



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES  
ACATLÁN

RED LOCAL INALÁMBRICA (WLAN).

TESINA

QUE PARA OBTENER EL TÍTULO DE  
LIC. MATEMÁTICAS APLICADAS Y COMPUTACIÓN

PRESENTA

GLORIA LUCERO HERNÁNDEZ.

ASESOR: ALEJANDRO ROBERTO RUBIO PÉREZ.

SEPTIEMBRE 2006.



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

## AGRADECIMIENTOS

A Jehová:

Por estar siempre conmigo, protegerme e iluminarme para terminar mi sueño, y por darme fuerzas para enfrentar la adversidad que se me presenta en mi camino.

A mis padres:

Dedico este trabajo a mis padres, por darme el bello regalo de la vida, además de su infinita paciencia, ternura y amor. Por creer en mí.

A mi hermano Lucio:

Por estar siempre pendiente de mí, por su apoyo económico, moral y su confianza. Además de su ejemplo de responsabilidad, infinitamente gracias.

A mi hermano Daniel:

Por haberme motivado a terminar la carrera, además de ser un ejemplo para mí.

A Normita, Erwin y Mary:

Por su apoyo incondicional, además de ser cómplices en la búsqueda del camino del amor y la confianza, los amo.

A mis sobrinitos:

Gracias por haber traído alegría a mi vida, y llenarla con sus ocurrencias, los amo pequeños traviesos.

A mis amigos:

Agradezco, su amistad y los momentos que pasamos juntos, además de su apoyo incondicional, a todos mil gracias.

A mi asesor:

Por compartir conmigo sus conocimientos, su tiempo y su infinita paciencia, gracias Lic. Alejandro Roberto Rubio Pérez.

## INDICE GENERAL

### Contenido

Introducción .....	5
CAPÍTULO 1. FUNDAMENTOS DE REDES INALÁMBRICAS.	
1.1. Antecedentes de redes inalámbricas.....	6
1.2. Principales tecnologías para redes inalámbricas .....	18
1.3. Definición de red inalámbrica de área local .....	21
CAPÍTULO 2. REQUERIMIENTOS NECESARIOS.	
2.1. Hardware.....	23
2.2. Protocolos.....	27
2.3. Software .....	31
CAPÍTULO 3. SEGURIDAD.	
3.1. Los riesgos .....	35
3.2. Seguridad en redes inalámbricas .....	38
3.3. Medidas de protección .....	41
3.4. Ventajas e inconvenientes de una red wlan .....	42
CAPÍTULO 4. APLICACIONES DE LAS REDES LOCALES INALÁMBRICAS.	
4.1. Aplicaciones en la organización .....	45
4.2. Red pública de área local .....	46
Anexo I .....	50
Conclusiones.....	51
Bibliografía .....	52
Glosario .....	53

## Introducción

La transmisión inalámbrica es una de las áreas de mayor potencial en la evolución futura de las telecomunicaciones.

Las redes inalámbricas de área local (WLAN), son un sistema de comunicación de datos flexible muy utilizado a fin de satisfacer necesidades de: Movilidad, porque nos ofrece información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red y de ésta forma se obtiene una mayor productividad. Además las tecnologías inalámbricas tienen muchos usos prácticos, por ejemplo: Facilidad de instalación porque evita obras para instalar cable por muros y techos a esto le aumentamos otra gran ventaja que es la flexibilidad, ya que permite llegar donde el cable no puede y nos brinda como resultado una considerable reducción de costos, porque a veces se presentan cambios frecuentes, también en caso de las personas que viajan con equipos portátiles pueden conectarse a Internet a través de “estaciones base” instaladas en aeropuertos, restaurantes y hoteles.

El costo inicialmente más alto de la red sin cable es significativamente más bajo a la larga, además de tener mayor tiempo de vida y menor gasto de instalación. Con respecto a la escalabilidad resulta más sencillo el cambio de topología de red y permite la reubicación de terminales y la rapidez consecuente de instalación.

La disponibilidad de conexiones inalámbricas y redes LAN inalámbricas puede ampliar la libertad de los usuarios de la red a la hora de resolver varios problemas asociados a las redes con cableado fijo y, en algunos casos, incluso reducir los gastos de implementación de las redes.

# CAPÍTULO 1

## FUNDAMENTOS DE REDES INALÁMBRICAS

# CAPÍTULO 1. FUNDAMENTOS DE REDES INALÁMBRICAS.

## 1.1. Antecedentes de Redes Inalámbricas.

Las redes inalámbricas nacen como evolución de los sistemas de acceso y transmiten información, además cumplen fundamentalmente el objetivo de facilitar el acceso a información remota, de esta manera permite a los usuarios establecer conexiones inalámbricas a través de largas distancias y entretenimiento interactivo.

Definición de una red de área local: La definición más general de una red de área local (Local Area Network, LAN), es la de *“una red de comunicaciones utilizada por una sola organización a través de una distancia limitada, la cual permite a los usuarios compartir información y recursos como: espacio en disco duro, impresoras, CD-ROM, etc.”*.

Una red de área local inalámbrica (WLAN): *Es un sistema de comunicación de datos flexible que puede reemplazar o extender una red de área local cableada (LAN) para ofrecer funcionalidad adicional.* Una red de área local cableada tradicional (LAN) envía paquetes de datos desde un equipo a otro a través de cables; una red de área local inalámbrica (WLAN), por el contrario, depende de ondas de radio para transferir datos. Los datos son sobrepuestos en una onda de radio por medio de un proceso denominado modulación, esta onda portadora, actúa entonces como el medio de transmisión, haciendo la función del cable.

Las redes inalámbricas se diferencian de las convencionales principalmente en la Capa Física y la Capa de Enlace de Datos, según el modelo de referencia OSI. La Capa Física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos denominada MAC, se encarga de describir como se empaquetan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse. Los dos medios usados para reemplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

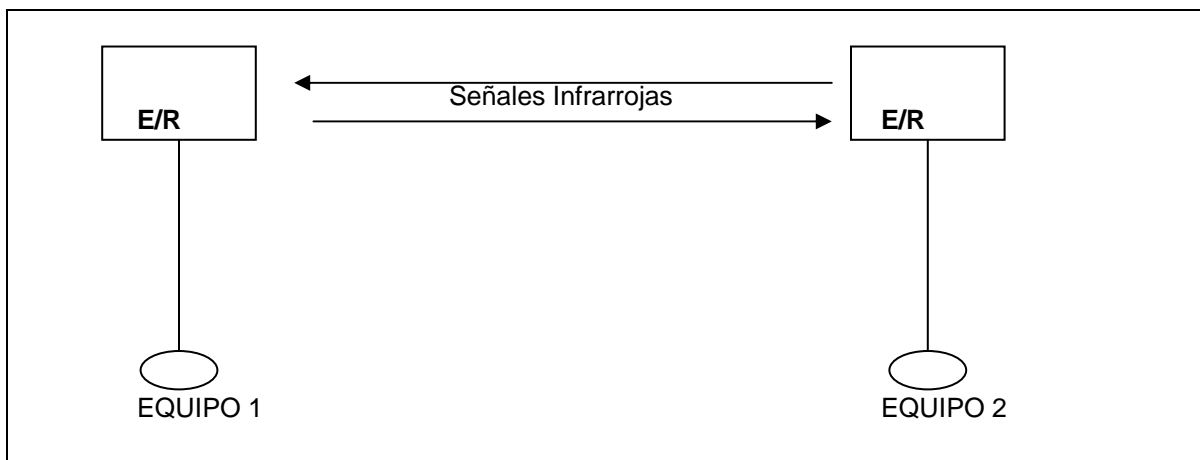
Las WLAN utilizan un medio de transmisión, pero en lugar de utilizar cable de par trenzado o fibra óptica, como las LAN, las WLAN utilizan infrarrojos (IR) o radiofrecuencias (RF). La radiofrecuencia es más popular debido a su mayor alcance, ancho de banda y cobertura.

Entre las tecnologías que utilizan las WLANs, tenemos las de radio frecuencia y las de infrarrojos.

Las estaciones con tecnología infrarroja pueden usar tres modos diferentes de radiación para intercambiar la energía óptica entre transmisores/receptores estos son:

Punto a Punto, Cuasi difuso y Difuso.

Modo *punto a punto*: El tipo de emisión por parte del transmisor se hace de forma direccional, y por ello las estaciones deben verse directamente, para poder dirigir el haz de luz directamente de una hacia la otra, obviamente esta es una desventaja porque las estaciones tienen que quedar de frente este método se usa en redes inalámbricas Token Ring, donde el anillo está formado por una unión de enlaces punto a punto entre las distintas estaciones. Es el que menor poder óptico consume, pero no debe haber obstáculos entre las dos estaciones. En la topología de Ethernet se puede usar el enlace punto a punto,



PUNTO-A-PUNTO



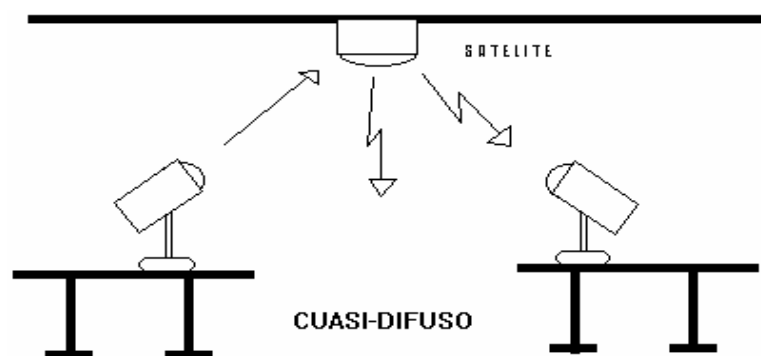
Modo *cuasi difuso*: Éste consiste en una emisión radial, es decir, que la emisión se produce en todas direcciones. Cuando una estación emite una señal óptica, ésta puede ser recibida por todas las estaciones al mismo tiempo, al contrario que el modo punto a punto. Para conseguir esto, lo que se hace es transmitir a diferentes superficies reflejantes, las cuales dirigirán el haz de luz hacia las estaciones receptoras. No es necesaria la línea de vista entre dos estaciones, pero si deben estarlo con la línea de reflexión.

Y dependiendo de cómo sea esta superficie reflejante, la podemos clasificar en dos tipos de reflexión: Pasiva y activa.

En la reflexión pasiva, la superficie reflejante simplemente refleja la señal, debido a las cualidades reflexivas del material y el reflector debe de tener altas propiedades reflectivas y dispersivas.

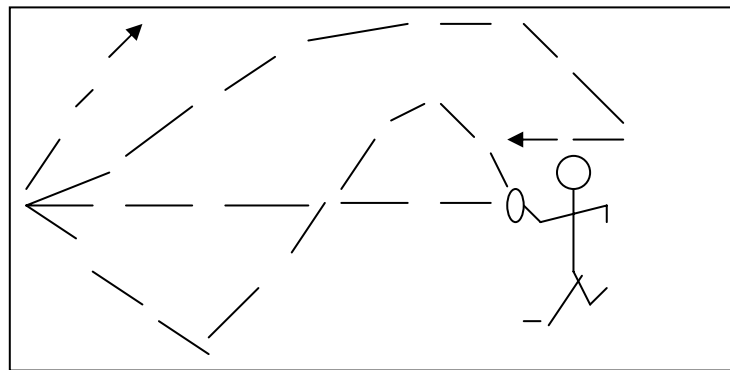
Y en la reflexión activa, el medio reflejante no sólo refleja la señal, sino que además la amplifica, en este caso el medio reflejante se conoce como satélite.

Es importante destacar que, la reflexión pasiva es más flexible y barata, requiere de una mayor potencia de emisión por parte de las estaciones, debido al echo de no contar con etapa repetidora.



Modo de *emisión difusa*: Es radial, es decir, que cuando una estación emite una señal óptica, ésta puede ser recibida por todas las estaciones al mismo tiempo, el poder de salida de la señal óptica de una estación debe ser suficiente para llenar completamente el total del cuarto, mediante múltiples reflexiones, en paredes y obstáculos del cuarto, por lo tanto la línea de vista no es necesaria y la estación se puede orientar hacia cualquier lado. El modo difuso es el más flexible, en términos de localización y posición de la estación, sin embargo esta flexibilidad esta a costa de excesivas emisiones ópticas.

Por lo tanto requiere de una potencia de emisión mayor que los modos Punto a Punto y Cuasi difuso, puesto que el número de rebotes incide directamente en el camino recorrido por la señal y las pérdidas aumentan.



Modo Difuso

La desventaja de las redes infrarrojas es el espacio, generalmente se utilizan en redes en las cuales sus estaciones se encuentran en un solo cuarto o piso, en caso de que se tengan oficinas en diferentes edificios se colocarán los receptores/emisores en las ventanas de los edificios de esta forma se lleva a cabo la comunicación.

Con respecto a las comunicaciones inalámbricas que utilizan radiofrecuencia pueden clasificarse en:

- ◆ **Sistemas de banda estrecha (narrow band) o de frecuencia dedicada**, esta señal atraviesa paredes por lo que alcanza una red bastante amplia, sin embargo tiene problemas con las reflexiones que sufren las ondas de radio, para establecer esto hay que evitar las posibles interferencias.
- ◆ **Sistemas basados en espectro disperso o extendido (spread spectrum)**. La FCC (Federal Communications Commission) Comisión Federal de Comunicaciones, Organismo Gubernamental encargado del control y regulación del sector de las Telecomunicaciones en los Estados Unidos. Es la más utilizada en las LANs inalámbricas. En 1985 permitió la operación sin licencia de dispositivos que utilicen 1 watt de energía o menos, en tres bandas de frecuencias: 902 a 928 MHz, 2.400 a 2.483 MHz, y 5.725 a 5.850 MHz. Deberá ser utilizada en las bandas ISM. Esta técnica a sido utilizada en aplicaciones militares, la idea es reducir la densidad de energía abajo del nivel del ruido ambiental de tal manera que la señal no sea detectable. El objetivo en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia. Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente y son las siguientes:
  - ◆ **Secuencia directa:** En este método la información que es transmitida es multiplicada por una secuencia binaria pseudoaleatoria y el receptor recibirá correctamente la información, sólo si la secuencia es conocida. Como cada transmisor opera una secuencia diferente, es probable que varios transmisores operen en la misma área sin interferencia.
  - ◆ **Salto de frecuencia:** Este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, por ejemplo las bandas de 2.4 y 5.8 Mhz que son utilizadas por hornos de microondas.

Los sistemas que usan salto de frecuencia consumen menos potencia que los que emplean secuencia directa y son más económicos. Pero cualquiera de los dos métodos es seguro ya que es difícil de violar.

## WLAN 802.11

Este estándar está desarrollado por el Instituto de Ingeniería Eléctrica y Electrónica IEEE 802.11, establece las normas a seguir por cualquier fabricante de dispositivos Wireless para que puedan ser compatibles entre sí. El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2.4 GHz, o infrarroja, con regímenes binarios de 1 a 2 Mbit/s. El método de acceso al medio es mediante escucha pero sin detección de colisión, que se conoce como DFWMAC (Distributed Foundation Wireless MAC), Protocolo de MAC inalámbrico de fundamento distribuido, es el procedimiento de saludo de cuatro vías utilizado, está diseñado tanto para aplicaciones de infraestructura como de ad-hoc. Para verificar si el interlocutor está en contacto de radio con el nodo de origen. Para esto se incorpora en el protocolo de MAC un saludo adicional (DFWMAC).

Estos son los estándares más importantes:

- ◆ IEEE802.11a: Hasta 54 Mbps (megabits por segundo) de ancho de banda disponible, trabajando en la frecuencia de 5 GHz.
- ◆ IEEE802.11b: Hasta 11 Mbps. Este es el más utilizado, trabajando en la frecuencia de 2,4 GHz.
- ◆ IEEE802.11g: Estándar hasta 54 Mbps, trabajando en la frecuencia de 2,4 GHz como 802.11a.

Por ser un estándar mundial, muchos fabricantes están creando equipos Wireless, para otras aplicaciones como pueden ser: servidores de impresión o cámaras Web.

Para minimizar la interferencia, las regulaciones de FCC estipulan una técnica de señal de transmisión llamada *spread-spectrum modulation* tiene una potencia de transmisión máxima de 1 Watt. Deberá ser utilizada en la banda ISM. Esta técnica ha sido utilizada en aplicaciones militares.

La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. La técnica de señal de transmisión llamada *spread-spectrum modulation* es utilizada en aplicaciones militares y el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia.

La mayor parte de las LAN inalámbricas utilizan la banda de frecuencia de 2,4 gigahercios (GHz), la única parte del espectro de RF que se reserva en todo el mundo para dispositivos sin licencia. La libertad y flexibilidad de la Redes inalámbricas pueden aplicarse tanto dentro de los edificios como entre edificios. Es decir la tecnología Wireless nos permite montar una red no solo en algunos metros sino en kilómetros. En este trabajo menciono algunas tablas de frecuencias de uso libre en México.

Refiriéndonos exclusivamente a la banda UHF, Ultra High Frequencies Banda del espectro electromagnético que ocupa el rango de frecuencias de 300 MHz a 3 GHz (802.11a y 802.11b están en ésta frecuencia). La Secretaria de Comunicaciones y Transporte estableció una serie de frecuencias de uso libre clasificadas de acuerdo al siguiente orden.

1.- FRECUENCIAS PARA EQUIPOS OPERANDO DE 5 WATTS DE POTENCIA APARENTE RADIADA:

464.4875 a	467.8625 Mhz
464.5000 a	467.8750 Mhz
464.5125 a	467.8875 Mhz
464.5375 a	467.9000 Mhz
464.5500 a	467.9125 Mhz
464.5625 a	467.9250 Mhz
467.8375 a	467.9375 Mhz
467.8500 a	

2.- FRECUENCIAS PARA EQUIPOS PORTÁTILES, MÓVILES Y BASES OPERANDO A UN MÁXIMO DE 40 WATTS DE POTENCIA APARENTE RADIADA.

450.2625 a	455.3625 Mhz
450.2750 a	455.3750 Mhz
450.2875 a	455.3875 Mhz
455.2625 a	455.4000 Mhz
455.2750 a	455.4125 Mhz
455.2875 a	455.4250 Mhz
455.3000 a	455.4375 Mhz
455.3125 a	455.4500 Mhz
455.3250 a	455.4625 Mhz
455.3375 a	455.4750 Mhz
455.3500 a	455.4875 Mhz

3.- FRECUENCIAS DE USO FAMILIAR PARA EQUIPOS QUE OPERAN A UN MÁXIMO DE 0.5 WATTS DE POTENCIA APARENTE RADIADA.

462.5625 a 467.5625 Mhz  
462.5875 a 467.5875 Mhz  
462.6125 a 467.6125 Mhz  
462.6375 a 467.6375 Mhz  
462.6625 a 467.6625 Mhz  
462.6875 a 467.6875 Mhz  
462.7125 a 467.7125 Mhz

FRECUENCIAS LIBRES EN MEXICO DE VHF

Refiriéndonos exclusivamente a la banda VHF, Very High Frequencies Banda del espectro electromagnético que ocupa el rango de frecuencias de 30MHz a 300MHz, la Secretaria de Comunicaciones y Transportes estableció una serie de frecuencias de uso libre clasificadas de acuerdo al siguiente orden:

1.- FRECUENCIAS PARA EQUIPOS OPERANDO DE 5 WATTS DE POTENCIA APARENTE RADIADA:

151.6125 Mhz  
151.6250 Mhz  
151.6375 Mhz  
154.5875 Mhz  
154.6000 Mhz  
154.6125 Mhz

2.- FRECUENCIAS PARA EQUIPOS PORTÁTILES, MÓVILES Y BASES OPERANDO A UN MÁXIMO DE 40 WATTS DE POTENCIA APARENTE RADIADA.

153.0125 a	159.1125 Mhz
153.0250 a	159.1250 Mhz
153.0375 a	159.1375 Mhz
153.0500 a	159.1500 Mhz
153.0625 a	159.1625 Mhz
153.0750 a	159.1750 Mhz
153.0875 a	159.1875 Mhz
153.1000 a	159.2000 Mhz
153.1125 a	163.0125 Mhz
153.1250 a	163.0250 Mhz
153.1375 a	163.0375 Mhz
153.1500 a	163.0500 Mhz
153.1625 a	163.0625 Mhz
153.1750 a	163.0750 Mhz
153.1875 a	163.0875 Mhz
153.2000 a	163.1000 Mhz
153.2125 a	163.1125 Mhz
153.2250 a	163.1250 Mhz
153.2375 a	163.1375 Mhz
159.0125 a	163.1500 Mhz
159.0250 a	163.1625 Mhz
159.0375 a	163.1750 Mhz
159.0500 a	163.1875 Mhz
159.0625 a	163.2000 Mhz
159.0750 a	163.2125 Mhz
159.0875 a	163.2250 Mhz
159.1000 a	163.2375 Mhz

**NOTA:**

Desviación permitida +/- 2.5 KHz., 12.5KHz separación de canales  
No se permiten repetidores.

La Secretaria de Comunicaciones y Transportes establece un acuerdo por el que se establecen bandas de frecuencias del espectro radioeléctrico de uso libre. Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos. Secretaría de Comunicaciones y Transportes.

Con fundamento en los artículos 36 de la Ley Orgánica de la Administración Pública Federal; 7, 10 y demás aplicables de la Ley Federal de Telecomunicaciones, y 3o., 6o., 25, 26 y 38 del Reglamento Interior de la Secretaría de Comunicaciones y Transportes, y considerando que de conformidad con el artículo 7, fracción I, de la Ley Federal de Telecomunicaciones, la Secretaría deberá planear, formular y conducir las políticas y programas, así como regular el desarrollo de las telecomunicaciones, con base en el Plan Nacional de Desarrollo y los programas sectoriales correspondientes, que en términos de la fracción VI del citado artículo 7 de la Ley Federal de Telecomunicaciones, corresponde a la Secretaría elaborar y mantener actualizado el cuadro nacional de atribución de frecuencias, respecto del cual deben considerarse las bandas de frecuencias del espectro radioeléctrico de uso libre, que el artículo 10, fracción I, de la Ley Federal de Telecomunicaciones contempla la clasificación de bandas de frecuencia de espectro de uso libre que pueden ser utilizadas por el público en general sin necesidad de concesión, permiso o registro, que se presenta una creciente demanda en el país del servicio de radiocomunicación privada y que para promover el desarrollo de estos servicios se hace necesario que la Secretaría determine las bandas de frecuencias que serán destinadas al espectro de uso libre, que tanto por sus características técnicas como por su ocupación, resulta conveniente que algunas bandas de frecuencias de VHF y UHF se destinen al espectro de uso libre, y que los usuarios de las bandas de uso libre deben operar bajo condiciones y parámetros técnicos previamente establecidos, se hace del conocimiento del público en general el siguiente acuerdo por el que se establecen bandas de frecuencias del espectro radioeléctrico de uso libre.

ARTÍCULO PRIMERO.- El presente Acuerdo tiene por objeto establecer bandas de frecuencias del espectro radioeléctrico de uso libre en VHF y UHF, de conformidad con el artículo 10, fracción I, de la Ley Federal de Telecomunicaciones.

En consecuencia, las bandas de frecuencias a que se refiere el presente Acuerdo podrán ser utilizadas por el público en general sin necesidad de concesión, permiso o registro, siempre que el equipo se encuentre homologado en términos del artículo 3, fracción V, de la mencionada Ley.



ARTÍCULO SEGUNDO.- Son bandas de frecuencias del espectro radioeléctrico de uso libre, a nivel nacional, las siguientes:

A. Bandas de frecuencias en VHF:

- I. De 153.0125 MHz a 153.2375 MHz.
- II. De 159.0125 MHz a 159.2000 MHz.
- III. De 163.0125 MHz a 163.2375 MHz.

B. Bandas de frecuencias en UHF:

- I. De 450.2625 MHz a 450.4875 MHz.
- II. De 455.2625 MHz a 455.4875 MHz.
- III. De 463.7625 MHz a 463.9875 MHz.
- IV. De 468.7625 MHz a 468.9875 MHz.

Las frecuencias extremas de cada una de las bandas señaladas representan la frecuencia central del primero y último de los canales.

ARTÍCULO TERCERO.- Los equipos que se utilicen en las bandas de frecuencias de espectro de uso libre indicadas en los incisos A y B del ARTÍCULO SEGUNDO del presente Acuerdo, deberán ajustarse a las siguientes condiciones de operación:

- A. Sólo podrán operar los equipos móviles, portátiles y radiobases, con potencia máxima de 40 Watts de potencia radiada aparente (PRA). No se permitirán repetidores de ninguna clase.
- B. Para las antenas de las radiobases sólo se permitirán ubicaciones máximas de 400 metros sobre el nivel promedio del terreno (HAAT).
- C. Quedan prohibidos los enlaces con la red telefónica pública a través de las bandas de uso libre.
- D. Por lo que se refiere al ancho de canal:
  - I. A partir de la entrada en vigor del presente Acuerdo y hasta el 31 de diciembre de 1998, los equipos podrán operar con un ancho de

canal máximo de 25 kHz.

- II. El ancho de canal indicado en la fracción I anterior se reducirá a 12.5 kHz a partir del 1o. de enero de 1999.

E. Los equipos operarán en modalidad simplex y semidúplex con las siguientes características técnicas:

- I. Tipo de emisión: para el ancho de canal de 25 kHz será 16K0F3EJN (voz) y 16K0F2D (datos), mientras que para el ancho de canal de 12.5 kHz será 8K0F3EJN (voz) y 8KF2D (datos).
- III. Desviación máxima de portadora: para el ancho de canal de 25 kHz será + 5 kHz, mientras que para el ancho de canal de 12.5 kHz será + 2.5 kHz.

E. Contar con el certificado de homologación correspondiente.

ARTÍCULO CUARTO.- Con el fin de alcanzar un uso más racional y eficiente de las bandas de uso libre, materia de este Acuerdo, a partir del 1 de julio de 1997 los correspondientes equipos de radiocomunicación deberán contar con un sistema de silenciamiento por codificación de tonos continuos (CTCSS).

ARTÍCULO QUINTO.- Para no causar interferencias perjudiciales a los países vecinos no está permitido el empleo de estas nuevas bandas de uso libre, dentro de franjas fronterizas de 150 km.

#### TRANSITORIOS

PRIMERO.- El presente Acuerdo entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Es una gran ventaja montar una red sin utilizar cables ya que podemos montar y desmontar la red cuantas veces se requiera, por ejemplo: si la empresa no es propicia para montar una red con cableado LAN a causa de limitaciones del edificio o del presupuesto, como por ejemplo en edificios antiguos, espacios arrendados o cuando queremos montar un stand en una feria. También es de gran ayuda para las personas de negocios que siempre se encuentran viajando, porque pueden acceder a su información desde: Aeropuertos, hoteles, restaurantes, etc.

Esto también es una gran ventaja, por ejemplo si los ejecutivos de una empresa viven cerca de la empresa, ya no hay pretexto para no terminar su trabajo, ya que ahora con las redes Wireless ya puede conectar sus equipos desde la comodidad de su hogar a la red de su trabajo, esto obviamente les trae consigo muchas ventajas, como lo es acceso gratuito a Internet de banda ancha, teletrabajo sin límites, vídeo conferencia, vídeo vigilancia, acceso a la intranet.

Los sectores que se ven beneficiados son: La educación, la Banca, la hotelería, la industria, la medicina, manufacturación, almacenes, finanzas, etc. En México existen varias empresas que trabajan con redes inalámbricas para la distribución de sus productos, podemos hacer mención de: Bimbo, Jumex, Coca-Cola y Cuervo.

Es interesante saber que a pesar de las condiciones climatológicas, y de redes que se encuentren en edificios separados por varios kilómetros pueden comunicarse entre sí, por ejemplo, si tenemos que conectar dos redes de diferentes edificios se utiliza un Bridge inalámbrico o también pueden ser con cable de cobre tradicional o con fibra óptica, de esta forma los equipos de una red pueden ver y comunicarse con los equipos de la otra red como si se tratara de una sola. Los puentes inalámbricos transmiten los datos por el aire y esto tiene una gran ventaja, ya que de esta manera no necesitan licencias ni derechos de paso.

## 1.2. Principales tecnologías para redes inalámbricas.

En redes inalámbricas de área local existen tres tecnologías líderes en el mercado como es Infrarrojo, Bluetooth y Wi-Fi.

La **tecnología Infrarrojo** es un tipo de radiación electromagnético invisible para el ojo humano y los sistemas de comunicación los utilizan como emisión y recepción de haces de luz infrarroja. Por ejemplo, en controles de televisión, vídeo, equipos de música, etc. Estos aparatos ocupan la tecnología infrarrojo para su comunicación y también podemos mencionar a las agendas electrónicas, los teléfonos con cámara integrada y la mayoría de computadoras portátiles también incluyen un dispositivo infrarrojo como medio de

comunicación. A su vez estos dispositivos pueden ser divididos en dos categorías:

- ◆ *Infrarrojo de haz directo*: Es decir, que no debe haber obstáculos entre ambas terminales, ya que se requiere de una visibilidad directa.
- ◆ *Infrarrojo de haz difuso*: Aquí si podemos tener obstáculos entre ambas terminales ya que como el haz tiene mucha más potencia no hay problema alguno.

Las tasas de datos típicas para las comunicaciones IrDA (Infrared Data Association) Asociación de datos infrarrojos, son de aproximadamente 4 Mbps y además cuenta con la gran ventaja de que no están reguladas, su costo es bajo y es inmune a interferencias de los sistemas de radio de alta frecuencia, solo que hay un inconveniente son de corto alcance, y como no pueden traspasar objetos, además no son utilizados en el exterior porque la lluvia y la niebla les producen interferencias. El estándar original IEEE 802.11 antecesor de Wi-Fi contemplaba el uso de infrarrojos, pero nunca llegó a desarrollarse debido principalmente a los inconvenientes mencionados.

Podemos decir, que los sistemas infrarrojos son de los más eficaces sistemas de comunicaciones punto a punto para distancias cortas y se utiliza por millones de computadoras portátiles.

La IrDA (Infrared Data Association) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo y cuenta con dos estándares:

- ◆ IrDA-Control. Este protocolo es de baja velocidad y es utilizado en dispositivos de control remoto inalámbrico, por ejemplo los ratones de computadoras o joysticks.
- ◆ IrDA-Data. Este protocolo esta diseñado para distancias menores de un metro y a velocidades que van desde los 9.6 Kbps. Pero hay una versión que extiende el alcance a dos metros, sólo que con un coste de consumo energético alto, y otra que reduce el alcance a 30 cm, reduciendo el consumo de energético a la décima parte.

Al parecer la tecnología de infrarrojos resulta óptima en las comunicaciones a muy corto alcance. Y esto la convierte en compatible con tecnologías como Bluetooth, además es más segura la tecnología infrarrojo porque las emisiones de haces infrarrojos se quedan en un entorno mucho más privado que las propagaciones de ondas de radio.

**Bluetooth** es otra de las tecnologías más usadas fue desarrollada en 1994 por la empresa sueca Ericsson con el objetivo de que los teléfonos móviles tuvieran sus accesorios como son auriculares, computadoras, etc. Es decir, que no fue pensada esta tecnología para redes de computadoras sino más bien, para un teléfono móvil con su auricular, una computadora con su impresora, etc. El nombre de Bluetooth en español significa diente azul y procede del nombre que tenía el rey Harald Blaatlund II, un legendario guerrero danés del siglo X.

Esta tecnología basada en RF, ganó considerable interés y apoyo por parte de algunos fabricantes; está presente en una amplia variedad de dispositivos, tales como teléfonos celulares, PDA, laptops e impresoras.

Dos dispositivos Bluetooth pueden comunicarse en forma automática cuando se encuentran uno dentro del alcance del otro, lo cual hace a esta tecnología conveniente y fácil de utilizar. Sin embargo, la tasa de transmisión para Bluetooth es de 1 Mbps como máximo, y el alcance se limita a 30 pies (9.144 m) aproximadamente.

Bluetooth lleva sus comunicaciones mediante el modelo maestro-esclavo, una terminal maestro puede comunicarse hasta con siete esclavos simultáneamente, el maestro puede suspender las comunicaciones con un esclavo mediante una técnica llamada *parking* y puede activar las comunicaciones con un nuevo dispositivo esclavo. Y con esta técnica un maestro puede establecer comunicación con un máximo de 256 esclavos, donde sólo siete comunicaciones pueden permanecer activas simultáneamente, a este conjunto de relaciones maestro-esclavo se le llama piconet, cuando ocurre esto, se conoce como scatternet, lo que significa red dispersa.

Bluetooth utiliza las técnicas FHSS, Frequency Hopping Spectrum, Espectro Expandido por salto de Frecuencia en la banda de frecuencia 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. Por otro lado puede transmitir tanto voz como datos.

La tercera tecnología es **Wi-Fi** o *Fidelidad Inalámbrica*, también conocida como 802.11b, se ha convertido en un medio muy popular dado que más fabricantes lanzan productos de mayor calidad a precios razonables y por si fuera poco esta tecnología es compatible con diferentes fabricantes cosa que no era posible antes, de la llegada de Wi-Fi, ya que anteriormente se tenía que comprar todo con un solo fabricante, esto limitaba las soluciones que un sólo fabricante puede ofrecer.

Las implementaciones típicas para las redes inalámbricas 802.11b incluyen conectar laptops a redes corporativas y permitir a los usuarios de redes en el hogar conectar las PC, sin incorporar nuevos cables. Con una distancia de transmisión de aproximadamente 300 pies (91.44 m) y una velocidad máxima de 11 Mbps, versiones más recientes de esta tecnología permiten alcanzar los 22.54 y hasta los 100 Mbps.

Estas son las tres tecnologías líderes en el mercado de las redes inalámbricas de área local.

### **1.3. Definición de red inalámbrica de área local.**

La definición más general de una red de área local WLAN (Wireless Local Area Network), es la de “una red de comunicaciones que tiene una cobertura de unos cientos de metros y actualmente ya kilómetros, utilizada por una o varias organizaciones a través de una distancia limitada, la cual permite a los usuarios de un mismo edificio o grupo de edificios compartir información y recursos como: espacio en disco duro, impresoras, CD-ROM, etc. “

## CAPÍTULO 2

# REQUERIMIENTOS NECESARIOS

## CAPÍTULO 2. REQUERIMIENTOS NECESARIOS.

### 2.1. Hardware.

El hardware de una WLAN consiste en dos unidades principales incluye un punto de acceso o también conocidas como estaciones base que coordinan las comunicaciones, se conecta a la red y un adaptador inalámbrico o mejor conocida como tarjeta de red que se instala en la computadora, la mayoría de las redes que existen en el mercado funcionan igual.

Los componentes básicos de una red son los siguientes:

- ◆ *Adaptador de red:* Es necesario en cada Computadora que se desea incluir en la red.
- ◆ *Bridges:* Los “Bridges” ofrecen conexión inalámbrica punto a punto entre dos redes LAN, como en pisos diferentes.
- ◆ *Antenas:* Las antenas aumentan la cobertura de frecuencia de radio y extienden el rango de una WLAN 802.11.
- ◆ *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.
- ◆ *Enrutador o interruptor:* Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo, software, hardware o una combinación de ambos. Los puntos de acceso, generalmente hacen las funciones de router. A este equipo se le conoce en español por el nombre de ruteador.

**Adaptador Inalámbrico:** Un adaptador inalámbrico funciona como una tarjeta de interfase de red en inglés se les conoce como NIC, tradicionalmente los adaptadores de red vienen en forma de tarjeta de interface de red, la cual le permite a la PC del cliente, acceder a la red a través del punto de acceso inalámbrico. Los adaptadores de red son unas estaciones de radio que se



encargan de comunicarse con otros adaptadores de modo ad hoc, o con puntos de acceso. Es decir, de modo infraestructura, para mantener la computadora a la que se están conectados dentro de la red inalámbrica a la que se asocia. En conclusión, funciona como una tarjeta de interfase de red, la cual le permite a la PC del cliente acceder a la red a través del punto de acceso inalámbrico.

El NIC estándar facilita una base de enchufe en la parte posterior de la misma para conectar el cable de la red, Se dice: “tradicionalmente” porque también hay soluciones inalámbricas para redes menores, a veces se llega a elegir ese tipo de solución.

Un claro ejemplo es el teléfono inalámbrico ya que podemos hacer uso del mismo, desde cualquier punto de la casa sin llevar el cable de un lado para otro, es la misma idea, actualmente no todos los adaptadores de red son tarjetas, la mayoría de los adaptadores de red se conectan a un USB (Universal Serial Bus = bus de serie universal), que se nos suministra como estándar en buena parte de las computadoras modernas, si se quiere evitar operar en el interior de una computadora, la única norma inequívoca para la creación de una red es que se necesita tener instalado un adaptador en cada computadora.

Muchas Computadoras nuevas pueden estar configuradas ya con el adaptador de red instalado, incluyen de fábrica un puerto Ethernet RJ45 y para las computadoras portátiles tienen integrado un adaptador de red Wi-Fi. Existen en el mercado los siguientes adaptadores inalámbricos de red:

- ◆ Tarjetas PCMCIA: Su tamaño es como de una tarjeta de crédito solo que un 3% más larga, se inserta en los puertos PCMCIA de tipo II que suelen incorporar la mayoría de las computadoras portátiles, también hay tarjetas PCMCIA de Wi-Fi su precio es bajo.
- ◆ Tarjetas PCI o ISA: Las computadoras de sobremesa disponen de ranuras PCI o ISA donde se pueden instalar todo tipo de periféricos, entre las que están las tarjetas Wi-Fi, y no es fácil encontrar este tipo de tarjetas Wi-Fi en el mercado, la solución es instalar tarjetas conversoras de PCI a PCMCIA, estos conversores son tarjetas PCI o ISA las cuales se insertan en una ranura externa de la computadora y que ofrecen un puerto PCMCIA al exterior.
- ◆ Unidades USB: Se tratan de unidades inalámbricas que se conectan a la computadora ya sea portátil o de sobremesa, mediante un puerto USB, si la computadora ya tiene ocupados todos los puertos USB, en el mercado

existen multiplicadores de puertos USB que permiten sacar cuatro puertos de donde había uno.

Los adaptadores de red, tienen su controlador de dispositivo; es un software específico de cada sistema operativo y se instala de forma automática o manual, cuando se instala el adaptador. Un problema es que no todos los adaptadores disponen del controlador necesario para todos los sistemas operativos. La mayoría incluye para Windows, pero son pocos los que lo incluyen para Linux o Mac OS. Por eso es necesario saber si el controlador es compatible con el sistema operativo de la computadora que se va a instalar.

**Bridges:** Es un dispositivo que conecta a dos redes, también conocido como puente, de esta forma los equipos de una red pueden ver y comunicarse con los equipos de la otra red como si formaran parte de una misma, un ejemplo son los puntos de acceso ya que hacen las funciones de Bridges al interconectar una red cableada con una red inalámbrica. Existe un Bridge inalámbrico conocido como Wireless Bridge que interconecta dos redes remotas ya sean cableadas o no cableadas, y de esta forma se evita instalar o alquilar el cable.

En caso de redes en edificios distantes, se suelen instalar antenas directivas de alta ganancia en los techos lo que permite cubrir distancias en visión directa de hasta unos pocos kilómetros. Los parámetros inalámbricos (canal de frecuencia, bitrate, identificador de servicio-SSID, etc.) de ambos extremos deben ser idénticos para posibilitar la comunicación. Virtualmente se pueden encadenar un número ilimitado de parejas de bridges para enlazar infraestructuras muy distantes o con obstáculos entre sí.

**Antenas:** Existen varios tipos de antenas como la yagui, de panel, parabólica de disco, parabólica de rejilla, de techo, path, dipolo, planas, compactas, móviles, sectoriales, espiral, guía-onda, anular, etc. Aunque existen varios tipos de antenas, se clasifican en dos tipos y son:

- ◆ Omnidireccionales: Radian y captan la señal en todas las direcciones.
- ◆ Direccionales: Concentran su radiación en una dirección. Y tienen mayor alcance y ganancia que las omnidireccionales.

Las antenas más conocidas son las dipolo, emite su señal haciendo que la energía se propague paralela al dipolo y perpendicular al suelo, es importante elegir donde situar la antena para evitar interferencias que afectan a la comunicación de forma intermitente. Ya colocada la antena es importante hacer pruebas para ver posibles fallas, ya que sintonizar una antena no es difícil, pero si es necesario que este trabajo lo hagan dos personas, para que una este en la antena haciendo los cambios correspondientes, y otra en la computadora

verificando los resultados, es decir, los niveles de recepción de la señal para cada posición de la antena, de esta forma se puede saber cual es la mejor posición y orientación para la antena (Anexo I: Tipos de antenas).

**Punto de acceso:** Es un nodo especial en una red inalámbrica que actúa como punto centralizador y gestor del tráfico del resto del equipo es decir, terminales de cliente, subscriptos a él y dentro de la celda de cobertura. Es decir, que es el centro de las comunicaciones de la mayoría de las redes inalámbricas, no solo es el medio de intercomunicación de todos los terminales inalámbricos, sino que también es el puente de interconexión con la red fija e Internet.

Existen dos puntos de acceso:

- ◆ Puntos de acceso profesionales: Están diseñados para crear redes corporativas de tamaño medio o grande, son muy caros pero obviamente son mucho mejores en seguridad y perfecta integración con el resto de equipos.
- ◆ Puntos de acceso económicos: Son especialmente para pequeñas oficinas o para el hogar.

### **Características de los puntos de acceso**

Los puntos de acceso son unas cajas pequeñas de las que salen una o dos antenas, ya están mejorando su presentación algunos fabricantes y algunos puntos de acceso incluyen accesorios para poder ser puestos en la pared o en el techo y en el interior incluye un equipo de radio de 2.4 GHz, en el caso de 802.11b o 5 GHz, en el caso de 802.11a . Una o dos antenas que pueden o no apreciarse en el exterior, un software de gestión de las comunicaciones y puertos para conectar el punto de acceso a Internet o a la red cableada.

**Enrutador o interruptor:** Un router (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de computadora/computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

## 2.2. Protocolos.

Los protocolos son un conjunto de reglas utilizadas para recibir información en una red, es decir, que es un lenguaje con el cual se comunican las computadoras con otras, por la red, algo muy importante es que todos los dispositivos existentes en la red deben utilizar el mismo lenguaje. Las reglas determinan el formato de los datos que se transmiten y otros aspectos de la red, como por ejemplo la forma de detectar errores.

Es necesario que los datos tengan un formato claro y eficiente, se debe verificar los servicios que involucran como los protocolos de traducción de formatos, códigos y sintaxis de los lenguajes entre una computadora emisora y una receptora, y para esto contamos con el Modelo de Referencia de Interconexión de Sistemas Abiertos, al permitir que sistemas de cómputo disímiles se interconecten e interoperen, gracias a reglas preestablecidas que deben ir cumpliéndose nivel a nivel para su total desempeño logrando el concepto de InternetWorking. Este concepto da la idea de sistemas abiertos, y es donde las computas tienen lugar cubriendo desde los niveles más bajos de conectividad hasta esquemas de conversión de protocolos que requieren de un alto grado de integración.

### Concepto de Modelo OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, conocido mundialmente como Modelo OSI (Open System Interconnection), fue creado por la ISO (Organización Estándar Internacional) y en él pueden modelarse o referenciarse diversos dispositivos que reglamenta la ITU (Unión de Telecomunicación Internacional), con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes. Así, todo dispositivo de cómputo y telecomunicaciones podrá ser referenciado al modelo y por ende concebido como parte de un sistema interdependiente con características muy precisas en cada nivel.

El Modelo OSI cuenta con 7 capas o niveles:

- Nivel de Aplicación
- Nivel de Presentación
- Nivel de Sesión
- Nivel de Transporte
- Nivel de Red
- Nivel de Enlace de Datos
- Nivel Físico

## **Nivel de Aplicación**

Es el nivel más cercano al usuario y a diferencia de los demás niveles, por ser el más alto o el último, no proporciona un servicio a ningún otro nivel, en OSI el nivel de aplicación se refiere a las aplicaciones de red que vamos a utilizar para transportar las aplicaciones del usuario, es decir, que es una sesión específica de aplicación (API), en resumen son los programas que ve el usuario.

## **Nivel de Presentación**

Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformato de datos de la aplicación del usuario. Este nivel negocia la sintaxis de la transferencia de datos hacia el nivel de aplicación, se dice que la capa de Presentación es aquella que provee representación de datos, es decir, mantener la integridad y valor de los datos independientemente de la representación.

## **Nivel de Sesión**

Este nivel es el encargado de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. Establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas, se puede decir que la capa de Sesión es un espacio en tiempo que se asigna al acceder al sistema por medio de un login en el cual obtenemos acceso a los recursos del mismo servidor conocido como "circuitos virtuales". La información que utiliza nodos intermedios que puede seguir una trayectoria no lineal se conoce como "sin conexión".

## **Nivel de Transporte**

En este nivel se realiza y se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (del nivel 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama, notifica a las capas superiores si se está logrando la calidad requerida, utiliza reconocimientos, números de secuencia y control de flujo, en pocas palabras es la integridad de datos de extremo a extremo o sea que se encarga el flujo de datos del transmisor al receptor verificando la integridad de los mismos por medio de algoritmos de detección y corrección de errores.

## **Nivel de Red**

La capa de Red es la encargada de la información de enrutador e interceptores y aquella que maneja el Hardware (HW), ruteadores, puentes, multiplexores para mejorar el enrutamiento de los paquetes.

## **Enlace de Datos**

Es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar, se aplica en el contexto de redes WAN y LAN ya que como se estableció previamente la transmisión de datos no es más que el envío en forma ordenada de bits de información. Es el encargado de ofrecer un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores. Es en este nivel y mediante algoritmos como CRC (Cyclic Redundancy Check), donde se podrá validar la integridad física de la trama; mas no será corregida a este nivel sino que se le notificará al transmisor para su retransmisión, se lleva a cabo el direccionamiento físico de la información; es decir, se leerán los encabezados que definen las direcciones de los nodos (para el caso WAN) o de los segmentos (para el caso LAN) por donde viajarán las tramas. En Resumen se puede decir que la capa de Enlace de Datos es aquella que transmite la información como grupos de bits, o sea que transforma los bits en frames o paquetes por lo cual si recibimos se espera en conjunto de señales para convertirlos en caracteres en cambio si se manda se convierte directamente cada carácter en señales ya sean digitales o analógicos. La capa de Enlace de Datos denominada MAC (es un conjunto de protocolos de las redes inalámbricas que controla cómo los distintos dispositivos se comparten el uso del espectro radioeléctrico), se encarga de describir como se empaacan y verifican los bits de modo que no tengan errores en las redes.

## **Nivel Físico**

Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar, como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación. En Resumen se dice que la capa Físico transmite el flujo de bits sobre un medio físico y aquella que representa el cableado, las tarjetas y las señales de los dispositivos.

Cabe mencionar que la capa Mac define los procedimientos que hacen posible que los distintos dispositivos compartan el uso de este espectro radioeléctrico. Mientras que las distintas versiones del estándar 802.11 utilizan distintos sistemas para difundir su señal (su capa física es distinta), la capa MAC es la misma para todas ellas. Es muy similar a la utilizada por la red Ethernet, ambas utilizan técnicas conocidas como CSMA (Carrier Sense Multiple Access, Acceso Múltiple por Detección de Portadora), sin embargo la versión cableada

utiliza la tecnología CD (Collision Detection, Detección de Colisión), mientras que la versión inalámbrica utiliza la tecnología CA (Collision Avoidance, Evitación de Colisión).

Una colisión se produce cuando dos terminales intentan hacer uso del medio físico simultáneamente. La tecnología CD detecta que se ha producido una colisión y retransmite los datos, mientras que la tecnología CA dispone de procedimientos para evitar que se produzcan colisiones.

La razón de que haya dos sistemas es que, cuando el medio es un cable, un terminal puede transmitir y recibir al mismo tiempo, por lo que puede detectar las colisiones y cuando el medio es radioeléctrico un terminal no puede transmitir y recibir al mismo tiempo por el mismo canal (la transmisión dejaría opaca la recepción), por lo cual se tiene que hacer uso de una técnica que las evite.

La Capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía RF de la antena y determinando la fuerza de la señal recibida. Esta señal medida es conocida como RSSI, si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío. Y a la capa se le da el estado del canal vacío para la transmisión de los datos y si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares. El estándar proporciona otra opción CCA que puede estar sola o con las medidas RSSI. El sentido de la portadora puede usarse para determinar si está disponible.

Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11, el mejor método a utilizar depende de los niveles de interferencia en el entorno operativo.

### 2.3. Software.

Prácticamente aquí se incluye todo lo relacionado con los programas utilizados para el correcto funcionamiento de la red Wlan, desde sistemas operativos, controladores y estándares.

En la conexión inalámbrica de radiofrecuencia (en abreviatura RF) es una de las mejores opciones. La RF es el tipo de red inalámbrica más flexible y más rápida. La conexión inalámbrica RF se presenta en diferentes versiones, todas las cuales comienzan con el número 802.11. A continuación un desglose de estos estándares de red operativa RF:

- ◆ 802.11. Esta versión fue la red operativa original RF, que aportaba de 1 a 2 Mbps (alrededor de la décima parte de la velocidad de la tradicional red Ethernet) y operaba en la gama de 2.4 GHz. Esta tecnología presentaba ciertos problemas de interferencia frecuencial que se corrigieron en las versiones posteriores, con más velocidad.
- ◆ 802.11a. Este estándar se puede adquirir normalmente en las gamas de 6, 12 y 24 Mbps, si bien alcanza hasta los 54 Mbps. Utiliza frecuencias situadas en la gama de 5 GHz. Además, esta versión incorpora también cierto nivel de resistencia a las interferencias frecuenciales radioeléctricas.
- ◆ 802.11b. Mejorando la versión 802.11a, este estándar opera en la gama de 2.4GHz y puede funcionar con el equipamiento anterior del 802.11 (lo que significa que es compatible con el 802.11). La diferencia entre el 802.11b y el 802.11 es que el primero ha incorporado ciertas mejoras para evitar las interferencias de señal y puede superar la velocidad de 11Mbps en la transmisión de datos.
- ◆ U.S. Robotics 22Mbps 802.11b. Estos productos son compatibles con los estándares más antiguos 802.11b, y con los productos más modernos 802.11g. Estos productos tienen una velocidad de transmisión de datos que llega hasta el doble de la versión 802.11b, además de dar mayor cobertura aunque las computadoras estén a mayor distancia mantienen su interconexión, y mejoran el nivel de seguridad de la versión 802.11b.
- ◆ 802.11g. El siguiente estándar opera en la gama de frecuencias de 2.4GHz y puede alcanzar una velocidad de transmisión de datos de hasta 54 Mbps dentro de una distancia limitada. Es compatible con la versión 802.11b y funcionará tanto a 11 como a 22 Mbps con productos inalámbricos de U.S. Robotics. El estándar 802.11g es uno de los “grandes avances” de la



versión 802.11 y ofrece todas las mejores prestaciones de las variantes 802.11a y 802.11b.

Como ejemplo en una oficina u hogar puede incluir varios dispositivos que compitan por el mismo espectro de frecuencia sin licencia que utilizan las redes inalámbricas de la norma 802.11, éstas incluyen los dispositivos Bluetooth, los hornos de microondas y los teléfonos inalámbricos; todos ellos pueden ocasionar interferencia en la red, hay una carencia de estándares industriales bien definidos para atender la necesidad de una administración eficaz de las redes inalámbricas.

Dos soluciones que hoy por hoy lideran el sector son HomeRF y Wi-Fi (IEEE 802.11b), de estas dos, las tecnologías 802.11 disponen de una mayor aceptación en el mercado y están destinadas a solucionar las necesidades de las redes LAN inalámbricas para zonas activas empresariales, domésticas y públicas.

La alianza Wireless Ethernet Compatibility Alliance trabaja para proporcionar certificados de compatibilidad con los estándares 802.11, lo que ayuda a garantizar la interoperabilidad entre los distintos fabricantes, los estándares IEEE 802.11, principalmente 802.11b, y la solución propuesta por el grupo de trabajo HomeRF. Ambas soluciones no son interoperables entre sí ni con otras soluciones de redes LAN inalámbricas.

HomeRF está diseñado exclusivamente para el entorno doméstico, 802.11b se está implementando en hogares, en la pequeña y mediana empresa, en grandes organizaciones y en un número cada vez mayor de zonas activas de redes inalámbricas públicas. Algunos de los principales distribuidores de portátiles los equipa o tiene previsto equiparlos con tarjetas NIC 802.11b internas.

En la siguiente tabla se muestra una comparación de los estándares inalámbricos <sup>1</sup>:

CARACTERISTICA	802.11a	802.11b	802.11g	HiperLAN2
Regulador	IEEE (USA)	IEEE (USA)	IEEE (USA)	ETSI (EUROPA)
Banda de frecuencia	5 GHz	2.4 GHz	2.4 GHz	5 GHz
Modulación	OFDM	DSSS	OFDM	OFDM
Velocidad máxima	54 Mbps	11 Mbps	54 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	54,36,27,18,12,9 y 6
Número de canales sin sobreposición	8	3	3	8
Ancho de banda en un área.	432 Mbps (8x54)	33 Mbps (3x11)	162 Mbps (3x54)	432 Mbps (8x54)
Usuarios en un área	512	192	192	512
Eficiencia por canal (throughput)	18 Mbps	6 Mbps	12 Mbps	31 Mbps
Compatibilidad	Wi-Fi5	Wi-Fi	Wi-Fi	
A destacar	Alta velocidad y número de usuarios	Buen alcance y consumo de potencia	Compatibilidad on 802.11b y más alcance que 11a	Integrado en sistemas 3G (UMTS) y soporta QoS

<sup>1</sup>Tabla obtenida de Carballar Falcón, José A. *Cómo construir una red inalámbrica*.

# CAPÍTULO 3

# SEGURIDAD

## CAPÍTULO 3 SEGURIDAD

### 3.1. Los riesgos.

En las redes inalámbricas existen varios riesgos, entre los más comunes están la pérdida del equipo, infección de un virus, uso equivocado por personas autorizadas, uso fraudulento por personas no autorizadas, además de la falta de utilización del estándar con características básicas de seguridad en toda la industria es la causa más común de acceso no autorizado a una red.

En el caso de la pérdida del equipo de cómputo se puede hacer mención de los factores que la pueden provocar como son: factores ambientales como el fuego, la humedad, las inundaciones, el calor o el frío y los fallos en el suministro de energía; y contra interferencias humanas pueden ser planeado o accidental.

Los virus son programas informáticos que pueden directamente producir daños en la computadora y pueden ser utilizados para conseguir otros fines haciendo uso de la computadora o de la red en la que se elija.

También se puede dar el caso que al no existir restricciones para un usuario haga mal uso de sus privilegios o puede equivocarse, al hacer una ejecución.

En el caso de las personas no autorizadas, lo pueden hacer desde la misma computadora o desde otro lugar aprovechando las ventajas que brindan las redes inalámbricas, estas personas pueden:

- ◆ Escuchar: Con un receptor adecuado, los datos emitidos por un usuario pueden ser recogidos por terceras personas. Con la ayuda de programas como Airopeek, Aircrack-ng, NetStumbler o Wepcrack se puede saber si se encuentra el sistema WEP habilitado o no, además de saber la dirección MAC o el SSID.

- ◆ Acceder: Se configura un dispositivo para acceder a una red a la cual no se está autorizado.
- ◆ Romper la clave: Consiste en intentar adivinar la clave mediante varios intentos.
- ◆ Saturar: Se deja fuera de servicio la red y no puede ser utilizada ni por sus usuarios. Se satura el medio radioeléctrico con suficiente ruido, como para que sea imposible llevar a cabo cualquier comunicación.

La mayoría de estos ataques se producen mediante previa exploración de las redes inalámbricas. Esto, es conocido como War Driving, consiste en descubrir puntos de acceso mientras se conduce por la ciudad con una computadora portátil. Incluso si se añade un GPS, se puede ir tomando nota de las coordenadas exactas de los puntos de acceso.

Otro factor de riesgo que existe en las redes WLAN radica en su capacidad de extender la red de la corporación más allá de los límites físicos convencionales, es por ello que se deben proteger sus estaciones de trabajo, por lo que es recomendable instalar y reforzar la protección en los dispositivos habilitados para redes WLAN, todos los dispositivos WLAN necesitan contar con un firewall.

En la siguiente tabla se muestran algunas amenazas<sup>2</sup>:

<b>Amenaza</b>	<b>Descripción de la amenaza</b>
Interceptación (revelación de datos)	La interceptación de transmisiones de la red puede dar lugar a la revelación de datos confidenciales y de credenciales de usuario sin protección, además de a una posible usurpación de la identidad. Permite también que intrusos expertos recopilen información sobre los entornos de TI y la utilicen para atacar otros sistemas o datos que, de otra forma, no serían vulnerables.
Interceptación y modificación de los datos transmitidos	Si un atacante logra obtener acceso a la red, puede introducir un equipo falso que intercepte y modifique los datos comunicados entre dos usuarios autorizados.
Imitación	El acceso directo a la red interna permite que el intruso falsifique datos que parecen legítimos de manera que no sería posible desde fuera de la red, por ejemplo, un mensaje de correo electrónico de un usuario imitado. Los usuarios, incluso los administradores de sistemas, suelen confiar en los elementos originados dentro de la red mucho más que en los que proceden del exterior de la red corporativa.
Denegación del servicio (DoS)	Un agresor determinado puede activar un ataque de DoS de diversas maneras. Por ejemplo, la interrupción de las señales de radio se puede activar mediante algo tan simple como un microondas. Existen ataques más complejos cuyo objetivo son los protocolos inalámbricos de bajo nivel, y otros menos complejos cuyo objetivo son las redes mediante un gran incremento del tráfico aleatorio en la WLAN.
Carga libre (o robo de recursos)	Es posible que los intrusos sólo deseen utilizar su red como punto de libre acceso a Internet. Si bien esto no es tan grave como las demás amenazas, hará que, como mínimo, no sólo empeore el nivel de servicio prestado a los usuarios autorizados sino también que puedan introducirse virus y otras amenazas.
Amenazas accidentales	Algunas características de las WLAN facilitan la aparición de amenazas no intencionadas. Por ejemplo, un visitante autorizado podría iniciar el equipo portátil sin la intención de conectarse a la red, pero se conecta a su WLAN automáticamente. Así, el equipo portátil del visitante se convierte en un punto de entrada de virus en la red. Este tipo de amenaza sólo se da en WLAN desprotegidas.

<sup>2</sup> Tabla obtenida de <http://www.microsoft.com/>.

### 3.2. Seguridad en redes inalámbricas.

Como es evidente que ningún sistema de seguridad es completamente seguro, el objetivo de un sistema de seguridad es permitir el acceso a cualquier persona autorizada e impedirlo a cualquier otra no autorizada.

Sin embargo las redes Wlan tienen una desventaja ya que carecen de barreras físicas, esto las hace vulnerable a cualquier persona con conocimientos mínimos sobre seguridad y con una tarjeta Wi-Fi en su computadora puede, acceder a un punto de acceso de una red inalámbrica.

Y si a esto le aumentamos que la mayoría de los usuarios no le dan importancia a la seguridad y dejan la configuración del sistema como lo trae (depende del fabricante), y cuando alguien quiera entrar en el sistema lo primero que hará es comprobar si todavía tiene la configuración inicial y de esta forma el acceso al intruso es más fácil.

Por eso las redes inalámbricas vienen provistas con algunas medidas de seguridad, para evitar que personas ajenas al sistema tengan acceso, de esto se ha encargado el Instituto de ingenieros eléctricos y electrónicos (IEEE), junto con otros organismos normativos y consorcios, han mejorado los estándares de seguridad inalámbrica para permitir que las WLAN sean más seguras en conjunto con organismos normativos y los líderes del sector. Las WLAN pueden implementarse y utilizarse actualmente con un gran nivel de confianza en su seguridad.

Cuando se desarrollaron los primeros estándares para WLAN, IEEE 802.11, la seguridad no era un tema tan importante como lo es hoy, debido a que no se daban casos de amenazas a la seguridad de las WLAN y si se llegaban a dar eran muy pocos y no representaban un grave peligro a las WLAN, entonces surge ya la preocupación de la seguridad en las WLAN de primera generación, conocido como privacidad equivalente por cable (WEP). La WEP subestimó las medidas necesarias para "igualar" la seguridad del aire a la seguridad del cable. En contraposición, los métodos de seguridad de WLAN modernos se diseñaron para trabajar en un entorno hostil como el aire donde no existen unos perímetros físicos o de red claros.

Según estudios que se han realizado, demuestran que las redes inalámbricas (IEEE 802.11) no son suficientemente seguras, ante esto responde WECA (la asociación de fabricantes de productos y servicios inalámbricos que certifica los equipos Wi-Fi) que los ataques descritos siempre utilizan sistemas sofisticados que necesitan un esfuerzo y tiempo considerable para llevarlos a cabo y que WEP sigue siendo seguro, pero la verdad WEP no fue diseñado para ser un sistema de seguridad total.

WEP (*Wired Equivalent Privacy*, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802.11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.

WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación. Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional.

Es importante mencionar que la WEP estática de primera generación utiliza una contraseña compartida para proteger la red y los esquemas de seguridad que utilizan el cifrado WEP junto con una administración de claves de cifrado y una autenticación segura. Es decir que es un esquema de seguridad completo que incluye autenticación y protección de datos. Por otra parte, la WEP dinámica, define sólo el cifrado de datos y el método de integridad empleado como parte de soluciones más seguras.

Según el estándar, WEP debe proporcionar confidencialidad, autenticación y control de acceso en redes WLAN. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar obliga a escribir la clave manualmente en cada uno de los elementos de red, esto resulta complicado porque la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.



Para brindar un nivel alto en seguridad inalámbrica, se han unido la Alianza Wi-Fi, junto con el IEEE, y han sacado al mercado un nuevo producto (sistema de seguridad), conocido como WPA (Wi-Fi Protected Access, Acceso Wi-Fi Protegido).

WPA son especificaciones basadas en el estándar IEEE 802.11i que mejora fuertemente el nivel de protección de datos y el control de acceso de las redes inalámbricas Wi-Fi y la ventaja es que es compatible con las redes ya existentes y con el futuro sistema de seguridad integrada proporcionado por IEEE 802.11i.

### 3.3. Medidas de protección.

La forma de tener seguridad en las redes inalámbricas es de tener las técnicas adecuadas, sin embargo hay que estar conscientes de que ninguna técnica de protección es segura al cien por ciento.

Siempre van a existir riesgos, pero entre mayor sea el número de barreras de seguridad, menor será el riesgo. A continuación se presentan algunos de los riesgos que preocupan en el uso de cualquier tecnología de red: Pérdida del equipo, Infección por virus, uso equivocado por personas autorizadas, uso fraudulento por personas no autorizadas.

- ◆ Pérdida del equipo: Es importante evitar la pérdida del equipo o robo y de preferencia nunca dejar grabados en el equipo los nombres de usuarios y contraseña, menos escribir en papel.
- ◆ Infección por virus: Proteger el equipo con un Software antivirus.
- ◆ Uso equivocado por personas autorizadas: Esto puede ser intencionado o accidental, por ello es importante tener políticas de seguridad, para definir los puntos importantes que se deben tener en cuenta.
- ◆ Uso fraudulento por personas no autorizadas: Cambiar las claves de acceso y activar las medidas de seguridad no configuradas por defecto.

Una de las formas más simples para mantener la seguridad informática es mediante las claves de acceso, para ello es necesario que tenga una longitud mínima de seis caracteres, que no tenga significado, que no corresponda a las iniciales del nombre del usuario ni de la empresa, que no sea una letra repetida, que no este formada por letras contiguas del alfabeto, que no este formada por teclas contiguas del teclado, que mezcle letras mayúsculas, minúsculas y números y por último que se cambie constantemente las claves de acceso.

Otras recomendaciones de Weca es que no se debe decir nunca la clave, evitar el uso de claves estáticas, utilizar un firewall y examinar la red constantemente para comprobar que no existan conexiones no autorizadas.

Los principales proveedores de redes, los organismos reguladores y los analistas han centrado gran parte de sus esfuerzos en encontrar soluciones para hacer frente a estos problemas. De esta forma, se han generado una serie de respuestas a las preocupaciones sobre la seguridad de las WLAN. Las principales opciones son: No implementar tecnología de WLAN, Utilizar VPN para proteger los datos de la WLAN, Mantenerse fiel a la seguridad WEP estática 802.11, Utilizar

IPSec para proteger el tráfico de la WLAN. Utilizar la autenticación 802.1X y el cifrado de datos para proteger la WLAN.

### **3.4. Ventajas e Inconvenientes de una red Wlan.**

Las ventajas de la tecnología WLAN son su libertad de movimientos, sencillez en la reubicación de terminales y la rapidez consecuente de instalación. La solución inalámbrica resuelve la instalación de una red en aquellos lugares donde el cableado resulta inviable, por ejemplo en edificios históricos o en grandes naves industriales, donde la realización de canaletas para cableado podría dificultar el paso de transportes, así como en situaciones que impliquen gran movilidad de los terminales del usuario o la necesidad de disponer de vías alternativas por motivos de seguridad. Las ventajas de la WLAN se dividen en dos categorías principales: ventajas empresariales esenciales y ventajas operativas.

- ◆ Las ventajas empresariales esenciales incluyen productividad mejorada de los empleados, procesos empresariales más rápidos y eficaces, y mayor potencial para elaborar funciones corporativas totalmente nuevas.
- ◆ Las ventajas operativas incluyen costes de administración más bajos y un menor gasto de capital.

Las ventajas empresariales esenciales de las WLAN derivan de la flexibilidad y la movilidad de la plantilla. El personal se puede alejar de las mesas de trabajo y moverse fácilmente por las oficinas sin perder la conexión con la red. Es muy práctico observar algunos ejemplos sobre cómo un incremento de la movilidad y de la flexibilidad de la red puede beneficiar a las empresas.

Los trabajadores móviles que se desplazan de unas oficinas a otras y los teletrabajadores que acuden a la oficina se ahorran mucho tiempo y complicaciones si disponen de un acceso transparente a la red de área local (LAN) corporativa. La conexión es prácticamente instantánea y está disponible desde cualquier lugar con cobertura inalámbrica: no es necesario buscar puertos de red ni cables, ni pedir ayuda, para que le ayude a conectarse a la red.

Los trabajadores pueden permanecer en contacto desde cualquier lugar de la empresa. Utilizando el correo electrónico, los calendarios electrónicos y las tecnologías de chat, el personal puede estar conectado incluso cuando asiste a reuniones o trabaja en otro lugar que no sea su escritorio.

Otra ventaja es de que la información en línea está siempre disponible, de esta manera no será necesario hacer una pausa en las reuniones para esperar un

reporte sobre las cifras del último mes o la actualización de una presentación. Todo ello puede significar calidad y productividad de las reuniones.

Y si a esto le sumamos la comodidad de no estar atado siempre al mismo lugar, porque el personal ya no tendrá que estar siempre en sus escritorios, por lo que si es necesario algún cambio ya sea de escritorio o incluso de oficinas enteras serán más rápidos y fáciles, según lo requieran las nuevas estructuras de los equipos o los proyectos.

Los trabajadores y los procesos empresariales que antes no se veían afectados por la tecnología de la información se beneficiarán de los equipos, las aplicaciones y los dispositivos inalámbricos, que se podrán utilizar en áreas que hasta ahora no contaban con redes, como fábricas, hospitales, tiendas y restaurantes. Las principales ventajas operativas de la tecnología de WLAN son la reducción de los costos operativos y de capital.

El riesgo que supone transmitir sin proteger los datos de una red a cualquiera que se encuentre en las cercanías, existe un número sorprendente de WLAN que se han instalado sin ninguna característica de seguridad activada. La mayoría de las empresas han implementado algún tipo de seguridad inalámbrica; no obstante, suele tratarse de características básicas de primera generación, que no ofrecen una protección adecuada según los estándares actuales. La desventaja es que como no se tienen barreras físicas hace más fácil el acceso a los intrusos.

## CAPÍTULO 4

# APLICACIONES DE LAS REDES LOCALES INALÁMBRICAS.

## **CAPÍTULO 4 APLICACIONES DE LAS REDES LOCALES INALÁMBRICAS.**

### **4.1. Aplicaciones en la organización.**

Actualmente, las redes locales inalámbricas (WLAN) se encuentran instaladas en algunos entornos específicos, como almacenes, bancos, restaurantes, fábricas, hospitales y transporte. Las limitaciones que, de momento presenta esta tecnología ha hecho que sus mercados iniciales hayan sido los que utilizan información tipo "bursty" (períodos cortos de transmisión de información muy intensos seguidos de períodos de baja o nula actividad) y donde la exigencia clave consiste en que los trabajadores en desplazamiento puedan acceder de forma inmediata a la información a lo largo de un área concreta, como un almacén, un hospital, la planta de una fábrica o un entorno de distribución o de comercio al por menor; en general, en mercados verticales.

Las redes inalámbricas son útiles cuando los empleados tienen la necesidad de acceder a la información desde un lugar fuera de su escritorio o de la empresa, talvés en lugares geográficos difíciles de llegar o llevar información, es el caso de los médicos, agentes, personal de mantenimiento, etc.

Por ejemplo en México es el caso de Jumex, le permite una ventaja competitiva en cuanto al servicio al cliente y a su ciclo comercial, desde que se levanta el pedido hasta que llega la mercancía.

Lo anterior es posible gracias a dos aplicaciones del cómputo móvil: una es utilizada de manera externa por más de 60 vendedores y otra de radio frecuencia que se maneja sólo en el interior de la empresa. La tecnología de radio frecuencia cuenta con terminales portátiles dentro de la planta para el registro y la captura de todos los movimientos del producto terminal. Se dividió en tres fases:

1. Ingreso del producto terminado de almacén.
2. Envío de mercancías a los centros de distribución.
3. Entrega al cliente.

Este sistema de cómputo móvil es interno, es decir, a nivel de planta o computadora interna, donde a través de radio frecuencia y código de barras en los productos de Jumex se hace la recepción de materias provenientes de producción.

El cómputo móvil utilizado por los vendedores consta de un software del terminales o punto de venta que corre en equipos portátiles tipo hand held con los que el vendedor sale a la calle, llega al cliente y levanta sus pedidos, para posteriormente transmitirlos de la hand held a un servidor consolidado. Además los vendedores cuentan con una impresora portátil que recibe los datos de la hand

held por medio de rayos infrarrojos para imprimir una especie de ticket de enterado del pedido. De esta forma se gana tiempo en la recepción de los pedidos hacia los centros de distribución. Así, se tiene una forma más ágil de levantar los pedidos y de transmitir a los centros de distribución las necesidades de los clientes. También se disminuye un día en rutas remotas y hasta dos en foráneas. Y cuando los promotores levantan pedidos en lugares difíciles llegar por transporte terrestre para llevar la orden de pedido y entrega de mercancía, con las WLANs se reduce hasta 48 horas la entrega de pedidos. Por tal motivo cada vez más empresas están cambiando sus redes cableadas por redes inalámbricas.

#### **4.2. Red Pública de área local.**

En los últimos años las redes inalámbricas (WLAN, Wireless Local Area Network) tienen gran popularidad en mercados tales como hospitales, fabricas, bodegas, tiendas de autoservicio, tiendas departamentales, pequeños negocios y áreas académicas. Las redes inalámbricas permiten a los usuarios acceder información y recursos en tiempo real sin necesidad de estar físicamente en un sólo lugar esto es lo novedoso del producto y es por ello su gran demanda en el mercado, aunque hay empresas que aun se resisten al cambio.

Con WLANs la red por sí misma es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red y lo más importante incrementa la productividad y eficiencia en las actividades diarias de la empresa ya sea privada o pública, inclusive en lugares donde se brinda servicio al público en general, como es en eventos de espectáculos o compras o para las personas que requieren el uso del servicio de comunicación en los aeropuertos. Un usuario dentro de una red inalámbrica puede transmitir y recibir voz, datos y video dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de hasta 11 Mbps.

Muchos de los fabricantes de computadoras y equipos de comunicaciones como PDAs (Personal Digital Assistants), módems, microprocesadores inalámbricos, lectores de punto de venta y otros dispositivos están introduciendo aplicaciones en soporte a las comunicaciones inalámbricas. Las nuevas posibilidades que ofrecen las WLANs son permitir una fácil incorporación de nuevos usuarios a la red, ofrecen una alternativa de bajo costo a los sistemas cableados, además de la posibilidad de acceder cualquier base de datos o cualquier aplicación localizada dentro de la red.

Una comunidad inalámbrica puede convertirse, con la configuración adecuada, en una red pública y de esta forma puede ofrecer servicios

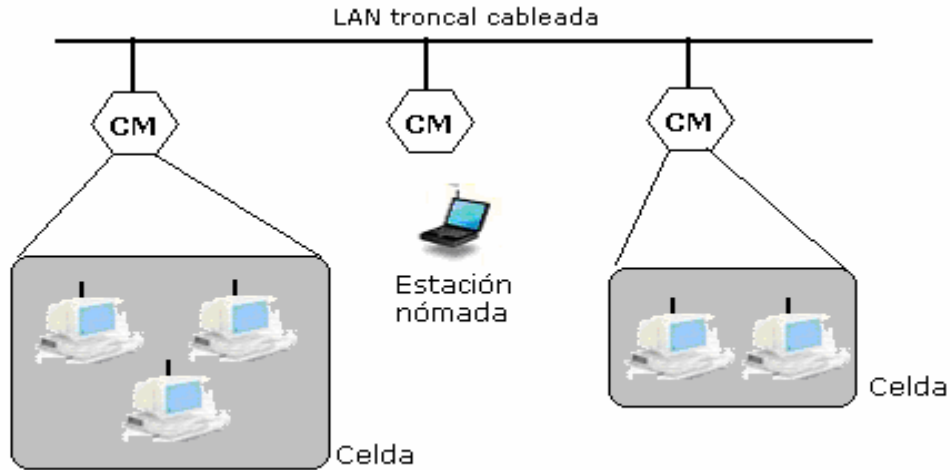
comerciales, por ejemplo para acceder a Internet, para reservaciones, uso de impresoras, programas de red, juegos, almacenamiento de información.

A este tipo de redes se les conoce como redes inalámbricas de acceso público, PWLAN (Public Wireless Local Area Network, Red Pública Inalámbrica de Área Local) o hot-spot (punto caliente).

Al proveedor de este tipo de servicios se le conoce como WIS (Wireless Internet Service Provider, Proveedor de Acceso Inalámbrico a Internet).

También es de gran utilidad en la televigilancia, en guarderías, construcciones y proyectos. Un ejemplo de la utilidad de este tipo de conexiones es posibilitar a un empleado que vuelve de viaje la transferencia de datos desde una computadora portátil a un servidor en la oficina. El acceso nómada resulta útil también en un entorno amplio como es un campus o un centro financiero situado lejos de un grupo de edificios.

En ambos casos los usuarios se pueden desplazar con sus computadoras portátiles y pueden conectarse con los servidores de una LAN inalámbrica desde distintos lugares. En la siguiente figura se puede observar un acceso nómada a una LAN inalámbrica con infraestructura estacionaria con una o más celdas con un módulo de control para cada una; dentro de cada celda pueden existir varios sistemas finales estacionarios. Las estaciones nómadas se pueden desplazar de una celda a otra.



Y también otra novedad es el increíble crecimiento de dos tecnologías emergentes, Red Local (LAN) Inalámbrica y Telefonía IP, se han unido para proveer una nueva y poderosa aplicación: Telefonía IP Inalámbrica.



Primero, el estándar para Redes Locales Inalámbricas (WLAN) 802.11 permitió entregar una solución práctica para redes inalámbricas de múltiples proveedores, y para múltiples aplicaciones. La Alianza Wi-Fi garantiza la interoperabilidad bajo 802.11 por medio de su proceso de pruebas para certificación Wi-Fi (Wireless Fidelity).

Para los clientes, el logotipo Wi-Fi asegura la interoperabilidad entre los puntos de acceso inalámbricos (APs) y los clientes inalámbricos de diversos fabricantes. Para los fabricantes, la interoperabilidad transparente es clave para asegurar que las redes Wi-Fi puedan soportar nuevas aplicaciones emergentes, como voz y video. Segundo, la Telefonía IP ha probado ser una alternativa viable y económica a las redes tradicionales de voz basadas en la conmutación de circuitos. En el mundo IP, particularmente en la LAN, donde la amplia disponibilidad de ancho de banda y el alto grado de control sobre las condiciones del tráfico ayudan a garantizar que la voz y los datos puedan coexistir pacíficamente dentro de la red.

La ubicuidad de las redes IP ha abierto la puerta a nuevas aplicaciones confiables, y con alta calidad de voz tanto en redes alámbricas como inalámbricas.

La Voz, como una aplicación sobre redes IP inalámbricas, presenta una serie de retos muy particulares para las redes Wi-Fi y uno de ellos es entregar audio de calidad aceptable, resultado de minimizar el retraso en la transmisión y recepción de los paquetes en un ambiente mezclado de voz y datos.

Estos son algunos ejemplos de aplicaciones de la Wlan en México:

Cuauhtémoc Naranjo, ejecutivo de Aeroméxico informa que los clientes que son socios del Club Premier tienen servicios de acceso inalámbrico a internet, los cuales utilizan herramientas de seguridad tales como sistemas de autenticación, detección de puntos de acceso no autorizados, encriptación SSL de extremo a extremo y filtrado de contenido, para garantizar el servicio, la compañía implementó soluciones de balanceo de cargas, administración de recursos de ancho de banda y capacidad de roaming para proporcionarles a los usuarios.

Flavio Castorena, director de telecomunicaciones del gobierno del Estado de México, reveló que la convergencia de las redes de voz y datos le permitió comunicar a ocho dependencias, lo cual se traduce en mayor funcionalidad y en ahorros en telefonía que alcanzan los \$2 millones de pesos mensuales.

Por su parte, Marco Espinoza, gerente de Telecomunicaciones de Infonavit, describió las ventajas de contar con una red convergente y otra privada IP en un instituto que tiene como premisa mejorar la atención al derechohabiente; sin embargo, recomendó considerar los costos de los servicios, infraestructura y personal requeridos y conducirse con precaución para evitar riesgos. Reconoció

que la solución convergente es idónea para dar salida a la demanda de servicios de telecomunicaciones que se reflejan en la respuesta a más de 1.2 millones de llamadas al call center y más de 2 millones de vistas al sitio de internet.

Informa Juan Carlos Medina, director de Sistemas de Jumex, que se disminuye en un día en rutas remotas y hasta 2 en rutas foráneas, en el caso de levantamiento de pedidos y entregas de mercancías. También es de gran ayuda para las encuestas dinámicas, que permite que el servidor central se den de alta encuestas y se realicen estudios de mercado, así como análisis de la cartera vencida para saber a qué clientes se les debe cobrar antes de venderles nuevamente.

No es del agrado de todos la tecnología inalámbrica ya que hay algunos que se quejan por los altos costos, sin embargo el lic. Francisco Argüelles (egresado de MAC, especialista en sistemas de Enterasys) comento en el panel ¿Cómo elegir la tecnología inalámbrica correcta?, habló de los retos de la seguridad en wireless, así como de las soluciones que la garantizan y la importancia de una red basada en políticas, interoperable y vigente, pero sobre todo, recomienda ser un usuario informado y con objetivos definidos.

## Conclusiones

Yo creo que las WLAN llegaron a facilitar el trabajo aunque todavía no las adoptamos del todo en nuestro país, sin embargo creo que es sólo el principio de una tendencia creciente.

Considero que me fueron útiles las materias de: Teleproceso, Sistemas de Información, Arquitectura de Computadoras y Optimización Combinatoria, claro que donde le tome amor a las redes fue cuando hice mi servicio social ya que tuve la oportunidad de realizarlo en el área de Redes en el Centro de Computo de la FESA (mi escuela).

Y para que todos tuviéramos un mejor desempeño y aprendizaje sugiero que se de prioridad a los alumnos de MAC, para las áreas de computación al momento de realizar el Servicio Social en la escuela, para de alguna forma estar más conectados a la carrera o implementar prácticas obligatorias, desde el primer semestre en Instituciones Gubernamentales para que cuando uno termine la carrera tenga la experiencia que en todos los trabajos solicitan, y de esta forma reafirmar los conocimientos con la práctica.

Yo en lo personal me siento satisfecha al realizar esta investigación porque he aprendido algo nuevo, que tal vez solo lo sabía muy superficialmente y ahora conozco un poco más a profundidad, el tema y eso me enriquece. Recomiendo que si alguna persona desea dedicarse a esto, primero conozca la teoría y después la practica ya que ambas van de la mano.

## Anexo I: Tipos de antenas.

**Antenas omnidireccionales:** Son aquellas que radian en todas direcciones y también pueden captar la señal procedente de todas las direcciones.

**Antenas direccionales:** Concentran la energía en una sola dirección consiguiendo obtener incrementar el alcance. Cuanto más direccional es una antena, mayor es su alcance.

**Antenas dipolo:** Son las más habituales, un dispositivo emite su señal haciendo que la energía se propague paralela al dipolo y perpendicular al suelo (polarización vertical).

**Antena yagui:** Es una antena direccional con una apertura de haz de entre 15 y 60 grados. Su ganancia varía entre los 6 y los 21 dBi. Estas antenas 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. Esta antena emite energía siguiendo un modelo semiesférico. Tienen ganancias de entre 12 y 22 dBi. Su mayor inconveniente es que, al ser plana, puede sufrir por la fuerza del viento si se sitúan el exterior.

**Antena parabólica:** Es una antena que tiene forma de disco cóncavo con la que se consigue unos haces muy direccionales. Es muy útil para comunicaciones punto a punto y se pueden conseguir ganancias de hasta 27 dBi. En el mercado existen distintas configuraciones de antenas parabólicas: redondas, mayadas, cuadradas, etc.

## Glosario

### 10BaseT

10BaseT es un estándar de IEEE (802.3) para el funcionamiento de redes (LANs) Ethernet de 10 Mbps (megabits por segundo) con cables de par trenzado y un concentrador de conexión.

### 802.11

802.11 es una interfaz a través del aire entre un cliente inalámbrico y una estación base; una familia de especificaciones desarrolladas por IEEE para la tecnología de LAN inalámbrica. 802.11b hace posibles las transmisiones a 11 Mbps en el ancho de banda de 2,4 GHz. El estándar 802.11a emergente utiliza el ancho de banda de 5 GHz, el cual tiene menos uso, y transmite los datos de forma inalámbrica a 54 Mbps.

### 802.11a

802.11a describe el estándar de red inalámbrica para una WLAN que funciona en la banda de radio de 5 GHz (ISM, la banda de frecuencia Industrial, científica y médica). Las WLAN basadas en 802.11a pueden obtener una velocidad máxima de 54 Mbps, lo que es una velocidad de datos casi cinco veces más rápida que el estándar 802.11b y pueden manejar más tráfico que las redes basadas en 802.11b.

### 802.11b

802.11b (conocido habitualmente como "Wi-Fi") describe el estándar de red inalámbrica de IEEE para una WLAN que funciona en la banda de radio de 2.4 GHz (ISM, la banda de frecuencia Industrial, científica y médica). Las WLAN basadas en 802.11b son mucho más habituales que las redes 802.11a o 802.11g y pueden conseguir una velocidad de datos máxima de 11 Mbps a una máxima distancia de aproximadamente 90 metros. 802.11b fue la primera tecnología WLAN que se ofreció a los consumidores e hizo posible la creación de redes inalámbricas instantáneas en las oficinas y los hogares. Los dispositivos certificados por la Alianza Wi-Fi llevan el logotipo oficial de Wi-Fi.

### 802.11g

802.11g es un estándar propuesto que describe un método de red inalámbrica para una WLAN que funciona en la banda de radio de 2.4 GHz (ISM, la banda de frecuencia Industrial, científica y médica). Mediante la tecnología OFDM (Orthogonal Frequency Division Multiplexing), las WLAN basadas en 802.11g podrán obtener una velocidad máxima de 54 Mbps. Los equipos compatibles con 802.11g, tal como los Puntos de acceso inalámbricos, podrán ofrecer la conectividad WLAN simultánea para los equipos 802.11g y 802.11b.

### Alianza Wi-Fi

Es una asociación internacional formada en 1999.

### Antena parabólica o plato satelital

Es un tipo de antena de reflector parabólico diseñado con el propósito específico de transmitir señales a y/o de recibirlas de satélites.

### AP (Punto de acceso)

Un punto de acceso inalámbrico es un concentrador que conecta varios clientes inalámbricos a una red local o a Internet. El punto de acceso puede ser un dispositivo de hardware autónomo o un equipo con un adaptador de red inalámbrico y el software apropiado. Los puntos de acceso inalámbricos están disponibles para 802.11a, 802.11b y banda doble 802.11 a/b (puntos de acceso con capacidad tanto para 802.11a como para 802.11b).

### Adaptador de red USB inalámbrico

Un adaptador de red USB inalámbrico es un adaptador de red inalámbrico que conecta un equipo a una red inalámbrica mediante el puerto USB del equipo, en lugar de enchufarse en el CardBus o el bus PCI (véase también Tarjeta PC inalámbrica). El adaptador de red USB inalámbrico proporciona la misma funcionalidad que la tarjeta PC inalámbrica o el adaptador de red inalámbrico interno, pero se instala más rápido y se puede mover de un equipo a otro.

### Alcance

Distancia física a través de la cual una red inalámbrica funciona de forma fiable. La mayoría de los sistemas Wi-Fi admiten un alcance de cien pies o más. Según el entorno y el tipo de antena utilizado, las señales Wi-Fi pueden tener un alcance de hasta una milla.

### Ancho de banda

Capacidad de transmisión de una red. El ancho de banda disponible depende de diversas variables, tales como la velocidad de transmisión de datos entre los dispositivos de la red, la sobrecarga de la red, la cantidad de usuarios y el tipo de dispositivo que conecta los equipos a la red. El ancho de banda es similar al diámetro de un conducto: entre más ancho es el conducto, mayor cantidad de agua fluirá cada segundo. Del mismo modo, entre más amplio es el ancho de banda, más datos podrán transmitirse cada segundo. El ancho de banda 802.11b estándar especifica un ancho de banda de 11 Mbps (megabits por segundo); 802.11a y 802.11g brindan un ancho de banda de 54 Mbps (véase Bits por segundo).

### Antena de diversidad

Sistema que utiliza dos antenas para optimizar la calidad de recepción y transmisión a la vez que reduce la interferencia.

### BPS (Bits por segundo)

Medida de la velocidad de transmisión de datos a través de líneas de comunicación. Indica la cantidad de bits que se pueden enviar o recibir cada segundo. Con frecuencia, se confunden los bits con segundo (bps) con los bytes por segundo (Bps). Los "bits" se utilizan para medir la velocidad de transmisión y los bytes para medir la capacidad de almacenamiento. Ocho bits de datos equivalen a un byte. Por lo tanto, si una red inalámbrica opera a un ancho de banda de 11 megabits por segundo (11 Mbps o 11 Mbits/s), envía los datos a 1,375 megabytes por segundo (1,375 MBps).

### Banda ancha

Este término se aplica a la transmisión de datos de alta velocidad, tal como cable, ISDN (Red digital de servicios integrados) y DSL (Línea de suscripción digital). Las tecnologías de banda ancha ofrecen conexiones más rápidas a Internet que los servicios de acceso telefónico tradicionales. Los servicios de banda ancha brindan acceso de alta velocidad a Internet a hogares y empresas, a la vez que liberan las líneas telefónicas para el uso simultáneo tradicional de voz. Al utilizar un servicio de banda ancha en equipos portátiles y de desktop, los usuarios tienen acceso a alta velocidad a Internet, correo electrónico y más.

### Bluetooth

Bluetooth es una tecnología de radio de corto alcance (2,4 GHz) que simplifica la comunicación entre los dispositivos de red y entre los dispositivos e Internet. También simplifica la sincronización de datos entre los dispositivos de red y otros equipos. Debido a que la tecnología Bluetooth no está diseñada para llevar cargas de alto tráfico, no es una tecnología apropiada para LAN o WLAN.

### Bridge

Puente. Es un dispositivo que interconecta dos redes que utilizan el mismo protocolo haciéndolas funcionar como si se tratara de una red. Los puntos de acceso hacen la función de bridge.

### Byte

Unidad de almacenamiento que puede alojar un solo carácter. La unidad más pequeña de información de un equipo es un bit. Un byte consiste de 8 bits consecutivos de información. La memoria se indica en términos de kilobytes (1.024 bytes), megabytes (1.048.576 bytes) y gigabytes (1.073.741.824 bytes).

### Capa de Enlace de Datos

Prepara la información a transmitir en trenes de bits (0 y 1 lógicos), representados internamente por impulsos de corriente continua. Para su transmisión por los medios de red, el host emisor debe transformar estas señales continuas en señales en corriente alterna, y para ello usa un sistema de codificación, generalmente el de Manchester, creando ondas pulsantes basadas en las series

de ondas de Fourier. Normalmente este proceso se lleva a cabo en chips especiales de la tarjeta de red del host o en dispositivos especiales, como un modem. Cuando los trenes de bits han sido convertidos en señales apropiadas, éstas son enviadas por los medios físicos hasta el host destino, en donde se procede el proceso inverso, transformándose las señales en sus trenes de bits originales, pudiendo ser procesados entonces por los diferentes protocolos de capa, recuperándose el mensaje original.

#### Capa Física

Transmite el flujo de bits sobre un medio físico y aquella que representa el cableado, las tarjetas y las señales de los dispositivos.

#### CRC (Cyclic Redundancy Check)

Comprobación Cíclica de Redundancia. Son unos datos adicionales que se adjuntan al final de la información para poder comprobar fácilmente que no ha habido errores en la transmisión. Los datos CRC son el resultado de hacer determinadas operaciones matemáticas con la información original. Como las operaciones son las mismas en origen y en destino, si el resultado no es el mismo, es que hay error en la transmisión.

#### Enrutador

Dispositivo que envía paquetes de datos de una red de área local (LAN) o red de área amplia (WAN) a otra. Dependiendo de las tablas y los protocolos de enrutamiento, los enrutadores pueden leer la dirección de red en cada marco transmitido y elegir la ruta de transmisión más eficaz, según las condiciones de tráfico, coste de línea, velocidad, conexiones fallidas y otros factores (véase Enrutador inalámbrico).

#### Enrutador inalámbrico

Dispositivo de red que enruta el tráfico IP a través de varias redes cableadas e IP inalámbricas. Los enrutadores inalámbricos se utilizan para construir WLAN independientes que se pueden comunicar entre sí y con Internet. Algunos puntos de acceso pueden funcionar ya sea como puerta de enlace inalámbrica o como enrutador inalámbrico, mientras que otros dispositivos funcionan solamente como enrutador inalámbrico (véase enrutador).

#### Espectro Expandido

Es un sistema de difusión de las señales radioléctricas. Este sistema utiliza un ancho de banda mayor al estrictamente necesario a cambio de conseguir reducir la vulnerabilidad a las interferencias y garantizar la coexistencia con otras transmisiones.

#### Ethernet

Es un tipo particular de red de área local. Tiene la particularidad de utilizar el mismo protocolo de comunicaciones que Internet (TCP/IP).

FCC (Federal Communications Commission).



Organismo gubernamental encargado del control y regulación del sector de las Telecomunicaciones en los Estados Unidos.

### Firewall

Es un código de programa que se graba en las unidades de hardware de los equipos. A través del firmware los fabricantes consiguen actualizar el hardware sin cambiar un chip. Estos códigos se guardan en unos chips de memoria conocidos como PROM. Estos chips tienen la particularidad de que no se borran cuando no tienen alimentación eléctrica y pueden ser reprogramados.

### Gateways

Son el enlace de conmutación entre la constelación satelital Globlastar y la red pública de telefonía. Estos reciben las transmisiones desde los satélites en órbita y las encaminan hacia la red terrena apropiada, un Gateways puede dar servicio a más de un país y esta conformado por 4 antenas y el equipo de transmisión, recepción y señalización, necesario para el control operacional y administrativo.

### GHz

Gigahertzio, equivale a un billón de ciclos por segundo.

### GPS

Sistema de localización geográfica vía satélite capaz de dar la localización de una persona u objeto dotado de un transmisor-receptor GPS con una precisión mínima de 10 metros. Es un sistema desarrollado y operado por el Departamento de Defensa de los EE.UU. Rusia tiene un sistema propio y la Unión Europea proyecta desarrollar el suyo.

### GSM (Sistema global para comunicaciones móviles)

Estándar mundial de comunicación celular digital que utiliza el acceso múltiple por división de tiempo (TDMA) de banda angosta, para la voz y el servicio de mensajes cortos (SMS). Un 56% de las suscripciones celulares del mundo utilizan la tecnología GSM, la cual representa la tecnología celular de mayor uso en el mundo. (Fuente: Gartner Dataquest: Los 20 principales operadores de red del mundo, 2001)

### HZ (hercio)

Abreviatura de la unidad internacional que mide la frecuencia y que es equivalente a la unidad anterior de ciclos por segundo. Un megahercio (MHz) equivale a un millón de hercios. Un gigahercio (GHz) equivale a mil millones de hercios. La frecuencia de energía eléctrica estándar de EE.UU. es de 60 hercios. La banda de frecuencia de radio de difusión AM es de 535 a 1605 kHz y la FM es de 88 a 108 MHz. Las redes locales 802.11b operan a 2,4 GHz.

### IEEE (Instituto de ingenieros eléctricos y electrónicos)

IEEE ( [www.ieee.org](http://www.ieee.org)) es una organización con sede en Nueva York, la cual incluye ingenieros y estudiantes de electrónica y otros campos relacionados. Tiene más de 300.000 miembros y se dedica al establecimiento de normas informáticas y de comunicación.

#### InternetWorking

Este concepto da la idea de sistemas abiertos, y es donde las compuertas tienen lugar cubriendo desde los niveles más bajos de conectividad hasta esquemas de conversión de protocolos que requieren de un alto grado de integración.

#### IP (Protocolo de Internet)

Reglas y especificaciones de codificación para el envío de datos. También determina si la red utiliza una arquitectura de grupos de trabajo o de cliente/servidor. La versión actual de IP es IPv4. Se encuentra en desarrollo una nueva versión denominada IPv6.

#### IrDA (Asociación de datos infrarrojos)

Grupo de fabricantes de dispositivos que desarrollaron un estándar para la transmisión de datos a través de ondas de luz infrarroja.

#### ISA

Industry Standard Architecture, Arquitectura Normalizada de la Industria. Este tipo de tarjetas es más barata que las tarjetas PCMCIA, aunque también son mayores en tamaño y de instalación algo más compleja (entre otras cosas, hay que abrir la computadora).

#### ISM

Son bandas de frecuencias para uso comercial y sin licencia (son las utilizadas por los teléfonos inalámbricos domésticos DECT, los microondas, o los dispositivos BlueTooth).

#### Kbps

Kilobits por segundo. Es una unidad de medida de la velocidad de transferencia de datos. Un kilobit por segundo significa que se transfieren 1.024 bits cada segundo. Un bit es la unidad más pequeña de información (un 0 o un 1).

#### KHz

Kilo hertzio, equivale a mil oscilaciones por segundo.

#### LAN (Red de área local)

Red de equipos que cubre un área relativamente pequeña y por lo general conecta estaciones de trabajo y PC, de modo que los usuarios se puedan comunicar entre sí, compartir datos o tener acceso a dispositivos, tales como impresoras láser. Cuando se conectan varias redes locales entre sí a través de líneas telefónicas u ondas de radio, se conoce como red de área amplia (WAN). El estándar de red

inalámbrica actual para redes locales es 802.11a con velocidades de datos de hasta 54 Mbps en comparación a 11 Mbps del estándar 802.11b. 802.11a permite varios usuarios inalámbricos simultáneos y aplicaciones de multimedia móvil mejoradas, tal como el vídeo fluido. Además, el estándar 802.11a opera en la banda de 5 GHz, la cual no presenta congestión y reduce la interferencia con los teléfonos inalámbricos.

#### MAC (Medium Access Control)

Control de Acceso al Medio. Es un conjunto de protocolos de las redes inalámbricas que controla cómo los distintos dispositivos se comparten el uso del espectro radioeléctrico.

#### Modelo de red ISO (Organización internacional de estándares)

Desarrollado por la Organización internacional de estándares, el modelo de red ISO especifica siete niveles en los protocolos de comunicación. Al estandarizar dichos niveles y las interfaces intermedias se facilita la modificación de distintas porciones de un protocolo dado a medida que las tecnologías avanzan o los sistemas requieren cambios, a la vez que se conserva un modelo de protocolo general estable. Los siete niveles son:

- Físico
- Vínculo de datos
- Red
- Transporte
- Sesión
- Presentación
- Aplicación

El estándar 802.11 comprende el nivel físico (PHY) y la porción inferior del nivel de vínculo de datos. La porción inferior del nivel de vínculo de datos por lo general se denomina subnivel de Control de medios de acceso (MAC).

#### Modulación

Engloba el conjunto de técnicas para transportar información sobre una onda portadora, típicamente una onda senoidal. Estas técnicas permiten un mejor aprovechamiento del canal de comunicación lo que permitirá transmitir más información simultánea y/o proteger la información de posibles interferencias y ruidos.

#### NIC

Network Interface Card en inglés lo que en español viene a ser Tarjeta de Interfaz de Red. El término puede referirse tanto a una tarjeta de red completa como a un sólo chip de ella, en el último caso este chip se encarga de servir como interface de ethernet entre el medio físico (por ejemplo un cable coaxial) y el equipo.

#### Paquete

Un recinto para un único elemento, circuito integrado, o circuito híbrido. Provee

protección hermética y no hermética, determina el factor de forma, y sirve como el primer nivel de interconexión externa del dispositivo mediante los terminales del paquete.

#### Puente

Producto que conecta una red local (LAN) a otra red local que utiliza el mismo protocolo (por ejemplo, inalámbrico, Ethernet o token ring). Los puentes inalámbricos se utilizan de forma común para unir edificios en complejos con varios edificios.

#### 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. El punto de acceso no sólo se utiliza para controlar las comunicaciones con las redes externas (redes cableadas e Internet).

#### Punto de conexión

Ubicaciones públicas tales como aeropuertos, centros comerciales y centros de conferencias que ya cuentan con redes inalámbricas de fácil acceso, generalmente 802.11b u 802.11a.

#### PCI

Peripheral Component Interconnect, Interconexión de Componentes Periféricos. Son unas especificaciones creadas por Intel y que definen un sistema de bus local que permite conectar al PC hasta 10 tarjetas de periféricos. El estándar PCI ha venido a reemplazar al antiguo estándar ISA (Industry Standard Architecture).

#### PCMCIA

Personal Computer Memory Card International Association, Asociación Internacional de Tarjetas de Memoria para Computadoras Personales. Se trata de una asociación de fabricantes de equipos que en 1989 sacó al mercado un tipo de puerto y de dispositivo de pequeño tamaño que permite que se le puedan instalar todo tipo de periféricos a las computadoras personales. En un principio se dedicaron sólo a ampliar la memoria, de ahí su nombre. Tanto el puerto como los dispositivos reciben el nombre de PCMCIA. En inglés se le conoce más coloquialmente como PC Card (tarjeta de PC).

#### SSID (Servici Set identifier)

Identificador del Conjunto de Servicios. Es el parámetro que identifica la red inalámbrica. También se le conoce como nombre de red.

#### Radiación electromagnética

Es una combinación de campos eléctricos y magnéticos oscilantes y perpendiculares entre sí que se propagan a través del espacio transportando energía de un lugar a otro. A diferencia de otros tipos de onda, como el sonido, que necesitan un medio material para propagarse, la radiación electromagnética se puede propagar en el vacío.

### RF (Frecuencia de radio)

Cubre una gama de frecuencias altas electromagnéticas utilizadas en las transmisiones de radio. En la comunicación, las señales RF transmiten datos mediante diversos métodos, tales como TDMA, CDMA, DSSS (secuencia directa de distribución de espectro) y otros. WLAN, PAN, Bluetooth\* y otras tecnologías inalámbricas utilizan señales RF para transmitir datos.

### Red de grupos de trabajo

Red informática inalámbrica o cableada que no tiene un servidor, un concentrador central ni un enrutador. Todos los equipos conectados a la red tienen la misma capacidad de actuar como servidor de red o cliente. Cada equipo cliente puede comunicarse con todos los equipos inalámbricos sin necesidad de hacerlo a través de un punto de acceso o concentrador. No obstante, debido a que no existe una estación central básica para controlar el tráfico o proveer acceso a Internet, las diversas señales pueden colisionar y reducir el rendimiento general.

### ROUTER

Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo software, hardware o una combinación de ambos. Los puntos de acceso, generalmente hacen las funciones de router. A este equipo también se le conoce en español por el nombre de enrutador.

### TCP (Protocolo de transmisión de comunicación)

Protocolo de comunicación utilizado junto con el protocolo de Internet (IP) para enviar datos en forma de unidades individuales (llamados paquetes) entre equipos a través Internet. El protocolo IP se encarga de la entrega de los datos y TCP lleva un seguimiento de los paquetes en los que se divide un mensaje para el enrutamiento eficaz a través de Internet. Por ejemplo, cuando se descarga una página web de un servidor web, nivel de programa TCP del servidor divide el archivo en paquetes, numera los paquetes y los envía de forma individual al nivel de programa IP. Aunque todos los paquetes tienen la misma dirección IP de destino, podrían enrutarse por separado a través de la red. En el otro extremo de la transmisión, TCP vuelve a ensamblar los paquetes individuales y espera hasta que todos han llegado para enviarlos como un solo archivo.

### Tarjeta PC inalámbrica

Adaptador 802.11 WLAN que se inserta en una ranura PCMCIA de equipos portátiles o de desktop. Las tarjetas PC inalámbricas permiten que los usuarios se conecten a redes inalámbricas. También se puede utilizar una tarjeta PC inalámbrica y un PC para compartir una conexión a Internet con una WLAN.

### Telefonía

Transmisión de señales de voz, datos, vídeo o imagen. Con frecuencia se utiliza para designar la integración del teléfono con PC u otros dispositivos. La telefonía

en Internet permite que los usuarios utilicen Internet como medio de transmisión para llamadas telefónicas. Aunque la telefonía en Internet no ofrece la misma calidad que los servicios telefónicos convencionales, permite que los usuarios realicen llamadas telefónicas gratuitas a cualquier parte del mundo. Los productos de telefonía en Internet se conocen como productos de telefonía IP, Voz a través de Internet (VOI) o Voz a través de IP (VOIP).

#### Telefonía IP

Conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y yendo un poco más allá, desarrollar una única red que se encargue de cursar todo tipo de comunicación, ya sea vocal o de datos.

#### Teletrabajo

Es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador de la empresa durante una parte importante de su horario laboral. Engloba una amplia gama de actividades y puede realizarse a tiempo completo o parcial. La actividad profesional en el teletrabajo implica el uso frecuente de métodos de procesamiento electrónico de información, y el uso permanente de algún medio de telecomunicación para el contacto entre el teletrabajador y la empresa.

#### UHF

Ultra High Frequency, así se le llama al rango de frecuencias entre 300 y 3000 MHz (802.11a y 802.11b están en ésta frecuencia).

#### USB

Universal Serial Bus, Bus Serie Universal. Interfaz serie de la computadora que permite conectar hasta 127 dispositivos (impresoras, adaptadores de red, escáneres, monitores, etc.) a una velocidad de 1.5 o 12 Mbps. Además, tiene la particularidad de que no es necesario apagar la computadora para conectar o desconectar los dispositivos.

#### VHF

Very High Frequencies Banda del espectro electromagnético que ocupa el rango de frecuencias de 30MHz a 300MHz.

#### Vídeo conferencia

Permite la comunicación entre dos personas a tiempo real con voz, imagen y sonido.

#### VPN (Red privada virtual)

Conexión de Internet segura que utiliza protocolos de codificación y túnel para crear una conexión segura o túnel con una red privada. Las VPN ofrecen conexiones altamente seguras entre clientes remotos, tales como oficinas

sucursales o personal ambulante, y la oficina central. Está disponible una variedad de enrutadores de VPN tanto para la oficina como para el hogar.

#### War Driving

El Wardriving es la técnica de ir con una computadora portátil en el coche buscando redes inalámbricas abiertas.

#### WECA

La asociación de fabricantes de productos y servicios inalámbricos que certifica los equipos Wi-Fi.

#### WEP (wired Equivalency Protocol)

Protocolo de Equivalencia con Red Cableada. Es el sistema de cifrado de datos que incorpora las redes Wi-Fi. El sistema WEP surgió con la idea de ofrecerle a las redes inalámbricas un estado de seguridad similar al que tienen las redes cableadas.

#### Wi-Fi (Fidelidad inalámbrica)

Nombre que se da a los equipos que cumplen con el estándar inalámbrico 802.11b, tal como lo define la alianza Wi-Fi. Los logotipos de Wi-Fi ayudan a identificar los componentes de red inalámbrica que tienen certificación para funcionar en WLAN 802.11b.

#### WLAN

WLAN son las siglas para Wireless Local Area Network (Red de área local inalámbrica) véase LAN.

## BIBLIOGRAFIA

- ◆ Carballar Falcón, José A. *Cómo construir una red inalámbrica*. México, D.F. 2004 Alfaomega Grupo Editor, S.A. de C.V.
- ◆ Lanic, *La Página de lanic con recursos para estudiantes* [en línea], lanic.utexas.edu, México, 2004, [fecha de consulta: 02 de Mayo del 2005], disponible en: [http://lanic.utexas.edu/la/Mexico/telecom/cap4\\_fn.html](http://lanic.utexas.edu/la/Mexico/telecom/cap4_fn.html).
- ◆ Monografías, *La Página de Monografías es para todo público interesado* [en línea], monografía.com, España, 2003, [fecha de consulta: 02 de Mayo del 2005], disponible en: <http://www.monografias.com/trabajos12/trdecom/trdecom.shtml>
- ◆ Intel, *La Página de Intel* [en línea], Intel.com, México, 2005, [fecha de consulta: 18 de Mayo del 2005], disponible en: [http://www.developer.intel.com/español/business/smallbusiness/wireless/unwire\\_smallbiz.htm](http://www.developer.intel.com/español/business/smallbusiness/wireless/unwire_smallbiz.htm).
- ◆ Support, *La Página de Support es para todo público interesado* [en línea], 2005, [fecha de consulta: 11 de Mayo del 2005], disponible en: <http://www.support.dell.com/support/edocs/network/R48972/sp/help/glossary.htm>.
- ◆ Monografías, *La Página de Monografías es para todo público interesado* [en línea], monografía.com, España, 2003, [fecha de consulta: 02 de Mayo del 2005], disponible en: <http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml>.
- ◆ Wikipedia, *La Página de Wikipedia es un diccionario* [en línea], fecha de consulta: 03 de agosto del 2005, disponible en [http://es.wikipedia.org/wiki/Antena\\_parab%C3%B3lica](http://es.wikipedia.org/wiki/Antena_parab%C3%B3lica).
- ◆ Microsoft, *La página de Microsoft en español, México, 2005, es para todo público interesado*. [fecha de consulta 07 de junio 2005], disponible en: [http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/Job\\_aids/JA1-ThreatTable.asp](http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/Job_aids/JA1-ThreatTable.asp).
- ◆ Developer, *La Página Developer es para todo público interesado* [en línea], 2005, [fecha de consulta: 8 de mayo del 2005], disponible en: <http://www.developer.intel.com/>.
- ◆ Cofetel, [en línea], cft.gob.mx, México, 2005, [fecha de consulta: 11 de Mayo del 2005], disponible en: [http://www.cft.gob.mx/cofetel/html/9\\_publica/acuerdos/17111995.pdf](http://www.cft.gob.mx/cofetel/html/9_publica/acuerdos/17111995.pdf).