# CAPITULO I

## 1. FUNDAMENTACIÓN TEÓRICA DE LA RED INALAMBRICA WLAN

### 1.1. Sistemas de Redes y Tendencia a las Telecomunicaciones

Desde los albores de la humanidad, un tema fundamental con respecto al desarrollo y progreso, ha sido la necesidad de comunicación entre unos y otros, presente a lo largo de la historia. En los últimos años los nuevos logros de la tecnología han sido la aparición de computadores, líneas telefónicas, celulares, redes alámbricas e inalámbricas, así como las satelitales.

El principio de la comunicación se establece mediante el habla en la relación entre emisor, mensaje y receptor. Pero la tecnología de hoy en día no solo debe hacer referencia a la transmisión de voz, sino debe intentar abarcar una mayor gamma de aplicaciones, llámese la transmisión de datos. Dada esta necesidad es que surgen las redes de computadores como la intranet, la extranet y el Internet. Referente al intercambio de voz y datos se hace indispensable la necesidad de estar conectados con el mundo entero a través de la Internet, de donde surgen algunos problemas concernientes a la aplicación de redes alámbricas debido a que se hace necesario el transporte de los equipos ya sea dentro de un local como al interior de alguna oficina.

Al presentarse esta necesidad se hizo parte de un grupo de estudio de mayor envergadura, desde las redes inalámbricas, la transferencia de datos vía

infrarrojo, así como en la aplicación de redes satelitales. Las mismas que han logrado satisfacer esta necesidad logrando la conexión de usuarios existentes en distintos lugares del mundo. La aplicación de la tecnología inalámbrica, viene teniendo un gran auge en velocidades de transmisión, aunque sin competir con la utilización de redes alámbricas o el uso de la fibra óptica, sin embargo cubren satisfactoriamente la necesidad del movimiento de los usuarios.

### 1.1.1. Sistemas de Redes

Una red inalámbrica de área local (Wireless LAN) es un sistema flexible de transmisión de datos implementados como una extensión, o como alternativa, de una red cableada.

Utiliza tecnología de radio frecuencia, transmite y recibe datos utilizando como medio el aire, minimizando la necesidad de una conexión de cable, permitiendo la combinación conectividad y movilidad.

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

La disponibilidad de la tecnología inalámbrica y de las redes (LAN) inalámbricas puede ampliar la libertad del usuario en red, resolver distintos problemas asociados con redes de cableado físico y en algunos casos, hasta reducir los costos de implementar redes. Sin embargo, junto con esta libertad, las redes inalámbricas conllevan también un nuevo conjunto de retos.

Hoy en día, existen varias soluciones para redes inalámbricas disponibles con distintos niveles de estandarización. Dos soluciones que actualmente son líderes en la industria son HomeRF y Wi-Fi™ (IEEE 802.11b). De estas dos, las tecnologías 802.11 cuentan con amplio apoyo en la industria y tienen la intención de resolver las necesidades empresariales del hogar y hasta de puntos de conexión públicos a redes inalámbricas. La alianza Wireless Ethernet Compatibility Alliance está trabajando para proporcionar la certificación de cumplimiento con los estándares 802.11, contribuyendo a garantizar la interoperabilidad entre las soluciones de los múltiples proveedores.

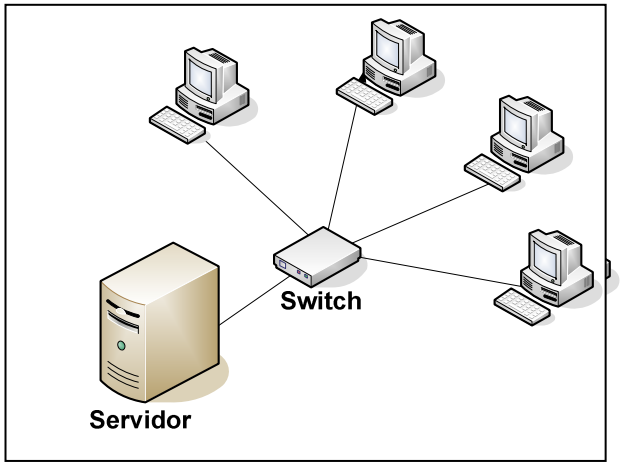
### 1.1.2. Definición

"Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos. A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas".[1]

Los ordenadores suelen estar conectados entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

**GRAFICO 1.1:** REDES

**FUENTE:** EL INVESTIGADOR




[1] RODRIGUEZ Jorge, Introducción a Las Redes De Área Local, McGraw Hill, México, 1998. Pág. 23-29

## 1.2. Elementos de una red inalámbrica

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

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps , las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de solo 10 Mbps.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una “Red Híbrida” y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de Redes Inalámbricas:

**De Larga Distancia.-** Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.

**De Corta Distancia.-** Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas son un medio para transmitir información de alto precio. Debido a que los módems celulares actualmente son más caros y delicados que los convencionales, ya que requieren circuiteria especial, que permite mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos. Otras desventajas de la transmisión celular son:

La carga de los teléfonos se termina fácilmente.

La transmisión celular se intercepta fácilmente (factor importante en lo relacionado con la seguridad).

Todas estas desventajas hacen que la comunicación celular se utilice poco, o únicamente para archivos muy pequeños como cartas, planos, etc. Pero se espera que con los avances en la compresión de datos, seguridad y algoritmos de verificación de errores se permita que las redes celulares sean una opción redituable en algunas situaciones.

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

públicas, pero bajo bandas de radio frecuencia restringida por la propia organización de sus sistemas de cómputo.

### 1.2.1. Servidor

Es la máquina principal de la red. Se encarga de administrar los recursos de ésta y el flujo de la información. Algunos servidores son dedicados, es decir, realizan tareas específicas. Por ejemplo, un servidor de impresión está dedicado a imprimir; un servidor de comunicaciones controla el flujo de los datos, etcétera.

**GRAFICO 1.2:** SERVIDORES
**FUENTE:** REDES DE COMPUTADORAS. ANDREW TANENBAUM

Para que una máquina sea un servidor es necesario que sea una computadora de alto rendimiento en cuanto a velocidad, procesamiento y gran capacidad en disco duro u otros medios de almacenamiento.

**Tipos de servidores**

En la actualidad existen una variedad de servidores para múltiples aplicaciones, que son utilizadas por instituciones públicas y privadas en las cuales podemos citar los siguientes.

**Servidor Web.**

Básicamente, Un servidor Web es un computador preparado y acondicionado para estar permanentemente conectado a una red de alta velocidad. Esta red de alta velocidad forma parte de Internet, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML.

**Servidores de Aplicaciones (***Application Servers***).**

Designados a veces como un tipo de *middleware* (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan. “Los servidores de aplicación también brindan a los desarrolladores una Interfaz para Programación de Aplicaciones (API), de tal manera que no tengan que preocuparse por el sistema operativo”. [2]

**Servidores Proxy** (**Proxy Server).**

Los servidores Proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

**Servidor de Base de Datos**

[2] http://wwww.monografias.com/trabajos18/redes-computadoras/redes-computadores.html

Los Servidores de Bases de datos (MySQL, ORACLE, etc.) permiten aprovechar la estabilidad y seguridad que el sistema operativo Linux le ofrece para maximizar entre otros:

- Manejo de sus bases de datos ya sea desde el mismo servidor o desde sus aplicaciones remotas.
- Sincronización de sus bases de datos o la de sus clientes entre varios servidores.
- Configuración de varios motores de bases de datos de acuerdo con las necesidades particulares, ya sea para manejo interno o remoto.

### 1.2.2. Terminales

Una terminal consiste en un teclado y una pantalla por lo cual puede considerarse un dispositivo para el ingreso de datos.

Algunas vienen como unidades independientes.

Las terminales son también denominadas:

- Terminal (Display Terminal)
- Monitor o Video Display Terminaos (VDT)

Una terminal boba (dumb terminal) no tiene capacidad de procesar o almacenar datos. Está conectada con una minicomputadora, computadora de gran porte o supercomputadora.

El teclado y la pantalla pueden ser de una sola pieza.

Una terminal inteligente o programable puede procesar o guardar información por sí misma, por lo menos hasta cierto punto. Las PC pueden ser usadas como terminales inteligentes.

**Clasificación de los terminales**

Todas son una buena opción como herramienta de soporte ideal para el funcionamiento en el manejo de datos:

**Key Based o Terminales basadas en teclado.**

Cuando se tiene una aplicación de manejo de datos intensiva que requiere una entrada manual de la información, una Terminal portátil de captura de datos con teclado es la respuesta. Construida con un teclado alfanumérico fácil de usar y una pantalla iluminada. Para un alto rendimiento en comunicaciones existen opciones batch y radiofrecuencia.

**Pen based o con pluma por contacto.**

La gran diferencia con estas terminales con pluma por contacto es que no contienen teclado. La información se manipula simulando el uso de una pluma que por contacto permite introducir datos. Estas terminales incrementan la eficacia, efectividad y resisten el uso rudo en trabajo pesado suficiente para trabajar virtualmente en cualquier lugar. Es la herramienta indispensable para trabajadores en movimiento en todas las industrias donde se requiere que la información se recolecte donde sea generada. Como muchas otras terminales portátiles existen opciones batch y radiofrecuencia.

**Montadas en un vehiculo**

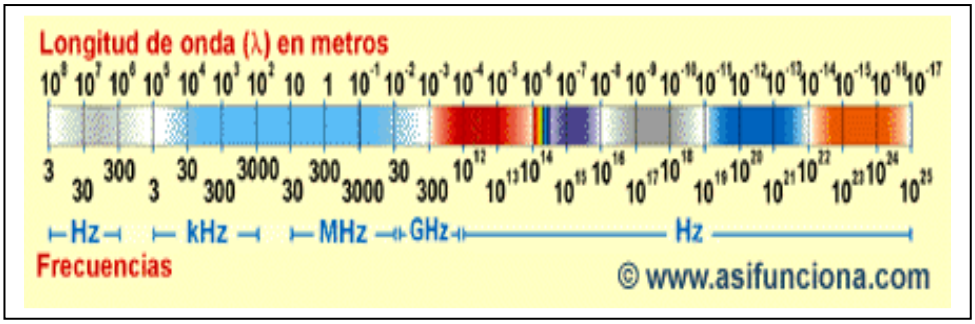
Cuando su necesidad sea contar con un dispositivo montado en un vehículo, como por ejemplo un montacargas, se cuenta con terminales

para la industria móvil. Estas terminales permiten al operador capturar, procesar y comunicar la información dondequiera que se encuentre; además pueden contener un lector de código de barras y permiten transmitir la información a un host remoto.

### 1.2.3. Espectro electromagnético

Se denomina **espectro electromagnético** al conjunto de ondas electromagnéticas o, más concretamente, a la radiación electromagnética que emite (espectro de emisión) o absorbe (espectro de absorción) una sustancia. Dicha radiación sirve para identificar la sustancia de manera análoga a una huella dactilar. Van desde las de menor longitud de onda, pasando por la luz ultravioleta, la luz visible y los rayos infrarrojos, hasta las ondas electromagnéticas de mayor longitud de onda, como son las ondas de radio. [3]

**GRAFICO 1.3:** ESPECTRO ELECTROMAGNÉTICO.
**FUENTE:** WIKIPEDIA, LA ENCICLOPEDIA LIBRE.

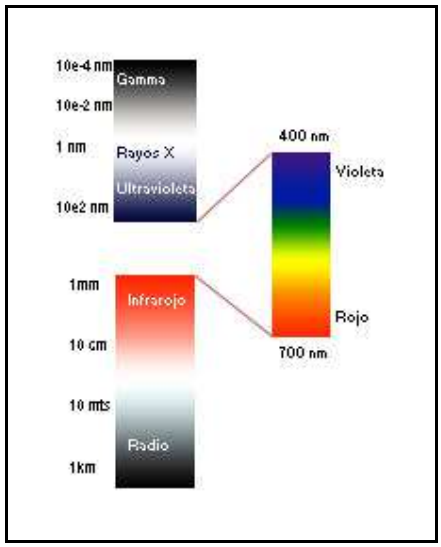



Si las ondas electromagnéticas se organizan en un continuo de acuerdo a sus longitudes obtenemos el espectro electromagnético en donde las

[3] Tomado de: www.wikipedia.net/espectroelectromgtco.htm

ondas mas largas (longitudes desde metros a kilómetros) se encuentran en un extremo (Radio) y las mas cortas en el otro (longitudes de onda de una billonésima de metros) (Gamma).

**GRAFICO 1.4:** ESPECTRO ELECTROMAGNÉTICO.
**FUENTE:** WIKIPEDIA, LA ENCICLOPEDIA LIBRE.




Luz Visible. Isaac Newton fue el primero en descomponer la luz visible blanca del Sol en sus componentes mediante la utilización de un prisma. La luz blanca está constituida por la combinación de ondas que tienen energías semejantes sin que alguna predomine sobre las otras. La radiación visible va desde 384x1012 hasta 769x1012 Hz. Las frecuencias mas bajas de la luz visible (longitud de onda larga) se perciben como rojas y las de mas alta frecuencia (longitud corta) aparecen violetas.

Rayos infrarrojos. La radiación infrarroja fue descubierta por el astrónomo William Herschel (1738-1822) en 1800, al medir una zona más caliente mas allá de la zona roja del espectro visible. La radiación infrarroja se localiza en el espectro entre 3x1011 Hz. hasta aproximadamente los 4x1014 Hz. La banda infrarroja se divide en tres secciones de acuerdo a su distancia a la zona visible: próxima (780 - 2500 nm), intermedia (2500 - 50000 nm) y lejana (50000 - 1mm). Toda molécula que tenga un temperatura superior al cero absoluto (-273º K)

emite rayos infrarrojos y su cantidad esta directamente relacionada con la temperatura del objeto.

Líneas espectrales.

Los átomos poseen un núcleo el cual tiene la mayor parte de su masa y toda su carga positiva. Rodeando al núcleo se encuentra un enjambre de electrones con carga negativa. En estado estable el átomo debe ser neutro, de esta manera, la carga positiva del núcleo se contrarresta con la carga negativa del los electrones.

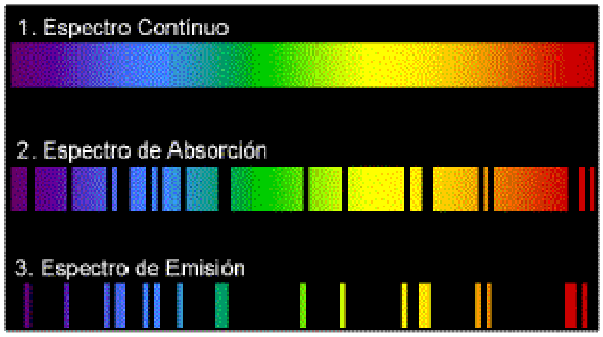
El núcleo está formado por dos tipos de partículas, los protones y los neutrones unidos por una fuerza llamada fuerza nuclear fuerte. Los protones tienen toda la carga positiva y el número de ellos da las características fisicoquímicas al átomo. De cada elemento químico se pueden tener varias formas o isótopos; en los isótopos el número protones se mantiene constante pero no el de neutrones. El hidrogeno por ejemplo tiene dos isótopos muy comunes el 1H y el 2H (deuterio) y uno menos común el tritio 3H. El número que precede al símbolo químico es el número de nucleones (protones y neutrones) que posee.

Los electrones de un átomo solo pueden encontrase en unas órbitas permitidas y no en cualquier posición con respecto al núcleo. Ahora bien, un electrón puede cambiar de una órbita a otra siempre y cuando la de destino esté desocupada. Al pasar un electrón a una órbita mas baja este necesita emitir energía, la cual libera en forma de paquete o cuanto. Para pasar a una órbita más alta requiere absorber energía en forma de cuanto de luz. El cuanto de luz emitido o absorbido es especifico para cada órbita de cada átomo específico. De esta manera al estudiar la energía electromagnética emitida o absorbida por un átomo se puede determinar que tipo de átomo es.

Cuando se tiene un material excitado como por ejemplo un gas calentado por la luz estelar, una gran multitud de sus átomos puede estar sufriendo cambios en la órbita de sus electrones y por este motivo se presenta gran cantidad de absorción y/o emisión de cuantos de energía. El estudio de estos fotones dan las "huellas" de identificación de los átomos presentes en el gas.

Al analizar el espectro proveniente de la luz de un gas o estrella se pueden apreciar "huecos" en el espectro estudiado (líneas espectrales de absorción), corresponden a las longitudes de onda absorbidas por el átomo. Igualmente al estudiar material incandescente podremos ver espectros con líneas característicamente brillantes a las que se denominan líneas de emisión. Las moléculas también emiten y absorben radiación en longitudes características, una de las utilizadas en astronomía es la emisión de 21 cm de las moléculas de hidrogeno.

**GRAFICO 1.5:** ESPECTRO ELECTROMAGNÉTICO.
**FUENTE:** WIKIPEDIA, LA ENCICLOPEDIA LIBRE.




**Cuerpo negro**

Todos los cuerpos emiten radiación electromagnética por el simple hecho de tener cierta temperatura. Para estudiar la liberación de energía por cuerpos calientes se debe considerar un objeto especial de características ideales en el cual toda la luz que absorba no se refleje; a tal objeto se le denomina cuerpo negro. Estos cuerpos negros emiten energía y lo hace

según un espectro característico, durante muchos años no se logró explicar la radiación de energía de un cuerpo negro hasta que Max Plank en 1900 lo hizo suponiendo que la energía se liberaba en paquetes o cuantos. La emisión de energía por parte de las estrella semeja mucho a la de un cuerpo negro (salvo por las líneas de absorción y emisión).

Cuando un objeto emite radiación de manera similar a un cuerpo negro se puede asegurar que esta energía es de tipo térmico; existe sin embargo otro tipo de energía electromagnética de tipo no térmico a la cual se le conoce como radiación sincrotón. Está es producida por partículas cargadas, casi siempre electrones, que giran alrededor de líneas de campo magnético y emiten radiación. La liberación de energía sincrotón tiene como característica que se emite en longitudes de onda muy pequeñas en el rango de los rayos X y Gamma.

Cuando existen líneas espectrales, estas líneas tiene cambios característicos, en presencia de campos magnéticos muy fuertes; las líneas espectrales se desdoblan en parejas con una distancia entre ellas relacionada a la magnitud del campo, a este fenómeno se le conoce como fenómeno de Zeeman.

### 1.2.4. Medio Ambiente

Se entiende por **medioambiente** o **medio ambiente** al entorno que afecta y condiciona especialmente las circunstancias de vida de las personas o la sociedad en su conjunto. Comprende el conjunto de valores naturales, sociales y culturales existentes en un lugar y un momento determinado, que influyen en la vida del hombre y en las generaciones venideras. Es decir, no se trata sólo del espacio en el que se desarrolla la vida sino que también abarca seres vivos, objetos, agua, suelo, aire y las relaciones entre ellos, así como elementos tan intangibles como la cultura.

### 1.2.5. Switch Inalámbrico

El Switch inalámbrico WS2000 es una poderosa solución integrada que simplifica y reduce los costos de la gestión de redes cableadas e inalámbricas (802.11a/b/g) en sucursales. El dispositivo integra router, puerta de enlace, servidor de seguridad, Power-over-Ethernet (PoE) y otras funciones, se elimina la necesidad de adquirir varios dispositivos y la complejidad de su gestión. La compatibilidad con extensiones Wi-Fi Multimedia (WMM) permite al WS2000 ofrecer el mejor rendimiento incluso en las aplicaciones más complejas con voz y vídeo.

**GRAFICO 1.6:** SWITCH INALÁMBRICO SYMBOL WS2000.
**FUENTE:** HTTP://WWW.ZETES.COM/ELINK/05Q1/SPAIN/WIRELESS-SWITCH.HTM.

### 1.2.6. Access Point

Un **punto de acceso inalámbrico** (**WAP** o **AP** por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar

"roaming". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso - se convierte en una red **ad-hoc**).”Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada”.[4]

**GRAFICO 1.7:** ACCES POINT.

**FUENTE:** HTTP://ES.WIKIPEDIA.ORG/WIKI/PUNTO_DE_ACCESO.

La infraestructura de un punto de acceso es simple: “Guardar y Repetir”, son dispositivos que validan y retransmiten los mensajes recibidos. Estos dispositivos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones. Las características a considerar son:

La antena del repetidor debe de estar a la altura del techo, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa.
La antena receptora debe de ser más compleja que la repetidora, así aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.

[4] http://www.pucelawireless.net/index.php?pagename=AccessPoint

Un punto de acceso compartido es un repetidor, al cual se le agrega la capacidad de seleccionar diferentes puntos de acceso para la retransmisión. (Esto no es posible en un sistema de estación-a-estación, en el cual no se aprovecharía el espectro y la eficiencia de poder, de un sistema basado en puntos de acceso)

La diferencia entre el techo y la mesa para algunas de las antenas puede ser considerable cuando existe en esta trayectoria un obstáculo o una obstrucción. En dos antenas iguales, el rango de una antena alta es 2x-4x, más que las antenas bajas, pero el nivel de interferencia es igual, por esto es posible proyectar un sistema basado en coberturas de punto de acceso, ignorando estaciones que no tengan rutas de propagación bien definidas entre si.

Los ángulos para que una antena de patrón vertical incremente su poder direccional de 1 a 6 están entre los 0° y los 30° bajo el nivel horizontal, y cuando el punto de acceso sea colocado en una esquina, su poder se podrá incrementar de 1 a 4 en su cobertura cuadral. El patrón horizontal se puede incrementar de 1 hasta 24 dependiendo del medio en que se propague la onda. En una estación, con antena no dirigida, el poder total de dirección no puede ser mucho mayor de 2 a 1 que en la de patrón vertical. Aparte de la distancia y la altura, el punto de acceso tiene una ventaja de hasta 10 Db en la recepción de transmisión de una estación sobre otra estación.

Estos 10 Db son considerados como una reducción en la transmisión de una estación, al momento de proyectar un sistema de estación-a-estación.

### 1.2.7. Tarjetas Inalámbricas

Basándome en la experiencia y los informes presentados por muchos de las personas integrantes del foro wireless presento esta tabla que recoge

algunas de las características que deben ser tenidas en cuenta a la hora de la elección de las mismas para la auditoria wireless. No se pondrá bajo ningún concepto ningún precio ni ninguna dirección donde poder adquirirlas ya que estos datos cambian constantemente y será estudio particular de cada persona en función de sus necesidades y de su economía.

TABLA 1.1: TABLA DE TARJETAS INALÁMBRICAS (ACTUALIZADO A (3-10-06)
FUENTE: HTTP://WWW.SYMBOL.COM.MX/INFO8.HTML

| Modelo | Chipset | Win | Lin | Inyección | Antena | Cobertura | Observaciones |
|---|---|---|---|---|---|---|---|
| AirisV257 mini-pci 11g | Ralink RT2500 | No | Si | Lx (??) | No | Buena | Mini PCI |
| Belkin F5D7050 | Ralink RT2570 | No | Si | Lx (b/g) | No | Normal | Barata. USB, R. V3 |
| CiscoAironet PCM352 | Aironet | airo | Si | No+?? | No | Buena | Necesario act. firmware |
| D-link DWL-510 | RTL8180L | airo | Si | Lx (b/g) | Si | Normal | PCI. R A1. RTL = Realtek |
| Edimax EW-7128g | Ralink RT2500 | No | Si | Lx (b/g) | Si | Normal | PCI |
| Gygabyte GN_WMAG | Atheros | airo | Si | Lx+?? | No | **Muy sorda** | PCMCIA -108M |
| Intellinet 54 Wireless | Ralink RT2500 | No | Si | Lx (b/g) | Si | **Sorda** | PCI. |
| IPW 2100 (Portatiles) | Intel Centrino | com | Si | No | No | Muy buena | Mini PCI. Cobertura OK |
| Linksys WMP54G v2 | Broadcom | Si | ?? | No | No | **Sorda** | Difícil linux-drivers V2 |
| Netgear WG311T (FS) | Atheros A2 | **??** | Si | Lx(b/g) | Si | **Sorda** | Sicodelica |
| Orinco Gold 8470WD | Atheros | airo/com | Si | Lx(b/g)+CV | Si | Normal | Pcmcia. Pigtail MC-Card |
| Senao2511cdplusext2 | Prism 2.5 | No | Si | Lx (b) | No | **Sorda** | Pcmcia. Pigtail MMCX |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SMC SMCWPCIT-G | Atheros | airo/com | Si | Lx(b/g)+CV | Si | Buena | PCI. Barata |
| Zcom XI-32HP+300W | Prism 2.5 | No | Si | Lx (b) | Si | Normal | Pcmcia. Pigtail MMCX |

La mayoría de tarjetas traen un zócalo vacío rotulado BOOT ROM, para incluir una ROM opcional que permite que el equipo arranque desde un servidor de la red con una imagen de un medio de arranque (generalmente un disquete), lo que permite usar equipos sin disco duro ni unidad de disquete. El que algunas placas madre ya incorporen esa ROM en su BIOS y la posibilidad de usar tarjetas CompactFlash en lugar del disco duro con sólo un adaptador, hace que comience a ser menos frecuente, principalmente en tarjetas de perfil bajo.

## 1.3. Tendencia de las Telecomunicaciones

### 1.3.1. Definiciones

Wi-Fi (o Wi-fi, WiFi, Wifi, wifi) (del inglés Wireless Fidelity) es un conjunto de estándares para redes inalámbricas basados en las especificaciones 802.11. Creado para ser utilizado en redes locales inalámbricas; es frecuente que en la actualidad también se utilice para acceder a Internet. Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance). El problema principal que pretende resolver la normalización es la compatibilidad. De esta forma en abril de 2000 WECA certifica la interoperatibilidad de equipos según la norma IEEE 802.11b bajo la marca Wi-Fi (Wíreless Fidelity, Fidelidad Inalámbrica).

Como la norma 802.11b ofrece una velocidad máxima de transferencia de 11 Mbps ya existen estándares que permiten velocidades superiores, WECA no se ha querido quedar atrás. Por ese motivo, WECA anunció

que empezaría a certificar también los equipos IEEE 802.11a de la banda de 5 Ghz mediante la marca Wi-Fi5. La norma IEEE.802.11 fue diseñada para sustituir a las capas físicas y MAC de la norma 802.3 (Ethernet).

### 1.3.2. Combinación de los sistemas

La red ofrece un rango amplio de opciones inalámbricas de implementación para cubrir áreas grandes y de última milla. Lo mejor es que la solución varía de acuerdo a los modelos de uso, el tiempo de implementación, la posición geográfica y la aplicación de red (tanto en datos, VoIP y vídeo. Los Wi-Fi WLANs coexistirán con WiMAX. El IEEE 802.16 el estándar con revisiones específicas se ocupa de dos modelos de uso:

"El estándar del 802.16-2004 del IEEE (el cuál revisa y reemplaza versiones del IEEE del 802.16a y 802.16d) es diseñado para el acceso fijo que el uso modela. Este estándar puede ser al que se refirió como "fijo inalámbrico" porque usa una antena en la que se coloca en el lugar estratégico del suscriptor. La antena se ubica generalmente en el techo parecido a un plato de la televisión del satélite. WiMAX acceso fijo funciona desde 2.5-GHz autorizado, 3.5-GHz y 5.8-GHz exento de licencia". [5]

### 1.3.3. La razón y su importancia

La informática inalámbrica no sólo ofrece la libertad de permanecer conectado a medida que se moviliza por una oficina o el hogar. Sino que también brinda la libertad de conectar un equipo portátil móvil a la Internet desde cualquier habitación en casa o desde cualquier lugar donde lo lleve.

[5] http://es.wikipedia.org/wiki/WiMAX

El deshacerse de los cables puede ser complicado. Implica el tener que enfrentarse a distintos estándares inalámbricos y todo el hardware y software resultante.

No obstante, la industria inalámbrica estableció el estándar 802.11 b (o WLAN) como el predominante en 1999, lo cual ha reducido los precios a medida que la demanda ha aumentado. En un futuro no lejano, el equipo para redes WiFi diseñado para las empresas y los hogares tendrán precios que equivalen a los de las redes cableadas, siendo fáciles de comprar y configurar.

Entre otras ventajas importantes de las redes inalámbricas tenemos:

- Implementación de redes de área loca! inalámbricas en edificios históricos, de difícil acceso y en general en entornos en donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red sin añadir costos adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Estas redes permiten el acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes, etc.
- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.

- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.

Interconexión de redes que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red local inalámbrica para interconectar dos o más redes de área local cableada situadas en dos edificios distintos.

### 1.3.4. Tecnología de redes de telecomunicaciones

Las redes de información y comunicaciones han venido experimentado vertiginosos cambios, debido a la constante evolución que en el campo de la informática se produce, mejorando la intercomunicación de miles y millones de usuarios que acceden a este servicio tanto en empresas como en instituciones educativas a nivel mundial, y es necesario seguir realizando estudios y mejorando su funcionalidad dotándola de mejores herramientas que la era moderna en la actualidad lo requiera.

El Internet es un claro ejemplo en el avance de tecnologías de redes informáticas ya que este tiene su característica de ser potente, solidó, confiable y puede ser adaptable a diferentes equipos de usuarios.

Con el desarrollo del proyecto se ha creado una herramienta de consulta accesible y clara, para quienes deseen ahondar sus conocimientos en lo que respecta a la creación de redes informáticas y su funcionamiento.
Con todos estos requerimientos se da ha conocer el presente proyecto, esperando que en él, se encuentre una fuente de consulta que despeje todas las necesidades y dudas de los usuarios.

#### 1.3.4.1. Inalámbricas

En un principio las redes inalámbricas fueron diseñadas para ofrecer sus ventajas de comunicación dentro de entornos empresariales. En este tipo de entornos las redes inalámbricas, fundamentalmente, complementan a las comunicaciones cableadas ya existentes en las empresas. Una red inalámbrica, formada por varios puntos de acceso, además de conectar equipos dentro de su área de cobertura se conecta a la red cableada de la empresa para proporcionar conectividad global dentro del entorno empresarial.

Actualmente, las redes WLAN se utilizan en un gran número de aplicaciones siendo sus posibles usos casi innumerables, sólo determinables por la imaginación y necesidad de uso en cada caso. A continuación se describen de forma general algunos de esos casos, que podrían ser particularizados para cada uso en concreto.

## 1.4. Historia de las Redes

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread-spectrum"(frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas

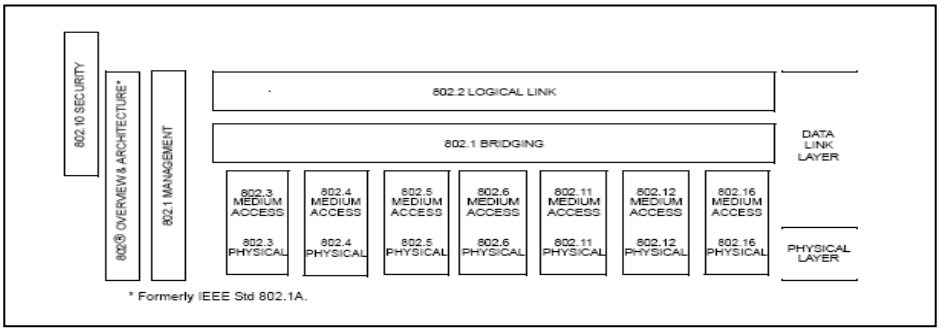
basadas en "spread-spectrum". IMS es una banda para uso comercial sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda. La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezara a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativos que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

**GRAFICO 1.8:** REDES WLAN
**FUENTE:** WWW.AIRONET.COM

### 1.4.1. Estándares de Calidad de las Redes Inalámbricas

El primer componente del estándar IEEE 802.11 fue ratificado en 1997 y luego en 1999, cuando también se realizaron las primeras extensiones. La estructura de los estándares de la IEEE es tal que las extensiones se elaboran como modificaciones del estándar original y se nombran agregándole una letra al nombre del estándar. En el caso de 802.11, tenemos extensiones 802.11a, 802.11b, etc. En realidad, el estándar 802.11 es sólo una parte de un conjunto más amplio de estándares de IEEE: el 802. La Figura  muestra esquemáticamente la estructura del conjunto de estándares 802, dedicado a las capas más bajas de arquitectura de redes.

**GRAFICO 1.9:** FAMILIA DE LOS ESTANDARES DE LA IEEE. 802.11
**FUENTE:** EL INVESTIGADOR




### 1.4.2. Características del estándar de la IEEE 802.11 b

Este estándar es una parte de una familia de los estándares para las redes del área local y metropolitana. Esta familia de los estándares con las capas de transmisión de la comprobación y de datos es de acuerdo a lo definido por el modelo de la referencia básica del Sistema Abierto de Interconexión de la Organización Internacional por Estandarización (ISO) (ISO/IEC 7498- 1:1994).

**Descripción**

Esta cláusula especifica la extensión de la alta tarifa del PHY para el sistema directo del espectro de la extensión de la secuencia (DSSS) (cláusula 15 del IEEE 802.11, en el año 1999, más luego se aplica como la alta tarifa PHY para la banda de 2.4 gigahertz señalada para los usos de ISM. Dicha extensión de las estructuras del sistema de DSSS en las capacidades de la tarifa de datos, según lo descrito en la cláusula 15 de IEEE 802.11, en el año 1999, para proporcionar 5.5 Mbit/s y 11 tarifas de datos de la carga útil de Mbit/s además del 1 Mbps y de 2 tarifas de Mbps. Para proporcionar las tarifas más altas, el código complementario 8-chip que afina (CCK) se emplea como el esquema de la modulación. La tarifa que salta es 11 megaciclos, que es igual que el sistema de DSSS descrito en la cláusula 15 de IEEE 802.11, del año 1999, así

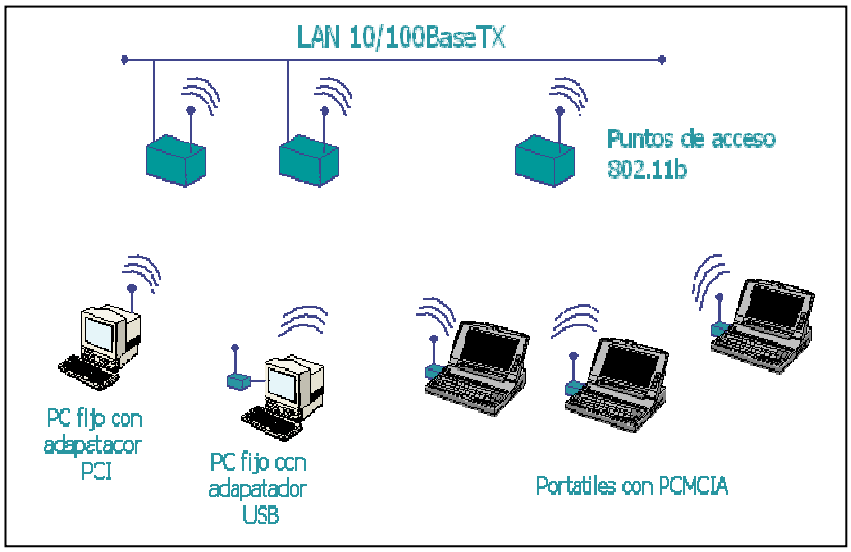
proporcionando la misma anchura de banda ocupada del canal. La nueva capacidad básica descrita en esta cláusula se llama el espectro directo de la extensión de la secuencia de la alta tarifa (hora DSSS). La alta tarifa básica PHY utiliza el mismo preámbulo y el jefe de PLCP que el DSSS PHY, así que PHYs puede coexistir en el mismo BSS y puede utilizar el mecanismo de la conmutación de la tarifa en la manera prevista.

### 1.4.3. Características del estándar de la IEEE 802.11 g

IEEE y 802.11g, son marcas de fábrica registradas en los EE.UU. Por el Instituto de Eléctricos y Ingenieros Electrónicos. Cada padrón de IEEE es sujeto a la evaluación por lo menos cada cinco años, para la revisión o la reafirmación. Los documentos de niveles de IEEE son desarrollados dentro de las sociedades de IEEE, y los padrones coordinadas por el comité de Estándar, sus padrones a través de un proceso de consenso, y aprobadas por el Instituto Estadounidense de Estándares Nacionales. La existencia de un padrón de IEEE no insinúa que no hay ninguna otra manera de producir, hacer pruebas, medir, comprar el mercado, o proveer otros bienes y servicios relacionados con el alcance del padrón. Esta enmienda es parte de una familia de padrones para junta local y redes de área metropolitana, en la cual se arregla con el reconocimiento físico, a las capas de enlace de datos. “La organización para interconexión (OSI) modelo de referencia básico de sistemas abiertos de normalización (ISO) (ISO/IEC 7498, los padrones se definen en algunos tipos de tecnologías de acceso mediano, y son asociados a medios de comunicación físicos,

apropiados para las aplicaciones especiales a los objetivos del sistema. Tiene un alcance de un Ancho de banda máximo de hasta 54 Mbps, Opera en el espectro de 2.4 Ghz sin necesidad de licencia, resulta ser compatible con el IEEE 802.11b, su Modulación es DSSS y OFDM".[6]

**GRAFICO 1.10:** ESTANDARES DE CALIDAD PARA LAS REDES INALAMBRICAS
**FUENTE:** EL INVESTIGADOR




### 1.4.4. Seguridades en la Red Inalámbrica de acuerdo a los estándares

A finales de la década de los 90, los líderes de la industria inalámbrica (3Com, Aironet, Lucent, Nokia, etc.) crean la WECA (Wireless Ethernet Compatibility Alliance), una alianza para la Compatibilidad Ethernet Inalámbrica, cuya misión es la de certificar la ínter funcionalidad y compatibilidad de los productos de redes inalámbricas 802.11b.

"Para que un intruso se pueda meter un nuestra red inalámbrica tiene que ser nodo o usuario, pero el peligro radica en poder escuchar nuestra transmisión. Vamos a dar unos pequeños consejos para poder estar más tranquilos con nuestra red inalámbrica. Todos estos puntos son consejos,

[6]"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 1999 Edition.

las redes inalámbricas están en pleno expansión y se pueden añadir ideas nuevas sobre una mejora de nuestra seguridad".[7]

***Medidas de Seguridad***

- Cambiar las claves por defecto cuando instalemos el software del Punto De Acceso.
- Control de acceso seguro con autentificación bidireccional.
- Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
- Configuración WEP (muy importante), la seguridad del cifrado de paquetes que se transmiten es fundamental en las redes inalámbricas, la codificación puede ser más o menos segura dependiendo del tamaño de la clave creada y su nivel, la más recomendable es de 128 Bits.
- Crear varias claves WEP, para el punto de acceso y los clientes y que varíen cada día.
- Utilizar opciones no compatibles, si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro.
- Radio de transmisión o extensión de cobertura, este punto no es muy común en todos los modelos, resulta más caro, pero si se puede controlar el radio de transmisión al círculo de nuestra red podemos conseguir un nivel de seguridad muy alto y bastante útil.

### 1.4.5. Vulnerabilidades

El protocolo 802.11 implementa **encriptación WEP**, pero no podemos mantener WEP como única estrategia de seguridad ya que no es del todo

[7]http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml.

seguro. Existen aplicaciones para Linux y Windows (como AiroPeek, AirSnort, AirMagnet o WEPCrack) que, escaneando el suficiente número de paquetes de información de una red Wi-Fi, son capaces de obtener las claves WEP utilizadas y permitir el acceso de *intrusos* a nuestra red. Más que hablar de **la gran regla de la seguridad** podemos hablar de una serie de estrategias que, aunque no definitivas de forma individual, en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos.

**Después de Wep**

WPA (Wi-Fi Protected Access), estándar desarrollado por la Wi-Fi alliance (WECA), que trata de ser el sustituto de WEP y es posible incorporarlo en algunos routers que no lo incorporan con una simple actualización de firmware. Esta está basada en los estándares IEEE 802.11i que mejoran de manera notoria la protección de datos y control de acceso, pudiendo decirse que el nivel de protección es alto ya que mejora el cifrado de datos mediante TKIP (Temporal Key Integrity Protocol) mediante claves de sesión dinámica por usuario, sesión y paquete, pero es necesario acceder a través de un server de autentificación y que asegura la confidencialidad de datos. Y por otro lado, WPA también ofrece la autentificación de los usuarios mediante el estándar 802.11x y EAP (Extensible Aunthentication Protocol) que permite controlar a todos y cada uno de los usuarios que se conectan a la red, aunque también permite, si se quiere, el acceso al usuario anónimo.

**Ataques**

**Ataques A Las Redes Inalámbricas WLAN**

Veamos un poco los diferentes tipos de ataques a redes inalámbricas y como funcionan. Para comenzar, vamos a dividir los ataques en activos y

pasivos. Otros autores también definen más tipos de ataques, pero par ser mas prácticos, vamos a trabajar con estos dos.

El siguiente listado menciona algunos de los ataques más comunes:

**Ataques Activos.**

Los ataques activos buscan causar algún daño, como ser: perdida de confidencialidad, disponibilidad e integridad de información ó sistemas.

- **IP Spoofing:** El atacante cambia su dirección IP para poder pasar por alto controles de acceso.

- **MAC Address Spoofing:** El atacante cambia su dirección MAC para pasar por alto los controles de acceso de los Access Points. Como veremos mas adelante, la mayoría de los Access Points posee controles de acceso filtrando direcciones MAC.

- **ARP Poisoning:** Todos los equipos conectados a una red tienen una tabla ARP que asocia direcciones MAC a direcciones IP. Este tipo de ataque busca modificar estas tablas para poder redirigir el tráfico de un equipo a otro de manera controlada.

- **Man in the middle:** Este tipo de ataque se puede ejecutar una vez realizado un ARP Poisoning, en el cual se redirige todo el trafico saliente de un equipo (victima) a otro y este lo envía al destino original. Este tipo de ataque es transparente y la victima no se da cuenta que su trafico de red esta pasando por un tercero antes de llegar a destino.

- **MAC Flooding:** Este ataque se consiste en inundar la red con direcciones IP falsas, causando que el Switch pase a funcionar en modo de Hub, ya que no soporta tanto tráfico.

- **Denial of Service:** Este tipo de ataque busca dejar fuera de servicio a la red inalámbrica, utilizando todo el ancho de banda para enviar paquetes basura. También se utiliza normalmente para dejar fuera de servicio a servidores ó aplicaciones.

- **Injection:** El atacante puede insertar paquetes en la red inalámbrica causando que todos los clientes se desconecten ó inundar la red con paquetes basura (generando un DoS).

- **Replay:** El atacante captura paquetes y luego los reinserta en la red inalámbrica con o sin modificación.

- **Rouge AP:** El atacante pone su propio Access Point y engaña a los clientes pensando que es el Access Point verdadero. De esta forma, posee todo el control del tráfico.

**Ataques Pasivos.**

Los ataques pasivos, en cambio, son aquellos donde un tercero no realiza ningún ataque, simplemente escucha.

- **Eavesdropping:** El atacante simplemente escucha (generalmente con una notebook ó PDA) las comunicaciones entre un Access Point y sus clientes. Con este ataque se busca obtener información que es normalmente transmitida por la red, como ser: usuarios, contraseñas, direcciones IP, etc. Este tipo de ataque es el más peligroso, ya que abre las puertas a otros ataques.

Como hemos visto, los ataques son variados y todos pueden causar severos daños. En la siguiente sección, llamada “Anatomía de un ataque” demostraremos lo insegura que puede llegar a ser la tecnología inalámbrica para lo cual planteamos implementar seguridades en la red inalámbrica.