UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGON

DISEÑO E IMPLEMENTACION DE UNA WLAN

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

INGENIERO MECANICO ELECTRICO

P R E S E N T A:

CELIA IRENE RODRIGUEZ MEDINA

MARCELO CORTES GARCIA

MEXICO, D.F. **SEPTIEMBRE 2006**

Agradecimientos

Ing. Benito Barranco Castellanos.

Por su tiempo, su paciencia y su apoyo en la elaboración de esta tesis.

Mamá y Papá.

Por estar conmigo en los buenos y los malos momentos, por compartir conmigo las tristezas y las alegrías, por su tiempo y dedicación, por darme su cariño que fue lo que me impulso a seguir adelante en la vida. Gracias por todo!!

Nancy, Mario y Angeles, Daniel, Javier, Ricardo y Juan

Por ser mis hermanos y compartir conmigo los mejores momentos de mi vida y apoyarme para lograr mis objetivos.

Celia, Perla, Miriam, Efraín, Rodrigo y Marco

Por todo los que aprendí de ustedes y con ustedes, por su cariño, por su paciencia, por compartir conmigo muchos buenos y malos momentos, sobre todo por ser mis amigos y mi familia.

Marcelo Cortés García

A mis padres

Por todo lo el gran amor y sacrificio, por darme lo mejor de ustedes sin pedir nada a cambio, siempre seguros de que lograría realizar sueños y cumplir con mis metas, por todo el tiempo que me dedicaron desde que llegue a este mundo, el apoyo incondicional y los muchos consejos.

Gracias por hacer de mi la persona que soy.

Liliana, Marcela y Oscar.

Gracias por estar siempre conmigo, por ser mis mejores amigos, por crecer a mi lado y por enseñarme que en la vida hay que luchar por lo que se quiere, por soportarme, por ser siempre mi ejemplo a seguir y sobre todo por ser mis hermanos.

Máma Celia, Ruben, Edgar, Mario Alberto, Octavio, Ernesto, Socorro

Por que fueron parte de mis ejemplos a seguir, por compartir la vida, los triunfos y tropiezos, por todo lo que aprendí con ustedes y de ustedes, por todo su cariño pero sobre todo por ser mi familia.

Marcelo

Gracias por tu tiempo, tu apoyo, la paciencia, el esfuerzo pero más que nada por el cariño y todo lo que me enseñaste. Te agradezco todos esos buenos y malos momentos que hemos pasado. Gracias por ser mi amigo.

Ing. Benito Barranco

Por el tiempo y todo el apoyo para la realización de esta tesis.

Celia Irene Rodríguez Medina

INDICE

CAPITULO III
Diseño de la red inalámbrica.

Introducción

La evolución de la vida es cada vez más rápida, del mismo modo la evolución y los avances tecnológicos son más rápidos y sorprendentes la mayoría de estos enfocados a hacer que nuestra vida sea más simple y cómoda cubriendo nuestras necesidades.

Los seres humanos como sociedad necesitamos trabajar en equipo para lograr que cierto tipo de tareas sean resueltas y con esto se llegue al objetivo deseado. Sin embargo realizar un trabajo en equipo no es una tarea sencilla, se requiere de la disposición de las personas y de la ayuda de diferentes herramientas que les permitan comunicarse y compartir información entre las distintas personas que participan, pero en ocasiones estas personas no pueden estar ubicadas dentro de la misma habitación y el problema aumenta aun más si es que tienen que estar en constante movimiento.

En la actualidad una de las necesidades primordiales de los usuarios es la posibilidad de realizar sus diferentes actividades vía remota y con la facilidad de no tener que estar conectado al molesto cable, sobre todo para aquellos usuarios que cuentan con equipos portátiles y que sus actividades no les permiten permanecer en un solo sitio.

Con la aparición de las redes inalámbricas la movilidad de los usuarios se hizo posible, tanto para particulares como para las empresas que requieren que sus empleados tengan la libertad de mantenerse conectados y con acceso a la información mientras se moviliza por toda el edificio.

El concepto de movilidad es sencillo; podemos definir la movilidad como la libertad de ir y venir sin perder la conexión dentro de una cierta extensión de espacio, que puede ser una oficina, un edificio o el espacio abierto. Este concepto ha influido en el desarrollo de las nuevas tecnologías y en el mercado potencial para los dispositivos que ya cuentan con esta característica.

Es posible resolver estas necesidades con la combinación de la tecnología inalámbrica y las ya conocidas redes de computadoras; las cuales se pueden implementar dentro de cualquier edifico, ya sea en una empresa o en el hogar, permitiendo con esto que los usuarios cuenten con las ya conocidas características de una red pero añadiendo la ventaja de la movilidad que representa la tecnología inalámbrica.

Sin embargo la tecnología inalámbrica aun no alcanza su máximo desarrollo dentro del mundo de las redes de computadoras y por lo mismo presenta aun muchas desventajas en comparación con las redes cableadas que en la actualidad ya nos proporcionan velocidades de transmisión mayores a los 10 Mbps; así mismo a nivel de seguridad las redes cableadas proporcionan más seguridad que las redes inalámbricas por lo que es importante que antes de decidir por alguna de las dos tecnologías se analicen las necesidades de los usuarios.

Con esto no queremos decir que las redes inalámbricas llegaran a remplazar a las redes cableadas; por el contrario podemos tener una combinación de los dos tipos de redes dentro de un solo edificio de manera que tengamos una red híbrida; considerando a la parte cableada de nuestra red como la parte principal de esta y la parte inalámbrica que proporcione la movilidad adicional para que los equipos se desplacen con facilidad por todo el edificio.

Estas son algunas de las razones por las que las redes inalámbricas han tomado más auge en los últimos años y por las que se han vuelto una de las mejores opciones para las empresas hoy en día.

Esta tesis es un esfuerzo por medio del cual se planea aplicar la tecnología inalámbrica interconectando un grupo de computadoras que comparten información y recursos que además cuentan con salida a Internet.

El plan a seguir dentro del desarrollo de la tesis consta de tres capítulos que se distribuyen de la siguiente manera:

El capítulo I es una breve introducción a los diferentes tipos de redes existentes, la arquitectura, algunos protocolos de red, el modelo OSI, así como los medios de transmisión, enfocándonos un poco más a los medios de transmisión inalámbricos que se tratan con más detalle en los siguientes capítulos.

Dentro del capítulo II se describe un poco la historia y evolución que ha tenido la tecnología inalámbrica a lo largo de los años desde las primeras apariciones de las ondas de radio hasta la actualidad, estándares, velocidades de transmisión, tipos de modulación y seguridad.

En el capitulo II nos enfocamos al diseño de una red inalámbrica, tomando en consideración las ventajas, desventajas, dispositivos mas adecuados y algunas otras consideraciones necesarias.

Con este trabajo buscamos mostrar una de las muchas aplicaciones que tiene en la actualidad la tecnología inalámbrica; así como fortalecer nuestro conocimiento y experiencia en la aplicación y evolución de estas tecnologías.

Junio 2006.

Capitulo I

Tipos de Redes.

Introducción.

Una red de computadoras consiste en una o más computadoras conectadas por un medio físico y que ejecutan un software que permite a las computadoras comunicarse unas con las otras.

En los primeros años de las redes las grandes compañías, incluyendo IBM, Honeywell y Digital Equipment Corporation, crearon su propio estándar de cómo las computadoras debían conectarse. Estos estándares describían los mecanismos necesarios para mover datos de una computadora a otra. Estos primeros estándares, sin embargo, no eran del todo compatibles. Por ejemplo, las redes que se adherían al SNA (Systems Network Architecture) de IBM no podían comunicarse directamente con las redes usando el DNA (Digital Network Architecture) de DEC.

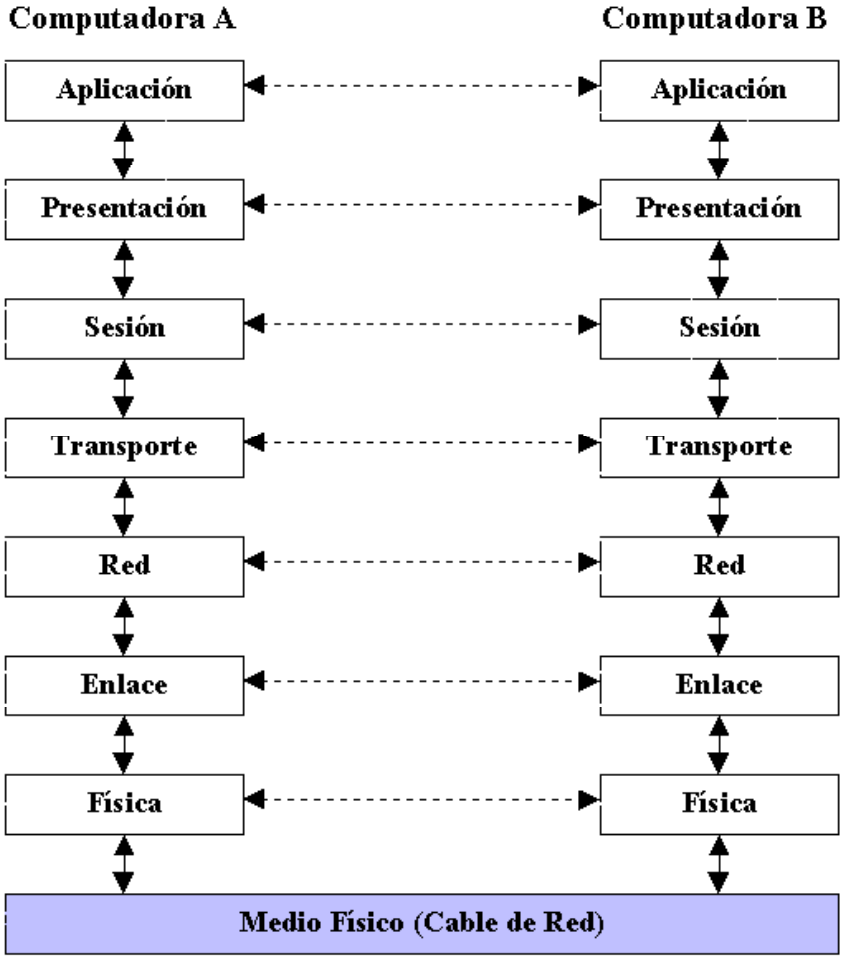
En años posteriores, organizaciones de estándares, incluyendo la Organización Internacional de Estandarización (ISO) y el instituto de Ingenieros Eléctricos y Electrónica (IEEE), desarrollaron modelos que llegaron a ser globalmente reconocidos y aceptados como estándares para el diseño de cualquier red de computadoras. Ambos modelos describen la red en términos de capas funcionales.

Modelo OSI.

En 1984, la Organización Internacional de Estandarización (ISO) desarrolló un modelo llamado OSI (Open Systems Interconectiòn, Interconexión de sistemas abiertos). El cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red.

Como se muestra en la figura, las capas OSI están numeradas de abajo hacia arriba. Las funciones más básicas, como el poner los bits de datos en el cable de la red están en la parte de abajo, mientras las funciones que atienden los detalles de las aplicaciones del usuario están arriba.

En el modelo OSI el propósito de cada capa es proveer los servicios para la siguiente capa superior, resguardando la capa de los detalles de como los servicios son implementados realmente. Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra computadora, cuando realmente cada capa se comunica sólo con las capas adyacentes de la misma computadora.



Con esta última figura se puede apreciar que a excepción de la capa más baja del modelo OSI, ninguna capa puede pasar información directamente a su contraparte en la otra computadora. La información que envía una computadora debe de pasar por todas las capas inferiores, La información entonces se mueve a través del cable de red hacia la computadora que recibe y hacia arriba a través de las capas de esta misma computadora hasta que llega al mismo nivel de la capa que envió la información. Por ejemplo, si la capa de red envía información desde la computadora A, esta información se mueve hacia abajo a través de las capas de Enlace y Física del lado que envía, pasa por el cable de red, y sube por las capas de Física y Enlace del lado de el receptor hasta llegar a la capa de red de la computadora B.

Las siete capas son del modelo OSI son:

Aplicación: Aplicaciones de red como emulación de una terminal o la transferencia de archivos.
Presentación: Se ocupa de dar formato a los datos y de su encriptado.
Sesión: Mantiene y establece las sesiones.
Transporte: Disposición de la entrega punto a punto.
Red: Entrega de paquetes, incluyendo ruteo.
Enlace: Elaboración de paquetes de unidades de información y verificación de errores.
Física Transmisión de bits a nivel de hardware.

La interacción entre las diferentes capas adyacentes se llama interface. La interface define que servicios la capa inferior ofrece a su capa superior y como esos servicios son accesados. Además, cada capa en una computadora actúa como si estuviera comunicándose directamente con la misma capa de la otra computadora. La serie de las reglas que se usan para la comunicación entre las capas se llama *protocolo.*

Medios de transmisión.

La información que maneja una computadora es de origen digital, encontrándose codificada a partir de un alfabeto de dos símbolos que se corresponden con 1 y 0 o, lo que es lo mismo, presencia o ausencia de una señal eléctrica. Para la transmisión de esta información entre dispositivos distintos a larga o corta distancia debe utilizarse un medio físico que asegure su correcta recepción en el destino.

Existen dos tipos de medios de transmisión de datos:

Medios guiados, que incluyen a los cables metálicos (cobre, aluminio, etc.) y de fibra óptica. El cable se instala normalmente en el interior de los edificios o bien en conductos subterráneos. Los cables metálicos pueden presentar una estructura coaxial o de par trenzado, y el cobre es el material preferido como núcleo de los elementos de transmisión de las redes. El cable de fibra óptica se encuentra disponible en forma de hebras simples o múltiples de plástico o fibra de vidrio.

Medios no guiados, relativos a las técnicas de transmisión de señales a través del aire y del espacio entre transmisor y receptor (radio enlaces). La transmisión por infrarrojos y microondas cae dentro de esta categoría.

Medios guiados

Par trenzado.

El cable de par trenzado consiste en un núcleo de hilos de cobre rodeados por un aislante, los cuales se encuentran trenzados por pares, de forma que cada par forma un circuito que puede transmitir datos. Un cable consta de un haz de uno o más pares trenzados rodeados por un aislante. El par trenzado sin apantallar (UTP, Unshielded Twisted Pair) es usual en la red telefónica, y el par trenzado apantallado (STP, Shielded Twisted Pair) proporciona protección frente a la diafonía. Precisamente es el trenzado el que previene los problemas de interferencia. Conforma una tecnología relativamente barata, bien conocida y sencilla de instalar. Es el cable utilizado en la mayoría de las instalaciones de redes de comunicaciones. Sin embargo, presenta una serie de características eléctricas que imponen ciertos límites a la transmisión. Por ejemplo, es resistente al flujo de electrones, lo que limita la distancia de transmisión. Produce radiación de energía en forma de señales que se pueden detectar, además de ser sensible a la radiación externa que puede producir distorsión sobre la transmisión. Sin embargo, los productos en uso admiten una velocidad de transmisión sobre Ethernet de hasta 100 Mbps.

Cable coaxial.

El cable coaxial consta de un núcleo de cobre sólido rodeado por un aislante, una especie de combinación entre pantalla y cable de tierra y un revestimiento protector exterior. En el pasado, el cable coaxial permitió una transmisión más alta (10 Mbps) que el cable de par trenzado, aunque las recientes técnicas de transmisión sobre par trenzado igualan e incluso superan la velocidad de transmisión por cable coaxial.

Sin embargo, los cables coaxiales pueden conectar los dispositivos de la red a distancias más largas que los de par trenzado. A pesar de ser el cable coaxial el medio tradicional de transmisión en redes basadas en Ethernet y ARCNET, la utilización de par trenzado y fibra óptica ya es muy común hoy en día sobre este tipo de redes.

Fibra óptica.

El cable de fibra óptica transmite señales luminosas (fotones) a través de un núcleo de dióxido de silicio puro tan diáfano que un espesor de más de tres millas del mismo no produce distorsión en una visión a su través. La transmisión fotónica no produce emisiones externas al cable, sin ser afectada por la radiación exterior. El cable de fibra se prefiere cuando existen ciertos requisitos de seguridad. La conversión electrónica de los valores lógicos 1 y 0 en destellos de luz permite la transmisión de las señales a través del cable de fibra óptica. Un diodo emisor de luz, situado en un extremo, emite destellos que se transmiten por el cable hasta el otro extremo, donde se recogen por un simple fotodetector y se convierten en señales eléctricas. Puesto que no existe

una resistencia a las señales transmitidas, la velocidad de transmisión por fibra óptica supera en prestaciones ampliamente a la transmisión por cable de cobre.

Radio enlaces.

Se basan en la propagación de ondas electromagnéticas a través del aire. Para ello sólo requieren un equipo emisor y un receptor, además de posibles repetidores intermedios para salvar la orografía del terreno, ya que este tipo de transmisión exige visibilidad entre los dos equipos emisor y receptor. En la actualidad existen los siguientes tipos de radioenlaces: de onda corta, sistemas terrestres de microondas y sistemas basados en satélites de comunicaciones. La transmisión mediante microondas se lleva a cabo en una gama de frecuencias que va desde 2 a 40 GHz. Cuando las distancias son extremadamente grandes, el número de repetidores sería también grande. Además, si tenemos en cuenta la superficie terrestre recubierta de agua donde la instalación de repetidores sería compleja, se utilizan los satélites de comunicaciones soportados sobre satélites artificiales geoestacionarios, es decir, que no modifican su posición respecto a la tierra.

Topología de red.

La topología de una red de área local es la forma en que las computadoras están unidos unos a otros, define la distribución de cada equipo en relación a la red y los demás equipos. Las topologías son criterios determinantes para la elección de las redes de área local, la reducción del costo de encaminamiento, la fiabilidad o tolerancia a fallos y su facilidad para localizarlos, y por último la facilidad de su instalación y reconfiguraciones futuras.

Las topologías más comunes en las redes de área local se citan a continuación:

- Estrella
- Bus
- Árbol
- Anillo
- Anillo modificado

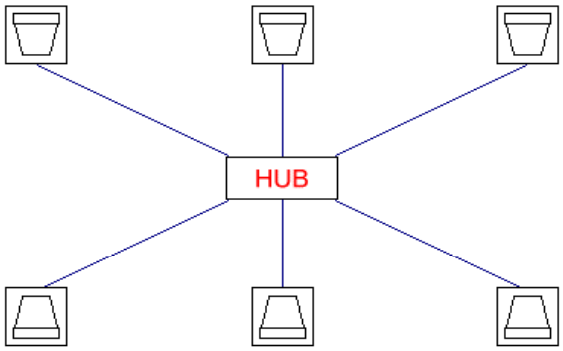
Atendiendo a los criterios antes citados, se presenta a continuación una descripción de los principales tipos de topologías de redes de área local.

Topología en estrella.

En la topología en estrella todos los equipos están conectados mediante enlaces bidireccionales a un equipo o nodo central que controla la red. Este nodo central asume las funciones de gestión y control de las comunicaciones proporcionando un camino entre cada dos equipos que deseen comunicarse.

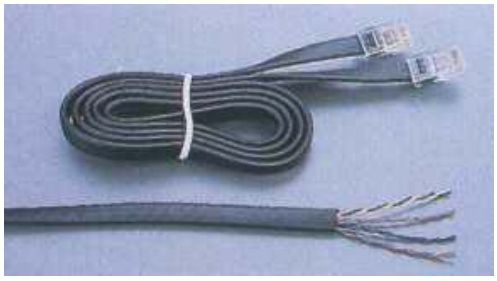
La principal ventaja de la topología en estrella es que el acceso a la red, es decir, la decisión de cuando un equipo puede o no transmitir, se halla bajo control del equipo central. Además la flexibilidad en cuanto a configuración, así como la localización y control de fallos es aceptable al estar todo el control en el nodo central. El gran inconveniente que tiene esta topología es que si falla el nodo central. Toda la red queda desactivada. Otros pequeños inconvenientes de este tipo de red son el costo de las uniones físicas puesto que cada equipo está unido a la unidad central por una línea individual, y además, las velocidades de transmisión son relativamente bajas.

La topología de una red de cable de par trenzado es una estrella cuyo centro es el hub, del cual parte un cable. Cuando alguno de estos cables se rompe, la comunicación sólo queda interrumpida entre esos equipos y la red, no afectando al resto.



Topología de una red de cable de par trenzado

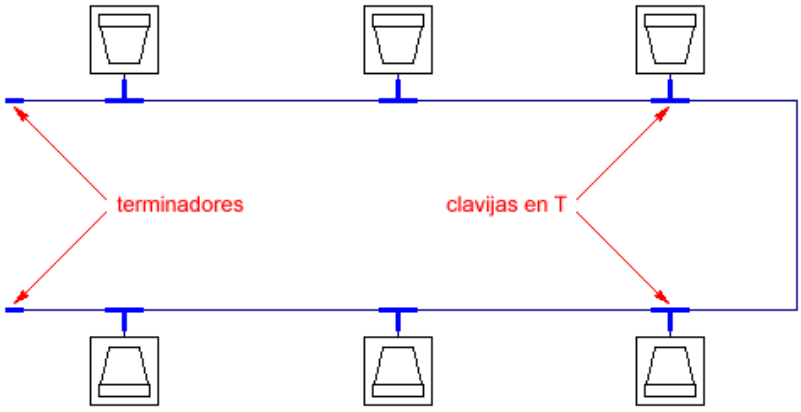
En este caso no necesitaremos de terminadores ni piezas en forma de T, ya que la conexión se realiza simplemente conectando la clavija tipo teléfono a la tarjeta de red y al hub. Al igual que para cable coaxial, existen tomas de pared para conectar la clavija, lo que puede ser interesante para cablear una oficina de un cierto tamaño dejando tomas preparadas para su uso futuro.



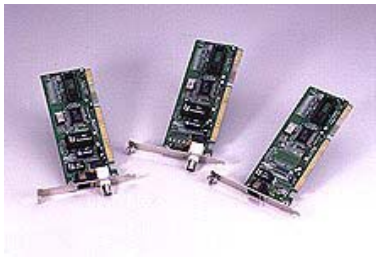
Topología en bus.

En esta topología todos los equipos se conectan a un único medio bidireccional lineal o bus con puntos de terminación bien definidos. Cuando un equipo transmite, su señal se propaga a ambos lados del emisor, a través del bus, hacia todos los equipos conectados al mismo, por este motivo, al bus se le denomina también canal de difusión. La mayor parte de los elementos de las redes en bus tienen la ventaja de ser elementos pasivos, es decir, todos los componentes activos se encuentran en los equipos por lo que una avería en un equipo no afecta más que a ella misma. Por otra parte, un inconveniente de este tipo de redes es que si falla el propio bus, queda afectada toda la red. Las principales ventajas que tiene esta topología es la facilidad de añadir y quitar equipos. Entre las desventajas se encuentra el hecho de que varios equipos quedan desconectados al fallar un tramo del bus.

La topología bus es una red de cable coaxial en una línea, una cadena de Computadores unidos a un único cable mediante unas piezas en forma de T que salen de éste. Si el cable se rompe se interrumpe la comunicación en toda la red, lo cual no ocurre si lo que se ha desconectado es sólo el extremo de la T que une al computador con el cable, en cuyo caso sólo ese equipo pierde la comunicación con la red.



Topología de una red de cable coaxial



En los extremos de la red deben existir dos pequeñas piezas denominados terminadores, y que deben ser de 50 Ohmios generalmente se unen a un extremo de la T de los dos computadores de los extremos.

Topología en árbol.

Es una variante de la topología en bus, consistente en un bus principal denominado tronco del que parten varios buses secundarios denominados ramas, cada una de las cuales es capaz de admitir varios equipos. Al igual que en la topología en bus, las señales se propagan por cada ramal de la red y llegan a todos los equipos. Además de las ventajas e inconvenientes de las redes en bus, la red en árbol tiene una mayor adaptabilidad al entorno físico donde se instala la red, con lo que el costo de cableado es aún menor.

Topología en anillo.

El anillo consiste en una serie de repetidores conectados entre sí mediante un único enlace de transmisión unidireccional que configura un camino cerrado. La información se transmite secuencialmente de un repetidor al siguiente a lo largo del anillo, de tal forma que cada repetidor regenera la señal que recibe y la retransmite al siguiente, salvo que la información esté dirigida a él, en cuyo caso la recibe en su memoria. Los repetidores constituyen un elemento activo de la red, siendo sus principales funciones las de contribuir al correcto funcionamiento del anillo ofreciendo todos los servicios necesarios y proporcionar el punto de acceso a los equipos de la red.

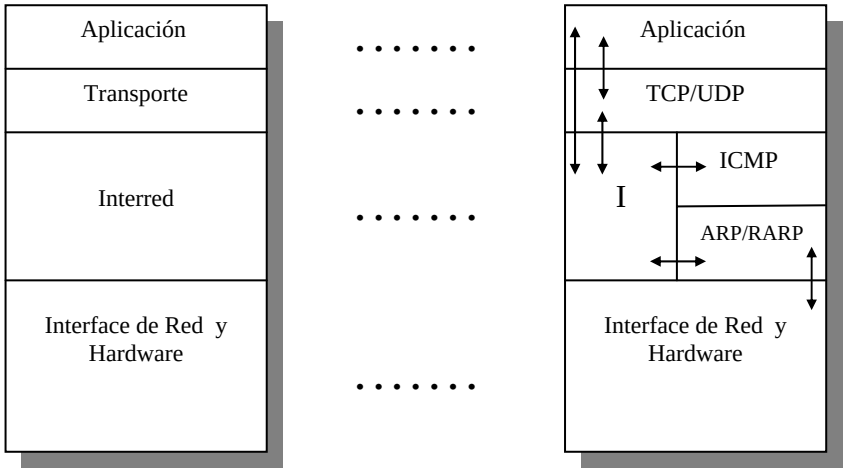
Normalmente los repetidores están integrados en las computadoras personales y en las estaciones de trabajo. Las redes en anillo permiten un control eficaz, debido a que, en cada momento, se puede conocer en que trama está circulando la señal, puesto que se conoce el último equipo por donde ha pasado y la primera a la que todavía no ha llegado. La desventaja fundamental es la falta de fiabilidad. Un fallo en el anillo inhabilitaría todos los equipos.

Topología en anillo modificado.

Es una variante de la red en anillo que trata de solucionar los problemas de la escasa fiabilidad que tienen estas redes facilitando algunas tareas como la instalación, mantenimiento y la reconfiguración. En general, se trata de topologías alternativas en las que la configuración física es distinta a la de anillo pero conserva la misma estructura lógica. El ejemplo más claro de este tipo de redes es el ofrecido por la red de pase de testigo en anillo (Token-Ring) consistente en una configuración física en estrella con una configuración lógica en anillo.

Presentación de TCP/IP.

El término genérico “TCP/IP” es indistintamente utilizado para referirse a los protocolos TCP e IP. No obstante que incluye otros protocolos, aplicaciones e incluso el medio utilizado de la red, un ejemplo de esos protocolos son: UDP, ARP y ICMP, y ejemplos de las aplicaciones que lo utilizan son: TELNET, FTP, y RCP.
(Estructura básica del protocolo TCP/IP)



Bajo esta estructura de protocolos representando por capas que se comunican es la forma como se realiza la comunicación de los equipos que se encuentran en una Internet. Cada computadora que se comunica utilizando tecnología de Internet tiene esta estructura lógica, ella además determina el comportamiento de la computadora en la Internet. Las cajas representan unidades de procesamiento de datos que se hace a través del elemento de proceso o computadora y las líneas que conectan a las cajas muestran el camino por el que deben circular los datos.

Terminología.

El nombre de la unidad de donde fluyen los datos para pasar a través de una Internet depende de su posición en la pila de protocolos. Esto es, si esta en la capa física de ethernet es denominado frame (trama) de ethernet; y si está entre el controlador de ethernet y el módulo IP (Internet Protocol) entonces se llama paquete IP; si se encuentra entre este y el módulo UDP entonces es llamado datagrama UDP; y si se encuentra entre el módulo IP y el módulo TCP se le llama segmento TCP; finalmente si se ubicara en una aplicación de red entonces se le denominará mensaje de aplicación.

Flujo de datos.

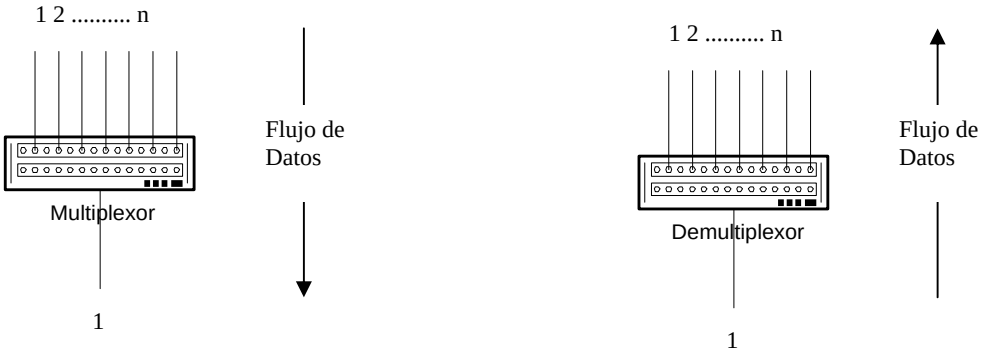
La información fluye a través de la pila de capas que integran el protocolo como se muestra en la figura (1.1). Para una aplicación que utiliza TCP los datos pasan entre la aplicación y el módulo de TCP, para una aplicación que utiliza UDP los datos pasaran a través de la aplicación y el módulo de UDP. Los módulos de TCP, UDP y el controlador de Ethernet son elementos que se comportan como multiplexores de n entradas a una salida, como multiplexores estos módulos hacen la selección de muchas entradas hacia una salida. Estos módulos a la vez también son demultiplexores de 1 a n. Como demultiplexores ellos hacen la selección de una entrada a muchas salidas de acuerdo a un campo en el formato del mensaje denominado campo de tipo en el encabezado del protocolo.

Si una trama de Ethernet llega en el controlador de Ethernet de la red, el paquete podrá pasar hacia arriba al módulo del ARP (Address Resolution Protocol) o al módulo del IP.

El valor del campo tipo en el formato del mensaje de Ethernet determina si un trama de Ethernet es pasado al ARP o al módulo del IP.

Si un paquete sube hacia el módulo IP la unidad de datos es pasada hacia una capa superior, ya sea al módulo TCP o UDP, esto es determinado por el valor del campo del protocolo en el encabezado IP.

Si es un datagrama UDP sube al módulo UDP, y el mensaje de aplicación es pasado hacia la capa superior, es decir hacia la aplicación de red, siempre en base al valor del campo del puerto en el encabezado del UDP.



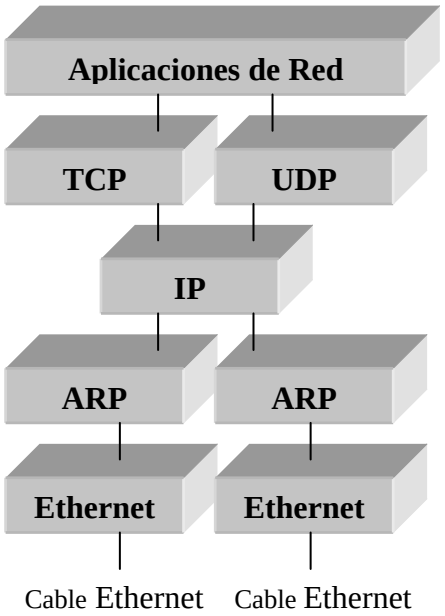
Si es un mensaje de TCP subirá al módulo TCP, y el mensaje de la aplicación se pasará a la aplicación de la red basado en el valor del campo del puerto en el encabezado de TCP.

Hacia abajo el multiplexado es simple porque de cada punto de inicio hay sólo un camino descendente; cada módulo de protocolo agrega su información al encabezado en el lugar que le corresponde para que el paquete pueda ser de multiplexado posteriormente en la computadora destino.

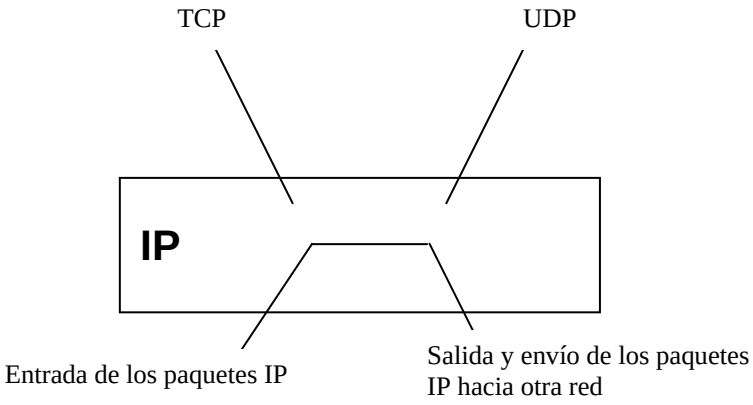
Los datos que pasan fuera de las aplicaciones a través de TCP o UDP convergen en el módulo de IP y se envían hacia la capa inferior a través de la interface de red de más bajo nivel (el controlador de la tarjeta red).

Aunque la tecnología del Internet soporta muchos medios diferentes de red, utilizaremos en esta introducción como un estándar a la red Ethernet porque es la red física más común utilizada con IP. Las direcciones de 6 bytes de Ethernet son únicas para cada interface y están localizadas en la parte más baja de la interface del controlador de Ethernet.

La computadora también tiene una dirección IP de 4 bytes, esta dirección está localizada en la interfaz más baja del módulo IP. La IP de un dispositivo debe ser única en toda la Internet.



El proceso de mandar un paquete de IP hacia otra red es llamado forwarding o pasado delante. Una computadora que ha estado especializada a la tarea de remitir los paquetes IP se le llama un ruteador IP.



IP crea una sola red lógica

EL módulo IP es importante en la tecnología de Internet. Cada controlador agrega su encabezado al mensaje y el mensaje pasa a la capa inferior subsecuente en la pila del protocolo y revisa su correspondiente encabezado una vez que el mensaje circula sobre la pila del protocolo hacia la aplicación.

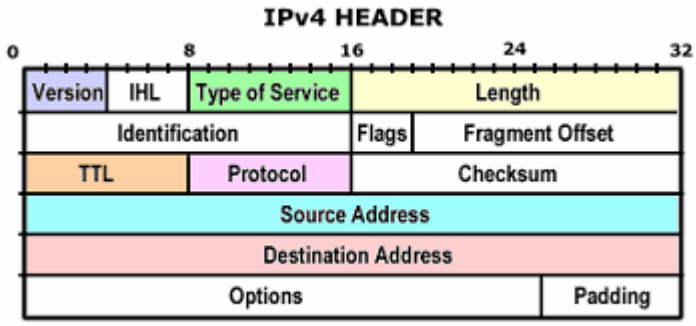
El encabezado IP contiene la dirección IP con la cual se construye una red lógica simple, desde múltiples redes físicas. Esta interconexión de redes físicas es la fuente del nombre de Internet.

El módulo IP oculta la capa del hardware de la red a las aplicaciones de la red, si se crea una nueva red física, su puede poner dentro de los servicios de la Internet implementando un nuevo controlador bajo el módulo IP. Esto hace que las aplicaciones de red permanezcan intactas ante el cambio de tecnología de hardware.

IP (Internet Protocol) Versión 4.

El Protocolo IP proporciona un sistema de distribución que es poco fiable si no inconfiable incluso en una base sólida. El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP/IP es el datagrama. Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta, fragmentados intencional o no intencionalmente para permitir que un nodo con un buffer limitado pueda recibir y almacenar todo o parte del datagrama. Es la responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar algún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la maquina origen (esto lo hace el protocolo ICMP).

El protocolo IP define cual será la ruta inicial por la que serán mandados los datos. Cuando los datagramas viajan de un equipo a otro, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. Al tamaño máximo se le denomina MTU (Maximum Transmission Unit), y ninguna red puede transmitir un paquete de tamaño mayor. El datagrama consiste en un encabezado y datos.



El campo versión que define cual versión de Internet se está utilizando, ocupa 4 bits. Este campo hace que diferentes versiones del protocolo IP puedan operar en la Internet. En el caso de esta introducción se tratará de la versión 4.

La longitud esta definida por un campo el cual ocupa 4 bits, y representa el número de octetos de la cabecera dividido por cuatro, lo que hace que este sea el número de grupos de 4 octetos en la cabecera.

Tipo de servicio (ToS). Este campo ocupa un octeto de la cabecera IP, y especifica la precedencia y la prioridad del datagrama IP. Los tres primeros bits del octeto indican su precedencia. Los valores de la precedencia pueden ser de 0 a 7. Cero es la precedencia normal, y 7 esta reservado para control de red. Muchos Gateways (Compuertas de enlace) ignoran este campo.

Los otros 4 bits definen el campo prioridad, que tiene un rango de 0 a 15. Las cuatro prioridades que están asignadas son: 0, (por defecto, servicio normal), 1 (minimizar el coste monetario), 2 (máxima fiabilidad), 4 (Maximizar la transferencia), 8 (El bit +4 igual a 1, define minimizar el retraso). Estos valores son utilizados por los enrutadores para direccionar las solicitudes de los usuarios.

Longitud Total. Este campo se utiliza para identificar el número de octetos en el datagrama total.

El valor del campo identificación es un número secuencial asignado por el Host origen. El campo ocupa dos octetos. Los números oscilan entre 0 y 65.535. Cuando se combinan con la dirección del Host forman un número único en la Internet. El número se usa para ayudar en el reensamblaje de los fragmentos de datagramas.

Fragmentos Offset. Cuando el tamaño de un datagrama excede el MTU, este se (divide) segmenta.

El fragmento Offset representa el desplazamiento de este segmento desde el inicio del datagrama entero.

El campo flag o bandera ocupa 3 bits y contiene dos subbanderas. El bit +5 del campo se utiliza para indicar el último datagrama fragmentado cuando toma valor cero. El bit +7 lo utiliza el servidor origen para evitar la fragmentación. Cuando este bit toma valor diferente de cero y la longitud de un datagrama excede el MTU, el datagrama es descartado y un mensaje de error es enviado al Host de origen por medio del protocolo ICMP.

El campo tiempo de vida ocupa un octeto. Representa el número máximo de segundos que un datagrama puede existir en Internet, antes de ser descartado. Un datagrama puede existir un máximo de 255 segundos. El número recomendado para IP es 64.

El host de origen del datagrama manda un mensaje ICMP cuando el datagrama es descartado.

El campo protocolo se utiliza para identificar la capa de mayor nivel más cercana usando el IP. Este es un campo de 0 bits, que normalmente identifica tanto la capa TCP (valor 6), como la capa UDP (valor 17) en el nivel de transporte, pero puede identificar hasta 255 protocolos de la capa de transporte.

Checksum. La verificación o prueba suma modulo 2, proporciona la seguridad de que el datagrama no ha sido dañado ni modificado. Este campo tiene una longitud de 16 bits.
La verificación por suma módulo 2 incluye todos los campos de todos los campos de la cabecera IP, incluido el mismo, cuyo valor es cero a efectos de cálculo.

Un Gateways o nodo que efectué alguna modificación en los campos de la cabecera (por ejemplo en el tiempo de vida), debe recalcular el valor del checksum antes de enviar el datagrama.

Dirección de Origen. Este campo contiene un identificador de red (Netid) y un identificador de Host (Hostid). El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C.

Dirección de Destino. Este campo contiene el Netid y el Hostid del destino. El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C o D

La existencia de este campo viene determinada por la longitud de la cabecera. Si esta es mayor de cinco, por lo menos existe una opción.

Aunque un Host no esta obligado a ofrecer opciones, puede aceptar y procesar opciones recibidas en un datagrama. El campo Opciones es de longitud variable. Cada octeto esta formado por los campos Copia, Clase de Opción y Número de Opción.

El campo Copia sirve para que cuando un datagrama va a ser fragmentado y viaja a través de nodos o Gateways. Cuando tiene valor 1, las opciones son las mismas para todos los fragmentos, pero si toma valor 0, las opciones son eliminadas.

Clase de Opción es un campo que cuando tiene valor 0, indica datagrama o control de red; Cuando tiene valor 2, indica depuración o medida. Los valores 1 y 3 están reservados para un uso futuro. El Número de Opción indica una acción específica.

Cuando esta presente el campo Pad, (completar) consiste en 1 a 3 octetos puestos a cero, si es necesario, para hacer que el número total de octetos en la cabecera sea divisible por cuatro.

El campo datos consiste en una cadena de octetos. Cada octeto tiene un valor entre 0 y 255. El tamaño de la cadena puede tener un mínimo y un máximo, dependiendo del medio físico. El tamaño máximo esta definido por la longitud total del datagrama. El tamaño del campo Datos en octetos es igual a: (Longitud Total del Datagrama) - (Longitud de la cabecera)

Puertos IP.

Un puerto es un número que identifica a una aplicación. Esta numeración se corresponde con una convención ya adoptada como estándar. Este número de puerto permite identificar a TCP el tipo de servicio que se le requiere. Muchos sistemas mantienen un fichero con los números de puerto y su servicio correspondiente.

Modelo IEEE.

Otro modelo de red fue desarrollado por el mismo instituto de Ingenieros Eléctricos y Electrónica (IEEE). Debido a la proliferación de Redes de Área Local (LAN) muchos productos aparecieron, y con ello la necesidad de una consistencia, entonces la IEEE empezó a definir estándares de red. El proyecto fue llamado 802, por el año y el mes en que empezó: Febrero de 1980.

Del proyecto 802 resultaron numerosos documentos, incluyendo los tres principales estándares para topologías de red.

- 802.3 define estándares para redes de bus, tales como Ethernet, que usa un mecanismo llamado CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

- 802.4 define estándares para redes de "token" en bus. (La arquitectura de ArcNet es similar a este estándar en muchas maneras).

- 80.5 define estándares para redes de "token-ring".

Arquitectura Ethernet.

A finales de 1960, la universidad de Hawai desarrolló una red de área amplia (WAN, Red que se extiende a través de un área geográfica mayor a una LAN). La universidad necesitaba conectar varias computadoras que estaban esparcidas a través de su campus. La pieza principal en el diseño de la red fue llamado Carrier-Sense Multiple Access with Collision

Detection Carrier-Sense (CSMA/CD). Significa que la computadora escucha el cable de la red y espera hasta un periodo de silencio para poder mandar su mensaje. Multiple Access se refiere a que múltiples computadoras pueden estar conectadas en el mismo cable de red.

Collision Detection es una protección contra mensajes chocando en el transito.

Este temprano diseño de red fue la fundación de lo que hoy es Ethernet. En 1972, Xerox Corporation creó el experimental Ethernet, y en 1975 introdujo el primer producto Ethernet. La versión original de este producto de red fue diseñado como un sistema de 2.94mbps (Megabits por segundos) conectando hasta 100 computadoras en un cable de un kilómetro.

El Ethernet de Xerox fue tan exitoso que Xerox, Intel y Digital crearon un estándar para Ethernet de 10mbps. Este diseño fue la base de la especificación IEEE 802.3. El producto Ethernet se apega en la mayoría de las partes del estándar 802.3.

El CSMA/CD funciona de la siguiente manera: cuando una computadora desea mandar información primero escucha el cable de la red para revisar que no se este usando en ese precioso momento (Carrier-Sense). Esto se oye muy sencillo, pero el problema reside en que dos o más computadoras al escuchar que no se esta usando el cable pueden mandar el exacto mismo momento su información (Multiple Access), y como solamente puede haber uno y sólo un mensaje en tránsito en el cable se produce una colisión. Entonces las computadoras detectan la colisión y deciden reenviar su información a un intervalo al azar, es importante que sea al azar ya que si ambas computadoras tuvieran el mismo intervalo fijo se produciría un ciclo vicioso de colisiones y reenvíos (Collision Detection). Así por ejemplo al detectar la colisión una computadora se espera tres milisegundos y la otra cinco milisegundos, siendo obvio que una computadora reenviara en primer lugar y la otra esperará a que el cable este de nuevo sin tránsito.

Evidentemente que en una misma red Ethernet al haber muchas computadoras tratando de enviar datos al mismo tiempo y/o al haber una transferencia masiva de datos se crea un gran porcentaje de colisiones y utilización. Si se pasa del 1% de colisiones y/o 15% de utilización de cable ya se dice que la red está saturada. Además, las señales de este tipo de red tienden a degradarse con la distancia debido a la resistencia, la capacidad u otros factores. Inclusive la señal todavía se puede distorsionar por las interferencias eléctricas exteriores generadas por los motores, las luces fluorescentes y otros dispositivos eléctricos.

Cuanto más se aumenta la velocidad de transmisión de los datos. Más susceptible es la señal a degradarse. Por esta razón las normas de Ethernet especifican los tipos de cables, los protectores y las distancias del mismo, la velocidad de transmisión y otros detalles para trabajar y proporcionar un servicio relativamente libre de errores en la mayoría de los entornos.

Las redes Ethernet pueden utilizar diferentes tipos de cableado, cada uno con sus beneficios y problemas. Los tres cableados más comunes son Thinnet, Thicknet, y Twisted Pair (Par trenzado).

Thinnet ó 10Base2 puede transmitir datos a 10mbps por Banda Base (señales digitales), pudiendo llegar el cableado hasta 185 metros. Se utiliza cable coaxial RG-58 el cual es bastante barato por lo que a esta red también se le conoce como CheapNet. Un mismo segmento de cable puede soportar hasta 30 computadoras. Es el más utilizado y recomendado para redes pequeñas. Utiliza la topología local bus, donde un mismo cable recorre todas y cada una de las computadoras.

Thicknet ó 10Base5 transmite datos a 10mbps por Banda Base en un cableado que puede alcanzar 500 metros. El cableado es grueso y es utilizado principalmente para largas oficinas o hasta todas las computadoras de un edificio. Del cable principal (backbone) salen cables usualmente Par Trenzado que se conectan a directamente a cada una de las computadoras. Se pueden conectar hasta 100 computadoras con este cableado en un mismo segmento.

Twisted Pair ó 10BaseT transmite datos a 10mbps por Banda Base y utiliza un Hub (concentrador) desde el cual con cable Par Trenzado se conecta cada una de las computadoras quedando en forma similar a estrella. El Hub queda en el centro de la estrella y funciona como "repetidor". El cable desde el Hub hasta la computadora no debe de medir más de 100 metros.

Arquitectura token ring.

La red Token-Ring es una implementación del estándar IEEE 802.5, en el cual se distingue más por su método de transmitir la información que por la forma en que se conectan las computadoras.

El primer diseño de una red de Token-Ring es atribuido a E. E. Newhall en 1969. IBM publicó por primera vez su topología de Token-Ring en marzo de 1982, cuando esta compañía presento los papeles para el proyecto 802 del IEEE. IBM anunció un producto Token-Ring en 1984, y en 1985 éste llegó a ser un estándar de ANSI/IEEE.

A diferencia del Ethernet, aquí un Token (Ficha Virtual) es pasado de computadora a computadora como si fuera una papa caliente. Cuando una computadora desea mandar información debe de esperar a que le llegue el Token vacío, cuando le llega utiliza el Token para mandar la información a otra computadora, entonces cuando la otra computadora recibe la información regresa el Token a la computadora que envió con el mensaje de que fue recibida la información. Así se libera el Token para volver a ser usado por cualquiera otra computadora. Aquí debido a que una computadora requiere el Token para enviar información no hay colisiones, el problema reside en el tiempo que debe esperar una computadora para obtener el Token sin utilizar.

Los datos en Token-Ring se transmiten a 4 ó 16mbps, depende de la implementación que se haga. Todos los equipos se deben de configurar con la misma velocidad para que funcione la red. Cada computadora se conecta a través de cable Par Trenzado ya sea blindado o no a un concentrador llamado MAU (Media Access Unit), y aunque la red queda físicamente en forma de estrella, lógicamente funciona en forma de anillo por el cual da vueltas el Token. En realidad es el MAU es que contiene internamente el anillo y si falla una conexión automáticamente la ignora para mantener cerrado el anillo.

Un MAU puede soportar hasta 72 computadoras conectadas y el cable del MAU a la computadora puede ser hasta de 100 metros utilizando Par Trenzado Blindado, o 45 metros sin blindaje. El Token-Ring es eficiente para mover datos a través de la red. En redes pequeñas a medianas con tráfico de datos pesado el Token Ring es más eficiente que Ethernet. Por el otro lado, el ruteo directo de datos en Ethernet tiende a ser un poco mejor en redes que incluyen un gran número de computadoras con tráfico bajo o moderado.

Componentes de una red local.

Para el funcionamiento de una red local se necesitan varios componentes que realizarán determinadas tareas. A grandes rasgos son los siguientes:

Estaciones de trabajo: Son todas aquellas microcomputadoras desde las cuales un usuario puede utilizar la red.

Servidor de Archivos: Es aquel equipo que permite compartir los archivos y programas que se encuentren en su(s) disco(s). Ordinariamente funciona también como servidor de impresoras.

Tarjetas de Red: Cada nodo de la red, o sea la estación de trabajo o servidor de archivos, debe contar con una tarjeta de red. La tarjeta de red del servidor de archivos puede ser ligeramente diferente de las utilizadas en las estaciones de trabajo.

Sistema de Cableado: Además del cable pueden ser necesarios algunos elementos adicionales asociados con él, como cajas de conexiones, conectores especiales, etc.

Sistema Operativo de Red: Adicionalmente al MS-DOS es necesario que exista un sistema operativo para que administre las funciones de la red. Este sistema tiene dos partes: la del servidor de archivos y de las estaciones de trabajo.

Software de Aplicación: En última instancia, todos los elementos anteriores, son el funcionamiento para que el usuario de cada equipo, pueda utilizar sus programas y archivos específicos. Este software puede ser tan amplio como se necesite ya que incluye procesadores de palabra, paquetes integrados, sistemas administrativos de contabilidad y áreas afines, sistemas especializados (Por ejemplo control de producción), correos electrónicos, etc.

Ventajas de las redes locales.

Entre las ventajas de utilizar una red se encuentran:

- Posibilidad de compartir periféricos costosos como son: impresoras láser, módem, fax, etc.
- Posibilidad de compartir grandes cantidades de información a través de distintos programas, bases de datos, etc., de manera que sea más fácil su uso y actualización.
- Reduce e incluso elimina la duplicidad de trabajos.
- Permite utilizar el correo electrónico para enviar o recibir mensajes de diferentes usuarios de la misma red e incluso de redes diferentes.
- Reemplaza o complementa minicomputadoras de forma eficiente y con un costo bastante más reducido.
- Establece enlaces con mainframes. De esta forma, una Computadora de gran potencia actúa como servidor haciendo que pueda acceder a los recursos disponibles cada una de las Computadoras personales conectadas.
- Permite mejorar la seguridad y control de la información que se utiliza, permitiendo el acceso de determinados usuarios únicamente a cierta información o impidiendo la modificación de diversos datos.

Inicialmente, la instalación de una red se realiza para compartir los dispositivos periféricos u otros dispositivos de salida caros, por ejemplo, las impresoras láser, los fax, etc.

Pero a medida que va creciendo la red, el compartir dichos dispositivos pierde relevancia en comparación con el resto de las ventajas. Las redes enlazan también a las personas proporcionando una herramienta efectiva para la comunicación a través del correo electrónico. Los mensajes se envían instantáneamente a través de la red, los planes de trabajo pueden actualizarse tan pronto como ocurran cambios y se pueden planificar las reuniones sin necesidad de llamadas telefónicas.

Transmisión inalámbrica.

Se utilizan medios no guiados, principalmente el aire. Se radia energía electromagnética por medio de una antena y luego se recibe esta energía con otra antena.

Hay dos configuraciones para la emisión y recepción de esta energía: direccional y omnidireccional. En la direccional la energía se concentra en un haz que se emite en una cierta dirección, por lo que tanto el emisor como el receptor deben estar alineados. En el método omnidireccional, la energía es dispersada en múltiples direcciones, por lo que varias antenas pueden captarla; mientras mas grande es la frecuencia de la señal a transmitir, más factible es la transmisión unidireccional.

Por tanto, para enlaces punto a punto se suelen utilizar microondas (altas frecuencias) Para los enlaces donde hay varios receptores posibles se utilizan las ondas de radio (bajas frecuencias). Los infrarrojos se utilizan para transmisiones a muy corta distancia (en una misma habitación).

Microondas terrestres.

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

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

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

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

Microondas por satélite.

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

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

Se suele utilizar este sistema para:

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

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

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

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

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

Infrarrojos.

No es una técnica muy usada. Se usan frecuencias muy altas para el transporte de datos. Como la luz, los infrarrojos no pueden traspasar objetos opacos. Por lo que o bien se utiliza una comunicación con línea de visión directa o bien es una difusión.

Sistemas directos baratos se utilizan en redes personales de área reducida y ocasionalmente en LAN's específicas. No es práctico para redes de usuarios móviles por lo que únicamente se implementa en subredes fijas. Los sistemas de difusión IR no requieren línea de visión pero las células están limitadas a habitaciones individuales.

Los emisores y receptores de infrarrojos deben estar alineados o bien estar en línea tras la posible reflexión de rayo en superficies como las paredes. En infrarrojos no existen problemas de seguridad ni de interferencias ya que estos rayos no pueden atravesar los objetos (paredes por ejemplo). Tampoco es

necesario permiso para su utilización (en microondas y ondas de radio si es necesario un permiso para asignar una frecuencia de uso).

WLAN

WLAN son las siglas en inglés de Wirless Local Area Network, o lo que es lo mismo Redes de Área Local Inalámbricas.

Es un sistema de comunicación de datos flexible utilizado como alternativa a la LAN cableada o como una extensión de ésta, ya que elimina la utilización de cables.

Las redes inalámbricas se desarrollan sobre una serie de tecnologías inalámbricas diferentes, cada una de las cuales tiene rutas claras de evolución a las redes de próxima generación para alinearse con las demandas y requisitos de operadores y suscriptores en todo el planeta, entre las que se incluyen: CDMA/CDMA2000 1X y 1xEV, TDMA, GSM, GPRS, EDGE y UMTS.

Es clara la alta dependencia en los negocios de la redes de comunicación. Por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad.

La red inalámbrica presenta las siguientes ventajas con respecto a la red tradicional:

- Movilidad: Que permite obtener información en tiempo real en cualquier lugar de la organización para todo usuario de la red; dejando una mayor productividad y posibilidades de servicio.
- Facilidad de instalación: Evita el trabajo de cableado.
- Flexibilidad: Permite llegar a lugares donde el cable no se puede instalar.
- Reducción de costes: Si se toma en cuenta que pueden existir cambios frecuentes en el entorno el coste inicialmente se reduce significativamente, además de tener mayor tiempo de vida y menor gasto de instalación.
- Escalabilidad: Son sencillos el cambio de topología de red. Así mismo la red puede ser más extensa sin tener que mover o instalar cables.

Sin embargo estas redes también presentan sus desventajas:

- Tiene un elevado coste inicial que se ve aun más acentuado en comparación con el bajo coste de las redes con cable.
- Sus bajas velocidades de transmisión ya que la máxima velocidad que se puede alcanzar es de 10 Mbps.

Según el diseño requerido se tienen distintas tecnologías aplicables:

- Banda estrecha. Se transmite y recibe en una específica banda de frecuencia lo más estrecha posible para el paso de información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias. Así mismo un filtro en el receptor de radio se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada.
- Banda ancha. Es el usado por la mayor parte de los sistemas sin cable. Fue desarrollado por los militares para una comunicación segura, fiable y en misiones críticas. Se consume más ancho de banda pero la señal es más fácil de detectar. El receptor conoce los parámetros de la señal que se ha difundido. En caso de no estar en la correcta frecuencia el receptor, la señal aparece como ruido de fondo. Hay dos tipos de tecnología en banda ancha:
  a) Frecuencia esperada (FHSS: Frecuency-Hopping Spread Spectrum): utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado es como tener un único canal lógico. Para un receptor no sincronizado FHSS es como un ruido de impulsos de corta duración.
  b) Secuencia directa (DSSS: Direct-Sequence Spread Spectrum): se genera un bit redundante por cada bit transmitido. Estos bits redundantes se conocen como chipping code. Entre más grande es la secuencia mayor es la probabilidad de reconstruir los datos originales. Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado.

Medios de transmisión WLAN.

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponer a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia.

Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto.

En una configuración típica de LAN sin cable los puntos de acceso conectan la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

La antena conectada al punto de acceso es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena.

La naturaleza de la conexión sin cable es transparente al sistema del cliente.

Configuración de la WLAN.

Pueden ser simples o complejas. La más básica se da entre dos equipos equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual.

Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.

Figura 1. Red peer-to-peer

Instalando un Punto de Acceso (APs) se puede doblar el rango al cuál los dispositivos pueden comunicarse, pues actúan como repetidores. Desde que el punto de acceso se conecta a la red cableada cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso puede servir a varios clientes, según el número de transmisiones que tienen lugar.

Figura 2. Cliente y punto de acceso

Los puntos de acceso tienen un rango finito, del orden de 150m en lugares cerrados y 300m en zonas abiertas. En zonas grandes es recomendable más de un punto de acceso que cubra el área con células de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Conocido como roaming.

Figura 3. Múltiples puntos de acceso y roaming.

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso. Estos extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión.

Figura 4. Uso de un punto de extensión.

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cuál permite una conexión sin cable en esta aplicación.

Figura 5**.** Utilización de antenas direccionales.

La distancia que pueden alcanzar las ondas de Radiofrecuencia (**RF**) o de Infrarrojos (**IR**) esta en función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso la gente, afectan a la propagación de la energía, por ejemplo los objetos sólidos bloquean las señales de infrarrojos dificultando la transmisión.

La mayor parte de los sistemas de redes inalámbricas usan RF porque pueden penetrar la mayor parte de obstáculos. El rango de cobertura de una Lan inalámbrica típica va de 30m. a 100m. Puede extenderse y tener posibilidad de alto grado de libertad y movilidad utilizando puntos de acceso (microcélulas).

La mayor parte de LAN's inalámbricas proporcionan un estándar de interconexión con redes cableadas como Ethernet o Token Ring. Los nodos de la red inalámbrica son soportados por el sistema de la red de la misma manera que cualquier otro nodo de una red LAN, aunque con los manejadores apropiados. Una vez instalado, la red trata los nodos inalámbricos igual que cualquier otro componente de la red.

Los consumidores deben ser conscientes de que los sistemas inalámbricos de redes LAN de distintos vendedores pueden no ser compatibles para operar juntos por tres razones:

- Diferentes tecnologías no interoperarán. Un sistema basado en la tecnología de Frecuencia esperada (FHSS) no se comunicará con otro basado en la tecnología de Secuencia directa (DSSS).
- Sistemas que utilizan distinta banda de frecuencias no podrán comunicar aunque utilicen la misma tecnología.
- Aún utilizando igual tecnología y banda de frecuencias ambos vendedores, los sistemas de cada uno no comunicarán debido a diferencias en la implementación de cada fabricante.

La naturaleza en que se basan las redes inalámbricas implica que cualquier otro producto que transmita energía a la misma frecuencia puede dar cierto grado de interferencia en un sistema Lan inalámbrico. Sin embargo la mayor parte de fabricantes diseñan sus productos teniendo en cuenta las interferencias por microondas. Otro problema es la colocación de varias redes inalámbricas en lugares próximos.

Las LAN inalámbricas son sencillas de usar ya que los usuarios necesitan muy poca información a añadir a la que ya tienen sobre redes Lan en general, para utilizar una Lan inalámbrica, porque la naturaleza inalámbrica de la red es transparente al usuario, las aplicaciones trabajan de igual manera que lo hacían en una red cableada.

Los productos de una Lan inalámbrica incorporan herramientas de diagnóstico para dirigir los problemas asociados a los elementos inalámbricos del sistema. Sin embargo, los productos están diseñados para que los usuarios rara vez tengan que utilizarlos.

Las LAN inalámbricas simplifican muchos de los problemas de instalación y configuración que atormentan a los que dirigen la red. Ya que únicamente los puntos de acceso de las redes inalámbricas necesitan cable, ya no es necesario llevar cable hasta el usuario final. La falta de cable hace también que los cambios, extensiones y desplazamientos sean operaciones triviales en una red inalámbrica. Finalmente, la naturaleza portable de las redes inalámbricas permite a los encargados de la red preconfigurar ésta y resolver problemas antes de su instalación en un lugar remoto. Una vez configurada la red puede llevarse de un lugar a otro con muy poca o ninguna modificación.

Puesto que la tecnología inalámbrica se ha desarrollado en aplicaciones militares, la seguridad ha sido uno de los criterios de diseño para los dispositivos inalámbricos. Normalmente se suministran elementos de seguridad dentro de la Lan inalámbrica, haciendo que estas sean más seguras que la mayor parte de redes cableadas. Es muy complicado que los receptores no sintonizados escuchar el tráfico que se da en la Lan.

Complejas técnicas de encriptado hacen imposible para todos, incluso los más sofisticados, acceder de forma no autorizada al tráfico de la red. En general los nodos individuales deben tener habilitada la seguridad antes de poder participar en el tráfico de la red.

La instalación de una Lan inalámbrica incluye los costes de infraestructura para los puntos de acceso y los costes de usuario par los adaptadores de la red inalámbrica. Los costes de infraestructura dependen fundamentalmente del número de puntos de acceso desplegados. El número de puntos de acceso depende de la cobertura requerida y del número y tipo de usuarios.

El coste de instalación y mantenimiento de una WLAN generalmente es más bajo que el coste de instalación y mantenimiento de una red cableada tradicional, por dos razones:

En primer lugar una red WLAN elimina directamente los costes de cableado y el trabajo asociado con la instalación y reparación.

En segundo lugar una red WLAN simplifica los cambios, desplazamientos y extensiones, por lo que se reducen los costes indirectos de los usuarios sin todo su equipo de trabajo y de administración.

Las redes WLAN pueden ser diseñadas para ser extremadamente simples o bastante complejas. WLAN's pueden soportar un amplio número de nodos y/o extensas áreas físicas añadiendo puntos de acceso para dar energía a la señal o para extender la cobertura.

Los productos WLAN de los usuarios finales están diseñados para funcionar sin corriente de alimentación, puesto que no existe conexión propia cableada. Los fabricantes emplean técnicas especiales para maximizar el uso de la energía del computador y el tiempo de vida de su batería.

La potencia de salida de los sistemas WLAN es muy baja, mucho menor que la de un teléfono móvil. Puesto que las señales de radio se atenúan con la distancia, la exposición a la energía de radio-frecuencia en el área de la WLAN es muy pequeña.

Las WLAN's deben cumplir las estrictas normas de seguridad dictadas por el gobierno y la industria. No se han atribuido nunca efectos secundarios en la salud a causa de una WLAN.

Debido a la diversidad de productos existentes se reconoció la necesidad de desarrollar normas internacionales para regular el uso de redes inalámbricas. En la actualidad existen dos normas una desarrollada por la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) la 802.11 y la otra es la europea desarrollada por el ETSI (Instituto de Estándares de Telecomunicaciones Europeo) conocida como Hiperlan.

El IEEE 802.11 define opciones de la capa física para la transmisión inalámbrica y la capa de protocolos MAC.

El estándar IEEE 802.11 define el protocolo para dos tipos de redes:

1. Redes Ad-hoc.
2. Redes cliente / servidor.

Una red Ad-hoc es una red simple donde se establecen comunicaciones entre los múltiples equipos en un área de cobertura dada sin el uso de un punto de acceso o servidor. La norma especifica la etiqueta que cada equipo debe observar para que todas ellas tengan un acceso justo a los medios de comunicación inalámbricos. Proporciona métodos de petición de arbitraje para utilizar el medio asegurando que el rendimiento se maximiza para todos los usuarios del conjunto de servicios base.

Las redes cliente / servidor utilizan un punto de acceso que controla la asignación del tiempo de transmisión para todos los equipos y permite que equipos móviles deambulen por la columna vertebral de la red cliente / servidor. El punto de acceso se usa para manejar el tráfico desde la radio móvil hasta las redes cliente / servidor cableadas o inalámbricas. Esta configuración permite coordinación puntual de todos los equipos en el área de servicios base y asegura un manejo apropiado del tráfico de datos. El punto de acceso dirige datos entre los equipos y otros equipos inalámbricos y/o el servidor de la red. Típicamente las WLAN controladas por un punto de acceso central proporcionará un rendimiento mucho mayor

La especificación de la capa MAC para la 802.11 tiene similitudes a la de Ethernet cableada de línea normal 802.3. El protocolo para 802.11 utiliza un tipo de método de acceso conocido como CSMA/CA (Carrier-Sense, Múltiple Access, Collision Avoidance). Este evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3. Es difícil descubrir colisiones en una red de transmisión RF y es por esta razón por la que se usa la anulación de colisión. La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación de canales 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 MAC se le da el estado del canal vacío para la transmisión de los datos. 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; el sentido de la portadora puede usarse para determinar si el canal 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.

El protocolo CSMA/CA permite opciones que pueden minimizar colisiones utilizando peticiones de envío (RTS), listo para enviar (CTS), datos y tramas de transmisión de reconocimientos (ACK), de una forma secuencial. Las comunicaciones se establecen cuando uno de los nodos inalámbricos envía una trama RTS. La trama RTS incluye el destino y la longitud del mensaje. La duración del mensaje es conocida como el vector de asignación de red (NAV). El NAV alerta a todos los otros en el medio, para retirarse durante la duración de la transmisión. Los equipos receptores emiten una trama CTS, que hace eco a los remitentes y al vector NAV. Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS empiezan de nuevo.

Después de que se recibe la trama de los datos, se devuelve una trama ACK, que verifica una transmisión de datos exitosa.

La norma HiperLan no tiene bien definidos algunos de sus parámetros operativos pero la especificación que se tiene hasta el momento es:

- Tasa de bits de usuario de 10 a 20 Mbps
- Alcance operativo de 50 metros.
- Medio de transmisión radiofrecuencia.
- Modulación de portadora única mediante una versión modificada de la modulación de cambio de fase en cuadratura (QPSK) y un ecualizador.
- Método de acceso CSMA/CD o CSMA/CA.

A fin de adaptarse a los diferentes tipos de modulación y medios, la capa física se divide en dos la subcapa de convergencia de capas físicas (PLC) y la subcapa dependiente del medio físico (PMD).

La PMD es diferente para los diferentes tipos de modulación y medios y la PLC realiza la conversión para hacer corresponder los servicios estándar que ofrecen en la interfaz.

Capitulo II

Comunicación inalámbrica y normatividad

Historia de la WLAN.

A pesar de que la tecnología inalámbrica empieza a tomar forma a partir de la década de los ochenta los verdaderos orígenes datan desde la aparición de la radiodifusión, considerado como el fundamento de las LAN inalámbricas.

Un dispositivo diseñado para producir ondas electromagnéticas mediante un cambio de la dirección de la corriente eléctrica, un proceso que se conoce como oscilación, es en esencia un transmisor. Con este principio Heinrich Hertz, en 1880, desarrollo un equipo que envió y recibió ondas electromagnéticas a través del aire. Este equipo era capaz de aumentar el número de ondas que se producían en un periodo determinado, su frecuencia y velocidad de cambio; de aquí que su nombre se convirtiera en la unidad de medida para la frecuencia. Mas tarde Guglielmo Marconi tomó estos primeros trabajos para crear una aplicación práctica conocida como la radio. En 1895 Marconi envió y recibió su primera transmisión de radio a través de ático de la villa de sus padres, el siguiente año logro realizar transmisiones de hasta una milla. A medida que mejoro sus transmisores y antenas las distancias se incrementaron rápidamente y significativamente; al descubrir el potencial de su equipo Marconi formó una compañía, la Wireless Telegraph and Signal Company Limited. Sus equipos inalámbricos se usaron para las comunicaciones entre los barcos y tierra firme, además de aplicaciones terrestres que reemplazaron los sistemas alámbricos.

El mundo de la tecnología inalámbrica ha recorrido un camino muy largo desde los primeros trabajos hasta la fecha. En 1923 el gobierno de Estados Unidos inició el proceso de dividir el espectro de frecuencias de radio en asignaciones para usos y usuarios específicos.

El mundo de la radio siguió innovando y Hedy Lamarr, actriz, y George Antheil, compositor, cooperaron para crear un sistema para emitir comunicaciones de radio de banda angosta a través de una banda ancha en el espectro de frecuencia, como un medio para guiar torpedos hacia sus blancos de una manera menos susceptible a las técnicas de obstrucción de frecuencias, espionaje. Esto se realizó con el fin de lograr que la frecuencia que utilizaban el controlador y el torpedo para comunicarse se cambiara o saltara de un canal al siguiente mediante un modelo predeterminado y coordinado; tomaron como referencia para el número de saltos, el número de teclas de un piano 88.

Para obstruir una señal que se extiende a través de una porción grande del espectro de frecuencia, debería ser obstruido todo el espectro en el que se distribuye la señal, al lograr que la señal saltara de una frecuencia a otra, dentro de un patrón determinado y solo conocido por el emisor y el receptor, el patrón tendría que ser descubierto por la parte interceptora.

En los años sesenta una computadora logró controlar los patrones de saltos en la frecuencia del espectro extendido, logrando que la comunicación por radio de espectro extendido se convirtiera en la base de las comunicaciones seguras, sólidas y libres de obstrucciones de las instituciones militares.

El primer precursor de las LAN inalámbricas es un sistema remoto de área amplia conocido como ALOHANET, un sistema inalámbrico que conectaba a las islas hawaianas; este fue el primer sistema creado para enviar paquetes de datos a través de radios con una velocidad de operación de 9,600 bps, así mismo representa la base de la tecnología de área local cableada Ethernet.

Para 1985 se establecieron las regulaciones que permitieron el uso público del espectro extendido. Por lo que un año mas tarde se crea en Toronto una compañía Telesystems SLW, que diseña una variación del sistema de cambio de frecuencia. En lugar de hacer que la señal de banda angosta saltara de una frecuencia a la siguiente a través de un ancho de banda establecido; Telesystems empleó un sistema que se conoce como secuencia directa, donde una señal de banda angosta se extiende a través de un conjunto de frecuencias más grandes. El resultado es similar, la señal de banda angosta que se extiende a través de un ancho de banda mas amplio es menos susceptible a las interferencias debido a que solo una parte de la señal multiplicada necesita alcanzar al receptor esperado para que la transmisión sea exitosa. Además la señal de secuencia directa proporcionaba en ese momento el mismo nivel de seguridad que el salto de frecuencia, en la medida que la capacidad disminuida por unidad del ancho de banda hacia que la señal fuera menos discernible del ruido.

En 1988 fue introducido al mercado el primer sistema comercial basado en la tecnología secuencia directa en el espectro extendido (DSSS); que trabajaban sobre una banda sin licencia establecida alrededor de 902 y 928 MHz. Debido a que esta banda se ubicaba cerca de la banda de los teléfonos celulares análogos, proporciona a los fabricantes la ventaja de construir sus dispositivos con componentes ya existentes que originalmente estaban destinados a los teléfonos.

Los primeros productos de Telesystems fueron diseñados como reemplazo de los cables, ya sea para conectar múltiples computadoras de escritorio con una estación central, o para conectar las redes de edificios separados de modo semejante a como funciona un puente. Al ejecutar NetWare de Novell, el sistema operativo de red y al proporcionar una velocidad de datos de aproximadamente 200 Kbps, estas se convirtieron en las primeras LAN inalámbricas para entornos de oficina. No obstante que estas redes representaban ventajas importantes, lo cierto es que estaban muy adelantados

a su tiempo y proporcionaban una relación entre precio y desempeño insuficiente para obtener el tipo de aceptación necesaria para sostenerse en el mercado.

Debido a que la operación de la banda de 900 MHz se proporciono para una infraestructura a través de Estado Unidos, Canadá y Australia existía una limitación para otras partes del mundo; por lo que los fabricantes empezaron a producir radios que operaban en la parte de los 2.4 GHz del espectro de frecuencia que estaba disponible para la operación libre de licencia en la mayor parte de Europa y Japón.

En 1991 diversos representantes de una variedad de partes interesadas emitieron una solicitud de autorización al Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) con el fin de establecer un estándar interoperable para las LAN inalámbrica; ya que la IEEE es una organización internacional, como regla se inclina hacia los estándares que tienen una aplicación alrededor de todo el mundo, por lo que la tendencia fue hacia el grupo recién formado en torno a la banda 2.4 GHz.

Dos años después los fundamentos del estándar estaban establecidos y en junio de 1997 el estándar 802.11 del IEEE fue ratificado. Este primer estándar proporcionaba velocidades de datos de 1 y 2 Mbps, una forma rudimentaria de cifrado de datos (Wired Equivalent Privacy WEP), así como la transmisión a través de las tecnologías de secuencia directa y de salto de frecuencia sobre una banda de 2.4 GHz además de los rayos infrarrojos. El primer estándar 802.11 marcó el comienzo de una nueva era y estableció los fundamentos para el siguiente estándar 802.11b que se ratifico en 1999 y ofrece una velocidad de datos de 11Mbps, aproximadamente la misma velocidad que el estándar Ethernet.

Estándares de WLAN

La definición de un estándar no es de ninguna manera banal. El aspecto aún más elemental de cuando se debe adoptar un estándar es tan importante como el estándar mismo, debido a que vivimos en un mundo donde los conceptos, desarrollo y despliegue de tecnología se realizan en periodos que disminuyen con rapidez.

En el mundo de las WLAN, tenemos la suerte de contar con ciertos estándares fundamentales que han sido ratificados a nivel global, por ejemplo, la frecuencia, la energía y el tiempo. Un enlace WLAN que opera a 2.4 GHz se entiende y acepta de la misma forma Japón, Inglaterra, Canadá y Estados Unidos.

La frecuencia de 2.4 GHz está, en la mayor parte de las naciones, apartada para el propósito de tener un sistema de frecuencia de radio libre de licencia y probablemente, es la única frecuencia que esta tan bien adoptada, desplegada y caracterizada.

Mas aún, dada la idea de la estandarización del ancho de banda, el uso WLAN de doble sentido sigue siendo de alguna forma nuevo para grupos reguladores, instituciones internacionales y grupos de desarrollo de estándares que luchan por el control y autoridad para asignar y dedicar, o ambas frecuencias especificas para usos particulares en diferentes países.

La falta de estándares en la frecuencia y en la potencia de salida a un nivel internacional ha obligado a algunos fabricantes de hardware a adoptar múltiples productos y diseñar unidades RF especificas, de manera que funcionen en asignaciones de bandas de frecuencias para países específicos. Si este enfoque no existiera, los países con bandas de frecuencias distintas a las de las principales superpotencias que generan ganancias, se quedarían sin alternativas para el ancho de banda asignado a las aplicaciones inalámbricas. Esta es una de las razones principales por las que algunas compañías han adoptado arquitecturas que permiten que el equipo interno, por ejemplo los direccionadores e interruptores en cada extremo de los enlaces de radiodifusión, sean independientes de la frecuencia portadora de la onda, canalización, requerimientos de energía y otros parámetros que residen en los radios que operan en la parte exterior de la red. Aún así, este enfoque requiere de múltiples unidades externas de uno o más proveedores de tecnologías, lo que depende del país en particular.

Desarrollo de los estándares.

Los estándares aparecen en las frases intermedias o finales del ciclo de vida de una tecnología, en lugar de la frase introductoria en la que llega una tecnología al mercado. En otras palabras, por lo común los estándares aparecen después de que se ha desplegado ampliamente las tecnologías y no al revés. El orden en el que surge un estándar normalmente es el siguiente:

1. Introducción de la tecnología nueva.
2. Interés relativamente alto de los desarrolladores.
3. Despliegue de la tecnología para los adoptadores tempranos.
4. Definición del estándar por uno o más proveedores de tecnología.
5. Establecimiento del estándar por una entidad de estándares.
6. Ratificación del estándar por los proveedores de la tecnología.

El orden anterior es el que en general refleja los estándares que crea el IEEE, no obstante que algunos estándares derivan esencialmente de los comentarios de solicitud mismos que se originan en el IEEE u otras entidades de estándares por ejemplo, el IETF. La información de estos RFC se convierte en estándares de facto debido a la adopción suficientemente amplia, aunque no siempre tienen que recorrer el proceso completo para la creación de los estándares que generalmente controla la IEEE.

La mayor parte de la formación de conceptos y evolución de las tecnologías nuevas en la industria de las redes la efectúan grupos de trabajo, comités y organizaciones que comparten ideas. Estos grupos están compuestos por miembros de distintos fabricantes, quienes compilan los documentos en proceso para llevarlos a sus compañías y trabajar en el desarrollo interno.

Existen tres estándares WLAN competidores desarrollados por organismos reconocidos internacionalmente, como el IEEE (Institute of Electrical and Electronics Engineers) y ETSI (European Telecommunications Standards Institute), que se han convertido en la base de los fabricantes para desarrollar sus productos.

1. HomeRF
2. Bluetooth
3. 802.11 (Wi-Fi)

Estándar HomeRF.

HomeRF es otra organización que ha desarrollado sus propios estándares para entrar de lleno al mundo de las redes inalámbricas. HomeRF ha sido desarrollado por el grupo de trabajo Home Radio Frequency, el cual está conformado por más de 50 compañías líderes en el ámbito mundial en las áreas de redes, periféricos, comunicaciones, software, semiconductores, etc. Este grupo fue fundado en marzo de 1988 para promover de manera masiva dispositivos de voz, datos y video alrededor de los hogares de manera inalámbrica; ya que tuvo sus orígenes en el teléfono inalámbrico digital mejorado.

El estándar HomeRF utiliza una combinación de CSMA/CD para los datos en paquetes y TDMA para el tráfico de voz y video, con el fin de optimizar el flujo del tráfico sobre una base de prioridad. La velocidad máxima de HomeRF es 10 Mbps, ideal para las aplicaciones caseras, aunque se manejan otras velocidades de 5, 1.6 y 0.8 Mbps en la banda de 2.4 GHz. Los medios mas importantes consideran que la prioridad es la transmisión y se identifica por los encabezados de la aplicación, mientras que el tráfico de voz y datos hace un balance del ancho de banda; usan buffers de tiempo y físicos para permitir el tráfico de voz y luego el de datos.

Este estándar incluye un conjunto impresionante de de capacidades de voz como identificador de llamadas, llamada en espera, regreso de llamadas e intercomunicación; debido a que esta baso en un estándar de voz desarrollado por las compañías telefónicas.

Según el grupo de trabajo, HomeRF es más ofrece más seguridad, los dispositivos consumen menos potencia que los productos de las tecnologías contrincantes, además de permitir aplicaciones para telefonía y video.

Estándar Bluetooth

Aunque Bluetooth en realidad es un estándar WLAN no compite directamente con el estándar 802.11 ya que Bluetooth tiene características diferentes, es una propuesta de especificación de radiofrecuencia por transmisión de corto alcance, transmisión de datos de punto a multipunto. Bluetooth puede transmitir a través de objetos sólidos no metálicos. Su potencia de transmisión es de hasta 100 Mw y su cable de unión nominal es de 10 cm a 10 m en teoría, pero se puede extender a 100 m mediante el incremento de transmisión de energía y se encuentra limitado a una velocidad de 1.5 Mbps; lo que es apenas una décima parte del estándar 802.11b. Su intención es conectar computadoras portátiles con teléfonos celulares, con PDA, con impresoras, las agendas electrónicas, los faxes, los teclados, los joysticks y prácticamente cualquier otro dispositivo digital.

Como características generales del Bluetooth podemos mencionar que el transmisor está integrado en un microchip de 9x9 milímetros y opera en una frecuencia de banda global de 2.4 GHz de la Industria Científica Médica (ISM) que asegura la compatibilidad universal y no requiere licencia para operar en ella. Usa la frecuencia de salto FH, con espectro extendido que cual divide la banda de frecuencia en un número de canales de salto. Durante la conexión, los transmisores de radio saltan de un canal a otro de forma aleatoria. Contiene servicios sincrónicos y asincrónicos; de fácil integración de TCP-IP.

En una red Bluetooth tenemos dos niveles, el primero es la picored (piconet), que se forma por un grupo de hasta ocho dispositivos, que se pueden ir adhiriendo de forma aleatoria. Las conexiones a la picored pueden ser entidad a entidad o establecer un “maestro” y el resto “esclavos” y el segundo es la red dispersa (scatter net), que se forma por múltiples, independientes y asíncronas picoredes.

Las primeras versiones de Bluetooth se emitieron a principios de 1999 y en la actualidad existen cerca de 2500 miembros de Bluetooth listados en el grupo de interés especial.

El estándar Bluetooth tiene dos puntos fuertes; el tamaño o forma que ofrece Bluetooth le permite conectarse en relojes de mano, PDA y otros dispositivos electrónicos pequeños en los que el tamaño es un criterio de diseño y el consumo de energía, Bluetooth usa 30 microamperes lo que representa una cantidad pequeña de energía, apenas una fracción de la empleada en un reloj de mano y utiliza ordenes de magnitudes mas bajas que las usadas por los teléfonos celulares.

En términos de seguridad cuenta con un método de cifrado, aunque con un esquema de saltos FHSS (espectro Extendido de Salto de Frecuencia) de 1600 saltos por segundo y un rango de 1 a 3 metros ocasionará que sea muy difícil interferir la comunicación a distancia.

Uno de los aspectos negativos de este estándar es que ha sido fuente de grandes discusiones; el grupo de interés especial predijo que para el año 2000 habría cerca de 200 millones de PC con dispositivos Bluetooth integrados en su fabricación, pero resulta que los fabricantes están adoptando tecnologías que aportan velocidades mas altas y rangos de transmisión y recepción mas extensos a los que proporciona Bluetooth; es por esto que la mayoría de los productos integran dispositivos con una opción 802.11.

Sin embargo en la actualidad la mayor parte de los productos Bluetooth que se encuentran en el mercado se usan principalmente para la conexión de teléfonos celulares, PDA, teclados, mouse, cámaras y dispositivos similares.

Las aplicaciones de Bluetooth son casi infinitas y permiten cambiar radicalmente la forma en la que los usuarios interactúan con los teléfonos móviles y otros dispositivos.

Las aplicaciones de Bluetooth se pueden agrupar dentro de la siguiente clasificación:

- Auriculares (Wireless headset) esta posibilidad permitirá la adopción de auriculares o audífonos al utilizar el teléfono; esto será posible aun si el aparato se encuentra dentro del portafolio o maleta.
- Puente de Internet (Internet bridge) Bluetooth permitirá que una computadora PC pueda acceder a Internet sin necesidad conectarse a una línea física de teléfono.
- Intercambio de archivos (File exchange) Esta opción permite el intercambio de archivos de computación sin la presencia de una red de infraestructura que lo sustente. Esta tecnología puede detectar automáticamente los aparatos Bluetooth dentro de una sala, por ejemplo, y transferir los archivos que la persona desee.
- Sincronización.- Bluetooth garantiza la sincronización inmediata entre los distintos aparatos equipados con este dispositivo

Impresión.- Los aparatos Bluetooth pueden identificar aquellas máquinas de impresión que cuentan con el dispositivo y mandar imprimir sus archivos

Wi – Fi

La expresión Wi-Fi (abreviatura de Wireless Fidelity) se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, Wireless Local Area Netwoks*).*

Wi- Fi es el nombre comercial desarrollado por un grupo comercio industrial llamado Wi – Fi Alliance. Este describe los productos de redes de área local inalámbricos basados en los estándares 802.11 del IEEE y esta diseñado para que tenga un nombre más accesible para los usuarios; al principio fue creado para describir solo los dispositivos con velocidades máximas de 11 Mbps que

operaban en la porción de 2.4 GHz del espectro de frecuencias y que cumplían con el estándar 802.11b, pero después se extendió para incluir los productos con velocidades de datos de 54Mbps que operan en la porción de 2.4 y 5 GHz del espectro de frecuencia y que están basados en las especificaciones 802.11g y 802.11a del IEEE. La siguiente tabla muestra todos los apartados provistos con la tecnología 802.11

Estándar	**Frecuencia portadora**	**Velocidad de datos**	**Resumen**
802.11a	5.1 - 5.2 GHz 5.2 - 5.3 GHz 5.7 - 5.8 GHz	54 Mbps	La potencia máxima es 40 mW en la banda 5.1, 250 mW en la banda 5.2 y 800 mW en 5.7
802.11b	2.4 – 2.485 GHz	11 Mbps	Es el estándar más popular
802.11c			Define las características que necesitan los AP para actuar como puentes.
802.11d			Múltiples dominios reguladores. Permite la comunicación en países que tienen restricciones sobre el uso de las frecuencias del protocolo 802.11
802.11e			Calidad de servicio. Actúa como arbitro en la comunicación permitiendo el envió de video y voz sobre IP
802.11f			Protocolo de conexión entre puntos de acceso IAPP (Inter-Access Point Protocol)
802.11g	2.4 – 2.485 GHz	36 o 54 Mbps	
802.11h			Selección dinámica de frecuencia DFS (Dynamic Frequency Selection) Además define el TPC (Transmit Power Control) según el cual la potencia de transmisión se adecua a la distancia a la que se encuentra el destinatario de la comunicación.
802.11i			Seguridad. Define la encriptación y la autentificación para complementar completar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP).
802.11j			Permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.
802.11i			Propuesto para el mantenimiento de las redes inalámbricas.

Velocidad y tipos de modulación.

Velocidades de datos.

Es importante observar que la especificación 802.11b que presenta los fundamentos para Wi-Fi soporta en realidad cuatro velocidades de datos en el mismo medio físico: 1, 2, 5.5 y 11 Mbps; en una porción de 80 MHz de amplitud del espectro de frecuencia iniciando en 2.4 GHz que luego se divide en 11 y 14 canales dependiendo de la cantidad exacta del espectro asignado.

El aumento o disminución del desempeño en las LAN inalámbricas no es una función de incrementar o disminuir el tamañote la capa física o cambiar la cantidad de ancho de banda, sino que es en función del tipo de modulación que se emplee.

El proceso de enviar datos desde un dispositivo digital como una computadora a través de ondas de radio es el mismo proceso que el usado para enviarlos a través de la línea telefónica. Debido a que las ondas de radio son analógicas es necesario usar un modem para convertir el flujo de 0 y 1 digital en un flujo analógico, un proceso conocido como modulación; del mismo modo también en el receptor se necesita un modem para convertir el flujo analógico en digital, un proceso que se llama demodulación.

La base de las cuatro velocidades de datos proporcionados por el estándar 802.11b son tres tipos de modulación:

1. Modulación de fase por desplazamiento binario (BPSK) para 1Mbps
2. Modulación de fase por desplazamiento en cuadratura (UPSK) para 2 Mbps
3. Modulación de código complementario (CCK) para 5.5 y 11 Mbps

Modulación BPSK

Una onda analógica se puede medir en términos de su potencia o amplitud; en términos de la cantidad de ondas por periodo o frecuencia; o en términos del momento en que la onda comienza su ciclo o fase. Al variar de manera simétrica estos parámetros se puede alterar la codificación y la transmisión de información.

Cuando hablamos de modulación por desplazamiento binario el término binario indica que la entrada para el proceso es simplemente un 0 o un 1; es decir solo son posibles dos estados, que en términos digitales se puede representar en un solo bit. Cuando el mensaje que se esta transmitiendo es tan simple como un si o un no, un encendido o un apagado se incrementa la posibilidad de que el mensaje sea recibido incluso a través de un medio con mucho ruido. La modulación BPSK es la más básica y por lo mismo el tipo de modulación más sólida; sin embargo, enviar una cantidad determinada de datos usando este tipo básico de modulación también requiere de una cantidad

más grande de transmisiones en comparación a las necesarias usando un tipo de modulación más complejo.

BPSK usa cambios o desplazamientos en los tiempos de inicio de una onda para indicar cual de los estados binarios se está codificando. Cada trama de datos que se envía comienza con un preámbulo que establece la línea base para la transmisión y precede a la información real que se transmite. Durante el proceso de reconocimiento entre el transmisor y el receptor los dispositivos se sincronizan de manera que se establece una de base común; los cambios en esta línea base o desplazamiento en la fase se usa para señalar que se hizo un cambio en la transmisión de un 0 a un 1 o viceversa. Debido a que BPSK es el más sólido de todos los tipos de modulación especificados por el estándar 802.11 es el que se emplea para todos los encabezados de las tramas, sin importar cuál tipo de modulación se use para la carga de información.

Modulación QPSK

La modulación de fase por desplazamiento en cuadratura es una variación de la modulación BPSK. También usa desplazamiento en la fase para codificar flujo de datos, sin embargo este flujo de datos no es simplemente estados binarios de 0 o 1, sino que es un conjunto de cuatro estados. Esto se representa con dos bits que dan como resultado cuatro estados: 00, 01, 10 y 11 después estos estados se codifican con base en los cambios en los tiempos de inicio de las ondas.

Por supuesto, discernir cuatro desplazamientos de fase en lugar de dos requiere de una señal más clara. La estación que envía intentará transmitir la carga usando tipos de modulación más alto para incrementar la velocidad. Si ocurre una cantidad grande de errores la estación emisora disminuirá en forma progresiva hasta tipos de modulación más simples y más eficaces, hasta que la trama se reciba con un número de errores aceptable. Este proceso de cambio de velocidad proporciona un medio automático de maximizar la velocidad de datos cuando aparecen condiciones como el ruido y la distancia, aunque a expensas del desempeño de la red.

Modulación CCK

La modulación de código complementaria proporciona una velocidad de 5.5 y 11 Mbps es un tipo de modulación mucho más sofisticado que los anteriores; para alcanzar las velocidades de datos más altas los dispositivos modulan la señal con BPSK y QPSK además de CCK. Con BPSK el radio inicia con un flujo de datos de 2 bits, con QPSK el radio comienza con un flujo de datos de 4 bits, CCK sigue este patrón exponencial al iniciar con un flujo de datos de 8 bits para alcanzar la velocidad de 11 Mbps y disminuye hasta un flujo de 4 bits cuando las condiciones dictan que se bebe usar una velocidad de datos de 5.5 Mbps.

Por supuesto, una transmisión que se modula dos veces requerirá de un canal más claro que la que se modula una vez lo que implica un intercambio entre el desempeño y el rango.

La velocidad de datos representa la velocidad con la cual viaja el paquete completo incluida la sobrecarga, definida como el medio para hacer llegar la carga, es decir los encabezados, y no toma en cuenta los errores en la transmisión que son lo suficientemente serios para dar como resultado un reenvió pero que no son tan frecuentes como para provocar un cambio en la velocidad.

Método de acceso al medio

El medio más eficiente para transmitir es un sistema donde todos los dispositivos tienen la capacidad de acceder al medio cuando necesiten hacerlo. Los estándares 802.11 usan como método más común de acceso al medio la Función de control distribuido DCF (Dstributed Coordination Function) que se basa en CSMA; sin embargo debido a las diferencias entre el cable de cobre y las frecuencias de radio la detección de colisiones no es posible; en lugar de esto el protocolo Elusión de colisiones (CA) especifico para aplicaciones inalámbricas se agrega a CSMA. Cuando un dispositivo opera en modo DCF primero debe sentir el medio antes de transmitir, si encuentra otro dispositivo que ya empezó su transmisión dará un paso atrás y esperará para volver a intentar la transmisión. Para incrementar la probabilidad de que la próxima vez que sienta el medio esté libre, la cantidad de tiempo que espera se genera en base aleatoria. La estación continuara este proceso hasta recibir un paquete de reconocimiento, o ack, desde la estación de destino indicando que el paquete ha sido recibido en forma exitosa.

Uno de los beneficios de CSMA y la una de las razones para su éxito como un método de acceso a medios para las tecnologías LAN con cable e inalámbricas, es que maximiza el desempeño de un ancho de banda limitado. El protocolo capacita a cada estación en la LAN para que envié datos cuando es necesario sin tener que esperar un turno. Este enfoque se puede aplicar al envió de datos como correo electrónico, un archivos en hoja de calculo o el tráfico web pero puede no funcionar bien cuando se envía tráfico con requerimiento a la latencia baja como audio y video. Para resolver lo anterior y permitir que una LAN trasporte datos al igual que voz y video, se han desarrollado distintos medios de asignar prioridades, por lo tanto promociona un nivel de calidad de servicio (QoS).

En las LAN CSMA cableadas se puede asumir que la estación emisora puede escuchar a todas las demás estaciones con las cuales comparte el medio. En las LAN inalámbricas sólo se puede asumir que todos los dispositivos del cliente pueden oír al punto de acceso y que todos los puntos de acceso pueden escuchar a todos los dispositivos del cliente; pero no podemos asumir que todos los dispositivos se pueden escuchar entre si, este problema se conoce como nodo escondido.

El estándar 802.11 resuelve este problema con una opción llamada RTS/CTS (Request to Send/ Clear to Send, Solicitud de envió /Libre para enviar), cuando este se habilita los dispositivos del cliente primero piden permiso para enviar un paquete de datos al punto de acceso enviando un paquete RTS y el punto de acceso responde con un paquete CTS si sabe que ninguna otra estación esta enviando datos en ese momento.

Si otra estación esta transmitiendo se le pide al dispositivo que se mantenga en estado de espera; esta espera un periodo especificado antes de enviar otro paquete RTS. Después de varias veces de que el dispositivo se mantuvo en estado de espera, comienza a enviar paquetes RTS usando intervalos conocidos como retroceso aleatorio con el fin de aumentar la posibilidad de recibir un paquete CTS por parte del dispositivo receptor.

El RTS/CTS es una buena forma de resolver el problema de los nodos ocultos, sin embargo introduce más tráfico y sobre carga al desempeño de la red, por lo que se debe de habilitar solo cuando sea necesario.

Potencia de transmisión.

La potencia de transmisión se puede entender como el volumen con que una señal de radio se puede escuchar; mientras mas grande sea la potencia de transmisión, será mas grande la distancia que la señal podrá alcanzar.

La potencia de transmisión en los dispositivos Wi-Fi se mide en miles de watts o miliwatts (mW) y las señales recorren decenas de pies.

Un circuito integrado Wi-Fi incluye una capa MAC, un circuito PHY de radio y un RF principal y un transmisor final. Todo esto en conjunto conforma el transmisor que normalmente proporciona una potencia de recepción y de salida aproximada de 30mW. Algunos fabricantes incluyen en su diseño un amplificador de potencia para incrementar el poder de transmisión que trae como consecuencia el incremento en la cantidad de potencia consumida.

Además de los miliwatts existe una unidad alterna para medir la potencia de transmisión, esta es el decibel (dB). Los decibeles no solo expresan una medida de potencia sino también la proporción de potencia o voltaje en términos de ganancia o pérdida. La unidad se expresa en forma logarítmica; la regla general es que 10 dB indica un crecimiento aproximado por un factor de 10, 20 dB un incremento aproximado a un factor de 100 y 30 dB a un factor de 1000. La ganancia o la pérdida se expresan con un signo + o – antes del valor.

Sensibilidad de recepción

La sensibilidad es una medida de la señal más débil que un radio puede recibir y remodular con éxito; esta se mide en decibeles al igual que la potencia de transmisión.

Debido a que los paquetes codificados con distintos tipos de modulación tienen diferentes requerimientos de sensibilidad de recepción, esta depende de la velocidad de datos. Por lo tanto si un radio puede proporcionar una sensibilidad de -85 dB a 11 Mbps, podría remodular exitosamente una señal más débil cuando se transmite a solo un Mbps.

Estándares para una WLAN de alto desempeño.

Los primeros dispositivos basados en el estándar 802.11b se ofrecían como productos capaces de proporcionar una velocidad de datos de 11 Mbps parecida a la de Ethernet; algo q en el sentido más estricto es cierto, sin embargo los 10 Mbps en Ethernet es más rápido que los 11 Mbps en Wi-Fi debido a la sobrecarga asociada al estándar 802.11b que excede la sobrecarga del estándar 802.3 que da como resultado una mejor capacidad de salida para Ethernet. Además Wi-Fi es por naturaleza un medio compartido lo que ocasiona que la velocidad de datos se divida entre el número de usuarios asociados al punto de acceso.

De forma parecida en la que la tecnología cableada ha avanzado, también los estándares inalámbricos se han desarrollado para proporcionar un desempaño que coincida con los requerimientos y las expectativas de los usuarios.

Los estándares 802.11a y 802.11g son dos estándares complementarios que proporcionan una velocidad de datos máxima de 54 Mbps una velocidad sustancialmente más grande que la ofrecida por el 802.11b.

A pesar de que el estándar 802.11a ha estado ratificado desde 1999, fue hasta finales del 2001 que comenzaron a aparecer los primeros productos compatibles con este.

Al igual que 802.11b los estándares 802.11a y 802.11g también proporcionan más de una velocidad de datos. Las velocidades básicas definidas en el estándar 802.11a son 6, 12 y 24 Mbps, la velocidad de 54 Mbps es una de opción, la razón de esto es que existe una relación inversamente proporcional entre la velocidad de datos y el rango.

La multiplexión por división ortogonal de frecuencia (OFDM) es un medio de transmisión y es el punto de comunicación entre 802.11a y 802.11g. OFDM se adapta particularmente bien para la transmisión de a través de frecuencias de radio. Es una técnica de transmisión, al igual que el Acceso múltiple por división de código (CDMA) el cual se usa en ciertos tipos de teléfonos portátiles, o el Espectro extendido de secuencia directa (DSSS), los cuales representan los medios de transmisión de espectro extendido especificados por 802.11b y que usan los dispositivos Wi-Fi de 11 Mbps.

OFDM es muy sólido en términos de interferencia y distorsión por múltiples trayectorias, hace uso eficiente de espectro mas eficiente que el de DSSS. Con OFDM un rango determinado de frecuencias se divide en canales separados o subportadores; durante la transmisión, estos canales subportadores u ortogonales se juntan o multiplexan.

Tanto para 802.11a como para 802.11g se usan diferentes tipos de modulación y cada uno de ellos codifica y aumenta el número de bits por transmisión para alcanzar las velocidades de datos más altas; mientras más grande sea el número de bits codificados, la señal tendrá que ser más clara para que la transmisión sea recibida y demodulada de forma exitosa. La sensibilidad de recepción especificada por 802.11a está entre -82 y -65 dBm, lo que representa una señal significativamente más potente en comparación con las que normalmente reciben los dispositivos 802.11b. Con la aplicación de OFDM en 802.11a y 802.11g se alcanzan los órdenes de modulación más altos y las velocidades de datos que 802.11b no puede alcanzar.

En 802.11a y 802.11g también se emplean los tipos de Modulación de fase por desplazamiento binario (BPSK) y la Modulación de fase por desplazamiento en cuadratura (QPSK). Cuando se usa la modulación BPSK, la velocidad que se alcanza es de 6 o 9 Mbps a diferencia de la velocidad de 1 Mbps en el caso de 802.11b, así mismo con la modulación QPSK se alcanza una velocidad de 12 a 18 Mbps.

En lugar de usar el tipo de Modulación de código complementaria (CCK) que se usa en el estándar 802.11b para velocidades de datos más altas, 802.11a y 802.11g usan una Modulación de amplitud en cuadratura (QAM) que realiza la codificación a través de los cambios de fase y también en los cambios en la amplitud. Cuando se codifica un solo bit son posibles dos símbolos, cuando se codifican dos bits son posibles 4 símbolos; usando la progresión exponencial para esto, cuando codificamos 4 bits son posibles 16 símbolos y cuando codificamos 6 estarán disponibles 64 símbolos. Por tanto, 16-QAM codifica 4 bits y proporciona velocidades de datos de 24 o 36 Mbps, mientras que 64-QAM codifica 6 bits y proporciona velocidades de 48 o 64 Mbps; el precio que se paga por las velocidades de datos más altas que ofrecen 802.11a y 802.11g está representado en términos de rango.

A pesar de que estos dos estándares comparten medios de transmisión y modulación, si existen diferencias 802.11a esta definido para operar en distintas bandas dentro de la porción de 5 GHz del espectro de frecuencia de radio; mientras que 802.11g opera en la misma banda de 2.4 GHz que usa 802.11b, estas bandas proporcionan distintos beneficios para cada tecnología así como distintos inconvenientes.

La forma de onda de 5 GHz proporciona algunas ventajas y desventajas en comparación con la forma de onda de la banda 2.4 GHz. Una onda de 5 GHz tiene aproximadamente la mitad de la longitud de una onda de 2.4 GHz. Estas ondas más cortas tienden a pasar a través del agua con una atenuación menor que las ondas más largas. Esto significa que en áreas con una gran densidad e personas los dispositivos 802.11a que operan a 5 GHz tenderán a obtener una ventaja en términos de la propagación de la señal y el rango resultante en comparación con los dispositivos 802.11b que operan en 2.4 GHz y como la banda de 5 GHz esta más limpia sufre menos interferencia por parte de otros dispositivos. Sin embargo tiene sus desventajas ya que la onda más corta de 5 GHz tiende a ser capturada con más facilidad por materiales de construcción comunes como concreto y la mampostería, y es más propensa a crear la propagación de múltiples trayectorias

La especificación 802.11a está diseñada para aprovechar 200 MHz que asignan a ocho canales, cada uno de 25MHz, en compasión con los 83 MHz de la banda de 2.4 GHz usada en 802.11b y 802.11g que asignan en tres canales de 22 MHz de amplitud que no se traslapan. Existen dos ventajas principales cuando tenemos un número más grande de canales disponibles, estas están representadas por el reciclaje y la capacidad de los canales. Suponiendo que en una empresa normalmente se instalan más de un punto de acceso dentro de un área determinada, lo que ofrece la cantidad más grande de canales que se pueden seleccionar, es más sencillo diseñar una LAN que no contenga dos puntos de acceso adyacentes; esto debido a que el tráfico de los dispositivos en el conjunto de las células traslapadas para el mismo canal da como resultado la interferencia mutua, lo que implica reducción en el desempeño. Mientras más canales existan hay menos complicación de los despliegues y el reciclaje de canales deja de ser un problema.

La capacidad de más canales no sólo hace que la arquitectura de la LAN sea más sencilla, sino que también proporciona una capacidad de red más grande. Debido a que una LAN inalámbrica es un medio compartido en el que cada usuario lucha por obtener una cantidad de ancho de banda determinada que provoca que el desempeño sea menor, de acuerdo al número de usuarios. Una forma para resolverlo es el de dividir un número de usuarios determinado dentro de una cantidad más grande de medios. En términos de Ethernet esto significa dividir a los usuarios dentro de una cantidad más grande de dominios de colisión incrementando la segmentación de la red y el uso libre de interruptores. El resultado del proceso es hacer conexiones conmutadas en donde cada cliente tiene su propio segmento. Ya que en las LAN inalámbricas la conmutación no es posible debido a que el medio de transmisión son las ondas de radio, los canales pueden representar los segmentos conmutados;

por lo tanto mientras existan más canales será mayor el número de segmentos a través de los cuales un número determinado de usuarios pueden estar divididos y a medida que la cantidad de usuarios por canal se acerca a uno, la arquitectura se asemeja más a una arquitectura conmutada.

A pesar de que los aspectos reguladores de operación dentro de la banda de 5GHz tiene un efecto positivo en el reciclaje y capacidad de canales, tiene su efecto negativo en el rango en comparación con los dispositivos que operan en la banda de 2.4GHz. La potencia de transmisión es una de las características que pueden impactar en el rango, esto es, entre más grande sea la potencia de transmisión será más grande el rango del dispositivo. Sin embargo a pesar de que las tolerancias en la potencia de transmisión varían dependiendo de la ubicación geográfica y de la banda en el espectro; las tolerancias de la potencia en la banda de 5 GHz son menores de lo q son en la de 2.4 GHz.

802.11g presenta un desempeño más alto y ofrece la compatibilidad con productos anteriores. Como ya vimos 802.11g usa el mismo tipo de transmisión y modulación que 802.11a por lo tanto soporta las mismas velocidades de datos; así mismo opera en la banda de 2.4GHz y soporta los tipos de modulación BPSK, QPSK y CCK de 802.11b, lo que proporciona la compatibilidad con productos anteriores.

Como 802.11g opera en la misma banda que 802.11b todas las regulaciones internacionales, restricciones, así como los problemas de interferencia que aplican para los productos 802.11b también aplican para los productos 802.11g.

A pesar de que 802.11g usa los mismos medios de transmisión que 802.11a y proporciona las mismas velocidades de datos, es probable que en la práctica no logre proporcionar una capacidad de salida tan alta como 802.11a, debido a todos los problemas de interferencia de la banda de 2.4GHz donde opera reducirá la capacidad de salida por los errores en la transmisión y los reenvios asociados a estos.

En la siguiente tabla se muestran algunas ventajas y desventajas de los estándares 802.11a y g

	802.11a	**802.11g**
Desempeño.	Ventaja. Con OFDM, la banda de 5 GHz y la ausencia de células mixtas proporcionan una mejor capacidad de salida.	Desventaja. Soporte para los estándares elevados, células mixtas y la operación en la banda de 2.4 GHz que podría estar potencialmente saturada, lo que daría como resultado una capacidad de salida menor.
Capacidad.	Ventaja. Con ocho canales proporciona una capacidad agregada de 432 Mbps.	Desventaja. Con solo tres canales proporciona una capacidad teórica de 162 Mbps.
Rango.	Desventaja. Una longitud de onda más corta y restricciones en la potencia de transmisión y la ganancia de la antena.	Ventaja. A pesar de no proporcionar el mismo rango que 802.11b debido a las velocidades de datos mas altas, si permite un rango mas grande que 802.11a.
Interferencia.	Ventaja. Opera en la banda de 5 GHz que es relativamente grande y no esta saturada.	Desventaja. Al operar en la banda pequeña de 2.4 GHz que esta saturada por teléfonos inalámbricos, dispositivos Bluetooth y otras LAN inalámbricas.
Migración.	Desventaja. Al proporcionar soporte solo para la transmisión OFDM, no es compatible con dispositivos anteriores.	Ventaja. Al operar en la banda heredada de 2.4 GHz y soportar DSSS, proporciona la compatibilidad con productos anteriores.
Flexibilidad de instalación.	Desventaja. Las regulaciones aplicadas a los cuatro canales inferiores restringen a los fabricantes el uso de de antenas integradas que no se pueden desconectar.	Ventajas. Permite antenas de 2.4 GHz auxiliares q pueden estar conectadas por cable.

Mediante la combinación de 802.11a y g se puede obtener lo mejor de los dos estándares, maximizando la capacidad y permitiendo la compatibilidad con productos anteriores. Los dispositivos de banda dual que soportan tanto 2.4 como 5 GHz con tres nodos, es decir que puede trabajar en 802.11a, b y g pueden llegar a tener un rápido desarrollo, ya que el controlador de acceso al medio (MAC) de 802.11 es común a todas las tecnologías, la función de la capa física (PHY) es modular y remodular indiferente a la frecuencia de transmisión y como la capa PHY de 802.11g es una combinación de las funciones de PHY 802.11a y 802.11b no se requiere de una capa física adicional. Integrar estas tecnologías es el objetivo de los fabricantes, llegar a obtener un solo radio capaz de soportar 802.11a, 802.11b y 802.11g.

Uno de las principales atractivos de Wi-Fi es que no requiere de licencia para operar, sin embargo, dependiendo del país existen varías regulaciones que impactan en el rango, escalabilidad, portabilidad, protección del producto y la capacidad.

Seguridad

La seguridad es un riesgo tanto para las redes inalámbricas como para las cableadas. Hasta la fecha, todas las tecnologías informáticas que han ido apareciendo en el mercado han sido susceptibles, de una u otra forma, de ser violadas en su integridad, confidencial o autenticidad de los datos que contiene.

La configuración segura de las redes inalámbricas presenta aún más retos, debido al hecho de que sólo alrededor de un 20% de las redes inalámbricas residenciales utilizan WEP (Privacidad equivalente a la de cables).

Conforme el equipo de redes inalámbricas se hace menos caro y está disponible más fácilmente, más gente está comprando productos portátiles e inalámbricos. La tecnología inalámbrica ofrece algo con lo que sólo se podía soñar anteriormente: acceso a la Internet desde cualquier lugar, sin importar si se está sentado en la silla del jardín o tomando un café late en un establecimiento.

Ciertamente, a diferencia de las redes cableadas, las redes inalámbricas emiten señales que pueden ser recogidas en el exterior con facilidad. Desde ese punto de vista, las redes inalámbricas tienen un riesgo añadido. De la misma forma es controlable el riesgo que tiene una red cableada de que un usuario remoto y desconocido pueda entrar en ella a través de su conexión de Internet. El riesgo siempre existe si no se toman las precauciones necesarias.

Se pueden mencionar cuatro categorías de riesgo que preocupan en el uso de cualquier tecnología de red

- Perdida del equipo
- Infección de virus
- Uso equivocado por personas autorizadas
- Uso fraudulento por personas no autorizadas

Pérdida del equipo

Muchas veces llegamos a almacenar en el disco duro de nuestro maquina una gran cantidad de información, información no solo profesional sino, incluso personal como listado de clientes, las cuentas de la empresa, las descripciones de productos, correspondencia con proveedores y clientes, etc.

Aparte del problema que es el exponer alguna de esta información a ojos indiscretos, existe un problema adicional y es que dicha maquina podría ser utilizado para acceder a la red de nuestra empresa. Este problema existe tanto si el equipo esta conectado a una red cableada como si lo esta a una red inalámbrica.

Si la red es cableada, el acceso se podría hacer desde cualquier parte del mundo vía Internet, este riesgo puede eliminarse fácilmente al deshabilitar las cuentas de acceso del usuario en cuestión. En la red inalámbrica, el acceso tendría que ser necesariamente desde una zona de cobertura, donde pueden cambiarse también todos los códigos de acceso.

Infección por virus

Como sabe, los virus son pequeños programas informáticos que pueden directamente producir daños en la maquina o ser utilizados para conseguir otros fines haciendo uso de la maquina o de la red en la que se aloja. Los virus afectan tanto a redes cableadas como inalámbricas.

Esto quiere decir que las medidas antivirus son las mismas, independientemente del tipo de red al que se encuentre conectado, se debe mantener el programa antivirus actualizado y disponer de firewall.

Uso equivocado por personas autorizadas

El mal uso del sistema, ya sea intencionado o accidental, por personas autorizadas a utilizarlo es una amenaza de la que es difícil protegerse. Una vez que el usuario ha pasado todos los niveles de seguridad y se encuentra dentro del sistema, es complicado controlar en detalle el uso que cada usuario hace de él.

Uso fraudulento por personas no autorizadas

Una desventaja que las redes inalámbricas Wi-Fi tienen frente a las redes cableadas, es el riesgo de uso fraudulento por personas no autorizadas, debido a que cualquier usuario puede conectarse a la red desde cualquier sitio sin necesidad de conectarse físicamente a ningún medio.

Los usos fraudulentos se pueden dar de varias formas como escuchar con un receptor adecuado, los datos emitidos por un usuario. De hecho, existen programas que facilitan esta labor; estos programas descubren datos como el SSID, la dirección MAC o si el sistema WEP. Configurar un dispositivo para acceder a una red para la que no se tiene autorización. Esto se puede hacer con una estación para que acceda a un punto de acceso existente o instalando un nuevo punto de acceso y, a través de él, conectar todas las maquinas externas que se deseen. Otra forma es intentar adivinar la clave de acceso de un usuario autorizado mediante intentos sucesivos y el atacante sólo tiene que tener la paciencia necesaria hasta dar con la clave correcta.

Conforme las masas adoptan la tecnología de inalámbricos, algunas de las limitaciones se hacen cada vez más evidentes. Para los proveedores de dispositivos inalámbricos, los retos más importantes son los que enfrentan los usuarios ordinarios durante la instalación y configuración iniciales de las redes inalámbricas.

Algunos de los problemas de instalación que se encuentran más comúnmente son:

- Suposición de conocimiento de la tecnología: Muchos fabricantes de productos suponen que los usuarios tienen una comprensión básica de la tecnología de redes inalámbricas. Pero los modelos de instalación actuales no son intuitivos para el usuario promedio.
- Métodos no convencionales para la configuración de dispositivos: Cada proveedor tiene un procedimiento distinto de instalación para su producto. Sin un método convencional de instalación de redes inalámbricas, hay una alta probabilidad de que los usuarios se confundan al tener que seguir distintos procedimientos para distintas piezas del equipo.
- Probabilidad de error: Muchos métodos de instalación requieren que los usuarios tecleen largas cadenas de datos en cada dispositivo que se está configurando, por lo que resulta muy fácil que los usuarios introduzcan errores que conduzcan a un fallo de la instalación.

Otra área crítica es la gran cantidad de puntos de acceso inalámbricos inseguros. Esto se traduce en problemas para las redes inalámbricas como son:

- La instalación de la seguridad no está integrada a la instalación de la red: La instalación de la seguridad a menudo es un paso de configuración separado que los usuarios no consideran, sin darse cuenta de la importancia de asegurar sus redes contra posibles ataques.

- Seguridad inadecuada de los estándares actuales: Los métodos de seguridad disponibles actualmente no son realmente seguros. WEP, el protocolo de seguridad que se usa más comúnmente, es inherentemente inseguro. Asimismo, necesita que todos los dispositivos en la red compartan la misma clave. Si alguien no autorizado averigua la clave en un dispositivo, toda la red está en riesgo. Un protocolo de seguridad más reciente que es sucesor de WP, el WPA-Personal, también tiene algunos problemas de seguridad.
- Desconexión de la red al activar la seguridad: Las redes LAN inalámbricas con frecuencia dejan de funcionar cuando los usuarios activan la seguridad. Esto normalmente ocurre cuando el usuario, sin darse cuenta, configura diferentes claves de cifrado en distintos dispositivos, lo que produce problemas debido a que los dispositivos en comunicación directa deben compartir la misma clave de cifrado.

Lo que el usuario promedio necesita no es sólo una interfaz gráfica de usuario (GUI) para configurar la red, sino un método para facilitar la instalación y seguridad. Tal método debe configurar la seguridad automáticamente, junto con la configuración básica de la red. El usuario no debe enterarse de los detalles de la seguridad a menos que desee hacerlo.

Muchas soluciones de hoy sacrifican la seguridad al no configurarla o al negociar parámetros de seguridad y conexión abiertamente, donde son vulnerables a los ataques. Una gran parte de esta configuración tiene lugar en los mismos canales de comunicación que necesitan asegurarse. Es virtualmente imposible, salvo en condiciones excepcionales, garantizar que este método proporcione una seguridad adecuada.

Para instalar redes inalámbricas de manera segura, nunca se deben distribuir las claves abiertamente por medio del canal dentro de banda. En vez de eso, es necesario utilizar un canal fuera de banda (OOB) para la instalación de red. Un canal fuera de banda se define como un canal distinto del canal normal de comunicaciones.

El canal OOB se puede usar para dar cierta información de configuración a los dispositivos que les ayude a conectarse por medio del canal dentro de banda y negociar los parámetros de seguridad. Más aún, se pueden seleccionar los canales OOB de manera que sea más difícil espiar los datos que se intercambian a través de ellos. El objetivo de un diseño correcto es hacer que sea improbable que un atacante pueda espiar o falsificar mensajes en los canales en banda y fuera de banda simultáneamente. Un ejemplo de un canal OOB es la unidad de almacenamiento flash de bus serie universal (USB). Otros posibles canales OOB pueden ser los infrarrojos, de frecuencia de radio (RFID), y otros.

La elección del canal OOB es muy importante para tener un proceso de introducción satisfactorio; además de proporcionar seguridad e integridad de los datos.

El caso de 802.1X.

Entre los productos inalámbricos actuales WEP es el método de seguridad preferido. El sistema de cifrado WEP consiste en aplicar a los datos originales la operación lógica XOR (O exclusiva) utilizando una clave generada de forma pseudoaleatoria. Los datos cifrados resultantes son los que se transmiten al medio. Para generar la clave pseudoaleatoria, se utiliza una clave secreta definida por el propio usuario y un vector de inicialización (IV, Initialization Vector). La clave secreta es única y debe estar configurada en todos los equipos y puntos de acceso.

La longitud de los datos cifrados excede en cuatro caracteres a la longitud de los datos originales. Estos cuatro caracteres reciben el nombre de ICV (Integrity Check Valué, 'Valor de Comprobación de Integridad') y se utilizan para que el receptor pueda comprobar la integridad de la información recibida. Una vez que llegan al destino los datos cifrados, se combina el IV con la clave secreta, distribuida a todas las estaciones, para generar la semilla que permitirá descifrar los datos

Una desventaja del WEP es que se comparte una sola clave entre todos los dispositivos de la red. Esta clave también debe darse a los invitados que deseen acceder a la red de manera temporal. Cuando el invitado se va y el dueño de la red desea prevenir que aquél tenga nuevamente acceso a la red, el dueño debe cambiar la clave en todos los dispositivos de la red. Lo mismo pasa cuando se pierde un dispositivo o cuando la clave se divulga de cualquier otra forma. Además, el WEP padece de un número de debilidades de seguridad conocidas públicamente que hacen que sea una opción menos conveniente.

La comunidad de inalámbricos, a través de IEEE y de Wi-Fi Alliance ha desarrollado un nuevo estándar de seguridad para redes LAN inalámbricas conocido como 802.11i. 802.11i ofrece una solución integral de seguridad para redes inalámbricas. El estándar fue ratificado en junio de 2004, así que apenas comienza a aparecer en los productos. Una solución intermedia, conocida como Wi-Fi Protected Access o WPA. WPA es un apartado de 802.11i previo al estándar diseñado con la facultad de actualización de software en los equipos previos. WPA está disponible en dos versiones, personal y empresarial.

WPA-Personal está destinado para su uso en el hogar. Tiene uno de los problemas del WEP toda la red utiliza la misma clave compartida. Aunque construye claves únicas de sesión entre los pares comunicantes de clientes por medio de la red, un cliente puede usar la clave compartida para atacar la sesión de otros dos clientes.

WPA-Enterprise se basa en 802.1X para cumplir los requisitos de autorización y autenticación. 802.1X es un estándar de seguridad para dar control de acceso a cualquier LAN basada en IEEE 802. El 802.1X introduce un servidor de autenticación (AS), que centraliza todas las decisiones de control de acceso en la red. El cliente y el servidor de autenticación intercambian mensajes 802.1X para autenticarse entre sí. El punto de acceso autoriza estos mensajes 802.1X. Mientras la autenticación no sea satisfactoria, el servidor de autenticación no permitirá que el punto de acceso acepte mensajes de datos del cliente, ni el cliente aceptará datos del punto de acceso. Como efecto lateral, el cliente y el servidor de autenticación construyen una clave única de sesión para proteger la transferencia subsiguiente de datos. Esta clave depende de la autenticación mutua del cliente y el servidor de autenticación, así que otros clientes no la conocen.

WPA se puede instalar en los equipos Wi-Fi existentes de una forma tan sencilla como instalar un pequeño software en los equipos. Una vez instalado, el nivel de seguridad adquirido es extremadamente alto, asegurándose que sólo los usuarios autorizados pueden acceder a la red y que los datos transmitidos permanecen completamente inaccesibles para cualquier usuario que no sea el destinatario.

Esta es una solución mucho más segura que el WEP que se utiliza actualmente. Si se implementa correcta y cuidadosamente, no suma ningún sacrificio significativo en términos de velocidad y facilidad de uso, y sí mejora la seguridad grandemente.

Las mayores ventajas que aporta WPA frente a WEP son dos:

Mejoras en el cifrado de datos mediante TKIP (Temporal Key Integrity Protocol, Protocolo Temporal de Integridad de Clave).Este sistema asegura la confidencialidad de los datos.

Autentificación de los usuarios mediante el estándar 802.1x y EAP (Extensible Authentication Protocol, Protocolo Extensible de Autentificación). Este sistema permite controlar a todos y cada uno de los usuarios que se conectan a la red. No obstante, si se desea, permite el acceso de usuarios anónimos.

La única manera de conseguir seguridad es manteniendo unas técnicas de protección adecuadas. Hay que ser conscientes de que ninguna técnica de protección es eficaz al cien por ciento. Siempre existe riesgo aunque sea pequeño. No obstante, a más barreras de seguridad, menor será el riesgo.

Capitulo III

Diseño de la red inalámbrica.

La mayoría de las redes inalámbricas que hay en el mercado (sean Wi-Fi o de otro tipo) funcionan de una manera similar: tienen unas estaciones base (puntos de acceso) que coordinan las comunicaciones y unas tarjetas de red (adaptadores de red) que se instalan en los equipos y que les permiten formar parte de la red.

Adicionalmente, existen antenas que permiten aumentar el alcance de los equipos Wi-Fi, así como *software* especializado que permite facilitar la labor de gestión y mantenimiento de la red inalámbrica.

Antes de describir las distintas componentes necesarias para crear una red Wi-Fi, es necesario describir las características más importantes para una selección adecuada de algún tipo arquitectura Wi-Fi, así como, los parámetros a considerar para su implementación.

Por qué instalar una red inalámbrica.

Las redes inalámbricas hacen exactamente el mismo trabajo que realizan las redes cableadas: interconectan equipos y otros dispositivos para permitirles compartir recursos. Las redes locales permiten interconectar desde dos equipos hasta cientos de ellos situados en un entorno donde la distancia máxima de un extremo a otro de la red suele ser de algunos cientos de metros. Esto quiere decir que las redes de área local se limitan generalmente al ámbito de un edificio. No obstante, distintas redes locales situadas en distintos edificios (edificios que pueden estar situados en distintas ciudades) pueden interconectarse entre sí formando un único entorno de red.

Las ventajas que ofrece una red de área local, ya sea cableada o inalámbrica, son las siguientes:

- Permite compartir periféricos: impresoras, escáneres, etc.
- Permite compartir los servicios de comunicaciones (ADSL, módem cable, RDSI, etc.)
- Permite compartir la información contenida en cada equipo.
- Permite compartir aplicaciones.

La pregunta seria si la red local que nos interesa instalar debe ser cableada o inalámbrica. Muchos usuarios responden a esta cuestión simplemente decidiéndose a instalar la última tecnología del mercado, es decir, la tecnología inalámbrica. El interés de disponer de la tecnología más moderna es valido y no cabe duda de que las redes inalámbricas ofrecen una mayor comodidad de uso o una mayor facilidad de instalación, pero toda tecnología tiene sus propias limitaciones.

Ventajas.

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

- **Movilidad.** La libertad de movimientos es uno de los beneficios más evidentes de las redes inalámbricas. Un equipo o cualquier otro dispositivo (por ejemplo, una PDA o una *webcam)* pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de si es posible o no hacer llegar un cable hasta ese sitio. Ya no es necesario estar atado a un cable para navegar por Internet, imprimir un documento o acceder a la información de nuestra red local corporativa o familiar. En la empresa se puede acceder a los recursos compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.

- **Desplazamiento.** Con un equipo portátil o PDA no sólo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación. Esto no sólo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio.

- **Flexibilidad.** Las redes inalámbricas no sólo nos permiten estar conectados mientras nos desplazamos con un equipo portátil, sino que también nos permiten colocar un equipo de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio en la configuración de la red. A veces, extender una red cableada no es una tarea fácil ni barata. Piense en edificios antiguos o en áreas apartadas. En muchas ocasiones acabamos colocando peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas. También es útil para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conecten a la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En los sitios donde pueda haber invitados que necesiten conexión a Internet (centros de formación, hoteles, cafés,

entornos de negocio o empresariales) las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

- **Ahorro de costes.** Diseñar e instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costes al permitir compartir recursos: acceso a Internet, impresoras, etc.

- **Escalabilidad**. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar un nuevo equipo cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o, lo que es peor, esperar hasta que el nuevo cableado quede instalado.

Desventajas.

Claro que no todo son ventajas, las redes inalámbricas también tienen algunos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

- **Menor ancho de banda.** Las redes de cable actuales trabajan a 1 Gbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tienen un precio superior al de los actuales equipos Wi-Fi.

- **Mayor inversión inicial.** Para la mayoría de las configuraciones de red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

- **Seguridad**. Como las redes inalámbricas no necesitan de un medio físico para funcionar, esto se considera una ventaja, pero se convierte en un inconveniente cuando pensamos que cualquier persona con un equipo portátil sólo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de los más fiables. A pesar de esto, también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA, descrito anteriormente) que hace a Wi-Fi mucho más confiable.

- **Interferencias.** Las redes inalámbricas funcionan utilizando el medio radioeléctrico en la banda de 2,4 GHz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias, incluida la de los vecinos. Este hecho hace que no se tenga la garantía de que nuestro entorno radioeléctrico esté completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

- **Incertidumbre tecnológica**. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11b). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad. Es posible que, cuando se popularice esta nueva tecnología, se deje de comercializar la actual. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades de los clientes y los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales.

Tecnología inalámbrica.

La tecnología inalámbrica en los hogares es un caso especial. Es raro encontrar una casa que tenga preinstalada una red cableada de datos. Sin embargo, aun contando con una única impresora, una única conexión a Internet (vía ADSL o cable), un único grabador de CD o un único escáner, cada vez es más normal disponer de más de un equipo en casa. Para poder compartir estos recursos, se puede instalar una rígida red cableada tendiendo cables a través de las paredes o configurar una red inalámbrica. Es cierto que esta última solución es más cara que la primera, pero también es más flexible, escalable, fácil de instalar y, además, permite movilidad.

El caso de las empresas puede ser similar al anterior, pero nos encontramos con un punto adicional. Las redes cableadas son un problema en aquellas empresas donde existe la posibilidad de cambiar la disposición de los puestos de trabajo. Sin embargo, para una red inalámbrica no supone ningún problema el cambiar un equipo de sitio.

El hecho de instalar una red inalámbrica no significa que toda la red tenga que ser inalámbrica. Las redes Wi-Fi son completamente compatibles con las redes locales cableadas Ethernet. Por tanto, la parte inalámbrica puede ser un complemento de la parte cableada. Se puede cablear lo que sea fácil cablear y dejar a Wi-Fi que resuelva la extensión de la red a aquellas áreas difíciles de cablear. También se puede disponer de una red de cable para unos usuarios y una red inalámbrica paralela para aquellos otros que por la labor que desempeñan necesitan disfrutar de la ventaja de la movilidad.

La redes inalámbricas son ideales, por ejemplo, si se necesita disponer de conexión a red en lugares abiertos (por ejemplo, un campus universitarios), en sitios públicos (centros comerciales, redes vecinales, servicios municipales, etc.) o sitios cerrados pero disponiendo de movilidad (almacenes, salas de reuniones, etc.).

Opciones a considerar.

Ya planteamos los puntos más importantes para confirmar que si necesitamos una red inalámbrica. Es hora de analizar qué tipo de red es la que le viene mejor a nuestras necesidades. Una red puede comunicar un par de equipos o a cientos de ellos, podemos tener a todos los equipos concentrados en una pequeña zona o dispersos por una gran área, dentro de un edificio, en varios edificios o en el exterior.

Las decisiones que hay que tomar a este respecto son las siguientes:

- Cuál será la estructura de la red, si se necesitaran instalar puntos de acceso y cuántos serán necesarios.
- Qué tarjeta o dispositivos inalámbricos instalaremos en cada equipo, PDA o cualquier otro equipo informático que necesitemos conectar.
- Qué tipo de antenas necesitaremos para poder cubrir toda el área para la que necesitamos disponer del servicio.
- Cómo conectaremos nuestra red inalámbrica a la red local cableada y a Internet.

Las diferentes estructuras de red.

Como ya se explico la IEEE802.11 tiene 3 diferentes arquitecturas, estas arquitecturas se vieron de forma muy técnica en el capitulo anterior. A continuación se explicaran las mismas arquitecturas de una forma más comercial.

IBSS (Independent Basic Service Set, “Conjunto de Servicios Básicos Independientes”).

Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre las distintas terminales que forman la red. En este caso no existe ninguna terminal principal que coordine al grupo, no existe punto de acceso. A esta modalidad también se le conoce como una red ad hoc (entre iguales) o peer to peer (punto a punto).

Ésta es una red de área local independiente que no está conectada a una infraestructura con cables y en la que todos los puertos están directamente conectados entre sí (lo que se conoce como topología de malla). Consiste simplemente en proveer a los equipos con una tarjeta de red inalámbrica de modo que todos hablen con todos. En este caso, no es necesario incorporar un punto de acceso. Presenta la ventaja de su sencillez pero, a cambio, crea una red aislada de otras redes y no ofrecer facilidades de seguridad ni gestión como cuando se dispone de una base.

La configuración de una WLAN en modo ad hoc se emplea para establecer una red cuando no exista una infraestructura inalámbrica o cuando no se requieran servicios, como cuando se trabaja con compañeros en una ubicación remota. Esta topología es común en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red; por ejemplo, un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

Figura 3.1 Red IBSS o ad hoc

BSS (Basic Service Set, “Conjunto de Servicios Básicos”).

En esta modalidad se añade un equipo llamado punto de acceso (AP o *Aceess Point*) que realiza las funciones de coordinación centralizada de la comunicación entre las distintas terminales de la red. Los puntos de acceso tienen funciones de *buffer* (memoria de almacenamiento intermedio) y de *gateway* (pasarela) con otras redes. A los equipos que hacen de pasarelas con otras redes externas se les conoce como *portales.* A la modalidad BSS también se la conoce como modo infraestructura.

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo. La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso.

Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación. La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para separar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica. El acceso a la red se administra mediante un protocolo, descrito anteriormente, que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representan la parte del protocolo que evita las colisiones. Observe que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

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

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

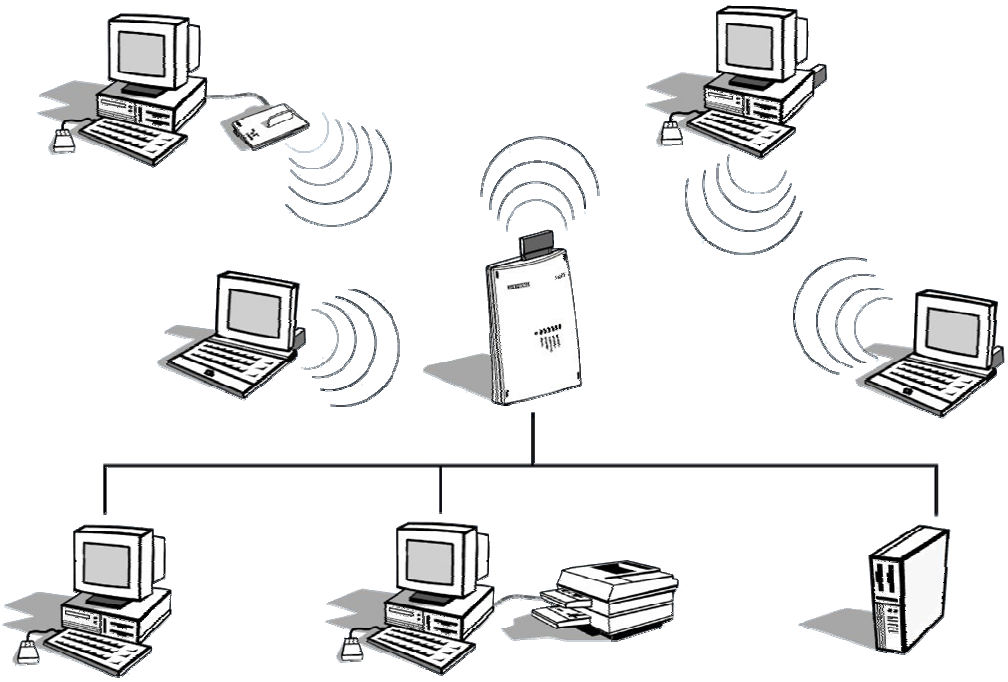


Figura.3.2 Estructura BSS o Infraestructura

ESS *(*Extended Service Set, "Conjunto de Servicios Extendido")

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

La configuración ESS permite crear una red local inalámbrica con una extensa área de cobertura. Para lograrlo se dispone de múltiples celdas BSS, cada una de las cuales cuenta con su punto de acceso. En esta configuración, las terminales pueden desplazarse por toda el área de cobertura sin perder la comunicación.

La configuración ESS resulta útil cuando es necesario cubrir una gran área de oficinas localizadas en distintas plantas, un espacio público o lugares con una alta concentración de terminales donde un solo punto de acceso resulta escaso.

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

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

Si un equipo pierde la comunicación con el AP, la reasociación con el nuevo AP se hace automáticamente sin que el usuario tenga que hacer nada. Desde el punto de vista del usuario, la conexión a una red ESS es idéntica a la conexión a una red BSS. La única diferencia es que se dispone de una mayor cobertura.

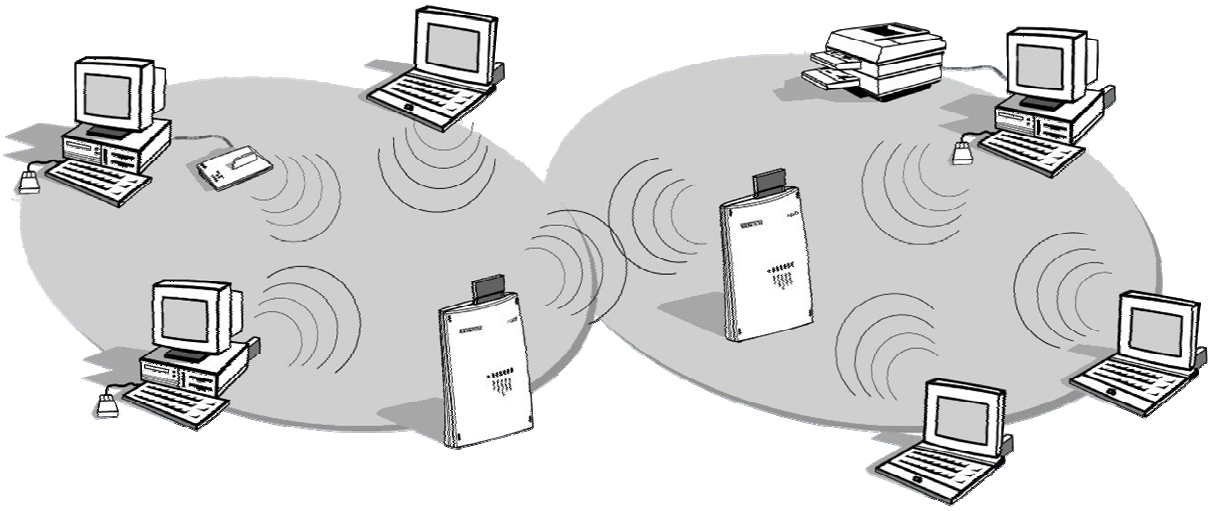


Figura.3. 3 Estructura ESS

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

Puntos de acceso.

Las comunicaciones *ad hoc* son muy fáciles de configurar y resultan muy interesantes cuando se necesita establecer una comunicación temporal entre dos equipos. Por otro lado, el modo infraestructura es el más adecuado para crear redes permanentes, aunque sean de tan sólo dos terminales. Las razones que nos llevan a esta conclusión son varias:

- El modo infraestructura ofrece un mayor alcance que en la modalidad *ad hoc.* Los terminales no tienen por qué estar dentro del área de cobertura el uno del otro; al tener un punto de acceso intermedio pueden, al menos, duplicar su distancia.

- El punto de acceso permite compartir el acceso a Internet entre todos sus terminales. Esto permite compartir un acceso de banda ancha entre todas las terminales que forman la red, sean dos o más.

- El punto de acceso permite crear redes con un mayor número de terminales.

- El punto de acceso ofrece características de gestión de la comunicación que no ofrece el modo *ad hoc.*

- El punto de acceso, al igual que cualquier red local, permite compartir los recursos de las terminales que forman la red como archivos, impresoras, etc.

Recientemente han aparecido en el mercado una alternativa al modo *ad hoc* conocida como *software* de punto de acceso. Esto consiste en configurar los equipos en modo *ad hoc* y hacer que uno de estos equipos haga las funciones de punto de acceso instalándole un programa especial, el *software* de punto de acceso.

Alcance.

Cuando nos decidimos a instalar una red inalámbrica, generalmente se parte de las necesidades de cobertura; es decir, pretendemos tener cobertura en toda la oficina, la casa, el entorno empresarial. Por lo que uno de los factores más importante de las redes inalámbricas es la cobertura. Esta depende tanto del alcance de los adaptadores de red (las tarjetas Wi-Fi), como de los puntos de acceso.

Los fabricantes anuncian que un punto de acceso o una tarjeta Wi-Fi llega a tener una cobertura de cientos de metros en espacio abierto con visibilidad directa entre terminales y sin interferencias de otros equipos que trabajen en la banda de 2,4 GHz. Hasta cierto punto es verdad, pero si el punto de acceso se instala en el interior de una casa u oficina, el alcance puede reducirse a unos 25 a 50 metros dependiendo de los obstáculos que haya en la habitación.

Por otro lado, la mayoría de los equipos Wi-Fi vienen equipados con un sistema que baja automáticamente la velocidad de transmisión conforme la señal de radio se va debilitando. Esto significa que, conforme se aumenta la distancia entre emisor y receptor, se puede ir disminuyendo la velocidad de transmisión de datos.

Además de la distancia, en el entorno existen otros factores que pueden afectar a la cobertura, como son las interferencias o las pérdidas de propagación debido a los obstáculos. De hecho, muchas de estas condiciones del entorno son cambiantes, por lo que en una posición puede haber cobertura en un momento dado y no haberla unos minutos más tarde.

Sin embargo, la única manera de saber exactamente si existe cobertura entre los equipos es instalando los equipos y haciendo una prueba real de cobertura.

Interferencias.

Dado que 802.11b utiliza la banda de 2,4 GHz y que estas frecuencias se encuentran en una banda abierta para usos industriales, científicos y médicos para los que no se necesita licencia, existe el riesgo de coincidir en el uso de la frecuencia con otros sistemas como los microondas, teléfonos inalámbricos, sistemas de televigílancia, dispositivos bluetooth o, incluso, otras redes inalámbricas. Estos pueden producir interferencias en las señales de radio de nuestra red. Una interferencia consiste en la presencia no deseada de señales radioeléctricas que interrumpen el normal funcionamiento del sistema.

Para evitar que una interferencia pueda cortar la comunicación, cuando el equipo Wi-Fi (protocolo MAC) detecta la presencia de una señal de interferencia, automáticamente entra en un periodo de espera en la idea de que, pasado dicho periodo, habrá pasado la interferencia. Evidentemente, esto hace que el servicio se degrade, pero no se interrumpe.

Desde el punto de vista del usuario, es imposible evitar las interferencias esporádicas, pero lo que sí se puede evitar son las interferencias constantes o periódicas. El sistema consiste en hacer pruebas de recepción de señal en la zona bajo sospecha. Estas pruebas pueden realizarse a distintas horas del día. A veces ocurre que las interferencias sólo se producen a la hora de la comida por el uso del microondas. Muchas de estas interferencias pueden evitarse sencillamente situando el punto de acceso en otro lugar, o moviendo la terminal.

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales. Antes de instalar es necesario hacer una inspección que nos ayudará a identificar los elementos que afecten negativamente a la señal inalámbrica.

La tabla siguiente muestra los materiales más comunes con los que puede existir algún tipo de dificultad para la transmisión y recepción de las radiofrecuencias, así como su nivel de interferencia.

MATERIAL	**EJEMPLO**	**INTERFERENCIAS**
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia / niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metal	Vigas	Muy alta

Como se vio anteriormente, debido a que las redes inalámbricas operan en un espectro de frecuencias utilizado por otras tecnologías, pueden existir interferencias que pueden afectar negativamente al rendimiento.

Equipo necesario para Wi-Fi.

Certificación de Equipo Wi-Fi.

Wi-Fi, o "Wireless Fidelity", es una asociación internacional sin ánimo de lucro formada en 1999 para asegurar la compatibilidad de los distintos productos de redes de área local inalámbrica basadas en la especificación IEEE 802.11. Esta alianza está formada actualmente por 183 miembros, y desde que comenzó la certificación de productos en marzo de 2,000,698 productos llevan el certificado Wi-Fi, asegurando la compatibilidad entre todos ellos.

La alianza Wi-Fi se estableció originalmente como WECA (Wireless Ethernet Compatibility Alliance) en agosto de 1999, por varias compañías líderes en tecnología en redes inalámbricas. Desde 1999, el número de miembros de la alianza Wi-Fi se ha incrementado dado que cada vez más compañías de productos electrónicos de consumo, proveedores de servicios de red y fabricantes de equipos se han dado cuenta de la necesidad de ofrecer a sus clientes compatibilidad inalámbrica entre sus productos.

Wi-Fi utiliza la tecnología de radio denominada IEEE 802.11b, 802.11a, 8011g ofreciendo seguridad, fiabilidad, y conectividad tanto entre equipos inalámbricos como en redes con hilos (utilizando IEEE 802.3 o Ethernet). Las redes Wi-Fi operan en las bandas de 2.4 y 5 GHz (no es necesario disponer de licencia), con una velocidad de 11Mbps (802.11b) o 54Mbps (802. 11a, g), ofreciendo un funcionamiento similar al de una red Ethernet.

Aunque lo más probable es que los equipos de diferentes fabricantes que cumplan técnicamente los mismos estándares sean compatibles, el certificado Wi-Fi asegura que no presentan ningún tipo de incidencias al trabajar conjuntamente en una red. Los aspectos que debe cubrir un equipo para obtener el certificado Wi-Fi son:

- Diversas pruebas para comprobar que sigue el estándar Wi-Fi.

- Pruebas rigurosas de compatibilidad para asegurar la conexión con cualquier otro producto con certificado Wi-Fi y en cualquier espacio (casa, oficina, aeropuerto, etc.) equipado con un acceso Wi-Fi.

Para que un equipo reciba el logotipo Wi-Fi es necesario que sea probado y verificado en los laboratorios de pruebas de esta asociación, asegurando que los productos con el logotipo Wi-Fi trabajan perfectamente unos con otros. Una vez que el producto inalámbrico pasa el proceso de pruebas, la compañía obtiene el sello Wi-Fi para dicho producto y puede utilizarlo con él. Es importante resaltar que el certificado lo recibe un producto en concreto, y no una familia de productos. Cada vez que el fabricante modifique alguno de sus componentes, el producto debe pasar por todo el programa de pruebas antes de obtener de nuevo el certificado Wi-Fi.

Para asegurar la compatibilidad, la alianza Wi-Fi trabaja con grupos técnicos de estándares como IEEE, y con compañías que trabajan en el desarrollo de futuras generaciones de redes inalámbricas. Este esfuerzo de cooperación asegura que los equipos trabajen con éxito en cualquier entorno Wi-Fi.

Hoy en día es posible encontrar espacios públicos equipados con redes inalámbricas Wi-Fi como cafeterías, hoteles, aeropuertos, etc., debido a que cada vez más viajeros y profesionales reclaman un acceso a Internet en el lugar donde se encuentren. Estas zonas Wi-Fi ofrecen acceso rápido y flexible a Internet. Básicamente sus características son:

- Acceso sencillo a Internet, sin problemas de conectividad con el equipo Wi-Fi que disponga, a través de un acceso de banda ancha.

- Una velocidad de entre 11 y 54 Mbs.

- Una conexión estable, a prueba de curiosos. Todas las zonas Wi-Fi soportan conexiones de redes privadas virtuales (VPN) que refuerzan la seguridad.

El Punto de Acceso más adecuado.

El punto de acceso es el centro de las comunicaciones de la mayoría de las redes inalámbricas. El punto de acceso no sólo es el medio de intercomunicación de todos los terminales inalámbricos, sino que también es el puente de interconexión con la red fija y con Internet.

Existen dos categorías de puntos de acceso:

- Puntos de acceso profesionales, diseñados para crear redes corporativas de tamaño medio o grande. Éstos suelen ser los más caros, pero incluyen mejores características, como mejoras en la seguridad y una mejor integración con el resto de equipos. Los líderes de este tipo de equipamiento son Cisco, 3Com, Agere/Orinoco (antiguamente conocidos como Lucent) y Nokia.

- Puntos de acceso económicos dirigidos a cubrir las necesidades de los usuarios de pequeñas oficinas o del hogar. Estos puntos de acceso ofrecen exactamente los mismos servicios que los anteriores, con la misma cobertura y las mismas velocidades. La diferencia se nota cuando se dispone de un gran número de usuarios. En estos casos, los puntos de acceso profesionales ofrecen mejores resultados, eso sí, multiplicando el precio por cuatro o cinco. Los que más puntos de acceso de tipo económico venden son Intel, 3Com, D-Link, Agere/Orinoco, NetGear Proxim y Linksys.

Aparte de lo anterior, cada equipo tiene sus propias características externas. Por ejemplo, algo que diferencia claramente a unos puntos de acceso de otros es el número y tipo de puertos que ofrece. Existen puntos de acceso que disponen hasta de un puerto de impresora, con su servidor de impresión, mientras que otros se limitan a ofrecer una conexión para red cableada o Internet.

Es habitual que los puntos de acceso se utilicen también como pasarela de conexión con otras redes; por ejemplo, con Internet. Desde este punto de vista, es importante tener en cuenta dos cosas: la primera es las características de *router* del punto de acceso: DHCP, NAT o propiedades de *firewall* son características que nos ayudarán en la configuración y manejo de las comunicaciones con Internet o con otras redes.

En el entorno corporativo suelen coexistir una red inalámbrica, para darle movilidad a los usuarios que la necesitan, junto con una red cableada, para darle conectividad al resto de usuarios. Generalmente, las redes corporativas utilizan el protocolo TCP/IP; no obstante, hay que tener en cuenta que en el mercado existen otros protocolos como SPX/IPX, NetBIOS, LANtastic, etc. Por tanto, conviene comprobar que el punto de acceso a utilizar sea compatible con el protocolo de red cableada con el que se va a conectar.

Por último, los equipos Wi-Fi tienen la ventaja de que tienen la garantía de interfuncionar sin problemas de acuerdo con la norma IEEE 802 lb. Esto es así, sin duda, en relación con los adaptadores de red; sin embargo, existe cierta incompatibilidad en relación con los puntos de acceso. La incompatibilidad aparece a la hora de mantener en servicio una comunicación cuando un usuario pasa del área de cobertura de un punto de acceso al de otro (conocido como *roaming*). En este caso, si los puntos de acceso son de distinto fabricante, es muy posible que se corte la comunicación. La comunicación se podrá volver a establecer con el nuevo punto de acceso, pero no se habrá producido una transferencia sin interrupciones, que es de lo que se pretende. Para evitar este problema, es recomendable que los puntos de acceso vecinos sean del mismo fabricante. Además, cuando todos los dispositivos son del mismo fabricante, es posible utilizar alguna característica adicional propietaria del fabricante.

En cualquier caso, el IEEE esta trabajando para solucionar este problema (grupo de trabajo IEEE 802.11 f). Esto no tiene nada que ver con las tarjetas inalámbricas que se conectan a los equipos; estas últimas si pueden proceder de fabricantes distintos sin ocasionar problemas.

Características Principales de los Puntos de Acceso.

Los puntos de acceso son unas pequeñas cajas de las que sobresalen una o dos antenas. Algunos fabricantes se han preocupado incluso de darles una forma estilizada que se salga de la forma típica de caja. Aunque la estética exterior de la caja pueda parecer un hecho sin importancia, en las redes para el hogar puede ser un punto a valorar. Por otro lado, a veces la estética es algo más que las apariencias. Unos puntos de acceso incluyen útiles para poderlos soportar en la pared o en el techo, mientras que otros carecen de este tipo de accesorios.

En cualquier caso, en su interior podemos encontrar lo mismo:

- Un equipo de radio (de 2,4 GHz, en el caso de 802.11b o 5 GHz, en el caso de 802.11a,g)
- Una o dos antenas (que pueden o no apreciarse exteriormente)
- Un *software* de gestión de las comunicaciones
- Puertos para conectar el punto de acceso a Internet o a la red cableada

La radio.

El objetivo principal de los puntos de acceso es comunicarse con las terminales vía radio Por tanto, lo principal de los puntos de acceso es su equipamiento de radio. Este equipamiento viene integrado en un conjunto de *chips* electrónicos conocidos como *chipsets.* Aunque en el mercado existen muchos fabricantes de puntos de acceso, son muchos menos los que fabrican *chipsets.* Dos de los principales fabricantes de *chipsets* Wi-Fi son Lucent e Intersil.

Desde el punto de vista del usuario, el funcionamiento de los distintos *chipsets* es idéntico. Además, entre ellos deben ser compatibles. No obstante, la teoría de la compatibilidad trae sorpresas a veces, por lo que resulta recomendable comprar equipos puntos de acceso y tarjetas inalámbricas que utilicen *chipsets* del mismo fabricante. La única forma de estar seguros de esto es comprar todo el equipamiento del mismo fabricante. Esto puede ser un contrasentido desde el punto de vista de la compatibilidad de la marca Wi-Fi, pero tiene sus ventajas prácticas.

Puertos del Punto de Acceso.

Los puntos de acceso necesitan disponer de puertos para poderse conectar con una red local cableada y con Internet. Para conseguir esto, los puntos de acceso cuentan con uno o más puertos 10/100Base-T (RJ-45). No obstante, dependiendo del modelo, nos podemos encontrar con los siguientes puertos:

- Un puerto especial para conectarse a un *hub* o *switch* de red de área local Ethemet *(uplink port).*

- Disponer internamente de un *hub,* por lo que ofrecen de dos a cuatro puertos exteriores para conectarles los equipos de red Ethernet de que disponga el usuario. Esto es ideal para el hogar o la pequeña oficina ya que evita la necesidad de disponer de un *hub* o *switch* independiente. En cualquier caso, si se necesitase de más de cuatro puertos, siempre se puede comprar otro *hub* y conectarlo al punto de acceso para extender la red.

- Un puerto serie RS-232 para que se le pueda conectar un módem de red telefónica (RTB o RDSI). Esta conexión a Internet a *56* Kbps o 64 Kbps puede ser utilizada como acceso principal a Internet o como acceso de seguridad en el caso de que falle la conexión de banda ancha (ADSL o cable módem).

- Un puerto paralelo o USB para conectarle una impresora. Esto permite compartir una impresora sin la obligación de tener un equipo encendido para poder mantener disponible la impresora. Además, la impresora no le ocuparía recursos a ningún equipo.

- Puerto para conectarle una antena exterior que le provea de un mayor alcance. Si se necesita que el punto de acceso ofrezca cobertura a una distancia superior a unos 100 metros, es importante contar con un punto de acceso que disponga de un conector de este tipo.

Los puntos de acceso ofrecen determinadas características que son configurables, como son las opciones de seguridad o de gestión de la red. La mayoría permiten llevar a cabo esta configuración a través de una interfaz basada en páginas *web.* Para hacer uso de esto, sólo se necesita instalar el *software* que incluye el punto de acceso.

No obstante, es importante saber que algunos puntos de acceso no utilizan una interfaz *web,* sino que requieren de la introducción directa de líneas comandos (lo que se conoce como CLI, *Command Line Interface*) o, incluso, requieren de un sistema operativo particular. Por ejemplo, Airport Base Station de Apple requiere disponer de un equipo con sistema operativo Mac. En cualquier caso, siempre es buena idea asegurarse de que el punto de acceso es compatible con nuestro sistema operativo.

La funcionalidad básica de los puntos de acceso o pasarela inalámbrica consiste en:

- Realizar la conversión de la señal de datos Ethernet a señales de radio (IEEE 802.11 para el caso de redes Wi-Fi), pudiendo ser un punto de conexión entre ambas redes.

- Actúa como elemento de interconexión entre diferentes clientes inalámbricos.

- Proporcionan un área de cobertura para los clientes inalámbricos. El espacio cubierto dependerá de la capacidad del equipo y sobre todo del entorno físico que se quiera cubrir: espacios exteriores o interiores con más o menos obstáculos.

- Pueden ofrecer funciones de "firewall" que permite aumentar la seguridad de la red. También pueden ofrecer mecanismos de autenticación para los clientes inalámbricos.

- Pueden ser configurados para crear diferentes escenarios de trabajo. Ofrecen facilidades de gestión.

Si es necesario ofrecer conexión inalámbrica a áreas más extensas, se pueden utilizar varias unidades bases conectadas entre sí, cada una cubriendo una parte del área total.

Adaptadores Inalámbricos de Red.

Los adaptadores de red son las tarjetas o dispositivos que se conectan a los equipos para que puedan funcionar dentro de una red inalámbrica. Estos equipos pueden recibir también el nombre de tarjetas de red o interfaces de red (NIC *Network Interface Cards*) es decir, cualquier tarjeta instalable o conectable a un equipo que sirve para integrarlo en una red, sea ésta cableada o inalámbrica.

Los adaptadores de red son fundamentalmente unas estaciones de radio que se encargan de comunicarse con otros adaptadores (modo *ad hoc)* o con un punto de acceso (modo infraestructura) para mantener al equipo al que están conectados dentro de la red inalámbrica a la que se asocie.

Como todos los equipos de radio, los adaptadores de red necesitan una antena. Esta suele venir integrada dentro del propio adaptador sin que externamente se note. Algunos adaptadores permiten identificar claramente su antena. En cualquier caso, la mayoría de los adaptadores incluyen un conector para poder disponer una antena externa. Este tipo de antenas aumentan grandemente el alcance del adaptador.

Tipos de Adaptadores De Red.

Recientemente están apareciendo en el mercado algunos equipos portátiles que ya tienen integrado un adaptador de red Wi-Fi. No obstante, aun existe la necesidad de que el adaptador de red sea un equipo independiente que haya que instalar o conectar al equipo o PDA.

Actualmente existen los siguientes tipos de adaptadores inalámbricos de red:

- **Tarjetas PCMCIA. S**on tarjetas que tienen un tamaño similar al de una tarjeta de crédito, como un 30% más larga y que se insertan en los puertos PCMCIA *(PC cara)* de tipo II que suelen incorporar la mayoría de los equipos portátiles. Los equipos de sobremesa no suelen contar con puertos PCMCIA.

- **Tarjetas PCI o ISA.** Los equipos de sobremesa no suelen disponer de ranuras PCMCIA. De lo que sí disponen son de ranuras PCI o ISA donde se pueden instalar todo tipo de tarjetas de periféricos, entre las que están las tarjetas Wi-Fi. No obstante también es posible instalar tarjetas conversoras de PCI o ISA a PCMCIA. Estos conversores son tarjetas PCI o ISA que se insertan en una ranura interna del equipo y que ofrecen un puerto PCMCIA al exterior. Evidentemente, adicionalmente haría falta disponer de la tarjeta PCMCIA.

- **Unidades USB.** Se trata de unidades inalámbricas que se conectan al equipo (portátil o sobremesa) mediante un puerto USB. Estas unidades son más propias de los equipos de sobremesa, ya que evitan tener que instalar en su interior un adaptador de tarjeta PCMCIA. No obstante, son válidas para todo tipo de equipos. Si el equipo ya tiene ocupados todos sus puertos USB existen multiplicadores de puertos USB que permiten sacar cuatro puertos de donde había uno.

Tarjetas PCMCIA.

Uno de los problemas que tenían antiguamente los equipos portátiles era que difícilmente podían ampliarse en sus prestaciones. Para instalarle una tarjeta de red o un módem a un equipo de sobremesa, bastaba con añadir en su interior la tarjeta correspondiente (ISA, PCI, etc.). Sin embargo, el interior de los portátiles, estuvo completamente cerrado hasta que aparecieron puertos especiales conocidos como PCMCIA *(Personal Computer Memory Card International Association*). Conocidas más coloquialmente como *PC Card* (tarjeta de PC).

Los puertos PCMCIA son una especie de ranura en la que se pueden insertar unas tarjetas del tamaño de una de crédito. Estas tarjetas quedan insertadas en el interior de la ranura, por lo que el equipo portátil no pierde su integridad y fácil portabilidad. En el mercado existen muchos tipos de tarjetas PCMCIA: módem, tarjetas de red Ethernet, discos duros, etc.

Las tarjetas PCMCIA las crearon en 1989 una asociación de fabricantes de equipos con el propósito inicial de desarrollar una norma *hardware* y *software* para tarjetas de memoria intercambiables. No obstante, la idea fue tan buena que se ha utilizado para todo tipo de periféricos.

Todas las tarjetas PCMCIA tienen un ancho de 54 milímetros, siendo su largo variable, pero con un mínimo de *85,6* milímetros. El hecho de ser variable se debe a que algunas tarjetas necesitan sobresalir hacía el exterior para mostrar algún tipo de conector, una antena o, simplemente, porque necesitan más espacio.

En cuanto al grosor de las tarjetas existen tres tipos: las tarjetas tipo I con un grosor de 3,3 milímetros utilizadas, por ejemplo, para ampliaciones de memoria, las de tipo II con un grosor de 5 milímetros, usadas habitualmente en los adaptadores de red inalámbricos, y las de tipo III con un grosor de 10,5 milímetros utilizadas por los discos duros.

Por una razón exclusivamente de espacio, cada tarjeta requiere su propio tipo de ranura en el equipo. Esto quiere decir que una ranura de tipo III admite cualquier tipo de tarjeta, mientras que una ranura de tipo I sólo admite tarjetas de este tipo. El tamaño más habitual de las tarjetas es el de tipo II.

Aparte del tamaño y del peso, otra de las características que aportan las tarjetas PCMCIA es su bajo consumo de energía y ser resistentes a los golpes típicos de los dispositivos móviles.

Los adaptadores Wi-Fi PCMCIA suelen ser de tipo II *y* la mayoría de los equipos portátiles incluyen una o dos ranuras PCMCIA de este tipo. Si tiene un equipo muy antiguo, será mejor que compruebe si admite este tipo de tarjetas antes de comprar el adaptador.

Figura 3.6 Tarjetas Wi-Fi PCMCIA

Adaptadores PCI e ISA.

Los equipos de sobremesa no suelen incluir ranuras PCMCIA. Estos equipos suelen disponer de suficiente espacio interior como para admitir la instalación de nuevos periféricos a base de tarjetas tipo PCI *(Peripheral Components Interconnect*) o ISA *(1ndustry Standard Architecture*). Este tipo de tarjetas son más baratas que las tarjetas PCMCIA, pero son mayores en tamaño y de instalación algo más compleja. Sin embargo difícilmente se encuentran en el mercado adaptadores inalámbricos de red de tipo PCI o ISA. Para resolver este problema existen los adaptadores USB o la tarjeta conversora de PCI o ISA a PCMCIA.

Una tarjeta conversora de PCI o ISA a PCMCIA es una tarjeta que se instala en el interior del equipo en una de las ranuras PCI o ISA disponibles y que ofrece al exterior una ranura PCMCIA (generalmente de tipo II o III). Dicho de otra manera, este conversor le añade una ranura PCMCIA al equipo.

Las tarjetas conversoras de este tipo suelen ser baratas, pero a este precio hay que añadirle el precio de la propia tarjeta PCMCIA, por lo que la conexión a la red inalámbrica del equipo de sobremesa pasa a ser algo más cara que la del equipo portátil.

El mayor inconveniente que presentan los dispositivos PCI e ISA es que requieren ser instalados en el interior del equipo, incluso los que anuncian ser *Plug&Play* (tipo conectar y funcionar) finalmente requieren que se les instale el software de los controladores.

Si se cuenta con un equipo que dispone tanto de ranuras PCI como ISA, es más aconsejable utilizar las de tipo PCI; ya que suelen dar menos problemas de instalación y requieren menos recursos del sistema. Por otro lado, ISA, también conocido como *bus* AT, puede transmitir información a una velocidad máxima de 16 MBps, mientras que PCI puede llegar a *528* Mbps.

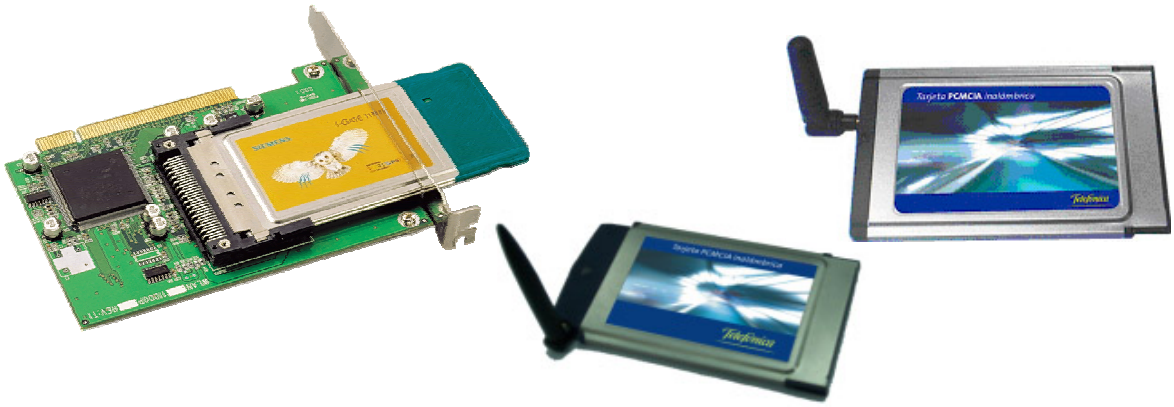


Figura 3.7 Tarjetas Wi-Fi PCI

Adaptadores USB.

USB *(Universal Serial Bus*) es un nuevo puerto de comunicaciones que se diseñó para poder mejorar la forma en cómo los periféricos se conectaban a los equipos. Antes de que apareciera USB, las únicas posibilidades de conectar un periférico a un equipo eran mediante el puerto serie o el puerto paralelo. El inconveniente mayor con estos puertos es que sólo se podían conseguir velocidades de transmisión de 115 Kbps. Adicionalmente, los equipos sólo disponían de un puerto paralelo y dos series, con lo que el número de dispositivos a conectar se reducía a tres; además, son puertos que no le permiten al equipo reconocer automáticamente el dispositivo que tienen conectado, ni alimentarlos a través del propio puerto y el USB vino a traer las siguientes ventajas:

- No hace falta apagar el equipo para conectar o desconectar un periférico USB.

- El equipo reconoce automáticamente los periféricos que se conectan mediante USB. Si es preciso, instalan automáticamente los controladores necesarios para hacerlo funcionar adecuadamente.

- Ofrecen una alta velocidad de transferencia de datos: hasta 12 Mbps.

- Permite conectar hasta 127 dispositivos USB. Incluso, aunque el equipo disponga de un solo puerto, basta con instalar un multiplicador de puertos (un *hub)* para disponer de más puertos USB.

- Ofrece alimentación eléctrica a los periféricos a través del propio conector USB.

- Los periféricos USB pueden apagarse automáticamente cuando detectan que no se están utilizando.

- Los periféricos USB se instalan automáticamente, sin necesidad de abrir el equipo.

Todo lo anterior ha hecho que los periféricos USB hayan ido desplazando poco a poco al resto de periféricos del mercado, hasta el punto de que ya existen equipos que no disponen de puertos serie ni paralelo, sino sólo puertos USB. Actualmente prácticamente todos los tipos de periféricos ofrecen la posibilidad de ser conectados al equipo a través de un puerto USB, tales como impresoras, módem, escáneres, cámaras, discos duros, etc.

Desde el punto de vista de los adaptadores de red inalámbrica, USB ofrece la ventaja de poder compartir el adaptador entre diferentes equipos según se necesite. Como instalar el adaptador es tan fácil como conectarlo al puerto USB, si un equipo necesita conectarse a la red, se le enchufa el adaptador y listo. Cuando no lo necesite, con desenchufarlo del puerto USB se tiene bastante.

Otras de las ventajas es que el adaptador puede reorientarse con respecto al punto de acceso para buscar una mejor cobertura, sin tener que mover el equipo.

El único inconveniente de los adaptadores USB es que son dispositivos externos al equipo. No quedan integrados dentro de él como lo hacen los adaptadores PCMCIA, PCI o ISA.

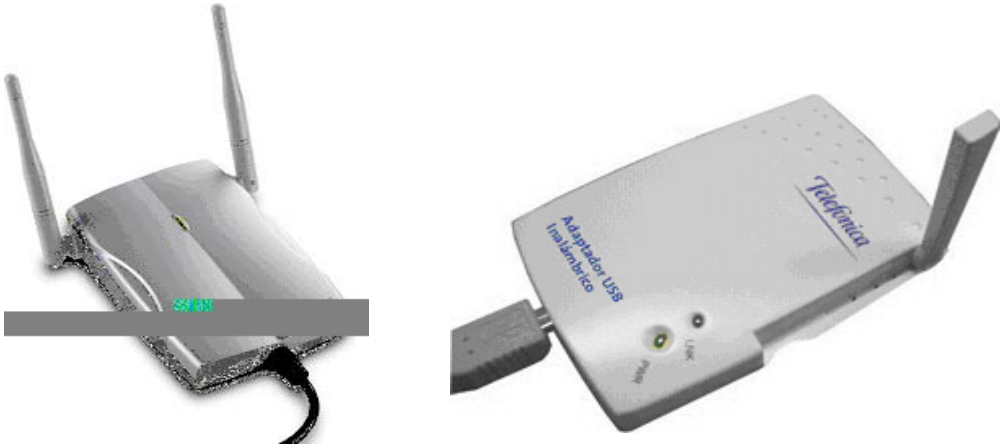


Figura. 3.8 Adaptadores USB para redes Wi-Fi

Adaptadores para PDA.

Un PDA es un pequeño equipo que cabe en la palma de la mano; también se les conoce como *PocketPC* (PC de bolsillo) o como *HandHeld PC* (PC de mano).

Debido a su pequeño tamaño, los PDA pueden llevarse siempre encima, por lo que suelen incluir aplicaciones que, son asistentes personales de su usuario como agenda de direcciones, agenda de actividades, lista de tareas, juegos, etc. Sin embargo, un PDA puede utilizarse también como herramienta de comunicación que permite al usuario acceder a Internet, ver páginas *web,* gestionar correos electrónicos, etc. Del mismo modo, las nuevas PDA incluyen versiones reducidas de programas de gestión tan conocidos como Microsoft Word, Excel, etc. En definitiva, un PDA es un pequeño equipo de gran utilidad debido precisamente a su pequeño tamaño.

Habitualmente, un PDA se conecta a Internet a través de un equipo personal. Los correos se escriben en el PDA, pero no se transmiten hasta que no se conectan mediante un cable o infrarrojos al equipo personal con el que se ha asociado previamente. También existe la posibilidad de conectarle un módem especial al PDA y acceder directamente a Internet a través de un proveedor de acceso. En este sentido, han aparecido en el mercado equipos PDA que incluyen en su interior un terminal móvil, o teléfonos móviles que incluyen en su interior las capacidades de los PDA.

Cualquiera de las soluciones anteriores tiene un inconveniente y es que no permite que el PDA esté conectado a Internet permanentemente, al menos, sin pagar unas altas tarifas por las llamadas telefónicas (del móvil o del fijo). Por otro lado, salvo en el caso del PDA con móvil, el PDA siempre estará conectado por cable para intercambiar sus datos con el equipo asociado o conectarse a Internet. Así, las redes inalámbricas le ofrecen al PDA la posibilidad de liberarse de las ataduras del cable.

En el mercado existen módulos adaptadores de red inalámbrica para los principales modelos de PDA: 3Com, Compaq, HP, Casio, etc. A la hora de comprar uno de estos dispositivos, es conveniente asegurarse de que es el adecuado para el modelo concreto de PDA de que se dispone. Estos módulos suelen ser tarjetas de tipo Compact Flash con una pequeña antena exterior.

Bridges.

Un *bridge* (puente) es un dispositivo que interconecta dos redes. Una vez interconectadas, los equipos de una red pueden ver y comunicarse con los equipos de la otra red como si todos formaran parte de la misma red. La mayoría de los puntos de acceso hacen las funciones de *bridges* al poder interconectar una red local cableada con la red inalámbrica. Esto hace posible que los equipos de la red inalámbrica utilicen las impresoras de la red cableada o accedan a los archivos de cualquiera de sus equipos.

No obstante, existe un equipo conocido como *bridge* inalámbrico *(Wireless Bridge)* que es algo distinto de un punto de acceso. Un *bridge* inalámbrico interconecta dos redes remotas, cableadas o no, mediante una conexión inalámbrica. Estas dos redes pueden ser interconectadas también mediante cable, pero los *bridges* inalámbricos evitan la necesidad de tener que instalar o alquilar el cable.

La solución inalámbrica requiere de dos equipos *bridges* inalámbricos, uno en cada extremo. En cualquier caso, estos equipos pueden ser utilizados para extender el área de cobertura de una red inalámbrica, sobre todo cuando se trata de interconectar zonas localizadas en edificios distintos o que no tienen una visibilidad directa para poder utilizar antenas externas direccionales.

Figura. 3.11 Puentes inalámbricos

Antenas.

Una antena es un dispositivo que permite la emisión y recepción de ondas electromagnéticas (ondas de radio). Esto quiere decir que las antenas convierten las señales eléctricas en ondas electromagnéticas, y viceversa.

Todos los equipos Wi-Fi ya incorporan sus propias antenas. No obstante, cuando se desea disponer de una red de mayor alcance o cobertura, resulta conveniente sustituir la antena incorporada en el equipo Wi-Fi por otra exterior con mayor ganancia

La mayoría de las antenas que incorporan los equipos Wi-Fi son antenas internas. Esto quiere decir que son antenas que vienen incluidas dentro de la unidad del punto de acceso o del adaptador de red. Las antenas internas ofrecen la gran ventaja de la comodidad al formar parte del propio dispositivo, pero tienen el inconveniente del alcance. Si se necesita aumentar el alcance sin instalar nuevos puntos de acceso, la mejor solución es colocar una antena externa. Con una buena antena externa, la señal Wi-Fi de un punto de acceso puede llegar a superar los 15 kilómetros de alcance siempre que no haya obstáculos, como edificios o árboles, y que la antena esté bien colocada.

La mayoría de los puntos de acceso y de los adaptadores de red admiten que se les conecte una antena externa. Existen antenas externas tanto para interiores como para exteriores de edificios.

Una antena es un dispositivo, generalmente formado por una o más varillas, destinado a la radiación y/o captación de ondas radioeléctricas. La antena de un equipo emisor radia las ondas radioeléctricas, mientras que la antena de un equipo receptor las capta. Un mismo equipo de radio, y su antena, puede ser utilizado tanto para transmitir como para recibir. Por cierto, a esto se le llama *transceiver (transmiter-receiver*).

Una comunicación en la que la información fluye en ambas direcciones recibe el nombre de bidireccional. Cuando la transmisión y recepción no se efectúa simultáneamente, sino alternativamente, se obtiene lo que se conoce como comunicación semidúplex *(half-dupplex*). Las comunicaciones Wi-Fi son bidireccionales semidúplex.

En el mercado existen muchos tipos de antenas que pueden funcionar bien en los entornos Wi-Fi. Sin embargo, es importante conocer algunos conceptos generales que nos ayudan a comprender mejor las características de los distintos tipos de antena.

Tipos de Antenas.

En el mercado existen tantos tipos de antenas como ha permitido la imaginación: yagui, de panel, parabólica de disco, parabólica de rejilla, de techo, *patch,* dipolo, planas, compactas, móviles, sectoriales, espiral, guía-onda, anular, etc. Todos estos tipos de antenas pueden agruparse en dos tipos primarios: omnidireccional y direccional.

Las antenas omnidireccionales son aquéllas que radian en todas direcciones y también pueden captar la señal procedente de todas las direcciones. Por el contrario, las antenas direccionales concentran su radiación en una dirección y sólo pueden captar la señal procedente de esa dirección. Las antenas direccionales tienen un mayor alcance y ganancia que las primeras a costa de concentrarse en una sola dirección.

En el caso de los equipos Wi-Fi, se suelen utilizar los tipos de antenas omnidireccionales para interiores y los tipos direccionales para exteriores.

Las antenas más habituales son las conocidas como dipolo. Un dipolo emite su señal haciendo que la energía se propague paralela al dipolo y perpendicular al suelo (polarización vertical). Si se girase la antena 90 grados, se obtendría una antena de polarización horizontal.

Las antenas direccionales concentran la energía en una sola dirección consiguiendo obtener incrementar el alcance. Cuanto más direccional es una antena, mayor es su alcance. Existen distintos modelos de antenas direccionales entre los que destacan los siguientes:

- La 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.

- La 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 en el exterior.

- La antena parabólica es una antena que tiene forma de disco cóncavo con la que se consiguen haces direccionales. Es 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.

- Además de las anteriores, existen otros diferentes tipos de antenas (dipolos, reflectores, etc.) que pueden ser utilizadas en las instalaciones Wi-Fi. En cualquier caso, siempre es conveniente asegurarse que la antena está construida para funcionar en la banda de 2,4 GHz.

Antena Direccional Antena de panel tipo patch
Antena Omnidireccional

Figura. 3.10 Antenas externas para Wi-Fi

La mayoría de los puntos de acceso vienen equipados con una doble antena. Esta doble antena se utiliza para obtener diversidad en la recepción. Cada antena, aunque sólo estén separadas unos centímetros, puede recibir la señal en distintas condiciones en cada momento. El sistema elige la mejor de las señales en cada momento evitando de esta forma muchos de los posibles problemas de mala recepción.

Diseño de la red.

Una vez decidido para añadir un sistema inalámbrico necesitamos determinar como empezar y que productos son los indicados para soportar las aplicaciones, movilidad, rangos, seguridad y otras características de la red.

Para diseñar cualquier red después de haber determinado las necesidades del usuario es importante la definición del área de cobertura. Es importante contar con un diagrama adecuado de las instalaciones en donde se muestre la cobertura que necesitamos tomar en cuenta para la WLAN, así como determinar las velocidades mínimas que requieren los usuarios. Es igual de importante verificar si las instalaciones están construidas con materiales que permitan que las ondas de radio penetren en las áreas especifica. Las señales de 2.4 GHz penetran las construcciones normales de manera mas sencilla que las señales de 5 GHz; para lo que hay que realizar pruebas en las instalaciones procurando evitar la interferencia con los demás dispositivos como microondas, alarmas inalámbricas, dispositivos bluetooth, etc. las cuales se pueden evitar mediante la colocación adecuada de los AP y las antenas.

Del mismo modo debemos determinar cuantos usuarios están ubicados dentro del área; por ejemplo para usuarios de aplicaciones de oficina es suficiente entre 10 y 20 usuarios por punto de acceso para tener un desempeño razonable, si lo que necesitamos son transacciones pequeñas que requiere un ancho de banda pequeño como una casa el número de usuarios por AP puede aumentar.

Conclusión.

El modelo que presentamos es bastante sencillo solo interconectamos unas cuantas computadoras por medio de un access point con el fin de que se puedan comunicar por medio de la tecnología inalámbrica; es decir implementamos una red inalámbrica pequeña. Sin embargo aun se cuenta con partes cableadas dentro de la red.

Los resultados obtenidos al implementar la tecnología inalámbrica dentro del diseño de nuestra red fueron exitosos ya que los usuarios tuvieron la facilidad de realizar sus actividades diarias desde cualquier punto de la oficina o del edificio sin tener que interrumpirlas por la necesidad de cambiar de su ubicación.

Del mismo modo nos permite la conexión de nuevos equipos sin la necesidad de tender cables a lo largo de todo el edificio; aunque tiene la desventaja del número de puertos de acceso con que cuenta el access point y la distancia de cobertura, los cuales dependen del modelo y de las características del fabricante del dispositivo. Sin embargo se puede solucionar al instalar por lo menos dos access point más alambrados juntos con lo que lograremos obtener cobertura adicional.

Por otro lado se noto que la seguridad en la parte de la red inalámbrica es más deficiente que en la parte cableada debido a que aun no se cuenta con las herramientas que puedan cubrir esta parte de forma apropiada.

Al diseñar la red nos encontramos con varios puntos a considerar dentro de los cuales podemos destacar la pedida de información por interferencias debido a la distribución física de las oficinas y a los materiales de los muros y los muebles, todo esto se tomo en cuenta para la colocación de las antenas y los puntos de acceso para minimizar este problema y optimizar el flujo de información en la red.

Son innumerables las posibilidades que la conectividad inalámbrica trae para la vida de las personas, posibilidades que puedes ser explotadas tanto en el hogar como dentro del corporativo.

Nuevas tecnologías se siguen desarrollando enfocándose especialmente a la necesidad de movilidad, lo que provoca que cada vez más diversidad de equipos en el mercado, además de las nuevas posibilidades de crecimiento profesional, la participación y gubernamental.

La conectividad inalámbrica es un tema extremamente complejo y atractivo que merece una atención especial y aun más amplia para considerar todos sus aspectos.

A pesar del nivel de desarrollo actual, la tecnología inalámbrica ni siquiera se ha acercado a su límite. Actualmente se están concibiendo herramientas que cuentan con esta tecnología y que se perfilan para involucrarse en muchos procesos y que podrían darnos una ligera idea de cómo puede llegar a ser nuestra vida, y nos da la oportunidad de imaginar el concepto de la oficina del futuro.

Glosario.

10 BASE 2	Implementación de Ethernet de 10 Mbps en cable coaxial delgado. Su máximo segmento es de 200 metros.
10 BASE 5	Implementación de Ethernet de 10 Mbps en cable coaxial grueso. Su máximo segmento es de 500 metros.
10 BASE F	Especificación para red Ethernet de 10 Mbps en fibra óptica.
10 BASE T	Estándar de transmisión de Ethernet sobre MIT a 10 Mbps.
100 BASE FX	Especificación para correr Ethernet 100 Mbps sobre fibra óptica.
100 BASE T	Estándar de transmisión sobre MIT de velocidad 100 Mbps.
100 BASE T4	Especificación para correr Ethernet 100 Mbps sobre cable 3,4 y 5 MIT de 4 pares.
100 BASE TX	Esquema que ofrece 100 Mbps sobre cable categoría 5 MIT.
Algoritmo	Serie de pasos para realizar una tarea específica.
Ancho de banda	Relación de velocidad para la transmisión de dato medidos en Kbps (kilo baundios por segundo) y que representa la capacidad del canal de comunicación para transportar datos.
ANSI	Organización encargada de la documentación de los estándares en Estados Unidos.
ARCNet	Red de computadoras y recursos compartidos creado por Datapoint muy popular en los años setenta, cuyas características eran: bajo costo, cableado en estrella y velocidad hasta 2.5 Mbps.
ARP	Proceso en donde se asigna al número de la tarjeta una dirección formato TCP/IP.
Backbone network	Red de Infraestructura. Red que actúa como conductor primario del tráfico de datos de la red.

	Comúnmente recibe y manda información a otras redes.
BIT	Dígito binario, unidad mínima de información de los dos estados 0/1. Abreviación de Binary Digit que puede ser 0 o 1. Es la unidad básica de almacenamiento y proceso de una computadora. 8 bits = 1 byte.
BPS	Bits por segundo. Velocidad de transmisión serial.
Bridge	Puente. Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.
Buffer	Espacio físico de memoria destinado a guardar datos temporalmente.
BUS	Circuito de interconexión eléctrica para transmitir información.
Byte	Conjunto de 8 bits. Representa un carácter en lenguaje binario.
Carrier o portadora	Señal eléctrica que permite la modulación de otra señal que contiene la información. Se utiliza para la transmisión remota vía la infraestructura de comunicaciones.
CHIP SET	Referente al grupo de circuitos integrados que se utilizan para una función.
Colisión	Definido como un exceso en portadora eléctrica. Sucede en Ethernet cuando dos o más estaciones hablan al mismo tiempo y las señales de datos se pierden.
Concentrador	Equipo que se encarga, en primera instancia, de concentrar las señales. Algunos tienen funciones de repetir y retrasar la señal para evitar colisiones.
Conectividad	Estado que permite la transferencia de datos entre dos computadoras.

CSMA/CD Sensor de portadora de accesos múltiples con detección de colisiones. Método de transmisión de datos en donde todas las estaciones pueden mandar datos con una señal eléctrica sumada (portadora). En caso de que existan transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.

Dirección Destino En el lenguaje de redes es la computadora que envía los datos de una transmisión.

Dirección Fuente En el lenguaje de redes es la computadora que recibirá los datos en una transmisión.

DMA Procedimiento de bajo nivel que permite que un dispositivo secundario de puertos (externo) tenga acceso a los recursos de memoria sin que el microprocesador tenga que atender el proceso. *ISA* Compatible/8 ciclos de reloj/960 ns. *EISA* tipo A/6 ciclos de reloj/640 ns. *EISA* tipo B/4 ciclos de reloj/480 ns. *EISA* tipo C/1 ciclos de reloj/120 ns. *EISA* tipo F/3 ciclos de reloj/360 ns.

Dominio Grupo de computadoras de la red que está administrada y controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.

Encriptamiento Proceso basado en operaciones lógicas binarias para disfrazar un dato y evitar que sea leído por otra fuente distinta al destino.

Escalabilidad Característica de los equipos que nos permite ir aumentando velocidad y capacidad en: discos, memoria, procesadores y tarjetas periféricas.

Estación Computadora que puede realizar procesos.

Ethernet Estándar de red más popular e implementado. Utiliza *CSMA/CD* con una velocidad de 10 Mbps.

Fast Ethernet Topología de transmisión digital tipo Ethernet que transmite a 100 Mbps.

FDDI Estándar de transmisión de datos vía fibra óptica hasta de 100 Mbps con topología parecida a Token Ring/Token Passing.

File Server	Computadora dedicada a proveer y almacenar los archivos.
Firewall	Sinónimo de dispositivo de software o hardware encargado de proteger cualquier sistema de la entrada de personas no autorizadas. Regula, según las necesidades, los niveles internos de restricción a la información y autoriza el acceso a cierto tipo de datos.
FRAME	Cuadro. Forma en que se organiza la información. Normalmente cuenta con tres partes: encabezado (control, fuente y destino), campo (datos a enviar), y *CRC* de verificación (bits para corregir errores).
Frame Relay	Paquetes retrasados. Protocolo de comunicación asíncrono con dispositivo especial que atrasa el envío de grupos de información para mandarlos en paquetes de tamaño fijo.
FTP	Servicio que permite transferir archivos entre sistemas y entre redes remotas con sistemas diversos. De uso común en Internet.
Full Duplex	Característica de un canal de comunicación en el que dos terminales pueden mandar y recibir información simultáneamente.
Gateway	Dispositivo que permite conectar dos redes o sistemas diferentes. Es la puerta de entrada de una red hacia otra.
Gigabyte	*GB*, 1 073'741 824 bytes, formalmente es 1 K de MB.
GUI	Medio de desplegar las salidas para presentar al usuario un formato gráfico.
Half duplex	Característica de un canal de comunicación en el que dos terminales mandan y reciben información turnándose, una a la vez.
Hardware	Referente a dispositivos reales, físicos. Todos los componentes electrónicos, magnéticos y mecánicos de las computadoras.
Hexadecimal	Sistema numérico con base en 16, comúnmente utilizado por su estructura fácil de transformarse al binario.

Host	Computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir usuarios.
Host Adapter	Tarjeta que sirve de interfaz entre dispositivos periféricos y el sistema principal.
Hub	Dispositivo inteligente que sirve de infraestructura para la red. Comúnmente asociado con un concentrador 10 base T con unciones inteligentes de retraso de señal *(retiming)*, y retransmisión de la misma *(repeating)*.
ICMP	Componente de los protocolos TCP/IP que realiza las funciones de control y administración de transacciones.
IEEE	Agrupación de ingenieros que, entre otras funciones, documenta todos los desarrollos tecnológicos.
IEEE-802.1	Estándar definido relativo a los algoritmos para enrutamiento de cuadros o frames (la forma en que se encuentra la dirección destino).
IEEE-802.2	Define los métodos para controlar las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI) llamado LLC.
IEEE-802.3	Define las formas de protocolos Ethernet CSMA/CD en sus diferentes medios físicos (cables).
IEEE-802.4	Define cuadros Token Bus tipo ARCNET.
IEEE-802.5	Define hardware para Token Ring.
IEEE-802.6	Especificación para redes tipo MAN (de área metropolitana).
IEEE-802.7	Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes.
IEEE-802.8	Especificación para redes de fibra óptica tipo Token Passing/FDDI.
IEEE-802.9	Especificaciones de redes digitales que incluyen video.
IEEE-802.11	Estándar para redes inalámbricas con línea de vista.

IEEE-802.12	Comité para formar el estándar de 100 base VG que sustituye CSMA/CD por asignación de prioridades.
IEEE-802.14	Comité para formar el estándar de 100 base VG sin sustituir CSMA/CD.
Interface	Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para dos sistemas diferentes.
Internet	Red de redes con base en TCP/IP y acceso público mundial.
Interoperabilidad	Término referente a la capacidad de diferentes redes para comunicarse entre sí.
Intranet	Red de área amplia con gran infraestructura y acceso privado.
IP	Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.
IPX	Protocolo definido para redes Netware que tienen direcciones en tres campos (nodo, red y socket), lo cual le permite mantener varios enlaces entre redes y procesos en varios servidores.
ISA	Arquitectura de 16 bits para tarjetas y dispositivos. El más común en las computadoras personales.
ISO	Organización que especifica estándares de calidad internacionales.
Kilobyte	KB. 1024 bytes.
LANtastic	Sistema operativo para redes de igual a igual.
Link	Término utilizado para referirse a los componentes lógicos y físicos que permiten la comunicación entre dos sistemas.

Local bus	Agregado al bus ISA para aumentar el desempeño de las funciones de entrada/salida. Utiliza un bus adicional que interactúa directamente con el microprocesador para aumentar la velocidad de transferencia y volumen de datos. Dos buses de este tipo son los más comunes: el VESA desarrollado por varios fabricantes de interfaces de video y PCI desarrollado por Intel.
LPT	Abreviatura para asignar puertos paralelos.
MAC	Capa de control de acceso a medios. Capa del modelo de comunicación OSI, que es la encargada del control lógico del medio físico.
Mainframe	Cuadro principal o computadora principal en la cual se llevan a cabo todos los procesos.
MAN	Red de Area Metropolitana.
MAU	Dispositivo utilizado en topologías de estrella física para generar un círculo lógico. Todos se conectan a él, y él asigna quién tiene el Token Passing o derecho de transacción.
MCA	Tecnología de bus de 32 bits desarrollada para los sistemas PS/2. No se difundió mucho por ser tecnología propietaria, no compatible con otros estándares.
Megabyte	MB. 1'048,576 bytes. Formalmente es 1 K de KB.
Módem	Modulador-Demodulador. Dispositivo que convierte señales binarias a tonos transmitibles por vía telefónica.
NetBios	Interface estándar para procesos de red. Son los servidores de software y firmware entre la tarjeta y las aplicaciones.
Netware	Sistema operativo de red desarrollado y propiedad de Novell.
Nodo	Estación de trabajo con identificación propia que puede ser fuente y destino en la red.
OSI	Estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.

Paquete	Unidad de información a transmitir. No contiene dirección ni destino, tan sólo ruta (el siguiente punto a llegar).
PC cards	Dispositivos periféricos que agregan una amplia variedad de posibilidades a las computadoras: almacenamiento, memoria, manejo de periféricos, fax, red, comunicaciones, etc. Existen tres tipos de acuerdo a su tamaño.
PCI	Estándar de bus para periféricos que típicamente utiliza DMS tipo F y Fast IO bidireccional. Desarrollado por Intel.
PCMCIA	Estándar de bus para tarjetas periféricas de computadoras portátiles.
Peer-to-peer	Igual a igual. Forma de comunicación de red donde cada uno tiene las mismas tareas en el proceso.
Ping	Transmisión de datos de prueba para verificar la integridad de la comunicación entre dos sistemas.
Protocolo	Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.
Queue	Fila de espera. Grupo de procesos por realizar.
Repetidor	Dispositivo que transmite y amplifica la señal de la red.
RJ45	Conector para MIT 4 pares.
Router	Ruteador. Dispositivo que pasa todos los mensajes entre una red y otra distinguiendo a qué red pertenece el destino del mensaje.
RS232	Interface serial entre DTE y DCE.
Servidor	Equipo destinado a proveer y administrar los servicios de red, los recursos, las aplicaciones, los archivos y la seguridad de la misma.
Sincronía	Forma de transmisión de datos donde se necesita señal adicional de reloj para que el transmisor y el receptor funcionen a la misma velocidad.
SNA	Arquitectura de protocolos para redes.

SPX	Trabaja en el cuarto nivel de OSI. Brinda apoyo a IPX garantizando la llegada y controlando las secuencias.
STP	Cable de par trenzado con blindaje o aislamiento magnético.
TCP/IP	Protocolos definidos por catedráticos en el proyecto ARPANet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.
TELNET	Utilería de TCP/IP que permite un *logon* remoto sobre un *host*.
Terminador	Componente del cableado que empata la impedancia característica del cable para regular las señales eléctricas en la red.
Tiempo de acceso	Intervalo entre el tiempo de una solicitud de datos por el sistema y el tiempo en que el dispositivo los tiene disponibles.
Tiempo Real	Dominación de aquellos procesos que suceden simultáneamente o con una diferencia imperceptible de tiempo. Internet ofrece tiempo real dentro de muchos servicios donde a la ejecución de una acción existe una respuesta inmediata (llegada de correo electrónico).
Token Passing	Estafeta. Método de comunicación en red en el que cada elemento debe recibir el permiso para hablar o la estafeta.
Token Ring	Red local en la que el permiso para transmitir es secuencial o en anillo.
Topología	Descripción de las conexiones físicas de la red, el cableado y la forma en que éste se interconecta.
TP	Cable de pares trenzados.
Transciever	Dispositivo de Ethernet que permite el cambio de medio físico a cable.
Transductor	Dispositivo que convierte una energía a otro tipo. Un foco convierte energía eléctrica en luminosa y calórica.

Upgrade	Término utilizado en software referente al cambio de programas hacia los más recientes, nuevos y mejorados.
Usuario	Persona que trabaja con la estación de trabajo. El que realiza tareas de acceso a los recursos de la red pero no los modifica sustancialmente. Tiene derechos de uso pero no de mantenimiento mayor.
WAN	Red de área amplia que tiene nodos en diferentes localidades geográficas e implementa infraestructura de comunicaciones.
Workstation	Computadora que puede realizar procesos robustos de *front end*. Permite sacar máximo provecho a sus recursos de red.
X.25	Protocolo para red de paquetes conmutados. Generalmente se incluyen los protocolos X.3 y X.28 en estas redes.

Bibliografia

Wi – Fi, Como Construir una Red Inalámbrica
José A. Carballar
Ra – Ma,

Wi – Fi, Como Construir una Red Inalámbrica
José A. Carballar
Ra – Ma, 2003, 2ª ed.

Redes Locales
José Luís Raya y Cristina Raya
Ra – Ma, 2003, 2ª ed.

Redes en 24 horas
Matt Hayden, Aprendiendo
Prentice Hall.

Apuntes y Trabajos de Temas de Informática en General
Varios Autores
http://en.wikipedia.org/wiki/Wifi
http://www.cibercursos.net
http://www.wi-fi.org

TCP/IP Network Administration
Craig Hunt
editorial