algunas tarjetas necesitan sobresalir hacia el exterior para mostrar algún tipo de conector, una antena, o sólo necesitan más espacio.

Por su grosor las tarjetas se dividen en tres tipos: las tarjetas tipo I con un grosor de 3.3 milímetros, las de tipo II con 5 milímetros (son las más utilizadas) y las tipo III con 10.5 milímetros.

Cada una requiere su propio tipo de ranura en la computadora (las ranuras tipo III pueden admitir cualquier tipo de tarjeta, mientras que las tipo I sólo admiten las del mismo tipo).

Las tarjetas quedan insertadas en el interior de la ranura por lo que no representa ningún problema al guardar la computadora portátil o al transportarla. Otra de las características de las tarjetas PCMCIA es su bajo consumo de energía y son resistentes a los golpes que se presentan en la movilidad de los equipos.

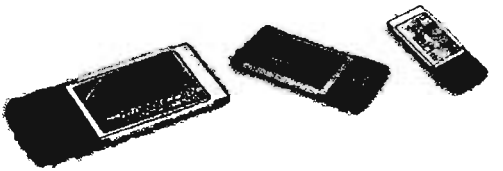


Figura 17. Tipos de adaptadores de red PCMCIA

Adaptadores PCI e ISA

ISA apareció a principios de los años ochenta y PCI fue creado en 1993, por lo que este último tipo de adaptadores es más común encontrarlos en computadoras de escritorio. Son de mayor tamaño que las PCMCIA, más baratas y de instalación más compleja ya que tiene que abrirse la computadora para introducirlas.

Otra forma en que son utilizadas es como tarjeta conversora de PCI o ISA a PCMCIA; al ser instalada en el interior del equipo en una de las ranuras PCI o ISA disponibles, ofrecen al exterior una ranura PCMCIA. Al ser usadas como conversoras se incrementa su costo por el uso necesario de tarjetas PCMCIA.

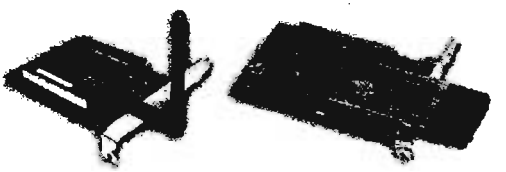


Figura 18. Adaptador de red PCI y conversor PCI a PCMCIA.

Adaptadores USB

USB apareció en 1993 como un nuevo puerto para mejorar la forma en como se conectaban los periféricos a las computadoras.

USB como adaptador de red inalámbrica ofrece la ventaja de poder compartir el adaptador entre diferentes terminales según se necesite, si un equipo requiere la conexión inalámbrica sólo tiene que conectarse el adaptador e ir intercambiando de equipo conforme se requiera; sólo hay que asegurarse de que el otro extremo del cable USB esté conectado al adaptador de red.

Otra ventaja es que puede reorientarse con respecto al punto de acceso para buscar una mejor cobertura sin tener que mover el equipo. La diferencia con los otros adaptadores, es que son dispositivos externos al equipo.

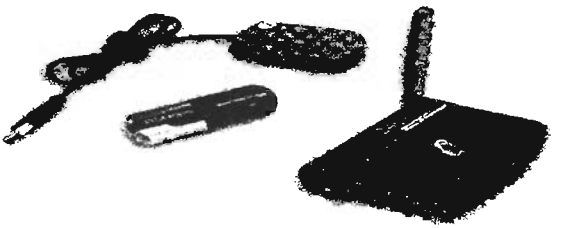


Figura 19. Adaptadores de red USB

Todos los tipos de adaptadores para su funcionamiento requieren de instalar un controlador de dispositivo.

IV.2.2 Puntos de acceso

El punto de acceso es el centro de las comunicaciones de la mayoría de las redes inalámbricas.

Existen dos categorías:

- Puntos de acceso profesionales, diseñados para crear redes corporativas de tamaño medio o grande; suelen ser más caros, pero incluyen mejoras en las características como la seguridad.

- Puntos de acceso económicos, dirigidos a cubrir las necesidades de los usuarios de pequeñas oficinas o del hogar. Ofrecen la misma cobertura y velocidad que los anteriores. La diferencia se basa en el número de usuarios que soportan y que son más baratos.

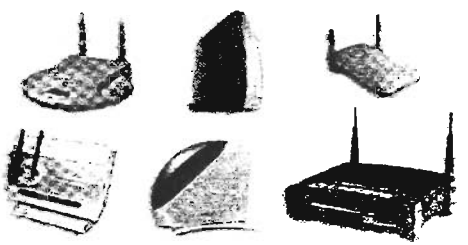


Figura 20. Distintos modelos de puntos de acceso

Algo que diferencia a los puntos de acceso es el número y tipo de puertos exteriores que ofrece. Una característica en comparación con los adaptadores de red es que entre puntos de acceso existe incompatibilidad cuando son de diversos fabricantes.

Los puntos de acceso son cajas pequeñas de las que sobresalen una o dos antenas y constan de:

◊ Un equipo de radio (de 2.4 Ghz para 802.11b).
◊ Una o dos antenas.
◊ Un software de gestión de las comunicaciones.
◊ Puertos para conectar a Internet o a la red cableada.

En cuanto a los puertos, son por lo menos uno o más 10/100 Base T para la conexión a la red cableada y/o Internet, aunque dependiendo del modelo pueden contener los siguientes:

* Un puerto especial para conectarse a un hub o switch.

* Debido a que pueden disponer internamente de un hub pueden tener de dos a cuatro puertos para conectar las computadoras de red cableada.

* Un puerto serie RS-232 para conectar un módem de red telefónica.

* Un puerto paralelo o USB para conectar una impresora.

* Puerto para conectar una antena exterior, para tener un mayor alcance.

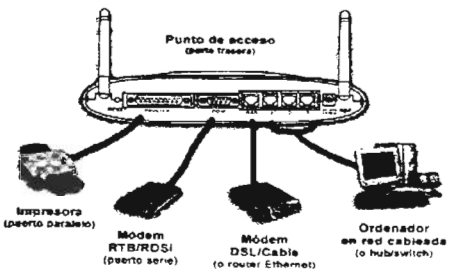


Figura 21. Puertos de un punto de acceso

Siempre hay que asegurase que el punto de acceso sea compatible con el sistema operativo con que cuente el usuario. Los adaptadores de red se deben configurar para funcionar con un punto de acceso.

Cada punto de acceso tiene un área de cobertura, es la zona dentro de la cual cualquier equipo se comunica con él y su tamaño depende de factores como:

♦ Localización del punto de acceso.
♦ Obstáculos entre la computadora y el punto de acceso.
♦ Interferencias radioeléctricas.
♦ Tipo de antenas utilizadas.

La colocación de los puntos de acceso depende a veces del lugar donde está el acceso a Internet o si es el caso donde esté la red cableada, aunque el lugar más propicio es el más alto posible y céntrico si es en una oficina o casa.

Siendo en un cuarto, oficina o al exterior existen cosas que afectan la propagación de la señal, por ello es necesario realizar un método llamado de prueba y error que consiste en una inspección previa, para decidir los lugares propicios para la localización y hacer pruebas de cobertura, sólo es necesario un punto de acceso y una computadora portátil para checar que la recepción sea la adecuada hasta encontrar la posición idónea.

Colocar tantos puntos de acceso como se requiera para que la cobertura sea total; cada uno tiene una cobertura entre los 30 y 400 metros dependiendo de las condiciones que se tenga, en espacios cerrados el alcance es menor, mientras que en espacio abierto es mayor.

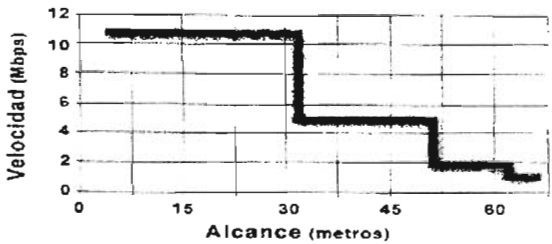


Figura 22. Gráfica velocidad x alcance de un punto de acceso en el interior de una oficina.

La potencia de transmisión varía entre los 100 miliWatts y 1 Watt, a más potencia es mayor el alcance. La velocidad para puntos de acceso basados en el estándar 802.11b es de 11 Mbps disponible para cada usuarios y utilizan la técnica DSSS.

En cuanto a la velocidad dependiendo de cuantos usuarios se tengan los 11 Mbps disminuirán para cada usuario, pero si se cuentan con dos o tres puntos de acceso, la velocidad aumentará a 22 ó 33 Mbps pero sólo para agilizar el manejo de la información por los puntos de acceso, las computadoras sólo podrán enviar y recibir la información a 11 Mbps.

Cuando se requiere instalar varios puntos de acceso se deben formular varias preguntas.

- Con cuántos usuarios va a contar la red.
- Qué área se pretende cubrir.
- Qué inconvenientes puede presentar el entorno.
- Qué posibles fuentes de interferencias existen.
- Cuál será la concentración de usuarios (en una misma zona).
- Qué equipamiento será necesario.
- La localización de los puntos de acceso.

- La selección de canales.
- Qué nivel de seguridad se necesitará.
- Cómo se interconectará la red inalámbrica a Internet y a la red cableada (si existe).
- Se necesitará expandir la red a futuro.
- Quién administrará la red.

IV.2.3 Bridges

Un bridge o puente es un dispositivo que sirve para interconectar dos redes. Un bridge inalámbrico interconecta dos redes remotas (cableadas o no) mediante una conexión inalámbrica. No son muy utilizados en redes inalámbricas debido a que los puntos de acceso hacen su función al conectar las redes inalámbricas con las cableadas.

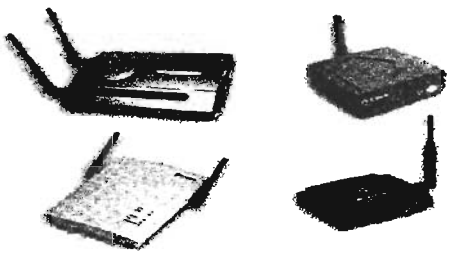


Figura 23. Equipos bridge

Los bridges inalámbricos pueden servir para extender el área de cobertura sobre todo cuando no se tiene una visibilidad directa para colocar una antena. La comunicación se realiza con un bridge en cada extremo.

IV.2.4 Antenas

Una antena es un dispositivo destinado a la radiación y/o captación de ondas radioeléctricas. La antena emisora radia las ondas y la antena receptora las capta, un mismo equipo de radio, y su antena, puede transmitir y recibir información; reciben el nombre de transceiver.

Algunas características con que cuenta una antena son:

Ganancia.- Es el grado de amplificación de la señal. Está es una característica que tienen las antenas de todos los dispositivos que intervienen en una red inalámbrica. Las antenas de los puntos de acceso tienen una ganancia mayor en comparación con las de los adaptadores de red. Se mide en decibelios (dB).

Patrón de radiación.- El patrón de radiación es un gráfico o diagrama polar sobre el que se representa la fuerza de los campos electromagnéticos radiados por una antena. La forma depende del modelo de la antena. Un tipo de antenas llamadas omnidireccionales

emiten en todas direcciones y tienen menor alcance que las antenas direccionales. Los modelos de antenas comerciales publican sus patrones de radiación entre sus características; se representa en dos planos perpendiculares conocidos como azimut y elevación.

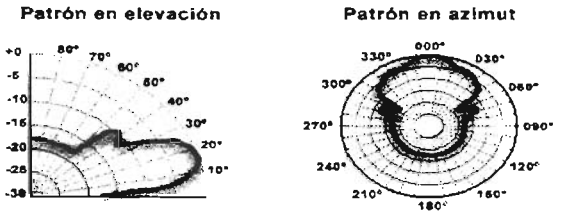


Figura 24. Patrón de radiación de una antena

Polarización.- Describe la orientación de los campos magnéticos que irradia o recibe la antena. Las formas más comunes son:

- Vertical. Cuando el campo electromagnético generado es vertical con respecto al horizonte terrestre (de arriba a abajo).
- Horizontal. Cuando el campo es paralelo al horizonte terrestre.
- Circular. Cuando el campo rota de vertical a horizontal y viceversa, creando movimientos circulares en todas direcciones.
- Elíptica. Cuando el campo se mueve como en la polarización circular pero con diferente fuerza en las distintas direcciones.

La polarización de ambas antenas en la comunicación debe ser la misma para que haya menos pérdida de ganancia.

Pérdida de propagación.- Es la cantidad de señal necesaria para llegar de un extremo a otro de la transmisión, es decir, es la cantidad de señal que se pierde al atravesar un espacio. Su valor se mide en decibelios (dB).

Tipos de antenas

Todos los tipos de antenas pueden agruparse en dos tipos: omnidireccional y direccional.

Las antenas omnidireccionales son aquellas que radian en todas direcciones y pueden captar la señal procedente de todas las direcciones. Son mejores para utilizarse en interiores.

Las antenas direccionales concentran su radiación en una dirección y sólo pueden captar la señal procedente de esa dirección. Se suelen utilizar en el exterior, tienen mayor alcance y ganancia que las omnidireccionales.

Las antenas más comunes son:

® Antena yagui. Es una antena direccional, suelen venir montadas en el interior de una cobertura cilíndrica.

® Antena de panel tipo patch (parche). Es una antena plana para ser montada en la pared. Aunque su mayor inconveniente es ser plana porque puede sufrir por la fuerza del viento si se sitúan en el exterior.

® Antena parabólica. Tienen forma de disco cóncavo con la que se consigue haces direccionales.

® Antenas omnidireccionales. Cuentan con las características antes mencionadas.

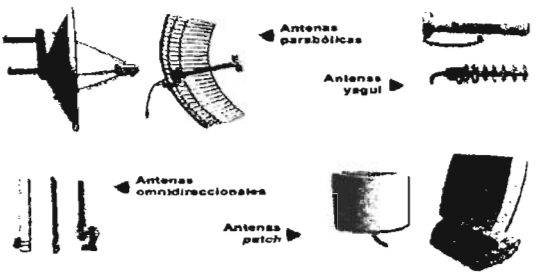


Figura 25. Diferentes tipos de antenas

A continuación se muestra como propagan la señal las antenas mencionadas anteriormente.

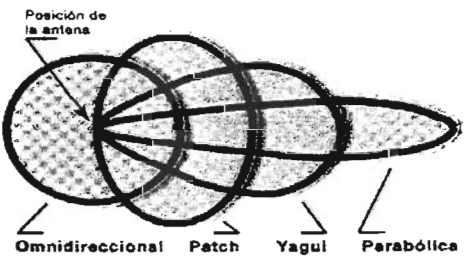


Figura 26. Propagación de la señal en distintas antenas

IV.2.4.1 Cable

Las antenas externas se conectan a los equipos mediante un cable, el cual es de tipo coaxial. Mientras más corto sea menor pérdida habrá.

Para comprar el cable, hay que asegurarse que sea óptimo para la frecuencia de 2.4 Ghz y también dependiendo del tipo de cable varía la pérdida que puede presentarse.

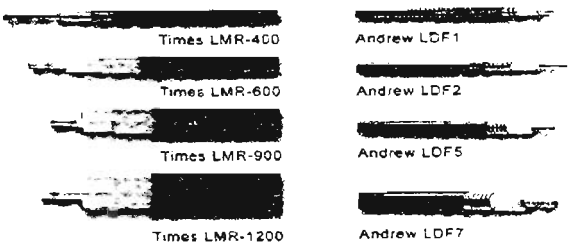


Figura 27. Ejemplos de cables

Tipo de cable	Pérdida 802.11b (2.4Ghz) dB/100m	Pérdida 802.11a (5.3 Ghz) dB/100m
LMR-200	54.2	82.4
LMR-240	41.5	63.6
LMR-400	21.7	33.7
LMR-600	14.2	22.6
LMR-900	9.58	15.1
LMR-1200	7.27	11.7
LMR- 1700	5.51	
3/8" LDF	19.4	26.6
1/2" LDF	12.8	21.6
7/8" LDF	7.5	12.5
1 1/4" LDF	5.6	9.2
1 5/8" LDF	4.6	8.2
RG-58	105.6	169.2
RG-8X	75.8	134.2
RG-213/214	49.9	93.8
9913	25.3	45.3

Pérdidas en distintos tipos de cables

El cable tiene soldado un conector en cada extremo y es recomendable comprarlo completo con sus conectores ya puestos.

IV.2.4.2 Conectores

Para conectar el cable a la antena y a los dispositivos se utilizan conectores. Tanto la antena como los dispositivos disponen de un conector donde se deben enchufar sus correspondientes del cable. Para hacer esto existen conectores conocidos como tipo macho y tipo hembra. Sólo los que son de distinto tipo pueden conectarse entre sí.

Los tipos de conectores más comunes son:

O N (marina). Es el conector más habitual para antenas de 2.4 Ghz, es tipo rosca.

O BNC (conector tipo bayoneta de la marina). Es un conector barato utilizado para redes cableadas, es muy común pero poco apto para trabajar en la frecuencia de 2.4 Ghz.

O TNC (conector BNC enroscado). Es una versión roscada del conector BNC. Es apto para frecuencias de hasta 12 Ghz.

O SMA (conector subminiatura). Son conectores muy pequeños, van roscados y trabajan con frecuencias de hasta 18 Ghz.

O SMC. Es una versión más pequeña que los tipos SMA. Son aptos para frecuencias de hasta 10 Ghz. Su mayor inconveniente es que tienen alta pérdida.

O APC-7 (conector Amphenol de precisión). Es un conector con muy poca pérdida y muy caro. Tiene la particularidad de que no tiene tipo macho ni hembra.

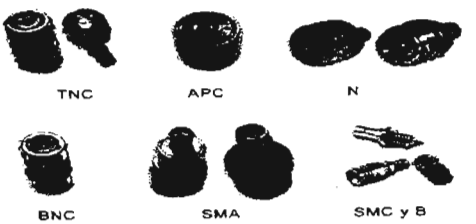


Figura 28. Tipos de conectores

Tanto el cable como el conector añaden pérdidas a la señal. Para evitar que haya mayores pérdidas hay que procurar usar un cable lo más corto posible y el número de conectores imprescindibles.

IV.2.4.3 Pigtail

Los adaptadores de red no disponen de un conector tipo N, esto quiere decir que no se puede conectar directamente el cable de la antena al equipo. Por tanto, para permitir la conexión es imprescindible conseguir un adaptador (pigtail) del conector tipo N al del tipo del equipo.

También se pueden fabricar, pero se debe tener presente que puede dañar al equipo.

Figura 29. Pigtail comercial (arriba) y fabricado (abajo)

IV.3 Proceso de configuración

Al pensar en instalar una red inalámbrica, además de que tipo de dispositivos se va a requerir, se tiene que tener en cuenta una serie de puntos con los cuales se hace que exista una comunicación eficiente, ya que cada elemento de la red debe tener ciertos parámetros configurados como:

φ Tipo de red. Primero se debe conocer que red se va a necesitar.

φ Nombre de red. Elegir un nombre para la red, ya que todos los componentes deben tener configurado el mismo. Una medida importante es que los puntos de acceso ya tienen un nombre configurado por defecto, así que hay que cambiárselo.

φ Seguridad. Todos los equipos deben tener configurado el cifrado WEP como medida mínima de seguridad y se puede elegir otras, las cuales se nombraron anteriormente en el capitulo anterior. Siempre teniendo en cuenta que en cada dispositivo que forme parte de la red deben estar configurados los mismos mecanismos de seguridad.

φ Canal. Los equipos con el estándar 802.11b disponen de 11 canales de 11 Mbps cada uno. Para los adaptadores de red no es necesario configurar el canal ya que lo tomará automáticamente del punto de acceso con el que este asociado. Los puntos de acceso ya vienen con un canal configurado, pero puede ser cambiado.

Si hay varios puntos de acceso en la red hay que tener configurado diferente canal para cada uno y con distancia entre ellos, es decir, canales salteados. Recordando que sólo pueden existir tres puntos de acceso en una zona, ya que a cada canal corresponde una frecuencia determinada es conveniente una separación de 25 Mhz entre cada uno, de lo contrario pueden existir interferencias.

CANAL	Frecuencia (Mhz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462

Cada punto debe ser el mismo en cada equipo de la red, por lo tanto para incorporar un equipo sólo se deben copiar para que tenga acceso.

Otra característica en los puntos de acceso que se debe considerar es la capacidad en cuanto a usuarios, ya que dependiendo de la marca varía; por lo tanto se tratará este

punto más adelante, ya que para la decisión de que puntos de acceso son más convenientes para la red se necesitan conocer varios aspectos.

IV.4 Características del diseño para una red inalámbrica

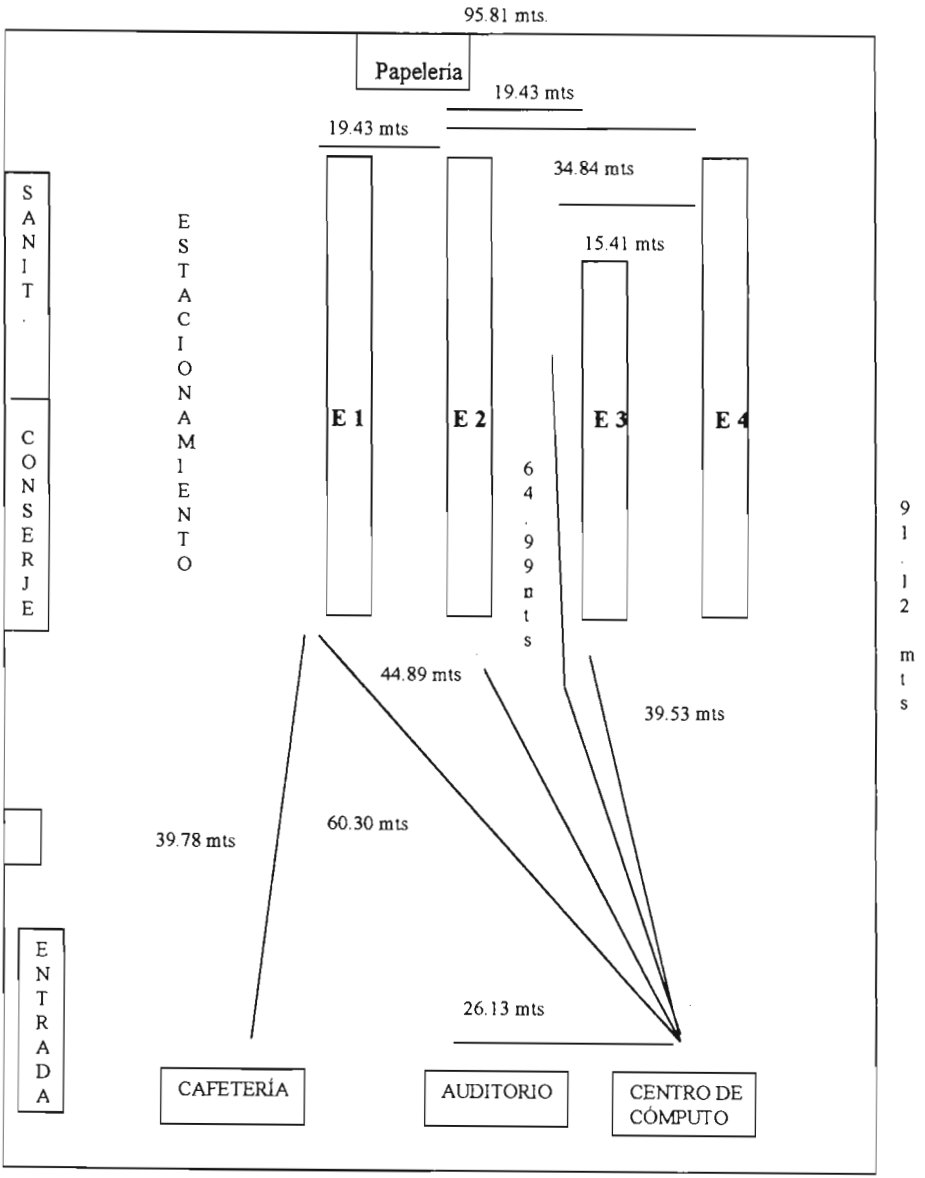
Para realizar un buen diseño hay que hacer un análisis previamente, definiendo las necesidades, analizar el terreno y estudiar los posibles inconvenientes. Para ello es necesario considerar los siguientes pasos:

1. Determinar las necesidades, dentro del cual hay que conocer lo siguiente:

◈ Características del recinto.- Es necesario hacer un reconocimiento físico del área. Es por ello que se presenta un plano del lugar y un listado de las características de la Escuela Normal No. 4 de Ciudad Nezahualcóyotl en donde se realiza la propuesta.

Medidas de los edificios		
Edificios	Dimensiones (m)	Altura (m)
E 1	36.18 x 8.71	6.08
E2	36.85 x 8.71	6.08
E3	29.48 x 8.71	3.07
E4	37.52 x 9.38	3.95
Centro de cómputo	12.73 x 8.71	3.06
Auditorio	10.72 x 4.02	3.10
Papelería	5.36 x 2.68	2.66
Área total de la escuela 95.81 x 91.12 = 8730.2072 m^2		

PLANO DE LA ESCUELA NORMAL No. 4 DE CIUDAD NEZAHUALCÓYOTL



◈ Número de usuarios.- El total de usuarios contando alumnos de ambos turnos (matutino y vespertino), personal administrativo y profesores hay 850 personas.

◈ Prestaciones necesarias de la red.- Para conocer cuales son las prestaciones que requieren los usuarios, se hizo un sondeo, en donde se realizaron las siguientes preguntas a algunos alumnos, profesores y personal administrativo.

→ ¿Qué tipo de servicios requieren para su trabajo y/o desempeño académico dentro de la Escuela?

→ ¿Cree necesario contar con servicio de impresiones?

→ ¿Necesita facilidad para intercambiar archivos entre diferentes áreas de la Escuela?

→ ¿Qué tipo de servicios de Internet requiere?

En donde se concluyó que lo que desean es contar con servicios de Internet como: correo electrónico, buscadores, consulta de horarios de clases, calificaciones e inscripciones. Para el personal administrativo y profesores además de lo anterior requieren el servicio de impresiones e intercambio de archivos.

Lo cual va a variar de acuerdo al administrador de la red, al igual que el manejo del acceso a los servicios de Internet.

◈ Integración e interoperatividad con otras redes.- Dentro de la Escuela se encontró con una red cableada perteneciente al centro de cómputo, es por esta razón que se ha inclinado a utilizar dispositivos que sean compatibles con dichas redes. Debido a que para la propuesta de red inalámbrica se tiene contemplado tener un servidor, se tomará el que se encuentra dentro del centro de cómputo para ocuparlo, ya que es el que está actualmente en uso como tal.

2. Conocer cuales son las áreas a cubrir y en donde es necesario asegurar la comunicación.

- Áreas al aire libre (explanada).
- Centro de cómputo.
- Auditorio.
- Edificios 1, 2, 3.

De acuerdo a las medidas del lugar y las áreas que hay que cubrir se va a necesitar:

- Dos puntos de acceso con las siguientes características. (ya que para dar soporte a todos los usuarios con uno no basta).

× Distancias de cobertura de 100 metros mínimo.
× Que soporte 200 usuarios cada uno.
× Compatibilidad con redes cableadas.

- Tarjetas de red inalámbricas (PCMCIA para portátiles y USB para computadoras de escritorio), una por cada usuario.

- Cable coaxial de baja pérdida para interconectar los puntos de acceso a la red cableada.

3. Hay que tomar en cuenta que existe una fuente de interferencia en el comedor, un horno de microondas, el cual sólo es usado en ciertas ocasiones.

IV.4.1 Integración

Una vez que se han analizado las características y necesidades de la institución y los usuarios, el siguiente paso es hacer un estudio de donde es conveniente colocar los puntos de acceso para garantizar el servicio.

Lo primero es conocer en que lugar ubicar cada punto de acceso de acuerdo a la concurrencia de usuarios y la distancia a cubrir.

Para el primer punto de acceso se considera conveniente colocarlo en el centro de cómputo de la Escuela para hacer la conexión con la red cableada y ya que la concurrencia de usuarios es de entre 150 y 250 con un sólo dispositivo bastará para cubrir toda el área.

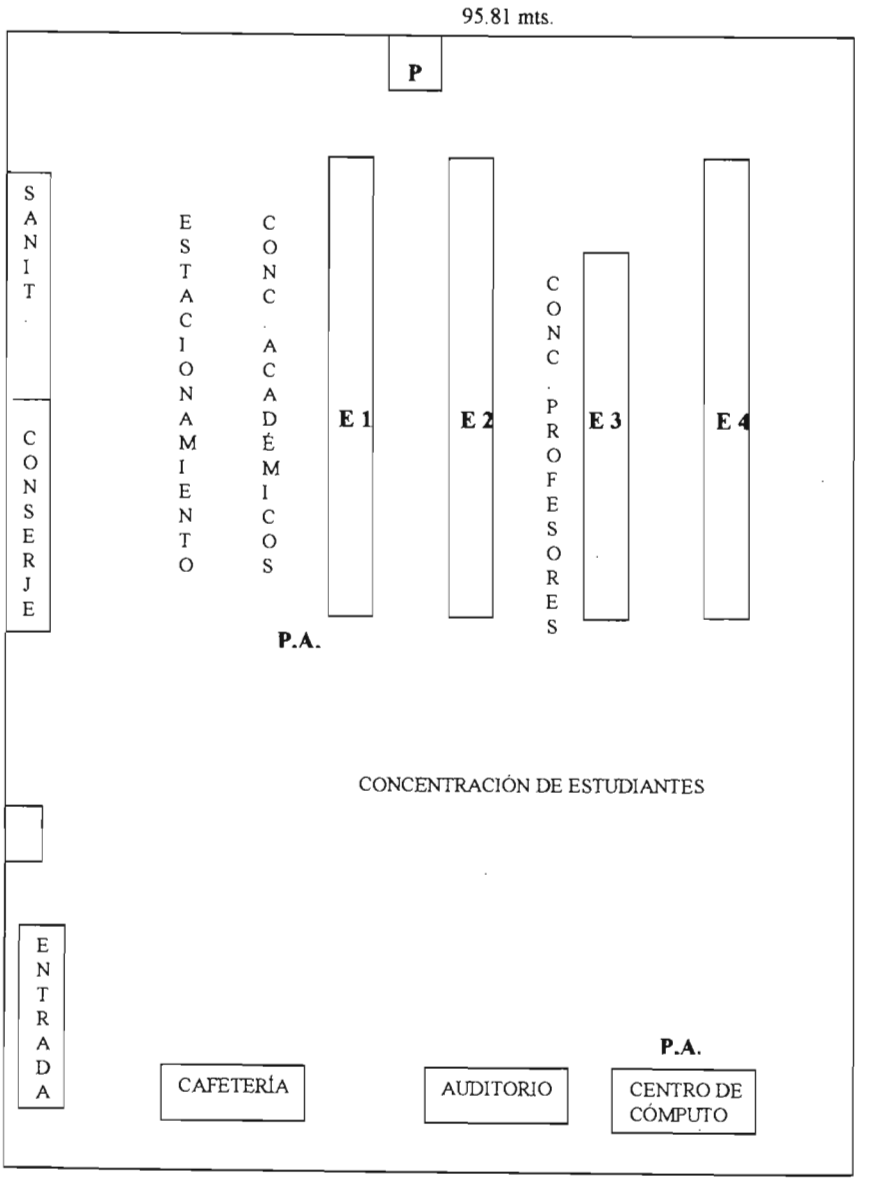
Otro punto de acceso será colocado en el edificio 1 ya que la distancia más larga se encuentra entre esté lugar y el otro punto de acceso. En el lugar hay una cantidad de usuarios que oscila entre 200 y 250; así se obtendrá una cobertura total.

Esta contemplación se hizo basándose en pruebas realizadas para la conexión, colocando cada punto de acceso en diferentes lugares y probando que hay comunicación. Como se mencionó antes el horno de microondas provoca interferencias pero son mínimas. Otra característica que se tomó en cuenta es la infraestructura de los edificios y no existe ningún inconveniente ya que la señal llega en cualquier dirección.

Como sólo se consideró colocar dos puntos de acceso, se puede disponer, si lo requiere de agregar uno más, ya que de esta forma habrá mayor cobertura, pero no excederá el máximo de tres puntos de acceso en una misma zona, y así agilizar la comunicación entre usuarios y soportar un mayor número de éstos.

A continuación se presenta un plano con la implementación de los equipos y los lugares donde existe mayor concurrencia de usuarios.

PLANO CON LA IMPLEMENTACIÓN DE LOS EQUIPOS



Existen otras medidas que se deberán considerar a futuro las cuales son:

© Verificar periódicamente el número de usuarios, aplicaciones utilizadas, las zonas y áreas pico y ver la posibilidad de poner más puntos de acceso si lo requiere para garantizar la comunicación.

© Mantener un control sobre el número de usuarios que pueden tener acceso a la red.

© Coordinar y vigilar que se mantenga el equipo en buenas condiciones.

Una vez que se analiza el lugar físico en donde se va a realizar la instalación, el siguiente paso a seguir es:

~ La configuración de los dispositivos.

~ La colocación.

~ La administración.

En el capítulo siguiente se realizan dichos procesos.

CAPÍTULO 5
PROPUESTA

V.1 Introducción

Existen varios puntos que cabe recordar y tomar en cuenta:

Las redes inalámbricas no requieren permiso de la COFETEL, por lo tanto no necesitan de algún tipo de licencia y eso acorta el tiempo de instalación.

El tipo de configuración que se va a utilizar es el conocido como infraestructura por las características a que se hicieron referencia en el capítulo anterior.

El método de acceso al medio (reglas que van a decir si se puede o no acceder a la red), que utiliza las redes inalámbricas es CSMA/CA[6].

El sistema operativo en los equipos es Windows en diferentes versiones 95/98, XP,2000.

Pero la propuesta sólo se basa en la parte inalámbrica, se hará uso de algunos equipos que se encuentran en la escuela para sintetizar el proceso de instalación y bajar costos.

La conexión de una red inalámbrica con Internet se lleva a cabo a través de un router y se comparte a la red inalámbrica por medio de los puntos de acceso.

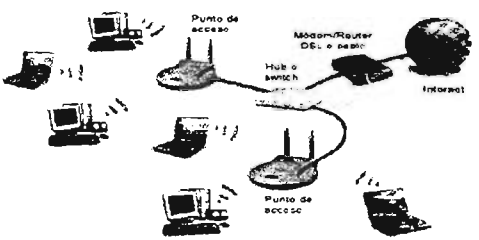


Figura 30. Conexión a Internet.

Existen diferentes modelos de puntos de acceso con diversas características, sin embargo es recomendable tener en cuenta las siguientes:

Disponer de un puerto 10/100 Base T por donde conectar un hub o switch de la red cableada que ya está conectada a Internet.

Un puerto RS-232 para conectar un módem vía telefónica, para que pueda ser utilizado como un acceso secundario a Internet, en caso de falla del acceso principal o

[6] Ver anexo "CSMA/CA".

disponer de un módem interno para línea telefónica, al cual sólo haya que conectarle el cable de la línea.

V.1.1 Direcciones IP

Dentro de los equipos para la red inalámbrica y cableada existe un parámetro que se debe configurar y para ello es necesario conocer algunas características.

Las direcciones IP son las direcciones que van a identificar a cada uno de los equipos en una red para las comunicaciones. Constan de cuatro cifras separadas por un punto, cada cifra está representada por 8 bits, por lo tanto el valor más alto que pueden tener cualquiera de las cifras es 255, es decir, existen 256 valores distintos (del 0 al 255).

Cada equipo que forme parte de una red debe disponer de una dirección IP, está es asignada por el usuario o administrador; los números que pueden asignarse se encuentran entre estos rangos, (ya que sólo los que estén dentro pueden ser compatibles con Internet):

De la 10.0.0.0 a la 10.255.255.255
De la 172.16.0.0 a la 172.31.255.255
De la 192.168.0.0 a la 192.168.255.255

Deben estar contenidos en cada uno de los equipos sin repetirse y todos dentro de un mismo rango.

La red inalámbrica que se propone se encuentra dentro del último rango.

Para la comunicación con Internet, se debe colocar en el router una dirección contenida dentro del rango de la red y otra dirección IP que lo identifique en Internet.

V.1.2 Máscara de subred

La máscara de subred es una forma de poder definir e identificar subredes dentro de una red mayor. Su valor lo tiene que definir y configurar el usuario o administrador.

Una dirección IP se descompone en dos partes: una identifica a la red, la otra al equipo dentro de esa red.

Para que sea más rápidamente la comunicación entre equipos hay que ahorrar tiempo, es ahí donde se encuentra la función de la máscara de subred, dependiendo de cuantas cifras de los cuatro valores de la dirección IP representan la red, el valor en la máscara será 255; para la que represente al equipo será un 0, cuando se tengan 256 equipos bastará con la última cifra, pero si se tienen más, entonces la penúltima cifra también debe ser 0.

Dirección IP	121.235.44.178		172.16.44.175		192.168.100.75	
	red	equipo	red	equipo	red	equipo
Máscara de subred	255.0.0.0		255.255.0.0		255.255.255.0	

La máscara de subred que se utilizó en está propuesta es 255.255.255.0 .Con esto se conseguirá que sólo sea necesario analizar la cifra destinada al equipo.

V.2 Elección de productos

Mediante una comparación de equipos[*] con el estándar 802.11b se decidió utilizar un tipo de puntos de acceso y adaptadores de red de la marca D-Link modelo DWL-900+ por sus características y costo.

- Tienen una cobertura de 100 metros en interiores y 400 metros en exteriores y soporta 180 usuarios.
- Configuración por CD de controladores o mediante la página en Internet del fabricante.
- Trabaja a una velocidad de 11 Mbps.
- Puede trabajar como punto de acceso, router o bridge según se configure.
- En cuanto a seguridad contiene el cifrado WEP de 128 bits, filtrado de direcciones MAC, filtrado de direcciones IP, desactivación de SSID.

Para evitar problemas de compatibilidad todo el equipo será de una misma marca.

En cuanto al costo de todos los dispositivos necesarios, son los siguientes:

1 Punto de Acceso	$ 1,058.05 pesos
1 Adaptador de red PCI	$ 416.81 pesos
1 Adaptador de red USB	$ 529.03 pesos
1 Adaptador de red PCMCIA	$ 363.60 pesos
1 cable UTP nivel 5	$ 81 pesos

*Los precios varían en el momento de compra de acuerdo al tipo de cambio.

V.3 Configuración de los Puntos de Acceso

Antes de colocar los puntos de acceso hay que configurarlos. La mayoría de los fabricantes ya incluyen una en sus equipos, pero es mejor cambiar estos valores por seguridad.

[*] Ver anexo "Comparación de características y precios en dispositivos inalámbricos".

Los pasos para la configuración son los siguientes:

Establecer una conexión entre un equipo y el punto de acceso; se puede llevar a cabo de dos formas: vía inalámbrica configurando un adaptador de red; vía cable conectando un cable UTP del equipo al punto de acceso.

Para simplificar el proceso se conecta el servidor del centro de cómputo con el punto de acceso mediante el cable UTP para su configuración. Se encuentra habilitado el servidor DHCP, por lo tanto no es necesario realizar ninguna otra configuración para tener comunicación con el punto de acceso.

Se abre el navegador de Internet para accesar al servidor web del fabricante y realizar la configuración con el software más reciente, poniendo la dirección http://192.168.0.50 que es la dirección IP del punto de acceso proporcionado por el fabricante en el manual de usuario.

Cuando la página de configuración aparece inmediatamente pide el nombre de usuario y clave, el nombre de usuario se deja en blanco y como clave se coloca ***admin***, una vez dentro un asistente va a guiar la instalación.

Se introduce una clave de acceso o password para el punto de acceso, en este caso es *n4cnccagb*.

Seleccionar el nombre de red (SSID) que desee, el cual es *normneza*.

El tipo de red es infraestructura.

Por default el punto de acceso contiene el canal número 6, se deja intacto.

Se configura el punto de acceso en modo bridge ya que con ellos se unen dos partes en una sola red.

En cuanto a la seguridad se deja deshabilitada en la primera configuración de los puntos de acceso, ya que se habilita cuando se haya probado que la red funciona.

Para tener comunicación con el router se hace lo siguiente:

Averiguar la dirección IP del router : 192.168.1.100

Dentro de la página de configuración del punto de acceso se pulsa el botón LAN, enseguida pide la dirección IP en el recuadro IP Adress del punto de acceso para tener comunicación con el router debe ser del mismo rango, es aquí donde se cambia la dirección del punto de acceso, ya que no se deja en modo automático para obtenerlas. La nueva dirección es 192.168.1.81

En el siguiente recuadro se pone la máscara de subred, 255.255.255.0.

En el recuadro Puerta de enlace se introduce la dirección IP al que el punto de acceso tiene que enviar los datos con destino a Internet, por lo tanto es la dirección del router 192.168.1.100

A continuación aparece el recuadro de la dirección IP del servidor DNS, que es facilitada por el ISP; en DNS primario es 200.33.146.193 y en DNS secundario 200.33.146.201

Para que no sea necesario dar de alta a cada usuario en el punto de acceso por dirección IP, es necesario utilizar el modo DHCP con el cual se hace posible que la configuración de los adaptadores de red se actualice de forma automática al momento de encender la computadora.

Primero se pulsa sobre el botón DHCP y se habilita el servidor DHCP; en Starting IP Adress se pone 192.168.1.105 que es la dirección IP menor que dicho servidor puede otorgar a un usuario; en Ending IP Adress se coloca 192.168.1.254, siendo la dirección mayor que puede tener un usuario; el Lease time en 1 hora, después se pulsa en aplicar y el equipo se reinicia.

Al finalizar, está listo para ser colocado. El punto de acceso número dos se configura de la misma forma sólo se debe cambiar la dirección IP del punto de acceso dentro del mismo rango que la del router para que tengan comunicación, en este caso es 192.168.1.88, se cambia el canal a 11 para evitar alguna interferencia entre ambos equipos y se procede a su colocación.

V.4 Conexión de los puntos de acceso

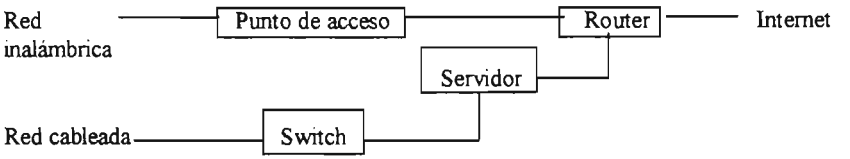
El primer punto de acceso se coloca en el centro de cómputo ya que ahí se encuentra el router y un servidor con las siguientes características:

Procesador Pentium IV
Disco duro de 40 Gb
Memoria RAM de 256 Mb
Tarjeta de red PCI 100
Sistema Operativo Windows XP
Cable de red tipo UTP nivel 5

Se utiliza ésta máquina ya que para disminuir costos es preferible hacer uso del equipo que ya se encuentra en operación dentro de la Escuela.

Un punto importante es que dicho servidor se encuentra conectado al router para proporcionar acceso a Internet en la red cableada, pero el punto de acceso se conecta directamente al router.

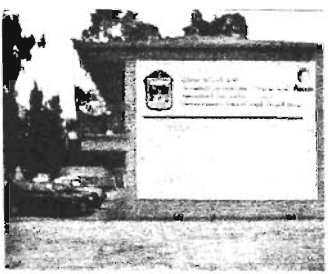
En el diagrama siguiente se muestra como está planeada la conexión.

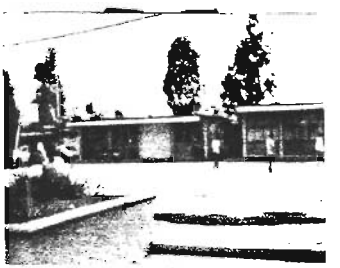


El segundo punto de acceso se coloca en el edificio 1 en donde se encuentra el área académico/administrativa de la escuela, que es donde está la información sobre inscripciones, calificaciones, horarios, periodo de exámenes, etc.

El punto de acceso queda conectado a un switch en donde están los demás equipos de esta área y cabe decir que la conexión se realiza en base a un cable UTP nivel 5. El lugar más propicio para colocar los puntos de acceso es en la parte alta de los edificios, para que la señal se propague mejor.

En las ilustraciones se observa el lugar donde se colocan los equipos.





Fotos de la Escuela Normal No. 4 de Ciudad Nezahualcóyotl.

Cabe aclarar que también podría conectarse cada punto de acceso a un switch en su respectivo lugar de conexión, pero para el primer punto, es preferible su conexión directa con el router por si existe algún problema con el servidor de la red cableada no afecte a la red inalámbrica.

Seguridad

Por último una vez que se comprueba que la red funciona, se habilita la seguridad, en WEP, se introduce una clave de 128 bits, en cada punto de acceso (con caracteres numéricos o alfabéticos). Se puede configurar hasta cuatro claves por seguridad, de las cuales sólo una esta activa y debe cambiarse periódicamente.

Contar con un antivirus instalado en todos los equipos, y actualizarlo constantemente.

Como otra opción de seguridad se dispone de un firewall instalado en cada equipo dentro de las instalaciones académicas para aumentar la seguridad.

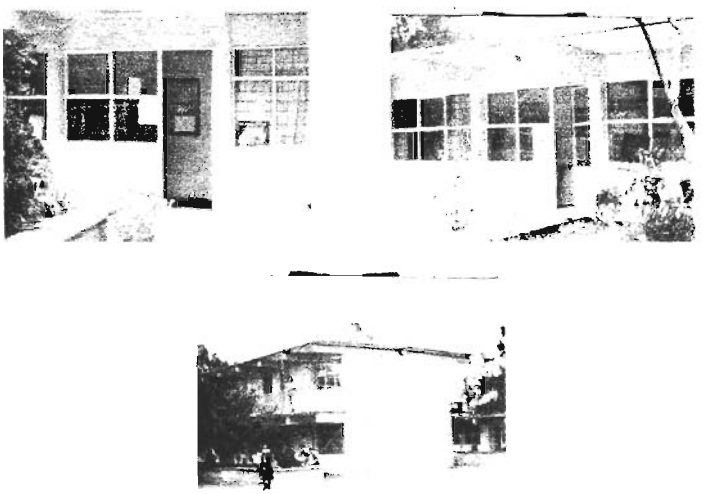
Se cambian las claves periódicamente como medida mínima de seguridad, además se deshabilita el nombre de red (SSID) para que no se esté transmitiendo.

Se tiene un listado de direcciones MAC de las tarjetas que se están en uso dentro de la Escuela y para préstamo a alumnos.

Como una medida extra de seguridad que en este caso no se ha implementado, se puede considerar el uso de WPA, instalándolo en todos los equipos que se encuentran dentro de las instalaciones, es decir, los que son propiedad de la Escuela.

V.5 Conexión de los Adaptadores de red

Se necesitan adaptadores de red PCMCIA para computadoras portátiles y USB para equipos de escritorio por la facilidad con que se conecta al equipo sin necesidad de abrirlo. Debido a que para las computadoras de escritorio ya se cuenta con una red cableada en el centro de cómputo y área administrativa/académica no será necesario cambiar su conexión. Para las demás computadoras de escritorio que se encuentran en otras áreas como la biblioteca y cubículos (que se encuentran en E2 y E3 respectivamente) si es necesario este tipo de adaptadores.



Imágenes de la biblioteca y cubículos.

Junto con los adaptadores de red se incluyen los controladores para realizar su configuración, en cada equipo debe realizarse.

V.6 Configuración de los adaptadores de red

Se comienza instalando los controladores. Dentro de la configuración hay que introducir los datos correspondientes.

Se piden los siguientes parámetros:

- Tipo de red: elegir el modo infraestructura.
- Nombre de red: normneza (como en los puntos de acceso).
- Seguridad: Deben ser los mismos que en el punto de acceso (habilitar el WEP).

Al haber habilitado el servidor DHCP en los puntos de acceso no hace falta configurar en cada computadora una dirección IP, ya que cada una la obtendrá automáticamente con sólo habilitar dicho modo.

V.6.1 Administración de cuentas

Antes de que los usuarios accedan a la red se debe restringir la entrada a los servicios que no se quieran compartir, esto se deja a cargo del administrador, será él quien decida a que recursos o máquinas se puede tener acceso.

Sólo es necesario colocar los datos de acceso a la red para cada usuario y con eso puede incorporarse.

Existen dos formas para que un usuario pueda acceder a la red inalámbrica:

- Cuando posee un adaptador de red, o pidiéndolo en préstamo.
- Después se configura y podrá disponer de los servicios.
- Por último termina su sesión y devuelve la tarjeta, si fue en préstamo.

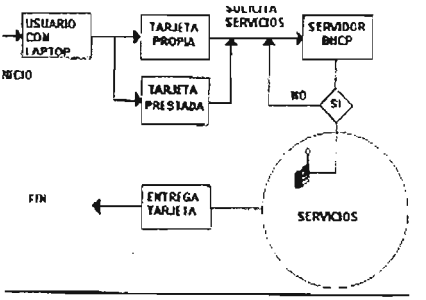


Figura 31.

V.7 Compartir recursos

Para compartir un recurso sólo se tiene que abrir el explorador; en el archivo, carpeta, impresora, etc., ir a la opción compartir, se debe especificar si se comparte en modo de sólo lectura, lectura y escritura, con clave, sin clave. (hecho por el administrador).

Puede ser que dependiendo de la versión de Windows que se tenga varie la forma de como compartir un archivo.

V.8 Comprobar la conexión

Es necesario hacer una comprobación de la conexión realizada para saber cuales equipos fueron debidamente configurados y corregir errores.

Para comprobar si existe una conexión lo que hay que hacer es abrir entorno de red y ver si hay equipos conectados.

Para acceder a algún recurso, archivo o carpeta hay que verificar si existe en el explorador, si está restringido con clave hay que introducirla.

V.8.1 Resolución de problemas

- Asegurarse que el equipo al que se pretende acceder está configurado.
- Comprobar que todos los dispositivos están encendidos, funcionando y bien conectados.
- Situar los equipos más cerca del punto de acceso evitando que haya obstáculos en medio. Una vez que se establece la conexión se pueden ir separando los equipos.
- Observar luces de los equipos para comprobar si están funcionando.
- Apagar y encender los equipos.
- Desconectar los equipos inalámbricos para que se reinicie la unidad.
- Comprobar que todos los parámetros como nombre de red, tipo de red, etc., sean los mismos.
- Comprobar que los sistemas de seguridad son los mismos y están configurados de la misma forma.
- Hacer cambio de adaptadores para ver si alguno tiene falla y cambiarlo.

V.9 Gestión de red

Existen algunas aplicaciones que permiten vigilar y gestionar la red, son implementadas con los adaptadores de red para que tengan información sobre la red a la que van a conectarse, por ejemplo la calidad de la señal, el estado de la conexión, etc.

Algunos puntos de acceso vienen con algún software que permite vigilar cuantos y cuales usuarios están activos. El punto de acceso que se ha utilizado en la propuesta, no contiene ningún software para está medida de seguridad, pero de considerarlo necesario dentro del plantel, se puede adquirir por separado.

ANEXOS

ANEXO 1. CAPAS WAP

Como se hizo referencia en el Capítulo II, el Protocolo de Aplicaciones Inalámbricas se divide en varias capas; a continuación se describen cada una de ellas.

Capa de aplicación (WAE).

Es un entorno de aplicación de propósito general basado en la combinación del Word Wide Web y tecnologías de comunicaciones móviles. Está enfocado principalmente sobre los aspectos del cliente de la arquitectura del sistema WAP, es decir, en los puntos relacionados con los agentes de usuario, ya que la parte más importante en la arquitectura es aquella que afecta principalmente a los equipos móviles.

Se divide en dos capas lógicas:

- Los agentes de usuario, que incluye aquellos elementos navegadores, agendas telefónicas, editores de mensajes, etc.
- Los servicios y formatos, que incluyen todos aquellos elementos y formatos comunes, accesibles a los agentes de usuario, tales como:

- El lenguaje denominado WML que es similar al HTML, pero optimizado para su uso en terminales móviles.
    - Un lenguaje denominado WMLScript, similar al JavaScript (un lenguaje para su uso en forma de Script).
    - Un conjunto de formatos de contenido, que son un conjunto de formatos de datos bien definidos entre los que se encuentran imágenes, entradas en la agenda de teléfonos e información de calendario.

Capa de sesión (WSP).

La capa de sesión se sitúa por debajo de la capa de Aplicación, proporcionando la capacidad necesaria para:

- Establecer una conexión fiable entre el cliente y el servidor, y liberar ésta conexión de una forma ordenada.
- Ponerse de acuerdo en un nivel común de funcionalidades del protocolo, a través de la negociación de las posibilidades.
- Intercambiar contenido entre el cliente y el servidor utilizando codificación compacta.
- Suspender y recuperar la sesión.

Capa de transacciones (WTP).

La capa de transacciones proporciona los servicios necesarios que soportan aplicaciones de "navegación" (del tipo petición/respuesta).

Sus características son:

Proporciona tres clases de servicios de transacción: clase 0: mensaje de solicitud no segura, sin mensaje de respuesta; clase 1: mensaje de solicitud segura, sin mensaje de respuesta; y clase 2: mensaje de solicitud segura, con un mensaje de respuesta segura.

La seguridad se consigue a través del uso de identificadores únicos de transacción, asentamientos, eliminación de duplicados y retransmisiones.

Seguridad opcional usuario a usuario.

El último asentamiento de la transacción puede contener algún tipo de información adicional relacionada con la transacción, como medidas de prestaciones, etc.

Se proporcionan mecanismos para minimizar el número de transacciones que se reenvía como resultado de paquetes duplicados.

Se permiten las transacciones asíncronas.

Capa de seguridad (WTLS).

La capa de seguridad constituye una capa modular, que depende del nivel de seguridad requerido por una determinada aplicación.

Tiene las siguientes características:

◊ Integridad de datos. Asegura que los datos intercambiados entre el equipo y el servidor de aplicaciones no hayan sido modificados y no sea información corrupta.

◊ Privacidad de los datos. Asegura que la información intercambiada entre el equipo y un servidor de aplicaciones no pueda ser entendida por terceras partes que puedan interceptar el flujo de datos.

◊ Autentificación. Contiene servicios para establecer la autenticidad del equipo y del servidor de aplicaciones.

El WTLS puede ser utilizado para la realización de comunicación segura entre equipos, por ejemplo, en el caso de operaciones de comercio electrónico entre equipos móviles.

Capa de transporte (WDP).

La capa de transporte es la encargada de proporcionar un servicio fiable a las capas superiores de WAP como:

- Direccionamiento por número de puerto.
- Segmentación.
- Detección de errores opcional.

ANEXO 2. COMPARACIÓN DE CARACTERÍSTICAS Y PRECIOS EN DISPOSITIVOS INALÁMBRICOS

Al verificar los dispositivos existentes en el mercado de las redes inalámbricas se encontraron diferentes características en cada uno, las cuales se enumeran en la siguiente tabla comparativa.

Puntos de acceso

Fabricantes	3COM	Linksys	Cisco	Siemens	Netgear
Modelo	AP8700	WAP11	Aironet 1200 Series Modelo empresarial	Speed Stream 2524	ME102
Precio	$12,121.97 pesos	$1,091.97 pesos	$15,430.97 pesos	$1,091.97 pesos	$981.67 pesos
Seguridad	WEP de 128 bits Desactivación de SSID Filtrado de direcciones MAC Soporta autentificación 802.1x y WPA	WEP de 128 bits Filtrado de direcciones MAC Desactivación de SSID	WEP de 128 bits Desactivación de SSID Filtrado de direcciones MAC Soporta autentificación 802.1x y RADIUS	WEP de 128 bits Desactivación de SSID Filtrado de direcciones MAC	WEP de 128 bits Desactivación de SSID Filtrado de direcciones MAC
Velocidad	Máx. 20.2 Mbps	Máx. 4.9 Mbps	Máx.13.6 Mbps	Máx. 3.8 Mbps	Máx. 4.4 Mbps
Configuración	Puede ser configurado por medio de un CD de controladores que contiene un asistente de instalación.	Dentro del controlador contiene una utilería que configura automáticamente	Puede ser configurado desde la página de Internet de la compañía, en donde se ofrece la versión más reciente	Se configura por medio de los controladores incluidos.	Su configuración se realiza por medio del CD de controladores incluido.
Distancia	100 mts. en interior 550 mts. en exterior	70 mts. en interior 200 mts en exterior	150 mts. en interior 550 mts. en exterior	50 mts. en interior 300 mts. en exterior	100 mts. en interior 350 mts en exterior
No. Usuarios	300	150	300	100	150

Adaptadores de red PCMCIA

Fabricantes	3COM	Linksys	Cisco	Siemens	Netgear
Precio	$1,091.97 pesos	$761.07 pesos	$2,194.97 pesos	$650.77 pesos	$981.67 pesos

* Los precios varían al momento de la compra dependiendo del tipo de cambio.

ANEXO 3. CSMA/CA

La capa de control de acceso al medio (MAC) que es la misma para todos los equipos de una red, define los procedimientos que hacen posible que los distintos dispositivos compartan el uso del espectro radioeléctrico. Utiliza el método de acceso conocido como Censo de Portadora con Múltiple Acceso/Evitación de Colisión (CSMA/CA), para la tecnología inalámbrica.

Una colisión se produce cuando dos equipos intentan hacer uso del medio físico simultáneamente. El método CA dispone de procedimientos para evitar que se produzcan colisiones.

Las colisiones pueden producirse porque dos equipos a la espera elijan el mismo número de intervalos para transmitir después de la emisión en curso. En este caso reintentan ampliando exponencialmente el rango de intervalos y vuelven a elegir. Infieren que se ha producido cuando no reciben el ACK esperado.

Ya que en el medio radioeléctrico un equipo no puede transmitir y recibir al mismo tiempo por el mismo canal (la transmisión dejaría opaca a la recepción), al no poder detectar las posibles colisiones, no hay más que disponer de una técnica que las evite.

Modo de trabajo.

CSMA/CA impone a un equipo que desee transmitir, que previamente escuche el medio para detectar si otro emisor está realizando esta función.

Si es así, esperará un tiempo aleatorio para sondear de nuevo el medio.

Cuando detecte que el medio está libre, emitirá una solicitud de ocupación que será escuchada por el sistema que gestione los permisos (el punto de acceso).

Si se concede el acceso, podrá realizar la emisión.

Al terminar espera a que el receptor le envíe una confirmación, si ésta no se produce dentro de un tiempo prefijado considera que se ha producido una colisión, en cuyo caso repite el proceso desde el principio.

ANEXO 4. ESTÁNDARES

Bluetooth

La tecnología Bluetooth es una especificación que describe un método de conectividad móvil universal con el cual se pueden interconectar teléfonos celulares, computadoras y muchos otros dispositivos portátiles, utilizando una conexión inalámbrica de corto alcance.

Bluetooth utiliza la técnica FHSS en la banda de frecuencias de 2.4 Ghz. Puede establecer comunicaciones asimétricas donde la velocidad máxima en una dirección es de 721 Kbps y 57.6 Kbps en la otra o comunicaciones simétricas de 432.6 Kbps en ambas direcciones; puede transmitir voz y datos.

La versión 1.1 permite la comunicación a 721 Kbps, mientras la versión 1.2 consigue hasta los 10 Mbps y la versión 2.0 tiene una velocidad de 12 Mbps.

Las medidas de seguridad que incorpora son una dirección única y pública (una dirección IEEE de 48 bits) para cada usuario, dos llaves secretas y un número aleatorio nuevo para cada transacción. La cobertura que ofrece este tipo de dispositivos es de sólo 10 metros.

Frecuencia de longitud de onda	2.4 Ghz (2.400 - 2.4835)
Velocidad máxima	v1.1 721 Kbps, v1.2 10 Mbps, v2.0 12 Mbps
Medidas de seguridad	Dirección pública única para cada usuario, dos llaves secretas y un número aleatorio diferente para cada nueva transacción.
Rango de operación óptima	10 metros
Adaptado para un propósito específico o tipo de dispositivo	Teléfonos inalámbricos, PDA's, Computadoras portátiles.
Interfase de aire	FHSS

Tabla. Características de Bluetooth

HomeRF

HomeRF utiliza la técnica FHSS y trabaja en la banda de frecuencias de los 2.4 Ghz.

La velocidad máxima de HomeRF es 10 Mbps, ideal para las aplicaciones caseras, aunque se manejan otras velocidades de 5, 1.6 y 0.8 Mbps. HomeRF ofrece seguridad, los dispositivos consumen menos potencia que los productos de otras tecnologías, además de permitir aplicaciones para telefonía y video.

Frecuencia longitud de onda	2.4 Ghz
Velocidad máxima	10 Mbps, 5 Mbps, 1.6 Mbps, 0.8 Mbps
Medidas de seguridad	Cifrado de 128 bits, saltos en frecuencia, identificadores de red de 48 bits
Rango de operación óptima	Cubre el entorno de casa
Adaptado para un propósito específico o para un tipo de dispositivo	Computadoras portátiles, gateways, módems de cable con gateways inalámbricos empotrados
Interfase de aire	FHSS

Tabla. Características de HomeRF

DECT

Trabaja en la banda de frecuencias de 1.9 Ghz y utiliza la técnica TDMA. La velocidad máxima actual a la que trabaja DECT es de 2 Mbps, aunque a futuro puede ampliarse hasta 20 Mbps.

Frecuencia longitud de onda	1.9 Ghz
Velocidad máxima	2 Mbps hasta 20 Mbps a futuro
Rango de operación óptima	Hasta 17 kilómetros con la velocidad de 20 Mbps
Adaptado para un propósito específico o para un tipo de dispositivo	Teléfonos inalámbricos
Interfase de aire	TDMA

Tabla. Características de DECT

HiperLAN

HiperLAN trabaja en la banda de frecuencias de 5 Ghz y alcanza velocidades de hasta 24 Mbps.

HiperLAN/2 ofrece velocidades de transmisión de 54 Mbps utilizando el sistema OFDM y también ofrece soporte QoS. Las frecuencias utilizadas son de 5.25 a 5.35 Ghz para sistemas de interior a 200 miliWatts de potencia y de 5.47 a 5.725 Ghz para sistemas de exterior a 1000 miliWatts de potencia.

Hay dos tipos de conexiones, punto a punto y punto a multipunto. Las conexiones punto a punto son bidireccionales, mientras que las conexiones punto a multipunto son unidireccionales y siempre en el sentido hacia la terminal móvil.

Frecuencia longitud de onda	5 Ghz (5.15 – 5.3 Ghz)
Velocidad máxima	6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 27 Mbps, 36 Mbps, 54 Mbps
Medidas de seguridad	Un esquema de cifrado-descifrado de uso opcional
Rango de operación óptima	Máximo 150 metros
Adaptado para un propósito específico o para un tipo de dispositivo	Vídeo y comunicaciones de Internet
Interfase de aire	OFDM

Tabla Características de HiperLAN

ANEXO 5. MODELO OSI

La Organización Internacional de Normalización (ISO) creó un modelo de referencia que permite estructurar las comunicaciones en siete capas, llamado modelo OSI (Interconexión de Sistemas Abiertos).

Cada capa se encarga de realizar una tarea distinta y perfectamente coordinada con el resto de las capas, no hay comunicación entre ellas, sólo se pasan los datos. La capa sólo sabe recibir información, hacer su trabajo dependiendo de cada una y pasarlos a la siguiente.

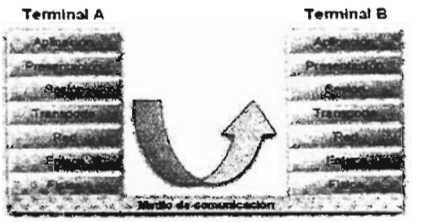


Figura 32.

Las capas del Modelo OSI son:

Capa física. Esta capa define las propiedades físicas de los componentes y de todos los medios físicos de la red (frecuencias de radio utilizadas, cómo se transmiten las señales, etc.)

Capa de enlace. Esta capa define como se organizan los datos que se transmiten, como se forman los grupos de datos (paquetes, tramas, etc.) y como se asegura que los datos llegan al destino sin errores.

Capa de red. Esta capa se encarga de ver por cual camino va la información y decidir la ruta más conveniente para pasar la información, también organiza las cosas para que distintas comunicaciones puedan hacer uso de la red.

Capa de transporte. Esta capa define las características de la entrega de los datos sin tener daño o alteraciones.

Capa de sesión. Esta capa establece la comunicación entre equipos, la mantiene y la finaliza.

Capa de presentación. Esta capa define como es presentada la información transmitida.

Capa de aplicación. Define como interactúan los datos con los distintos protocolos de aplicaciones que van a trabajar con la red.

CONCLUSIONES

Hoy en día las redes inalámbricas han tomado un gran auge debido a la necesidad de movimiento que se requiere. Este tipo de comunicación se puede considerar como la más práctica y fácil de implementar pues no se requieren licencias de uso.

Indudablemente las áreas académicas requieren del uso de comunicaciones móviles, para facilitar el manejo de información en cualquier lugar. También como es sabido el uso de Internet se ha vuelto una necesidad, más que un lujo, es por ello que se debe tener contemplado las técnicas necesarias para realizar una conexión fácil.

Al realizar una propuesta de red inalámbrica de área local se debe tomar en cuenta varias características del recinto, las cuales se han tomado en cuenta en el presente trabajo para lograr un resultado satisfactorio. Dentro de la Escuela Normal No. 4 de Ciudad Nezahualcóyotl, en donde se llevó a cabo la propuesta, se constató que era necesario contar con una comunicación vía inalámbrica, para facilitar las tareas tanto a alumnos como profesores y académicos.

Por otro lado como ya se ha mencionado dentro de la investigación, la implementación de las redes de este tipo son mucho más baratas que las cableadas. Por ello, tomando en cuenta todas las consideraciones pertinentes se resolvió que la mejor forma era creando una red inalámbrica.

Ya que en ciudades donde el espacio de radio está muy saturado por frecuencias de radio AM y FM, comunicaciones empresariales, ciertos dispositivos que se utilizan a diario como teléfonos inalámbricos, etc., se debe tener cuidado al comprar los equipos para realizar una implementación de una red inalámbrica.

Al llevar a cabo las pruebas necesarias para verificar que puede existir una comunicación sin cables, se pudo percatar de las facilidades y dificultades existentes, y llegar a la conclusión que el proyecto era factible. Por lo tanto será benéfico para la Institución hacer uso de ésta tecnología para su mejora académica.

GLOSARIO

10 Base T. Es el estándar de Ethernet que permite velocidades de transmisión de 10 Mbps en cable coaxial delgado.

100 Base T. Es el estándar de Ethernet que permite velocidades de transmisión de 100 Mbps.

2G. Sistema basado en la tecnología GSM para telefonía celular, capaz de transmitir datos a 13 Kbps.

ACK. Número que se obtiene como respuesta del equipo al que se envío la información, para saber si ésta llego.

Administrador. Persona responsable del mantenimiento y/o gestión de una red o de un servidor de red.

Adress (dirección). Cada equipo conectado a una red dispone de una dirección que lo identifica. Puede estar dada en forma numérica o alfanumérica.

Ancho de banda (Bandwidth). Es la cantidad de datos que puede circular en un medio por unidad de tiempo. Se mide generalmente en bits por segundos. También puede hacer referencia a un rango de frecuencias.

AP (Punto de Acceso). Es el equipo de la red inalámbrica que se encarga de gestionar las comunicaciones de todos los dispositivos que forman la red; también hace de puente en las comunicaciones con las redes externas (cableadas e Internet).

ARP. Protocolo de Resolución de Direcciones. Es un protocolo que se utiliza para averiguar la dirección del enlace correspondiente a la dirección IP.

Banda ancha. Hace referencia a las comunicaciones que transmiten datos a alta velocidad. Se suele considerar banda ancha a cualquier comunicación con velocidad superior a 64 Kbps.

Banda Angosta. Es un sistema de radio que transmite y recibe información en una radio de frecuencia específica. La banda amplia mantiene la frecuencia de la señal de radio tan angostamente sea posible para pasar la información.

Banda de frecuencias. Es un rango de frecuencias del espectro radioeléctrico. El espectro radioeléctrico está dividido en bandas de frecuencias que regulatoriamente son utilizadas para distintas finalidades.

Bit. Es la unidad más pequeña de información. Puede tomar el valor de 0 ó 1.

Bluetooth. Es una tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de 10 mts.). Esta pensado para comunicar una computadora con sus periféricos.

BPSK. Modulación Binaria por Salto de Fase. (Binary Phase-Shift Keying).

Bridge (Puente). Es un dispositivo que interconecta dos redes haciéndolas funcionar como si se tratara de una sola.

Browser (micronavegador). Programa que permite acceder a los recursos web de Internet.

BSS. Conjunto de Servicios Básicos. Configuración de red inalámbrica que consta de un punto de acceso.

Buffer. Espacio físico de memoria destinado a guardar datos temporalmente.

Byte. Unidad de información formada por 8 bits.

Canal. Porción de la banda de frecuencias en la que trabaja una red inalámbrica.

CCK. Salto de Código Complementario. (Complementary Code Keying).

CDMA. Acceso Múltiple por división de Código. Es un estándar de transmisión que separa canales de voz usando tecnología de espectro ensanchado.

Clave. Es una palabra o secuencia de caracteres que se utiliza para confirmar la identidad de un usuario.

COFETEL. Comisión Federal de Telecomunicaciones. Organismo gubernamental encargado de llevar el control de frecuencias y licencias para comunicaciones.

CRC. Comprobación Cíclica de Redundancia. Son datos adicionales que se adjuntan al final de la información para comprobar fácilmente que no ha habido errores en la transmisión.

CSMA/CA. Censo de Portadora con Múltiple Acceso/Evitación de Colisión. Es el sistema que emplean las redes inalámbricas para las comunicaciones entre los distintos dispositivos. Evita que dos dispositivos puedan intentar hacer uso del medio simultáneamente.

Datagrama. Agrupamiento lógico de información enviada como unidad de la capa de red en un medio de transmisión.

Decibelios (dB). Es una unidad que mide la relación entre dos valores, la relación señal/ruido o la ganancia. Utiliza una escala logarítmica.

DECT. Telecomunicaciones Digitales Inalámbricas Mejoradas.

DHCP. Protocolo de Configuración Dinámica del Host. Es un protocolo que permite que un servidor asigne dinámicamente las direcciones IP a los equipos conforme las van necesitando.

Dirección IP. Es una cadena numérica que identifica a los equipos conectados a Internet.

Dirección MAC. Es un número único que asignan los fabricantes a los dispositivos de red. Es permanente y viene grabado en el equipo para permitir identificarlo. Están formadas por 12 caracteres alfanuméricos.

DNS. Sistema de Nombres de Dominio. Es el encargado de traducir los nombres de dominio de los equipos conectados a Internet en direcciones IP.

DSSS. Espectro Expandido por Secuencia Directa. Es la técnica de modulación utilizada por los sistemas IEEE 802.11b para transmitir datos a alta velocidad (11Mbps).

Emisor. Equipo que se encarga de enviar información.

ESS. Conjunto de Servicios Extendido. Es la configuración de red inalámbrica formada por más de un punto de acceso.

Ethernet. Estándar de red de área local más implementado. Trabaja a una velocidad de 10 Mbps.

ETSI. Instituto Europeo de Normas de Telecomunicaciones.

Espectro expandido. Es un sistema de difusión de señales radioeléctricas.

FCC. Comisión Federal de Comunicaciones. Agencia federal del gobierno de EUA encargada de regular y administrar en materia de telecomunicaciones.

FHSS. Espectro Expandido por Salto de Frecuencia. Técnica de modulación utilizada por los sistemas IEEE 802.11. Transmite datos a baja velocidad (1 Mbps).

Firewall. Dispositivo de seguridad que controla los accesos a una red local desde el exterior.

Fragmentación. Consiste en dividir los paquetes de información, haciéndolos más pequeños.

FTP. Protocolo de Transferencia de Archivos. Es un protocolo de Internet que permite transferir archivos de un equipo a otro.

Gateway (Pasarela). Es un dispositivo que transfiere datos entre dos redes incompatibles entre sí, adaptando el formato de los datos de una aplicación a otra o de una red a otra.

GFSP. Modulación Gausiana por Salto de Frecuencia.

Ghz. Gigahertz

GSM. Sistema Global para Comunicaciones Móviles. Sistema digital europeo para telefonía celular. Opera en la banda de 900 Mhz.

Hacker. Persona que se dedica a entrar ilegalmente en sistemas y redes de computadoras para robar, modificar o borrar información.

HiperLAN. Red de Área Local de Radio de Alto Rendimiento.

HomeRF. Radio Frecuencia del Hogar.

HOST. Cualquier computadora o dispositivo conectado a una red TCP/IP.

HTTP. Protocolo de Transporte de Hipertexto. Es el protocolo que se utiliza en Internet para transferir la información web.

Hub. Dispositivo utilizado en las redes de área local para interconectar los equipos de red. Se limita a recoger la información de un puerto y retransmitirla por el resto de los puertos sin hacer ningún tipo de análisis en ella.

IBSS. Conjunto de Servicios Básicos Independientes. La comunicación se lleva a cabo en forma directa entre computadoras

ICM. Bandas de aplicaciones Industriales, Científicas y Medicas.

ICMP. Protocolo de Mensajes de Control de Internet.

IEEE. Instituto de Ingenieros Eléctricos y Electrónicos.

Internet. Conjunto de redes, de ámbito mundial, conectadas entre sí mediante el protocolo IP.

IP. Protocolo de Internet. Protocolo utilizado por la mayoría de las redes de área local e Internet.

IPSec. Protocolo de redes privadas virtuales.

ISA. Arquitectura Normalizada de la Industria.

ISO. Organización Internacional para la Normalización. Organización que define los protocolos de comunicaciones utilizados por las redes públicas de conmutación de paquetes.

ISP. Proveedor de Servicios de Internet. Cualquier empresa que facilita el acceso a Internet.

Kbps. Kilo bits por segundo.

L2TP. Protocolo de Tunelado de Capa 2. Es un protocolo utilizado para crear redes privadas virtuales.

LAN. Red de Área Local.

LLC. Control de Enlace Lógico. Controla las tareas de interacción entre la tarjeta de red y el procesador.

MAC. Control de Acceso al Medio.

MAN. Red de Área Metropolitana.

Mbps. Mega bits por segundo

Mhz. Megahertz.

Módem. Dispositivo que se conecta a una computadora para poder transmitir datos por un medio de transmisión analógico.

Modulación. Se llama así al hecho de distorsionar una señal eléctrica o radioeléctrica para que contenga la información a transmitir.

Nodo. Se le llama nodo a cualquier computadora conectada a una red.

OFDM. Multiplexación Ortogonal por División de Frecuencias. Técnica de modulación por redes de área local inalámbricas, que permite velocidades de hasta 54 Mbps.

OSI. Interconexión de Sistemas Abiertos. Serie de protocolos normalizados por ISO.

PCI. Interconexión de Componentes Periféricos.

PCMCIA. Asociación Internacional de Tarjetas de Memoria para Computadoras Portátiles.

POP. Protocolo de Oficina de Correos. Protocolo que permite a los usuarios de computadoras personales acceder a un host y transferir a su computadora todo el correo dirigido a ellos.

PDA. Agenda Electrónica Personal.

PHY. Capa física. Se encarga de definir los medios físicos por donde se va a difundir la señal.

PPTP. Protocolo de Tunelado Punto a Punto. Protocolo de red privada virtual incluido en Windows.

Protocolo. Conjunto de normas que indican cómo deben actuar los equipos al comunicarse entre sí.

Puerto. Puede tener dos significados. Puede tratarse de un número que identifica una aplicación particular de Internet (número de puerto). O también se conoce como puerto al conector físico que utilizan las computadoras para comunicarse con los periféricos.

QoS. Calidad de Servicio.

QPSK. Modulación por Salto de Fase en Cuadratura.

RAM. Memoria de Acceso Aleatorio.

RC4. Algoritmo de codificación desarrollado en 1987 por RSA Data Security, usado en WEP y otras formas de codificación. Depende de una cifra de flujo de bytes pseudoaleatorios.

Receptor. Equipo que se encarga de recibir las señales que se transmiten.

Red. Conjunto de equipos conectados entre sí.

RF. Radio frecuencia.

Roaming. Posibilidad que tienen los equipos inalámbricos de desplazarse dentro del área de cobertura de una red inalámbrica sin perder la conexión.

Router. Dispositivo utilizado para transferir datos entre dos redes que utilizan un mismo protocolo.

RS-232. Puerto serie integrado en diferentes equipos.

Servidor. Equipo que ofrece servicios remotos a los usuarios.

Sistema Operativo. Es el encargado de gestionar y operar todos los recursos, hardware y software.

SMTP. Protocolo Simple de Transferencia de Correo. Protocolo en el que se basa el servicio de correo electrónico en Internet.

SSID. Identificador del Conjunto de Servicios. También se le conoce como nombre de red, es el parámetro que identifica a la red inalámbrica.

SWAP. Protocolo de Acceso Compartido.

Switch. Dispositivo al que se conectan los equipos para formar una red, o para conectar varias redes LAN, analiza la información y la envía sólo al equipo a la que está destinada.

Terminal. Los equipos que forman parte de una red inalámbrica.

TCP. Protocolo de Control de Transmisión.

TDMA. Acceso Múltiple por División de Tiempo.

Telnet. Aplicación de Internet que permite el acceso remoto a otros equipos de la red y trabajar como si fuese un usuario local.

Transceiver (transmisor-receptor). Es un equipo de radio que puede tanto transmitir como recibir señales.

UDP. Protocolo de Datagrama de Usuario. Permite el transporte de datos del equipo fuente al equipo destino.

USB. Bus Serie Universal.

UTP. Par trenzado sin blindaje. Tipo de cable utilizado para las conexiones de computadoras, se encuentra por categorías que trabajan a distintas velocidades. La categoría 5 trabaja 100 Mbps.

IV. Vector de inicialización.

Virus. Programa que contiene la característica de autoreproducirse, pasa de una a otra computadora a través de la red.

VPN. Red privada Virtual.

WAP. Protocolo de Aplicaciones Inalámbricas.

WECA. Alianza de Compatibilidad Ethernet Inalámbrica. Asociación de fabricantes de equipos de red inalámbrica.

WEP. Protocolo de Equivalencia con Red Cableada.

Wi-Fi. Fidelidad Inalámbrica. Marca creada por la asociación WECA con el objeto de fomentar la tecnología inalámbrica y asegurar la compatibilidad entre equipos.

Windows. Sistema Operativo creado por Microsoft.

WPA. Acceso Wi-Fi Protegido.

XOR. OR Exclusiva. Compuerta Lógica.

BIBLIOGRAFÍA

Carballar Falcón, José Antonio
Wi-Fi, Como construir una red inalámbrica
1era. Edición
México, D.F. 2004
Editorial Alfaomega
P.p. 275

PC Magazine en español
Agosto 2003.
Vol. 14, No. 8
Anticipe su futuro

PC Magazine en español
Enero 2003
Vol. 14, No. 1
¿Seguridad en el aire?
Sobre redes inalámbricas
Molina, Nadia
P. 6,10

PC Magazine en español
Septiembre 2003
Vol. 14, No. 9
Convierta su red en Wi-Fi
P. 64 - 65

Revista Red
Año XI
Junio 2001
No. 129
9 puntos rojos en las redes del nuevo milenio
Bernal, Samuel
P. 40 – 46

Revista Red
Año IX
Septiembre 2004
No. 70
La seguridad invisible, ¿Cómo tenerla en una WLAN?
Cabrera, Victor A.

Revista Red
Año IX
Agosto 2004
No. 69
Revolución Wireless... La cobertura hace la diferencia
Alcántara Castro, María Elena

Revista Red
Año IX
Junio 2004
No. 67
Wi-MAX: la nueva cara del wireless
Becerra, José Luis

Revista PC/Tips Byte
Abril 1992
Nicholas Baran
P. 94 – 100

PÁGINAS EN INTERNET

www.pcmag.com/wirelesslans

www.red.com.mx

www.terra.es/informatica/articulo/html/inf2208.htm

www.ieee.org

http://ultra04.agitec.gob.mx/cuadro/pdf/uhf.pdf

www.enterate.unam.mx/Articulos/2004/agosto/redes.htm

www.ieee802.org/11

www.standardieee.org

http://mx.drs.yahoo.com/S=21926150/K=sistema+de+banda+angosta+en+radio+frecuencia/v=2/SID=e/1=WS1/R=8/H=0/*

www.34t.com/box-docs.asp?doc=507

www.3com.com.mx

www.cisco.com

www.dlink.com

www.linksys.com

www.netgear.com

www.siemens.com

www.wirelessdevnet.com