UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

IMPLEMENTACIÓN DE TECNOLOGÍA INALÁMBRICA EN LA RED DE DATOS ESTRUCTURADA DEL CENTRO COMERCIAL(CECOSORI)

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

P R E S E N T A

ALEJANDRO RUISEÑOR MARTINEZ

ASESOR: M.C.ARTURO AUSTRIA CORNEJO

PACHUCA DE SOTO, HIDALGO. MAYO DE 2007

Agradecimientos

A mis padres y hermanos por enseñarme a ser mejor persona
y por su enorme sacrificio.
A mi asesor de tesis, M.C.Arturo Austria Cornejo.
A mis amigos y a mi novia, que siempre estan ahí cuando más los necesito.

Resumen

La tesis presenta un panorama completo sobre la operación de las redes inalámbricas así como la metodología a seguir para su correcta instalación y funcionamiento.
Asímismo se describiran las tecnologías más recientes empleadas en los sistemas de redes inalámbricas, todo esto para poderlo aplicar para realizar un proyecto para proporcionar un mejor funcionamiento, facilidad, accesibilidad, servicio para una red comercial.

El objetivo de la tesis es mejorar los servicios de mesa de control, recibo, consumos internos, caja general, atención al cliente etc, de la tienda de autoservicio Mercado Soriana 136. Todos los sistemas de los centros comerciales son muy similares, su control de mercancia(entrada-salida), sus inventarios, recolección de valores, punto de venta y demás funcionalidades. Por eso realize éste estudio y es probable utilizarlo en la aplicación de cualquier área comercial.

Con la facilidad de administrar una red inalámbrica, con gastos no tan altos en su instalación y movilidad, los servicios y las funcionalidades serían mejores y así abrir nuevas formas de servicio y de administración. El principal propósito de diseñar una red consiste en que todas las computadoras que forman parte de ella se encuentren en condiciones de compartir su información y sus recursos con las demás. De esta manera, se estaría ahorrando dinero, debido a que si se colocara un dispositivo, por ejemplo, una impresora, todas las computadoras de la red podrían utilizarlo. Las redes inalámbricas son aquéllas que carecen de cables. Gracias a las ondas de radio, se lograron redes de computadoras de este tipo. Esta tecnología facilita en primer lugar el acceso a recursos en lugares donde se imposibilita la utilización de cable. Además, las redes pueden ampliar una ya existente y facilitar el acceso a usuarios que se encuentren en un lugar remoto, sin la necesidad de conectar sus computadoras a un hub o a un switch por medio de cables.

Los usuarios podrían acceder a la red de su empresa o a la computadora de su casa en forma inalámbrica, sin configuraciones adicionales. Claro que para esto se necesitará no sólo de los materiales, sino también de los conocimientos básicos para lograrlo. El aprendizaje de éstos últimos representa el objetivo de esta tesis, que tiene como fin lograr que se puedan armar redes inalámbricas en forma eficiente y ágil.

En el transcurso de los capítulos, veremos detalladamente todas las cuestiones que debemos considerar para lograr una tarea exitosa, también todas las medidas de seguridad que es necesario tener en cuenta.

Índice general

Índice de Tablas

Índice de figuras

Capítulo 1

Introducción

1.1. Introducción

El capítulo ofrece una introducción a los conceptos básicos de las redes inalámbricas, se muestran los tipos, componentes básicos. Además en este capítulo se define el estado del arte, así como los objetivos a alcanzar, así también la propuesta de solución. Esta investigación se basa en la Ethernet inalámbrica su norma base es la IEEE 802.11 que se denomina WLAN (wireless local area network). Es un sistema de comunicación de datos inalámbrica flexible, muy utilizado como alternativa a la LAN cableada ó como extensión de esta.

En los ultimos años las redes de área local inalámbricas (WLAN) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas.

Las WLAN permiten a los usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar y transmiten datos por radiofrecuencias en lugar de hacerlo a través de cable coaxial, par trenzado o fibra óptica, lo cual permite mayor movilidad a los usuarios al minimizarce las conexiones cableadas.

Las WLAN van adquiriendo importancia en muchos campos, como en la industria, almacenes, tiendas, compañias, gobierno ó para manufacturación, en los que se transmite la información en tiempo real a una terminal central o en casa para compartir un acceso a internet entre varias computadoras, la PC o cualquier terminal movíl se conecta a la red inalámbrica utilizando un adaptador PCMCIA(Personal Computer Memory Card International Association, Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales), miniPCI, adaptador PCI(Peripheral Component Interconnect, Interconexión de Componentes Periféricos), adaptador USB, ya sea según nuestras necesidades y las características de nuestro equipo.

Figura 1.1: Adaptador PCMCIA [33]

Figura 1.2: Adaptador PCI [33]

Figura 1.3: Adaptador USB [34]

Las redes inalámbricas las clasificaremos en 4 tipos que son:

1. Redes tipo Ad-hoc o punto a punto.
2. Redes personales.
3. Redes móviles privadas o de consumo.
4. IEEE 802.11(a, b, g).

1.2. Planteamiento del problema

Desde hace poco tiempo, se está viviendo lo que puede significar una revolución en el uso de las tecnologías de la información tal y como lo conocemos.

De una forma callada, las redes inalámbricas(WLAN), se están introduciendo en el mercado de consumo gracias a unos precios populares, las aplicaciones de las redes inalámbricas son infinitas. De momento van a crear una nueva forma de usar la información, la cual estará al alcance de todos en cualquier lugar (en el que haya cobertura).

Por ejemplo en las grandes ciudades por fin se podría llevar a cabo un control definitivo del tráfico con el fin de evitar atascos, limitando la velocidad máxima y/o indicando rutas alternativas en tiempo real, o por ejemplo en un supermercado todo lo que se venda se va descontando en tiempo real de una base de datos donde se encuentra el total de los productos y todo se registra en una terminal movíl y con esta se pueden checar productos en existencia o no, etc.

El centro comercial CECOSORI tutelar 136 cuenta con varias problematicas, una de ellas es la forma de imprimir documentos y las etiquetas de anaquel, otra de las problematicas es cuando se necesita mover equipos de un lugar a otro, ya que no se cuenta con suficientes rocetas, en linea de cajas perdida de tiempo en cobro cuando son productos con volumen, y mejoramiento de equipo inalámbrico.

La principal ventaja de una red wireless frente a una de cables es la movilidad. En la actualidad, muchos usuarios y empleados de empresas requieren para sus tareas acceder en forma remota a sus archivos, trabajos y recursos. Las redes inalámbricas wireless permiten hacerlo evitando que el usuario viaje hasta su empresa o alguna máquina u oficina en especial o su casa para poder acceder a los recursos de su red de datos. Aparte de que son más simples y menos complejas en su administración.

1.3. Objetivos generales

Los objetivos generales de este trabajo son:

- Conocer los aspectos generales sobre los sistemas WLAN.
- Conocer a fondo las tegnologías de las redes inalámbricas.
- Conocer la arquitectura de los sistemas WLAN.
- Realizar un estudio del funcionamiento de la red de datos estructura del centro comercial (CECOSORI).
- Aplicar los conocimientos aprendidos para realizar todo inalámbricamente en la red de datos estructurada del centro comercial (CECOSORI) ya sea cobro, servicio al cliente, pedidos, caja general, operación del sistema etc.

1.4. Justificación

El hecho que una red no posea cables tiene muchas ventajas, nos permite adaptarlas a cualquier estructura y prescíndir de la instalación de pisos técnicos y de cables molestos que crucen oficinas, habitaciones, paredes, entre otros elementos.

Algunas de las ventajas son:

Movilidad: Permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Lo cual supone mayor productividad y posibilidades de servicio.

Facilidad de instalación: Al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la comodidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios de la red.

Flexibilidad: Puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso por ej. parques naturales, reservas o zonas escarpadas.

Escalabilidad: El cambio de topología de red es sencillo y trata igual pequeñas y grandes redes.

Todo esto conlleva a algo que le interesa mucho a una empresa: reducción de costos.

Realizaremos el estudio de la red de datos estructurada del supermercado CECOSORI, analizaremos su funcionamiento y la rediseñaremos su red inalámbrica, con esto mejoraremos costos de tienda, y mayor facilidad de administración.

1.5. Solución del problema

Se propone instalar cuatro access point Cisco 1200 series Aironet, y a cada máquina que estará en la red se le colocará una tarjeta de red Cisco Aironet 350 series, las antenas se colocaron estrategicamente para que todo el espacio quede con señal. Con esto se tendrá señal en todo el espacio de la tienda y las máquinas tendrán conectividad, y el equipo inalámbrico tendría conexión

Se recomienda cambiar la tecnología movíl por una más reciente(Intermec) y adquirir lectores de barras inalámbricos para la linea de cajas e impresoras portátiles para los departamentos correspondientes, para la impresión de etiquetas de anaquel, compares, ambos de la misma marca antes mencionada

Para la impresión de documentos se recomienda colocar impresoras Lexmark con un servidor de impresión, en puntos estrategicos, como informes, mesa de control, gerencia, y caja general.

1.6. Estado del arte

La tecnología de redes inalámbricas se conoce mejor como WLAN en realidad se trata de tecnología de radio. Por lo tanto la historia de Wi-Fi u 802.11 existe apartir de la década de los ochenta, pero en realidad la tecnología empezó 100 años atrás. A continuación hablaremos un poco de esto.

La radio fué el fundamento de la LAN inalámbrica, los primeros trabajos en electromagnética, representan los fundamentos de la radio. El teórico escocés James Clerk Maxwell impulsó por primera vez, la noción de las ondas electromagnéticas en 1864, con esto desarrollando un proceso que se llama oscilación.

Basándose en ello el alemán Heinrich Hertz desarrolló un equipo en el año 1880, en el que envía y recibió ondas electromagnéticas a través del aire, este equipo era capaz de incrementar el número de ondas que se producían en un periodo determinado, su frecuencia y su velocidad de oscilación, esto se convirtió en una unidad de medida para las frecuencias, donde 1 hertz(Hz) significa una oscilación o un ciclo completo por segundo. Las medidas más comunes es el kilohertz que representa miles de ondas por segundo, megahertz, gigahertz.

Fue Guglielmo Marconi quien tomó estos primeros trabajos para llevarlos a una aplicación práctica, la transmisión de sonido fue la primera aplicación de las comunicaciones de datos. En la década siguiente al trabajo de Hertz, Marconi conjuntó sus descubrimientos con los de Samuel Morse.

Marconi pensó que si era posible transmitir señales binarias (puntos y guiones)a través de un cable, también debería ser posible enviar este tipo de señales a través de una onda electromagnética y usarlas como medio de comunicación, fué en 1895 cuando Marconi envío y recibió sus primeras transmisiones de radio, al año siguiente logró realizar transmisiones de aproximadamente una milla. A medida que mejoró sus transmisiones y antenas, las distancias se incrementaron rápidamente y con esto nació la radio, 1896 obtuvo su primera patente y en 1896 formó en Inglaterra una compañia llamada "Wireless Telegraph and Signal Company". Enquad 1898 el equipo telegráfico inalámbrico de Marconi se usaba para las comunicaciones entre los barcos y tierra firme.

Thomas Edison fue el que impulsó los sistemas inalámbricos que se desplegaron comercialmente en Estados Unidos, lo que dio como resultado la fundación General Electric, el trabajo de Edison se basó en el de Marconi y en el de uno de los empleados que colaboró con él, Nicola Tesla, estos científicos fuerón los creadores de la radio, y los que mejoraron estas ideas y con ellas se marco el comienzo de la era dorada de la radio, fueron David Sarnoff, Alexander Popov, Lee DeForest.

Para transmitir una señal de radio se hace a través del espectro de frecuencias y en el año de 1985, la FCC(Comisión Federal de Co Comunicaciones) por primera vez asignó porciones del espectro de frecuencia de radio que las entidades "industriales, científicas, médicas"(ISM) podrían usar sin necesidad de una licencia.

La operación de estas bandas ISM estaba y sigue vigente hasta hoy en día protegida bajo las reglas de la FCC.

Los sistemas inalámbricos de adquisición de datos fueron los precursores de la LAN inalámbrica, y comenzaron a aparecer en 1985. La venta de productos, el entorno de puntos de ventas, almacenamiento compartido, centros de distribución, existe la necesidad de que un agente de ventas o gerente de inventario, recorra libremente las instalaciones llevendo con sigo una terminal para adquirir datos, por ejemplo, un escáner de código de barras, y con esto ir recolectando datos que estén en continuo contacto en tiempo real con el sistema de inventarios, la comunicación a través de las ondas de radio representa la forma natural para lograr esto.

ALOHANET, un sistema inalámbrico que conectaba a las islas hawaianas fue el primer sistema creado para enviar paquetes de datos a través de radios, y no sólo es el precursor de las LAN inalámbricas, sino que también representa la base de la tecnología de área local cableada predominante: Ethernet.

En 1988 se realizaron mejoras adicionales a estos sistemas, al integrar el radio en la terminal de adquisición de datos, el sistema del usuario paso de ser de una unidad de tres piezas a una de dos.

En 1986 un año después de que se había regularizado la FCC, que permitieron el uso de radios, se abrió el espacio para comercializar esta tecnología. En Toronto se creó una compañía llamada Telesystem SLW, para exportar este desarrollo.

Los primeros productos de Telesystems fueron diseñados como reemplazos del cableado, ya sea para conectar múltiples computadoras de escritorio con una estación base central de manera muy parecida en la que funcionaría en una red Ethernet, o para conectar las redes en edificios separados. Otra empresa llamada Telxon comenzó a ofrecer los radios sin licencia de Telesystems en sus terminales de adquisición de datos, como una alternativa para los radios de banda angosta, esto ocasionó que los clientes se dieran cuenta de las ventajas de la nueva oferta libre de licencias.

La operación de la banda de 2.4 Ghz (banda libre) tuvo ventajas importantes respecto a la banda de 900 hz, al operar en una banda abierta, un fabricante puede construir un solo radio que mediante unos cambios puede venderse en todo el mundo.

Al notar el beneficio mutuo de definir estándares de la industria para las LAN inalámbricas, en 1991 varios fabricantes como Telxon, NCR, Proxim Technology y Symbol, emitieron una solicitud al IEEE, a fin de establecer un estándar interoperable para las LAN inalámbricas, en 1993 los fundamentos para un estándar estaban establecidos, y en 1997 el estándar 802.11 del IEEE fue ratificado, este estándar

marcó el comienzo de una nueva era y estableció los fundamentos para el siguiente estándar 802.11b que fue ratificado en 1999.

1.7. Estructura de la tesis

La organización de la tesis se presenta de la siguiente forma:

En el capítulo 2 se muestra la clasificación redes inalámbricas y sus antecedentes.

En el capítulo 3 explicamos los estádares de la IEEE 802.11 así como las tegnologías de las redes inalámbricas, antenas, puntos de acceso, barricales y switch.

En el capítulo 4 se muestran los protocolos de seguridad como WP, WPA2, WEB, encriptación.

En el capítulo 5 se muestra el funcionamiento de la red de datos estructurada del centro comercial (CECOSO) y rediseñaremos la red utilizando tecnología inalámbrica.

Capítulo 2

Clasificación del las redes inalámbricas

2.1. Introducción

En este capítulo se describe la clasificación de las redes inalámbricas. Así como también sus antecedentes, conceptos, aplicaciones, ventajas y desventajas de las distintas clasificaciones. Antes que nada se menciona lo que es una red, una red es un conjunto de computadoras interconectadas entre si, ya sea por medio de cables u ondas de radio(wireless). El primer propósito de una red consiste en que todas las computadoras que conforman parte de ella se encuentren en condiciones de compartir su información y sus recursos con los demás.

Con lo antes mencionado ahora se define lo que es una red inalámbrica.

Es la red inalámbrica una red que carece de cables, y se conecta por ondas de radio. Las redes WLAN son una ampliación de las redes LAN (redes de areá local). La mayoría de las grandes organizaciones tienen muchas LAN conectadas mediante redes tipo BN(redes troncales).

Estas LAN proporcionan acceso a una variedad de servidores, computadoras e internet. Las LAN trabajan con 3 tecnologías que son las LAN Ethernet tradicional (IEEE 802.3), LAN Ethernet conmutada y la Ethernet inalámbrica (IEEE 802.11), hay otras tecnologías como la token ring y arcnet, pero el mundo a cambiado y actualmente domina la Ethernet.[1]

Desde hace poco tiempo, se esta viviendo una revolución en el uso de las tecnologías de la información actual. Hoy en día es clara la alta dependencia de las actividades empresariales e institucionales de las redes de comunicación, la posibilidad de compartir información sin que sea necesario utilizar una conexión física permite mayor movilidad y comodidad.

De una forma callada las **redes inalámbricas o Wireless Networks** se estan introduciendo en el mercado gracias a precios populares y a los fabricantes que son mayoritariamente particulares y que han visto las enormes posibilidades de esta tecnología.

La diferencia fundamental entre las redes inalámbricas y las redes alambricas es el modo de transmisión, la primera transmite sus datos por radiofrecuencias y la segunda por medio de cables ya sea fibra óptica, par trenzado, coaxial.

Las WLAN es un sistema de comunicación de datos flexible muy utilizado como alternativa a las redes LAN cableada o como extención de esta. Utiliza tecnología de radio frecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas.[1]

Las WLAN van adquiriendo importancia en muchos campos como en la industria, gobierno, manufactura, centros comerciales, almacenes, en los que se transmiten la información en tiempo real a una terminal central. Cada día se reconocen este tipo de redes en un amplio número de negocios y se augura una gran extensión de las mismas y altas ganancias.

Con las WLANs la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores.

Pero no solamente encuentran aplicación en las empresas, sino que su extensión a ambientes públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios.

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

2.1.1. Antecedentes

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en los Proceeding del IEEE, puede considerarse como el punto de partida de esta tecnología.[4]

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del spread spectrum (espectro extendido), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la Agencia Federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical,esta es una banda para uso comercial sin licencia) 902-928 MHz, 2,400- 2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en spread spectrum.

La asignación de una banda de frecuencias propició una mayor actividad en la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.[4]

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

- Gran cantidad de técnicas, tecnologías y normas existentes en el ámbito de las comunicaciones móviles debido a que los diferentes fabricantes han ido desarrollando sus propias soluciones, utilizando frecuencias y tecnologías muy distintas y normalmente incompatibles. No existía una norma y menos un estándar.

- Altos precios que reflejan los costos de investigación para desarrollar soluciones tecnológicas propias.

- Reducidas prestaciones si las comparamos con las redes cableadas: las redes inalámbricas únicamente permiten el soporte de datos, mientras que por una red de cableado podemos llevar multitud de aplicaciones tanto de voz, como de datos, vídeo, etc. y además, velocidades de transmisión significativamente menores.

Sin embargo, se viene produciendo estos últimos años un crecimiento explosivo en este mercado debido a distintas razones:

- El desarrollo del mercado de los laptops y los PDA (Personal Digital Assistant), y en general de sistemas y equipos de informática portátiles hacen posible que sus usuarios puedan estar en continuo movimiento, al mismo tiempo que están en contacto con los servidores y con los otros ordenadores de la red, es decir, la WLAN permite movilidad y acceso simultáneo a la red.

- La conclusión de la norma IEEE 802.11(2) para redes locales inalámbricas, que introduce varios factores positivos.

- Finalmente, los grandes avances que se han logrado en tecnologías inalámbricas de interconexión y los que se tiene previsto alcanzar en proyectos. En este aspecto cabe destacar las mejoras de prestaciones propuestas por IEEE 802.11 en cuanto a velocidad, mejoras incrementales.

2.1.2. Normalización

En 1990, en el IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN. Pero no es hasta 1994 cuando aparece el primer borrador, y en junio de 1997 que se da por finalizada la norma. En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Personal Communications Systems).En ese mismo año, la ETSI (European Telecommunications Standards Institute), a través del comité ETSI-RES 10, inicia actuaciones para crear una norma a la que denomina HiperLAN (High Performance LAN) para, en 1993, asignar las bandas de 5,2 y 17,1 GHz.

En 1993 también se constituye la IRDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos. En 1996, finalmente, un grupo de empresas del sector de informática móvil y de servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de productos y servicios interoperativos.
Entre los miembros fundadores de WLI Forum se encuentran empresas como ALPS Electronic, AMP, Data General, Contron, Seiko, Epson y Zenith Data Systems.[4]

En un futuro no lejano, el previsible aumento del ancho de banda asociado a las redes inalámbricas y consecuentemente, la posibilidad del multimedia móvil, permitirá atraer a mercados de carácter horizontal que surgirán en nuevos sectores, al mismo tiempo que se reforzarán los mercados verticales ya existentes.[2]

2.1.3. Decidiendo por una WLAN

En nuestro medio nos hemos visto atacados por diversas opciones, unas muy complicadas, otras muy caras, otras difíciles de instalar u otras que simplemente no funcionan.

Expondremos una solución muy sencilla y muy eficiente y al alcance de todas las empresas. En la búsqueda de la solución ideal nos hemos topado con DLINK, una empresa que ofrece soluciones de redes a todo nivel con soporte local. Es una empresa Taiwanesa con 16 años de experiencia internacional en redes físicas e inalámbricas. Cuando hablamos de WLAN tendremos unas grandes de posibilidades por tener a alguien que nos respalde y podamos consultar se vuelve muy importante para la funcionalidad de nuestra red.

Hay una tendencia mundial en las redes inalámbricas las podemos encontrar en aeropuertos, campus universitarios, cafés y en ciudades que se están difundiendo rápidamente por lo que no es de extrañarse que las empresas vean en las WLANs solución a sus necesidades de comunicación. Si tenemos los productos adecuados, crear una red inalámbrica no es nada complicado y si tenemos el soporte correcto aún menos. En una red típica basta con tener las tarjetas inalámbricas para las computadoras, ya sea USB, PCI o PCMCIA; los puntos de acceso(access points); y verificar que no hayan obstáculos muy grandes para logar la transmisión. Lo más interesante es que las WLAN siguen evolucionando y actualmente llegan a velocidades de 108 Mbps en el estándar 802.11g como en los productos AirPlus XtremeG de DLINK.[13]

2.2. Clasificación de las redes inalámbricas

Vamos a clasificar las redes inalámbricas en:

1. Redes punto a punto o ad-hoc.
2. Redes personales.
3. Redes móviles privadas o de consumo.
4. Redes inalámbricas IEEE 802.11(a,b,g).

2.3. Redes punto a punto o ad-hoc

Esta configuración es la más básica es la llamada de igual a igual o ad-hoc y consiste en una red de dos o más terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas. Para que la comunicación entre estas estaciones sea posible hace falta que se vean mutuamente de manera directa, es decir, que cada una de ellas esté en el rango de cobertura radioeléctrica de la otra. Las redes de tipo ad-hoc son muy sencillas de implementar y no requieren ningún tipo de gestión administrativa.[12,22]

En una red inalámbrica ad-hoc todos los nodos cooperan dinámicamente para establecer y mantener el ruteo en la red ayudando a enviar paquetes hacia otros nodos. El protocolo de ruteo es una parte muy importante en el funcionamiento de una red ad-hoc. Uno de los principales protocolos de ruteo para este tipo de redes es el Dynamic Source Routing(DSR). Su principal caracteristica es el uso de ruteo fuente. El DSR esta compuesto por dos mecanismos:descubrimiento de ruta y mantenimiento de ruta.En respuesta a un descubrimiento de ruta o a través de información de ruteo un nodo aprende y almacena multiples rutas en su cache. Una red ad-hoc es una colección de nodos móviles inalámbricos formando una red temporal sin ayuda de ninguna administración o algún soporte de servicios.[5]

Las figuras 2.1, 2.2 muestran un ejemplo de una red ad-hoc sencilla de tres nodos móviles y dos, usando interfaces de redes inalámbricas. En esta red el nodo C no esta dentro del rango de transmisión del nodo A y viceversa, si A y C desean intercambiar paquetes entre ellos necesitaran los servicios del nodo B que se encuentra en el rango de transmisión de ambos.

El problema de ruteo de una red ad-hoc real es más complicado de lo que se muestra en este ejemplo, debido a las caracteristicas de propagación inherentes no uniformes de las transmisiones inalámbricas y a la posibilidad de que cualquier nodo en la red pueda moverse en cualquier momento.

Los nodos en la red ad-hoc son móviles y pueden correr con una baja cantidad de energia haciendo que sus radios de transmisión sean pequeños. La operación intermitente de algunos nodos y la movilidad requieren intercambiar reconfiguraciones de rutas y por lo tanto, intercambios frecuentes de información de control lo que aumenta la posibilidad de perdida de paquetes y el retardo en la entrega de los mismos.Estas características hacen que el protocolo de ruteo implementado afecte directamente el funcionamiento y el rendimiento de una red inalámbrica ad-hoc.

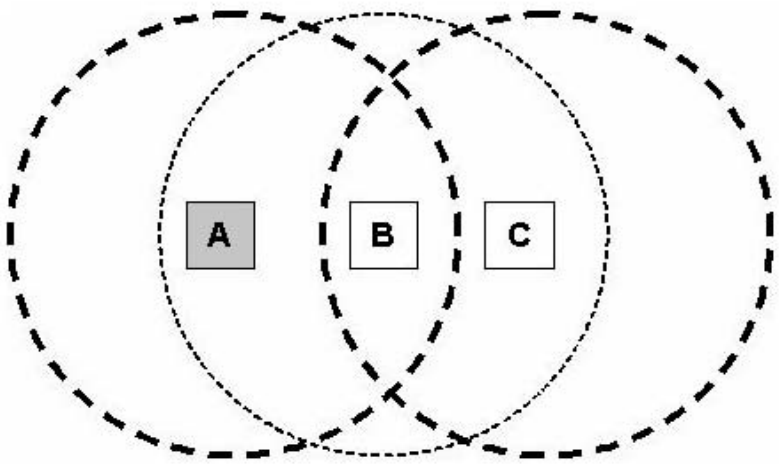

Figura 2.1: Red inalámbrica ad-hoc de tres nodos[5].

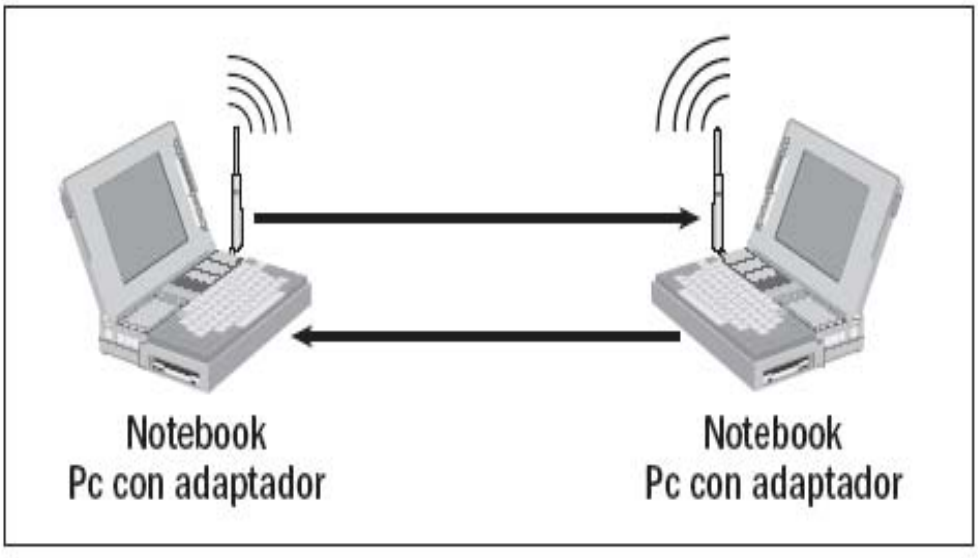

Figura 2.2: Red inalámbrica ad-hoc de dos nodos[5].

2.3.1. Protocolos de ruteo

Existen dos protocolos de ruteo, los convencionales y los basados en el mecanismo sobre demanda. Un método natural para proveer ruteo en una red ad-hoc, es simplemente tratar a cada nodo movíl como un ruteador y correr los protocolos de ruteo convencionales entre ellos. Por otra parte, algunos protocolos sobre demanda han sido desarrollados especificamente para redes inalámbricas ad-hoc.

El Dynamic Source Routing(DSR), su principal característica es el uso de ruteo fuente, que consiste en conocer la ruta completa nodo por nodo hacia el destino, llevan los paquetes en su cabecera. En el DSR para enviar un paquete de un nodo a otro,el nodo emisor construye una ruta fuente que colocará en la cabecera del paquete dándole la dirección de cada uno de los nodos de la red, a través de los cuales el paquete será enviado a fin de llegar al nodo destino. El nodo emisor transmite el paquete sobre su interfaz de red inalámbrica, para realizar el primer brinco (hop) indicado en la ruta fuente. Cuando un nodo recibe un paquete, si este nodo no es el destino final del paquete, simplemente transmite el paquete al siguiente nodo que se indica en la ruta fuente. Una vez que el paquete llega a su destino final el paquete es entregado a la capa de software de la red.[5]

Cada nodo movíl que participa en la red ad-hoc, mantiene un almacen de rutas (cache), en el cual se guardan las rutas que se han aprendido.Las formas en las que un nodo puede aprender una ruta son:

- En respuesta al descubrimiento de ruta un nodo aprenderá y almacenará multiples rutas a cualquier destino.
- Los nodos aprenden también de la información de ruteo de cualquier paquete que ellos envían o que ellos pueden escuchar al trabajar con su interfaz de red en nodo promiscuo(pueden escuchar cualquier paquete entre su rango de transmisión).

El protocolo DSR esta compuesto por dos mecanismos: Descubrimiento de ruta y mantenimiento de ruta, los cuales operan sobre demanda. Cuando un nodo envía un paquete a otro nodo, el nodo emisor primero revisa en su cache para verificar si existe una ruta fuente que lo comunique con el nodo destino. Si encuentra la ruta fuente el nodo emisor usará esta ruta para enviar el paquete.Si no la encuentra, el nodo emisor tratará de encontrar una usando el protocolo de descubrimiento de ruta. Mientras esta esperando que se complete el descubrimiento de ruta, el nodo continúa su proceso normal envía y recibe paquetes con otros nodos.

El monitoreo de la operación correcta de una ruta en uso se llama mantenimiento de ruta.Cuando el mantenimiento de ruta detecta un problema con una ruta en uso, el descubrimiento de ruta entra en acción para descubrir una nueva y correcta ruta, que establezca la comunicación con el nodo destino.

2.4. Redes personales

Dentro del ámbito de estas redes podemos integrar a dos principales tipos:

a- En primer lugar están las redes que se usan actualmente mediante el intercambio de información utilizando infrarrojos. Estas redes son muy limitadas dado su corto alcance, necesidad de "visión sin obstáculos"entre los dispositivos que se comunican y su baja velocidad (hasta 115 kbps). Se encuentran principalmente en ordenadores portátiles, PDAs (Agendas electrónicas personales), teléfonos móviles y algunas impresoras.

b- En segundo lugar el Bluetooth, estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles de nueva generación y algún que otro ordenador portátil.Su principal desventaja es que su puesta en marcha se ha ido retrasando desde hace años y la aparición del mismo ha ido plagada de diferencias e incompatibilidades entre los dispositivos de comunicación de los distintos fabricantes que ha imposibilitado su rápida adopción. Opera dentro de la banda de los 2.4 Ghz.

2.4.1. Redes con infrarojo

Los enlaces infrarrojos se encuentran limitados por el espacio y los obstáculos. El hecho de que la longitud de onda de los rayos infrarrojos sea tan pequeña (850-900 nm), hace que no pueda propagarse de la misma forma en que lo hacen las señales de radio.

Es por este motivo que las redes infrarrojas suelen estar dirigidas a oficinas o plantas de oficinas de reducido tamaño o estaciones que se encuentran en un solo cuarto o piso. Algunas compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores/emisores en las ventanas de los edificios.Las transmisiones de radio frecuencia tienen una desventaja: que los países están tratando de ponerse de acuerdo en cuanto a las bandas que cada uno puede utilizar, al momento de realizar este trabajo ya se han reunido varios países para tratar de organizarse en cuanto a que frecuencias pueden utilizar cada uno.[12,22]

La transmisión infrarroja no tiene este inconveniente por lo tanto es actualmente una alternativa para las redes inalámbricas.El principio de la comunicación de datos es una tecnología que se ha estudiado desde los 70ťs, Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar.

El mismo principio se usa para la comunicación de redes, se utiliza un "transreceptor"que envía un haz de luz infrarroja, hacia otro que la recibe.La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente.

IrDA. Organización internacional no lucrativa que tiene como objetivo la creación y promoción de estándares de interconexión mediante infrarrojos interoperativos, de bajo costo y que soporten modelos punto a punto de corto alcance.Constituida en 1993 y con sede en Walnut Creek (California), IrDA representa el punto de referencia en comunicaciones ópticas por infrarrojos inalámbricas.En la actualidad cuenta con más de 160 miembros que pertenecen a la industria de comunicaciones, componentes, ordenadores y periféricos, cable y telefonía, software, hardware y proveedores de servicios.

2.4.1.1 Modos de radiación infrarojos

A la hora de transmitir, las estaciones infrarrojas pueden usar tres tipos de métodos para ello: punto a punto, cuasi-difuso y difuso.

En el modo punto a punto (fig 2.3) los patrones de radiación del emisor y del receptor deben de estar lo más cerca posible, para que su alineación sea correcta. Como resultado, el modo punto-a-punto requiere una línea de vista entre las dos estaciones a comunicarse.

En el modo cuasi-difuso (fig. 2.4) el tipo de emisión es radial; esto es, la emisión se produce en todas direcciones, al contrario que en el modo punto a punto. Para conseguir esto, lo que se hace es transmitir hacia distintas superficies reflectantes, las cuales redirigirán el haz de luz hacia la/s estación/es receptora/s. De esta forma, se rompe la limitación impuesta en el modo punto a punto de la direccionalidad del enlace. En función de cómo sea esta superficie reflectante, podemos distinguir dos tipos de reflexión: pasiva y activa. En la reflexión pasiva, la superficie reflectante simplemente refleja la señal, debido a las cualidades reflexivas del material. En la reflexión activa, por el contrario, el medio reflectante

no sólo refleja la señal, sino que además la amplifica. En este caso, el medio reflectante se conoce como satélite. Destacar que, mientras la reflexión pasiva es más flexible y barata, requiere de una mayor potencia de emisión por parte de las estaciones, debido al hecho de no contar con etapa repetidora.

El modo de emisión difuso (fig. 2.5) se diferencia del cuasi-difuso en que debe ser capaz de abarcar, mediante múltiples reflexiones, todo el recinto en el cual se encuentran las estaciones. Obviamente, esto requiere una potencia de emisión mayor que los dos modos anteriores, puesto que el número de rebotes incide directamente en el camino recorrido por la señal y las pérdidas aumentan.

Según el caso que comentábamos antes de las empresas que utilizaban enlaces de un edificio a otro mediante antenas en las ventanas, podemos observar que, obviamente, este enlace será punto a punto, mientras que en las redes interiores lo más lógico es realizar enlaces difusos.

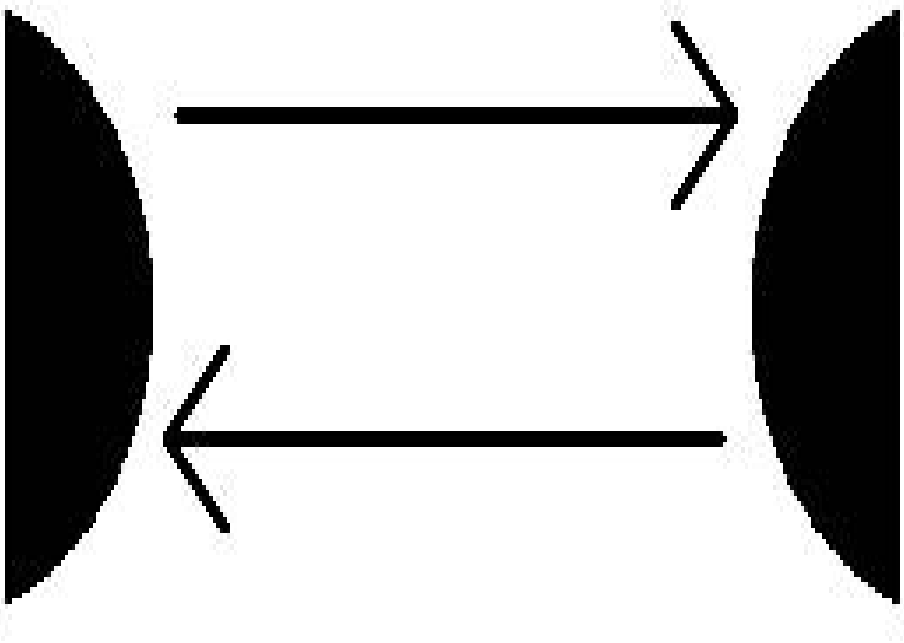

Figura 2.3: Punto a punto.

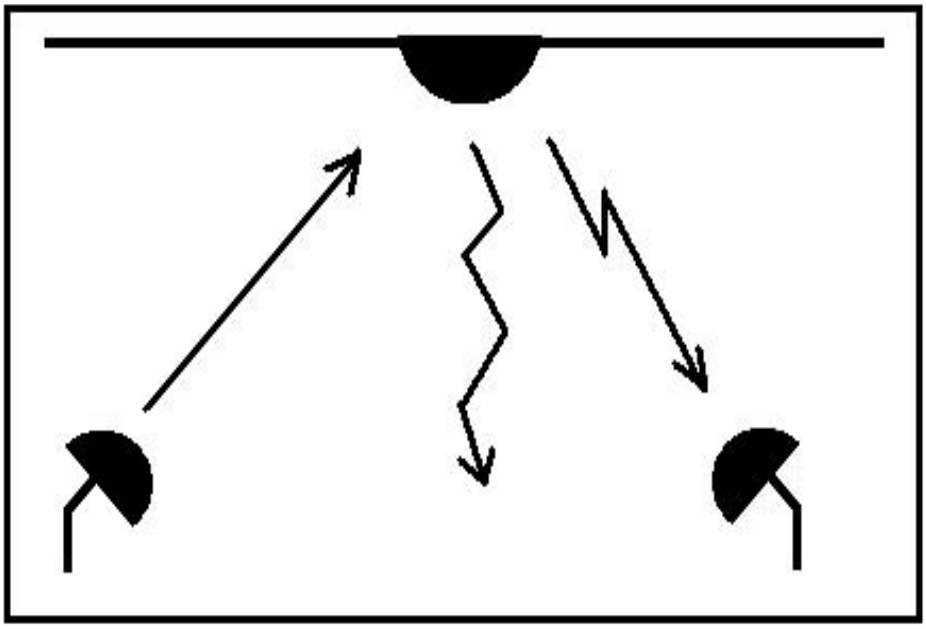

Figura 2.4: Cuasi-difuso.

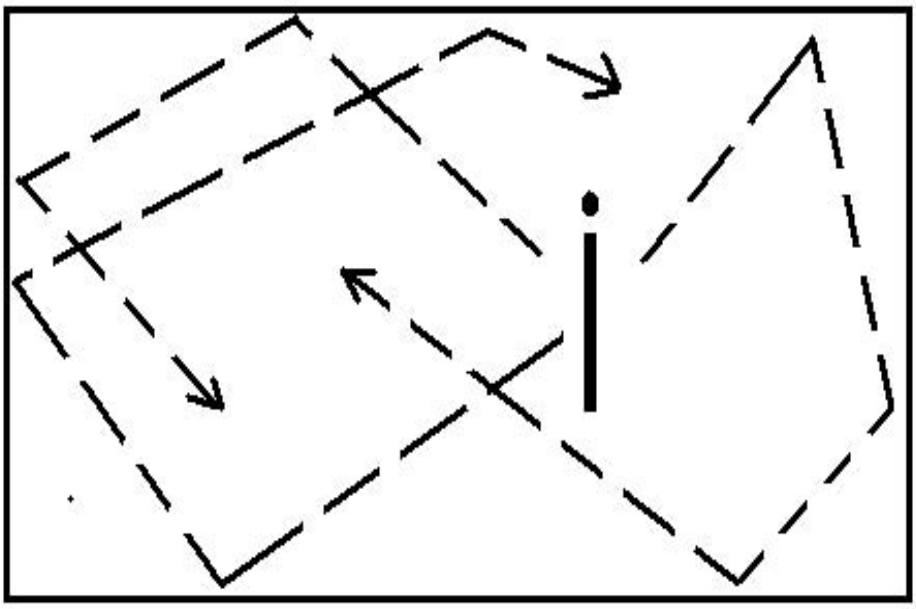

Figura 2.5: Difuso.

2.4.1.2 Tecnología de infrarrojos

La norma IEEE 802.11 no ha desarrollado todavía en profundidad esta área y solo menciona las características principales de la misma, a saber:[4]

- Transmisión infrarroja difusa.
- El receptor y el transmisor no tienen que ser dirigidos uno contra el otro y no necesitan una línea de vista (line-of-sight) limpia.
- Rango de unos 10 metros.
- Solo en edificios.
- 1 y 2 Mbps de transmisión.
- 850 a 950 nanometros de rango. (Frente al 850 a 900 nm que establece el IrDA).

2.4.1.3 Clasificación

De acuerdo al ángulo de apertura con que se emite la información en el transmisor, los sistemas infrarrojo pueden clasificarse en sistemas de corta apertura, también llamados de rayo dirigido y en sistemas de gran apertura, reflejados o difusos (diffused), recogidos por la norma 802.11.

- **Los sistemas infrarrojo de corta apertura**, están constituidos por un cono de haz infrarrojo altamente direccional y funcionan de manera similar a los controles remotos de los televisores y otros equipos de consumo.

  El emisor debe orientarse hacia el receptor antes de transferir información, lo que limita un tanto su funcionalidad. Por ejemplo, resulta muy complicado utilizar esta tecnología en dispositivos móviles, pues el emisor debe reorientarse constantemente.

  Resumiendo, este mecanismo solo es operativo en enlaces punto a punto exclusivamente. Por ello se considera que es un sistema inalámbrico pero no móvil, o sea que esta más orientado a la portabilidad que a la movilidad.

- **Los sistemas de gran apertura** permiten la información en ángulo mucho más amplio por lo que el transmisor no tiene que estar alineado con el receptor. Una topología muy común para redes locales inalámbricas basadas en esta tecnología, consiste en colocar en el techo de la oficina un nodo central llamado punto de acceso, hacia el cual dirigen los dispositivos inalámbricos su información, y desde el cual ésta es difundida hacia esos mismos dispositivos.

Desgraciadamente la dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor, que limita la velocidad de transmisión (la trayectoria reflejada llega con un retraso al receptor).

Esta es una de las dificultades que han retrasado el desarrollo de el sistema infrarrojo en la norma 802.11. La tecnología infrarroja cuenta con muchas características para utilizarse en WLANs: el infrarrojo ofrece una amplio ancho de banda que transmite señales a velocidades muy altas(alcanza los 10 Mbps); tiene una longitud de onda cercana a la de la luz y se comporta como ésta(no puede atravesar objetos sólidos como paredes, por lo que es inherentemente seguro contra receptores no deseados); debido a su alta frecuencia, presenta una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por dispositivos hechos por el hombre(motores, luces ambientales, etc.).

La transmisión infrarrojo con láser o con diodos no requiere autorización especial en ningún país(excepto por los organismos de salud que limitan la potencia de la señal transmitida); utiliza un protocolo simple y componentes sumamente económicos y de bajo consumo de potencia, una característica importante en dispositivos móviles portátiles (laptops, pdas).

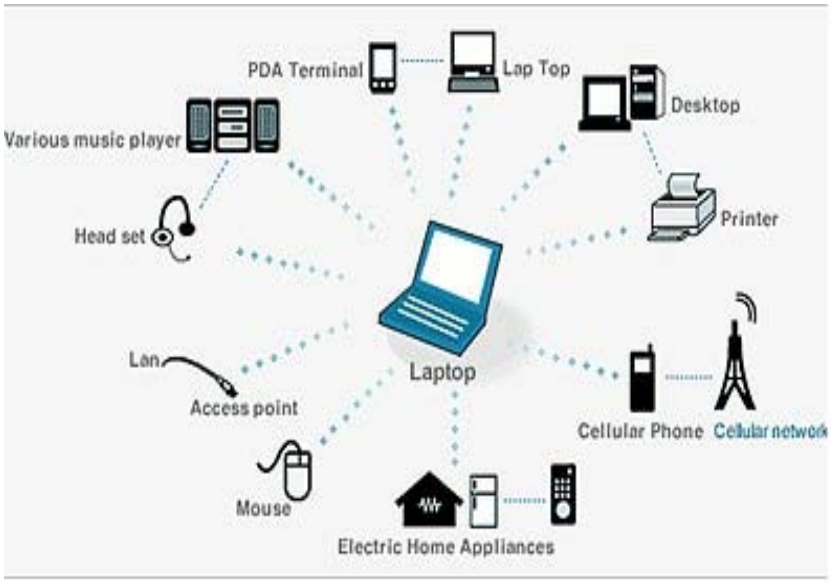

Figura 2.6: Conexiones actualmente usando tecnología de infrarrojos[35]

2.4.2. Redes con bluetooth

Las comunicaciones inalámbricas están presentes en muchas de nuestras actividades diarias y su uso ha llegado a ser tan común, que perdemos la percepción de lo útil y a veces indispensable que pueden llegar a ser. Las redes celulares para transmitir voz y datos han surgido para proveer la movilidad y disponibilidad de la comunicación. La utilización de sensores infrarrojos y de radiofrecuencia proveen la comodidad de controlar y operar a distancia aparatos electrónicos volviendo más sencillo nuestro quehacer diario.

Asimismo, la creación de estándares de comunicaciones inalámbricas en las redes de transmisión de datos ha abierto oportunidades de desarrollo de estas tecnologías, aprovechando la utilización de interfaces aéreas operadas bajo frecuencias no licenciadas. Bluetooth forma parte de las tecnologías creadas para proveer comunicación inalámbrica en áreas de uso personal. Sin embargo, su uso va más allá de la eliminación de cables, ya que es lo suficientemente flexible para permitir la creación de aplicaciones que abren un mundo con límite en la imaginación[14,24].

Bluetooth es una tecnología desarrollada por Ericsson en 1994, que hace factible la conectividad inalámbrica entre dispositivos a corta distancia, éstos pueden llegar a formar redes con diversos equipos de comunicación: computadoras móviles, radiolocalizadores, teléfonos celulares, PDAs, e inclusive, electrodomésticos. Lo que se busca con bluetooth es facilitar la sincronización de datos de computadoras móviles, teléfonos celulares y manejadores de dispositivos.

La tecnología bluetooth es de pequeña escala, bajo costo y se caracteriza por usar enlaces de radio de corto alcance entre móviles y otros dispositivos, como teléfonos celulares, puntos de accesos de red (access points) y computadoras. Esta tecnología opera en la banda de 2.4 GHz. Tiene la capacidad de atravesar paredes, por lo cual es ideal tanto para el trabajo móvil, como el trabajo en oficinas(fig 2.7).

2.4.2.1 Origenes

La versión 1.0 de la especificación bluetooth fue publicada en 1999, pero el desarrollo de esta tecnología empezó realmente 5 años atrás, en 1994, cuando la compañía Ericsson empezó a estudiar alternativas para comunicar los teléfonos celulares con otros dispositivos.

En 1994, la compañía de telecomunicaciones ERICSSON, comenzó un estudio para investigar la viabilidad de una interfaz de radio de baja potencia y bajo

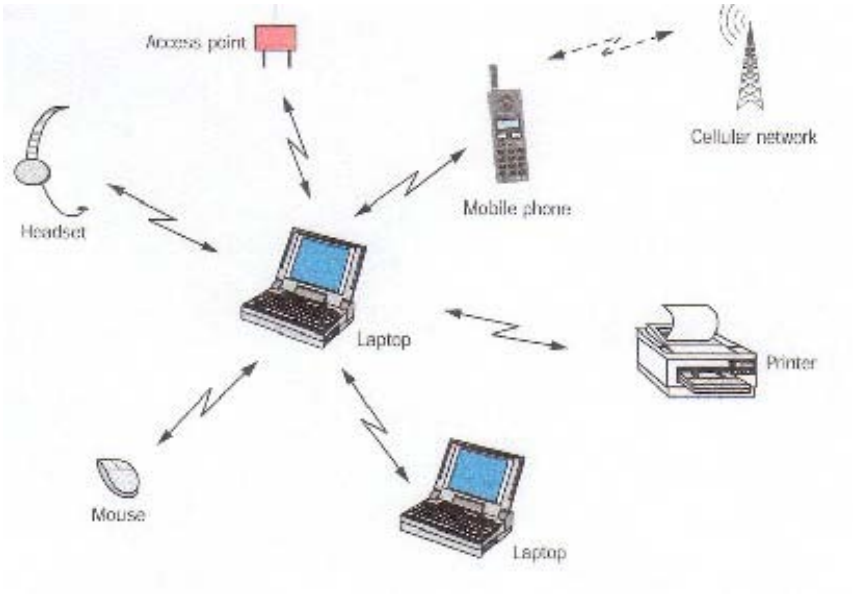

Figura 2.7: Conexiones actuales con bluetooth[35].

costo entre teléfonos móviles y sus accesorios. El objetivo era eliminar los cables entre los teléfonos móviles y tarjetas de PCs, dispositivos desktop, etc.[11,17]

El estudio fue parte de otro gran proyecto de investigación que involucraba multicomunicadores conectados a la red celular por medio de los teléfonos celulares. El ultimo enlace en dicha conexión debería ser un radio enlace de corto rango.A medida que el proyecto progresaba, se volvió claro que las aplicaciones que envuelven dicho enlace de corto rango serían ilimitadas.

A comienzos de 1997, Ericsson se aproxima a otros fabricantes de dispositivos portátiles para incrementar el interés en esta tecnología. El motivo era simple: para que el sistema fuera exitoso y utilizable, una cantidad grande de dispositivos portátiles deberían utilizar la misma tecnología de radioenlaces de corto alcance. En Febrero de 1998, cinco compañías, Ericsson, Nokia, IBM, Toshiba e Intel, forman un Grupo de Interés Especial (SIG).Dicho grupo contiene la mezcla perfecta en lo que es el área de negocios, dos líderes del mercado en telefonía móvil, dos líderes del mercado en computadoras laptop y un líder del mercado en tecnología de procesamiento de señales digitales. La meta era establecer la creación de una especificación global para conectividad sin hilos de corto alcance.

La razón del nombre es que en el siglo X el rey Harald II de Dinamarca,apodado "diente azul"(bluetooth) a causa de una enfermedad que le daba esta coloración

a su dentadura, reunificó bajo su reinado numerosos pequeños reinos que existían en Dinamarca y Noruega y que funcionaban con reglas distintas, lo mismo que hace la tecnología bluetooth, promovida por Ericsson (Suecia) y Nokia (Finlandia), dos países escandinavos.El 20 y el 21 de mayo de 1998, el consorcio de bluetooth se anuncio al público general de Londres, Inglaterra, San José, California, y Tokio, Japón, lo que provoco la adopción de la tecnología por varias compañías. El propósito del consorcio era establecer un dispositivo estándar y un software que lo controle. Actualmente ya pertenecen mas de 1.600 empresas al el SIG (Special Interest Group), que han adoptado esta tecnología para desarrollarla con sus propios productos, que empezaron a salir al mercado a finales del año 2000. Cada nueva compañía miembro del SIG recibe de las otras una licencia para implantar la especificación 1.0.

2.4.2.2 Como Funciona

Cada dispositivo deberá estar equipado con un microchip (tranceiver, fig 2.8) que transmite y recibe en la frecuencia de 2.4 GHz que esta disponible en todo el mundo (con algunas variaciones de ancho de banda en diferentes países). Además de los datos, están disponibles tres canales de voz. Cada dispositivo tiene una dirección única de 48 bits basado en el estándar IEEE 802. Las conexiones son uno a uno con un rango máximo de 10m (dependiendo del medio podría ser más).

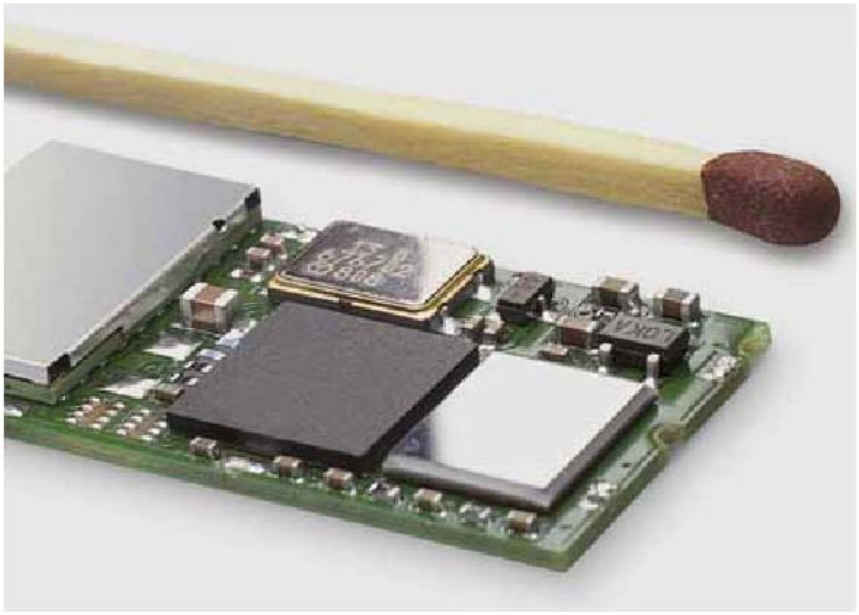

Figura 2.8: Microchip bluetooth[19]

Los datos se pueden intercambiar a velocidades de hasta 1 megabit por segundo(se esperan 2 megabits por segundo en la segunda generación de esta tecnología). Un esquema de "frequency hop"(saltos de frecuencia) permite a los dispositivos comunicarse inclusive en áreas donde existe una gran interferencia electromagnética.Además de que se provee de esquemas de encriptación y verificación.

Cada paquete de ambos dispositivos se sintonizan su radio transmisor a una frecuencia diferente, saltando de un canal a otro canal de radio; esta técnica se le conoce como espectro disperso con salto en frecuencia (FHSS, Frequency Hopping Spread Spectrum). De esta manera, los dispositivos Bluetooth utilizan toda la banda de 2.4 GHz y si una transmisión se interfiere sobre un canal, una retransmisión siempre ocurrirá sobre un canal diferente con la esperanza de que este canal esté libre. Cada ranura de tiempo tiene una duración de 625 microsegundos y generalmente los dispositivos saltan una vez por paquete, o sea, saltan cada ranura, cada 3 ranuras o cada 5 ranuras.

Como bluetooth fue diseñado para aplicaciones móviles de poca potencia, la potencia del radio transmisor debe ser minimizada.Tres diferentes clases de niveles de potencias están definidas, las cuales proveen rangos de operación de aproximadamente 10, 20 y 100 metros: El más bajo nivel de potencia cubre 10 metros, el más alto nivel logra cubrir distancias de hasta 100 metros.

Bluetooth soporta hasta 780 Kbps, los cuales pueden ser utilizados para transferir unidireccionalmente 721 Kbps y 57.6 Kbps en la dirección de retorno o hasta 432.6 Kbps de manera simétrica en ambas direcciones. Aunque estas velocidades están limitadas para cierto tipo de aplicaciones como video, aplicaciones como transferencia de archivos e impresión caen perfectas en tal ancho de banda.

2.4.2.3 Características

- **Tecnología inalámbrica.** Reemplaza la conexión alámbrica en distancias que no exceden los 10 metros, alcanzando velocidades del rango de 1Mbps.

- **Comunicación automática.** La estructura de los protocolos que lo forman favorece la comunicación automática sin necesidad de que el usuario la inicie.

- **Bajo consumo de potencia.** Lo pequeño de los dispositivos y su portabilidad requieren de un uso adecuado de la energía, el cual provee esta tecnología.

- **Bajo costo.** Los dispositivos de comunicación que soporta pueden experimentar un incremento en su costo no mayor a 20 dólares con tendencia a bajar.Asimismo, su operación se efectúa bajo una banda de frecuencias no licenciada (2.4GHZ), lo que ayuda a su bajo costo.

- **Integración de servicios.** Puede soportar transmisiones de voz y datos de manera simultánea.

- **Transmisión omnidireccional.** Debido a que basa su comunicación en radiofrecuencia, no requiere línea de vista y permite configuraciones punto-multipunto.

- **Seguridad.** Utiliza Spread Spectrum Frequency Hopping como técnica de multiplexaje, lo que disminuye el riesgo de que las comunicaciones sean interceptadas o presenten interferencia con otras aplicaciones. Provee también especificaciones para autenticar dispositivos que intenten conectarse a la red bluetooth, así como cifrado en el manejo de llaves para proteger la información.

- **Establecimiento de redes.** Tiene la característica de formar redes en una topología donde un dispositivo hace las veces de maestro y hasta siete más operando como esclavos. Esta configuración se conoce como piconet. Un grupo de piconets, no más de diez, es referido como Scatternet.

2.4.2.4 ¿Que es un piconet?

Bluetooth se ha diseñado para operar de manera multi-usuario. Los dispositivos pueden habilitarse para comunicarse entre sí e intercambiar datos. Hasta ocho usuarios o dispositivos pueden formar una piconet y hasta diez piconets pueden co-existir en la misma área de cobertura. Dado que cada enlace es codificado y protegido contra interferencia y pérdida de enlace, bluetooth es como una red inalámbrica de corto alcance muy segura.[17]

- Canales máximos de datos: 7 por piconet.
- Rango esperado del sistema: hasta 721 kbit/s por piconet.
- Número de dispositivos: 8 por piconet y hasta 10 piconets.
- Alimentación: 2,7 voltios.
- Consumo de potencia: desde 30 uA a 30 mA transmitiendo.

- Tamaño del Módulo: 0.5 pulgadas cuadradas (9x9 mm).
- Interferencia: bluetooth minimiza la interferencia potencial al emplear saltos rápidos en frecuencia 1600 veces por segundo.

En cuanto a interferencias con otros dispositivos, hay que tener cuidado con los que operan en la misma banda.Por ejemplo, lo mismo que está prohibido el uso de teléfonos móviles en los aviones, se puede prohibir el uso de cualquier otro dispositivo que incorpore un chip bluetooth, ya que podría interferir con los elemento de navegación, pero esto es más complicado puesto que ha sido diseñado para mantener una comunicación continua, incluso en movimiento, y dentro de maletines, no percibiéndose el usuario (por descuido) ni la tripulación de la nave, de que se está utilizando.

Las diferentes partes del sistema bluetooth son:

- Una unidad de radio.
- Una unidad de control del enlace.
- Gestión del enlace.
- Funciones software.

2.4.2.5 Bluetooth es adaptado por la IEEE

En marzo del 2002 la IEEE aprobó finalmente el estándar IEEE 802.15.1 compatible totalmente con la tecnología bluetooth v1.1. En este estándar se definen las especificaciones de la capa física y MAC (medium access control) para las redes WPANs.

El nuevo estándar permitirá una mayor validez y soporte en el mercado de las especificaciones de bluetooth, además es un recurso adicional para aquellos que implementen dispositivos basados en esta tecnología.

Anteriormente a la estandarización, dispositivos bluetooth no podían coexistir con los dispositivos basados en IEEE 802.11b debido a que ambos se interferían entre sí.

Otro esfuerzo importante para buscar la interoperatibilidad entre dos sistemas lo están haciendo la compañía Intersil Corp, fabricante de chips para el protocolo IEEE 802.11b (Wi-Fi) y la compañía Silicon Wave Inc.fabricante de sistemas de radio de bluetooth.Este esfuerzo entre Wi-Fi y bluetooth es conocido como blue802 y permitirá la operación simultánea de estos dos protocolos inalámbricos.

2.5. Redes móviles privadas o de consumo

También conocido como radiocomunicaciones en grupo cerrado de usuario, es un servicio de telefonía móvil que solo se presta a un grupo de personas, en una determinada zona geográfica, el funcionamiento es idéntico al de las redes publicas, con pequeñas diferencias, hay dos tipos de servicio.

En la primera cada grupo de usuarios y solo ellos, utiliza una determinada frecuencia. En la segunda el sistema se encarga de asignar las frecuencias libres entre los diferentes grupos, por lo que no hay una correspondencia grupofrecuencia.

Entre los primeros sistemas podemos destacar EDACS, controlado por un equipo fabricado por Ericsson, muy utilizado por bomberos, equipos de salvamento, policías, ambulancias.

Es un sistema muy seguro, capaza de establecer la comunicación en condiciones muy adversas.Los segundos se denominan sistemas Trunking, y su funcionamiento es muy parecido al de la telefonía móvil automática (TMA), uno de los primeros sistemas analógicos de telefonía móvil publica.[18]

La mayor diferencia es que cuando no hay un canal libre para establecer una comunicación, TMA descarta la llamada y el usuario debe reintentarlo después, mientras que las redes Trunking gestionan estas llamadas, estableciendo una cola de espera, dos de los sistemas Trunking más populares son Taunet, que es analógico, y Tetra, que es digital. Este ultimo es el resultado de un estándar europeo, y su equivalente estadounidense es el APCO25. Ofrecen otras posibilidades, aparte de la comunicación vocal, como envío de mensajes cortos, transmisión de datos, conexión a redes telefónicas públicas.

Sistema trunking EDACS:Este Sistema ocupa un lugar privilegiado dentro del mercado de las comunicaciones por su excelencia en prestación y confiabilidad.

Es un producto originalmente desarrollado por Ericsson cuyo protocolo es el denominado EDACS que significa Ehanced Digital Access Communications System. Es un Sistema de radio troncalizada de acceso digital que posee canal de control el cual administra todas las comunicaciones que se cursan en el sistema. Esta tecnología permite implementar sistemas con los requisitos más exigentes tales como comunicaciones analógicas, digitales, digitales encriptadas, claves de encriptación en las comunicaciones digitales y comunicación de datos.

También incorpora funciones avanzadas como ser reprogramación de terminales por aire, reagrupamiento dinámico por aire, transmisión de datos multisitio, llamadas de emergencia, prioridades en las comunicaciones, deshabilitar/habilitar por aire radios robadas, etc.

2.5.1. Redes GSM

Global System for Mobile communications (Sistema Global para las Comunicaciones Móviles), anteriormente conocida como "Group Special Mobile"(GSM, Grupo Especial Móvil) es un estándar mundial para teléfonos móviles digitales.El estándar fue creado por la CEPT y posteriormente desarrollado por ETSI como un estándar para los teléfonos móviles europeos, con la intención de desarrollar una norma que fuera adoptada mundialmente.Es el estándar predominante en europa, así como el mayoritario en el resto del mundo.[25]

GSM es un sistema de comunicación basado en el uso de células digitales que se desarrollo para crear un sistema para móviles único que sirviese de estándar para europa y que fuese compatible con los servicios existentes y futuros sobre ISDN (Integrated Services Digital Network) o RDSI (Red Digital de Servicios Integrados).

Las comunicaciones basadas en células aparece en los laboratorios Bell en los Estados Unidos allá por el año 1970 apareciendo los primeros sistemas comerciales a principios de los 80.La situación que se vivía en estos primeros años de la década de los 80 era curiosa ya que los sistemas existentes hasta ese momento eran sistemas analógicos, que habían tenido mucho éxito en los países nórdicos y en el Reino Unido sin embargo la nueva tecnología digital basada en células presentaba un panorama un tanto desolador ya que cada país había desarrollado su propio sistema lo que implicaba algunos problemas muy importantes; por un lado tenemos que la operatividad del terminal acababa donde acababa los límites de cada país y por otro lado el mercado para cada tipo de terminal era muy limitado y estaba restringido al país en donde el dispositivo fuese a ser utilizado.

Para solucionar estos problemas en el año 1982 el CEPT creo el denominado Groupe Spécial Mobile o GSM para desarrollar un sistema basado en células de radio y que sirviesen para todos los países europeos.En el año 1989 todas las responsabilidades que había tenido hasta ahora el CEPT se traspasan al European Telecommunications Standards Institute o ETSI, que va a ser el encargado de regular desde este momento todos los aspectos de las comunicaciones a través de GSM, los primeros sistemas comerciales basados en este nueva red aparece en el año 1991.

2.5.1.1 Descripción de los sistemas celulares

Hemos dicho que GSM es un sistema basado en células de radio, vamos a ver que significa esto asi como las diferentes organizaciones que surgen de una idea en principio muy simple.

Los sistemas celulares se basan en la división del área de cobertura de un operador en lo que se denomina células (cells), estas células se caracterizan por su tamaño que viene determinado por la potencia del transmisor pero de un modo muy particular ya que lo que se persigue siempre en los sistemas celulares es que la potencia de transmisión sea lo más baja posible a fin de poder reutilizar el mayor número de frecuencias. El porque de tener el mayor número de frecuencias disponibles tiene que ver con que a mayor número de frecuencias libres mayor es el número de usuarios que pueden hacer uso del sistema ya que cada uno puede usar una frecuencia sin interferir en la de otro usuario. De este modo todas las bandas de frecuencias se distribuyen sobre las células a lo largo del área de cobertura del operador de manera que todos los canales de radio se encuentran disponibles para ser usados en cada grupo de células (clusters) lo cual no sucedería si se produjese una emisión de la señal con una potencia superior ya que se podria interferir en otras células adyacentes interfiriendo en las frecuencias disponibles. Como podemos imaginar, la distancia que debe existir entre dos células debe ser los suficientemente grande como para que no se produzca interferencia entre ellas, hay que decir también que hay determinados canales que se reservan para labores de señalización y control de toda la red.

Todo lo explicado anteriormente se resume en dos condiciones que las células deben de verificar para que este sistema funcione:

1.- El nivel de potencia del transmisor debe de ser el mínimo para reducir las interferencias con los transmisores de las células vecinas.

2.- Las celulas vecinas no pueden compartir los mismos canales, el motivo es similar al anterior, reducir el nivel de interferencias.

Las células se unen las unas a las otras mediante cable (lo más normal) o bien mediante radio enlaces asi como con la red telefonica fija.

Una vez que tenemos claro el concepto de célula el siguiente nivel de organización que existe en GSM es el de cluster, que no es más que un conjunto de células agrupadas entre si, estos clusteres suelen agrupar conjuntos de 4, 7, 12 o 21 células distintas que se distribuyen por todo el área de cobertura del operador.

2.5.1.2 Tipos de celulas

En GSM se distinguen cuatro tipos de células:

- Macrocelulas (Macrocells): Son celulas de gran tamaño utilizadas en áreas de terreno muy grandes y donde la distancia entre areas pobladas es muy distantes entre si.

- Microcelulas (Microcells): Se utilizan por el contrario en áreas donde hay una gran densidad de población, el objetivo al hacer esto es el que comentabamos antes cuando describiamos que era una célula, a mayor número de células mayor número de canales disponibles que pueden ser utilizados por más usuarios simultaneamente.

Celulas selectivas (Selectived Cells): En muchas ocasiones no interesa que una celula tenga una cobertura de 360 grados sino que interesa que tenga un alcance y un radio de acción determinado, en este caso es donde aparecen las celulas selectivas, el caso más típico de celulas de este tipo son aquellas que se disponen en las entradas de los túneles en los cuales no tiene sentido que la celula tenga un radio de acción total (360 grados) sino un radio de acción que vaya a lo largo del tunel.

Celulas Sombrilla (Umbrella Cells): Este tipo de células se utilizan en aquellos casos en los que tenemos un elevado número de células de tamaño pequeño y continuamente se estan produciendo cambios (handovers) de terminal de una celula a otra, para evitar que suceda esto lo que hacemos es agrupar conjuntos de microcelulas de modo que aumentamos la potencia de la nueva célula formada y podemos reducir el número de handovers que se producen.

2.5.1.3 Arquitectura de una red GSM

Todas las redes GSM se pueden dividir en cuatro partes fundamentales y bien diferenciadas:

1. La Estación Movíl o Mobile Station (MS): Consta a su vez de dos elementos básicos que debemos conocer, por un lado el terminal o equipo móvil y por otro lado el SIM o Subscriber Identity Module.Con respecto a los terminales, tenemos que comentar es que la diferencia entre unos y otros radica fundamentalmente en la potencia que tienen que va desde los 20 watios (generalmente instalados en vehiculos) hasta los 2 watios de nuestros terminales.

El SIM es una pequeña tarjeta inteligente que sirve para identificar las características de nuestro terminal. Esta tarjeta como todos sabemos se inserta en el interior del móvil y permite al usuario acceder a todos los servicios que haya disponibles por su usuario, como podemos ver sin la tarjeta SIM el terminal no nos sirve de nada por que no podemos hacer uso de la red. Como también sabemos, el SIM esta protegido por un número de cuatro dígitos que recibe el nombre de PIN o Personal Identification Number. La mayor ventaja de las tarjetas SIM es que proporcionan movilidad al usuario ya que puede cambiar de terminal y llevarse consigo el SIM. Una vez que se introduce el PIN en el terminal, el terminal va a ponerse a buscar redes GSM que esten disponibles y va a tratar de validarse en ellas, una vez que la red (generalmente la que tenemos contratada) ha validado nuestro terminal el telefono queda registrado en la célula que lo ha validado.

2. La Estación Base o Base Station Subsystem (BSS): Sirve para conectar a las estaciones móviles con los NSS, además de ser los encargados de la transmisión y recepción. Como los MS también constan de dos elementos diferenciados; La Base Transceiver Station (BTS) o Base Station y la Base Station Controller (BSC). La BTS consta de transceivers y antenas usadas en cada célula de la red y que suelen estar situadas en el centro de la célula, generalmente su potencia de transmisión determinan el tamaño de la célula.Los BSC se utilizan como controladores de los BTS y tienen como funciones principales las de estar al cargo de los handovers, los frequency hopping y los controles de las frecuencias de radio de los BTS.

3. El Subsistema de Conmutación y Red o Network and Switching Subsystem (NSS): Este sistema se encarga de administrar las comunicaciones que se realizan entre los diferentes usuarios de la red; para poder hacer este trabajo la NSS se divide en siete sistemas diferentes, cada uno con una misión dentro de la red:

   a) Mobile Services Switching Center (MSC): Es el componente central del NSS y se encarga de realizar las labores de conmutación dentro de la red, así como de proporcionar conexión con otras redes.

   b) Gatewaq Mobile Services Switching Center (GMSC): Un gateway es un dispositivo traductor (puede ser software o hardware que se encarga de interconectar dos redes haciendo que los protocolos de comunicaciones que existen an ambas redes se entiendan. Bien, la misión del GMSC es esta misma, servir de mediador entre las redes de telefonía fijas y la red GSM.

c) Home Location Registrer (HLR): El HLR es una base de datos que contiene información sobre los usuarios conectados a un determinado MSC. Entre la información que almacena el HLR tenemos fundamentalmente la localización el usuario y los servicios a los que tiene acceso. El HRL funciona en unión con en VLR que vemos a continuación.

d) Visitor Location Registrer (VLR): contiene toda la información sobre un usuario necesaria para que dicho usuario acceda a los servicios de red. Forma parte del HLR con quien comparte funcionalidad.

e) Authentication Center (AuC): Proporciona los parámetros necesarios para la autentificación de usuarios dentro de la red; también se encarga de soportar funciones de encriptación.

f) Equipment Identy Registrer (EIR): También se utiliza para proporcionar seguridad en las redes GSM pero a nivel de equipos válidos. La EIR contiene una base de datos con todos los terminales que son válidos para ser usados en la red. Esta base de datos contiene los International Mobile Equipment Identy o IMEI de cada terminal, de manera que si un determinado móvil trata de hacer uso de la red y su IMEI no se encuentra localizado en la base de datos del EIR no puede hacer uso de la red.

g) GSM Interworking Unit (GIWU): sirve como interfaz de comunicación entre diferentes redes para comunicación de datos.

4. Los subsistemas de soporte y operación u Operation and Suppñort Subsystem (OSS): Los OSS se conectan a diferentes NSS y BSC para controlar y monitorizar toda la red GSM.

2.5.1.4 Roadming y Hand-over

Una vez vista la arquitectura de red que tenemos en GSM vamos a ver dos aspectos que son fundamentales dentro del funcionamiento normal de una red GSM, nos referimos al roadming y al hand-over. En los apartados anteriores hemos visto que una red GSM se fundamenta en lo que hemos llamado célula y también comentábamos que una vez que introducíamos nuestro PIN en la terminal se procedía a buscar una red donde ser validado.

Estos dos aspectos conllevan una serie de consecuencias que son las que van a originar el roadming y el hand-over.

¿Qué se entiende por roadming?, el roadming se produce siempre que nos estamos validando dentro de la red GSM y el terminal no es capaz de encontrar la red en la cual somos clientes; esto pasa fundamentalmente cuando salimos de viaje al extranjero, donde existe la red, pero no es la de nuestro operador; en este caso, el roadming consiste en la utilización de la red que se encuentre disponible y con la que nuestro operador tiene un acuerdo de colaboración. De este modo, podemos seguir conectados con nuestro móvil a la red independientemente de que estemos fuera del alcance de nuestro operador habitual. Existe un problema con el roadming que tenemos que tener en cuenta y es que cuando nuestro terminal se encuentra en roadming sucede que en el caso de que alguien nos llame, el coste de la llamada se divide de manera que la persona que nos llama paga la parte nacional de la llamada y nosotros corremos con los gastos de la parte internacional; esto es debido a que en el roadming nuestro operador no sabe de antemano donde nos encontramos, ya que estamos en una red que no le pertenece y por tanto no puede establecer la tarifa que debe aplicar.

El concepto de hand-over tampoco es complicado y consiste en la transición que se produce cuando pasamos del rango de acción de una célula al rango de acción de otra. Esto se produce sobre todo cuando viajamos. El hand-over, por tanto, es el responsable de mantener el servicio de manera constante y de que las transiciones entre una célula y otra sean lo suficientemente pequeñas como para pasar desapercibidas por los usuarios.

2.5.1.5 GSM y radio enlaces

Hasta ahora, hemos estado viendo como es la red de GSM, pero no hemos dicho nada sobre otro elemento que resulta fundamental para el funcionamiento del sistema. Nos referimos a los radio enlaces.

A través del interfaz de radio, se produce la unión entre los dispositivos móviles y las infraestructuras fijas que hay en las células.

GSM tiene cuatro versiones principales basadas en la banda: GSM-850, GSM-900, GSM-1800 y GSM-1900. GSM-900 (900 MHz) y GSM-1800 (1,8 GHz) son utilizadas en la mayor parte del mundo, salvo en Estados Unidos, Canadá y el resto de América Latina que utilizan el CDMA, lugares en los que se utilizan las bandas de GSM-850 y GSM-1900 (1,9 GHz), ya que en EE.UU. Las bandas de 900 y 1800 MHz están ya ocupadas para usos militares. En la figura 2.9 podemos observar una estación base de GSM.

Inicialmente, GSM utilizó la frecuencia de 900 MHz con 124 pares de frecuencias separadas entre si por 200 khz, pero después las redes de telecomunicaciones públicas utilizaron las frecuencias de 1800 y 1900 MHz, con lo cual es habitual que los teléfonos móviles de hoy en día sean tribanda.

El GSM, se puede dedicar tanto a voz como a datos.Una llamada de voz utiliza un codificador GSM específico a velocidad total de 13Kbits/s, posteriormente se desarrolló un codec a velocidad mitad de 6.5Kbits/s que permitirá duclicar la capacidad de los canales TCH, se denomina FR (Full Rate) y HR (Half Rate) Una conexión de datos, permite el que el usuario utilice el móvil como un módem de 9600 bps, ya sea en modos circuito o paquetes en régimen síncrono/asíncrono. También admiten servicios de datos de una naturaleza no transparente con una velocidad neta de 12 Kbits/s.

Las implementaciones más veloces de GSM se denominan GPRS y EDGE, también denominadas generaciones intermedias o 2.5G, que conducen hacia la tercera generación 3G o UMTS. Los nuevos teléfonos GSM pueden ser controlados por un conjunto de comandos estándarizados Hayes AT, mediante cable o mediante una conexión inalámbrica (IrDA o bluetooth, este último incorporado en los teléfonos actuales).

Estas bandas de frecuencia, que vimos antes que son utilizadas para mantener diferentes comunicaciones simultáneas; hay dos mecanismos fundamentalmente utilizados para poder proporcionar acceso múltiple a un medio limitado, como son las frecuencias. Estos dos mecanismos se denominan FDMA o Frequency Division Multiple Access (Acceso Múltiple por división de Frecuencia) y TDMA o Time Division Multiple Access (Acceso Multiple por Division de Tiempo).

En el caso de FDMA a cada usuario se le asigna una frecuencia de manera que el máximo número de usuarios que pueden usar el sistema viene determinado por el máximo número de frecuencias disponibles. Mediante TDMA lo que se hace es que diferentes usuarios pueden utilizar el mismo canal; para ello, a cada usuario se le asigna un determinado tiempo en el cual puede hacer uso del canal.

Figura 2.9: Estación base GSM[25]

2.5.2. Redes GPRS

El servicio de radio transmisión de paquetes generales (GPRS) es considerada la generación 2.5, entre la segunda generación (GSM) y la tercera (UMTS).Proporciona altas velocidades de transferencia de datos (especialmente útil para conectar a Internet) y se utiliza en las redes GSM. GPRS es sólo una modificación de la forma de transmitir datos en una red GSM, pasando de la con-

mutación de circuitos en GSM (donde el circuito está permanentemente reservado mientras dure la comunicación aunque no se envíe información en un momento dado) a la conmutación de paquetes. GPRS es considerado como la extensión del servicio GSM con mayor potencial para proporcionar el salto cualitativo de los datos sobre servicios móviles. GPRS supone integrar en el sistema GSM un nuevo concepto de red y con él una nueva arquitectura específicamente diseñada para facilitar el acceso a las redes de paquetes, mayoritariamente orientadas al protocolo IP.[21]

Desde el punto de vista del operador de telefonía móvil es una forma sencilla de hacer la red desde GSM a una red UMTS puesto que las antenas sufren sólo ligeros cambios y los elementos nuevos de red necesarios para GPRS serán compartidos en el futuro con la red UMTS.

GPRS es básicamente una comunicación basada en paquetes de datos. Los timeslots (intervalos de tiempo) se asignan en GSM generalmente mediante una conexión conmutada, pero en GPRS los intervalos de tiempo se asignan a la conexión de paquetes, mediante un sistema basado en la necesidad. Esto significa que si no se envía ningún dato por el usuario, las frecuencias quedan libres para ser utilizadas por otros usuarios.

Que la conmutación sea por paquetes permite fundamentalmente la compartición de los recursos radio. Un usuario GPRS sólo usará la red cuando envíe o reciba un paquete de información, todo el tiempo que esté inactivo podrá ser utilizado por otros usuarios para enviar y recibir información.

Esto permite a los operadores dotar de más de un canal de comunicación sin miedo a saturar la red, de forma que mientras que en GSM sólo se ocupa un canal de recepción de datos del terminal a la red y otro canal de transmisión de datos desde la red al terminal, en GPRS es posible tener terminales que gestionen cuatro canales simultáneos de recepción y dos de transmisión, pasando de velocidades de 9,6 kbps en GSM a 40 kbps en recepción en GRPS y 20 kbps de transmisión.

Otra ventaja de la conmutación de paquetes es que, al ocuparse los recursos sólo cuando se transmite o recibe información, la tarifa por parte del operador de telefonía móvil sólo se produce por la información transmitida, no por el tiempo de conexión.

Los teléfonos GPRS pueden llevar un puerto bluetooth, IrDA, o conexión por cable para transferir datos al ordenador, cámaras digitales, móviles u otros dispositivos.

2.5.3. Ventajas de la tecnología GRPS

La mayor ventaja de GPRS no es la tecnológica en si misma sino los servicios que facilita. Entre las ventajas puramente tecnológicas respecto a la tecnología GSM, podemos destacar las siguientes:

1 Utilización de la voz y los datos a través del teléfono móvil, gracias a la separación de canales que transmiten de forma paralela. Podrá mantener conversaciones sin cortar la transmisión de datos.

2 Acceso permanente para datos.En contraste con la modalidad de conexión por llamada utilizada en GSM, permite ahorrar el tiempo de conexión cada vez que se requiere una información.

3 Velocidad de transmisión de datos, que permitirá aproximarse rápidamente a velocidades a las que estamos acostumbrados en las líneas fijas. Aunque en sus comienzos serán de 20 kbps, en pocos meses se pasará a más del doble, con lo que en poco tiempo la velocidad cuadriplicará el rendimiento de la tecnología GSM. Y el multiplicador continuará creciendo.

4 Facturación basada en el volumen de datos transferidos, en lugar de tarifas basadas en tiempo de conexión, con el consiguiente ahorro de costes cuando los volúmenes de transferencia sean mínimamente elevados.

2.5.4. Terminales que pueden utilizar la tecnología GPRS

Los beneficios que la tecnología GPRS aporta supone la necesidad de subir un escalón en la gama de teléfonos móviles, utilizando modelos más potentes que los actuales para que puedan manejar conjuntamente datos y voz, y que estén diseñados pensando en la funcionalidad requerida para servicios datos. Por ello, está próximo un cambio de tendencia en los terminales que irán desarrollando cada vez más capacidades de representación de la información con mayores pantallas, formas diferentes a las hoy conocidas y especialización de terminales según su uso: preferentemente voz; o voz y datos; o preferentemente datos. Así, veremos a corto plazo cinco tipos de terminales GPRS que irán desarrollando capacidades adicionales a medida que la tecnología vaya avanzando:

1. Teléfonos móviles similares a los actuales, con visor cada vez mayor y con mejor resolución. Estos terminales permitirán el uso de información escrita o gráfica de forma resumida y podrán cubrir la función de modem inalámbrico cuando se conectan a un ordenador portátil.

2. Terminales tipo agenda electrónica con funciones mixtas de voz y datos, que dispondrán de pantallas de mayor tamaño y capacidad gráfica, con un formato similar a los teléfonos móviles.

3. Terminales tipo ordenador personal de mano (PDA "Personal Digital Assistant"), con pantalla plana de mayor formato y gran capacidad gráfica.

4. Ordenadores portátiles que utilicen para su conexión inalámbrica un teléfono móvil GPRS o una tarjeta PCMCIA con capacidad de comunicación wireless.

5. Dispositivos muy diversos que utilizarán comunicación móvil y que estarán adaptados a una función muy especializada, como sistemas de navegación en los coches, tarjetas de comunicación inalámbrica en máquinas autoservicio, dispositivos de telemedida y telecontrol especializados, etc.

En resumen, GPRS define un método óptimo de acceso a redes IP, permitiendo al sistema GSM proporcionar capacidad y velocidades de acceso a internet e intranets, mejorando adicionalmente la eficacia de la red. Finalmente, GPRS proporcionará la posibilidad de desarrollar las redes GSM de hoy orientándolas hacia la red de tercera generación, UMTS, puesto que la capacidad para crear nuevos servicios basados en el protocolo IP y su flexibilidad de tarificar lo convierten en la plataforma perfecta para enlazar con la próxima generación del sistema de telecomunicaciones móviles.

2.6. Redes inalámbricas IEEE802.11(a,b,g)

El comité IEEE 802.11 es el encargado de desarrollar los estándares para las redes de área local inalámbricas.El estándar IEEE 802.11 se basa en el mismo marco de estándares que Ethernet. Esto garantiza un excelente nivel de interoperatividad y asegura una implantación sencilla de las funciones y dispositivos de interconexión Ethernet/WLAN.

A veces las infraestructuras de comunicación basadas en esquemas de cableado tradicionales no son factibles debido a motivos técnicos o económicos. En estos

casos, los productos inalámbricos se rigen como alternativas flexibles a las redes cableadas.La tecnología inalámbrica también ofrece excelentes soluciones cuando se necesitan instalaciones de red temporales. Estas son algunas de las aplicaciones habituales de las redes WLAN:

- Redes temporales.

- Motivos arquitectónicos.

- Aplicaciones móviles.

- Soluciones de red flexibles.

- LAN interconectadas.

El comité IEEE encargado de la tecnología de red de área local desarrolló el primer estándar para redes LAN inalámbricas (IEEE 802.11).

El IEEE revisó ese estándar en octubre de 1999 para conseguir una comunicación por RF a velocidades de datos más altas. El IEEE 802.11b resultante describe las características de las comunicaciones LAN RF de 11 Mbps.

El estándar IEEE 802.11 está en constante desarrollo. Existen varios grupos de trabajo encargados de proponer y definir nuevas mejoras al estándar WLAN.

El estándar 802.11 define varios métodos y tecnologías de transmisión para implantaciones de LAN inalámbricas. Este estándar no sólo engloba la tecnología de radiofrecuencia sino también la de infrarrojos. Asi mismo, incluye varias técnicas de transmisión como:

- Modulación por saltos de frecuencia (FHSS).
- Expectro de extensión de secuencia directa (DSSS).
- Multiplexación por división en frecuencias octogonales (OFDM).

2.6.1. IEEE 802.11

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI

(capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.[3]

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todas los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz.En la actualidad no se fabrican productos sobre este estándar.

El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11legacy."La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz. También se realizó una especificación sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos.

Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g.En la actualidad la mayoría de productos son de la especificación b y de la g (Actualmente se está desarrollando la 802.11n, que se espera que alcance los 500 Mbps). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i.Otros estándares de esta familia (c-f, h-j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores.

El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b.En 2005, la mayoría de los productos que se comercializan siguen el estándar 802.11g con compatibilidad hacia el 802.11b.Los estándares 802.11b y 802.11g utilizan bandas de 2,4 gigahercios (Ghz) que no necesitan de permisos para su uso. El estándar 802.11a utiliza la banda de 5 GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2,4 Ghz.

2.6.2. Normalización

Hay, al menos, dos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11.[3]

- Los estándares IEEE 802.11b e IEEE 802.11g que disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente. Existe también el estándar IEEE 802.11n que está en desarrollo y trabaja a 2.4 GHz a una velocidad de 108 Mbps. Aunque estas velocidades de 108 Mbps son capaces de alcanzarse ya con el estándar 802.11g gracias a técnicas de aceleramiento que consiguen duplicar la transferencia teórica. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N, sin embargo, no son del todo seguros ya que el estándar no está completamente revisado y aprobado.

- En los Estados Unidos y Japón, se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. En otras zonas, como la Unión Europea, 802.11a no está aprobado todavía para operar en la banda de 5 GHz, y los reguladores europeos están todavía considerando el uso del estándar europeo HIPERLAN.

La tecnología inalámbrica bluetooth también funciona a una frecuencia de 2.4 GHz por lo que puede presentar interferencias con Wi-Fi, sin embargo, en la versión 1.2 y mayores del estándar bluetooth se ha actualizado su especificación para que no haya interferencias en la utilización simultánea de ambas tecnologías.

Existen varias tecnologías de transmisión inalámbrica pero la más conocida es la WIFI, publicada bajo el standard 802.11, ésta ha variado a lo largo de los tiempos pues como todo en el mundo tecnológico, se han producido varios cambios o actualizaciones, como por ejemplo: 802.11a, 802.11b, 802.11g las cuales trabajan a diferentes velocidades:

- 802.11 = 1Mb.

- 802.11a = 54 Mb (Ésta trabaja a una frecuencia en el rango de los 5GHz).

- 802.11b = 11Mb (Trabaja a 2,4 GHz. Conserva compatibilidad con el Standard 802.11, de 1Mb).

- 802.11g = 54 Mb (Trabaja a 2,4 GHz. Puede alcanzar los 108 Mb con dispositivos del mismo fabricante, siempre que se den las condiciones óptimas y sólo si el fabricante hizo la adaptación).

2.6.3. Protocolos, 802.11 Legacy

Estándares inalámbricos.

802.11 802.11b 802.11g 802.11a

Extensiones de Estándares Inalámbricos

802.11e 802.11i 802.11d 802.11f 802.11h

802.11

Ancho de banda máximo de hasta 2 Mbps,opera en el espectro de 2.4 Ghz sin necesidad de licencia. Posible interferencia con hornos microondas, dispositivos bluetooth, y teléfonos DECT, puesto que operan en el mismo espectro de frecuencias. Sistemas de modulación FHSS(Espectro Distribuido con Saltos de Frecuencias) y DSSS (Espectro Ensanchado de Secuencia Directa).

802.11b

Ancho de banda máximo de hasta 11Mbps opera en el espectro de 2.4 Ghz sin necesidad de licencia. Las mismas interferencias que para 802.11 conocido como WIFI modulación DSSS Compatible con los equipos DSSS del estándar 802.11.

802.11g

Ancho de banda máximo de hasta 54 Mbps opera en el espectro de 2.4 Ghz sin necesidad de licencia. Compatible con 802.11b.Modulación DSSS y OFDM.

802.11a

Ancho de banda máximo de hasta 54 Mbps, opera en el espectro de 5 Ghz sin necesidad de licencia. Menos saturado, no es compatible con 802.11b y 802.11g Modulación de OFDM.

Extensiones de Estándares Inalámbricos.

802.11e

Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN. Se aplicará a los estándares físicos a, b y g de 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.

802.11i

Se refiere al objetivo mas frecuente del estándar 802.11, la seguridad. Se aplicará a los estándares físicos a, b y g de 802.11 Proporciona una alternativa a la privacidad equivalente cableada (WEP) con nuevos métodos de encriptación y procedimientos de autentificación. IEEE 802.1x constituye una parte clave de 802.11i.

802.11d

Constituye un complemento al nivel de control de acceso al medio (MAC) en 802.11 para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11. Permitirá a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

802.11f

Su objetivo es lograr la interoperabilidad de puntos de acceso (AP) dentro de una red WLAN mutiproveedor. El estándar define el registro de puntos de acceso (AP) dentro de una red y el intercambio de información entre dichos puntos de acceso cuando un usuario se traslada desde un punto de acceso a otro.

802.11h

El objetivo es cumplir los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tendrán control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario mas lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

2.7. Conclusiones

En este capítulo clasificamos las redes inalámbricas en 4 tipos,en cada una de estas clasificaciones explicamos sus variantes, sus ventajas, su manera de operar, y esto para conocer cada tipo de red inalámbrica que existe en la actualidad y que tipo de conexión ofrece.

Capítulo 3

Estándares de la IEEE de redes inalámbricas

3.1. Introducción

En este capítulo se describe de manera más especifica el funcionamiento del estándar IEEE 802.11. El IEEE 802.11 define opciones de la capa física para la transmisión inalámbrica y la capa de protocolos MAC.

El IEEE 802.11 representa el primer estándar para los productos WLAN, este fue el primero de los estándares definidos por la IEEE para aplicaciones WLAN y fue publicado en 1997. Funciona sobre la banda ISM (Industrial Scientific and Medical) o en castellano ICM (Industrial científica Médica) de 2.4 Ghz.

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 las múltiples estaciones en una área de cobertura dada sin el uso de un punto de acceso o servidor. La norma especifica la etiqueta que cada estación debe observar para que todas ellas tengan un acceso justo a los medios de comunicación inalámbricos. Proporciona métodos de petición para utilizar el medio para asegurarse de 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 todas las estaciones y permite que estaciones 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 todas las estaciones en el área de servicios base y asegura un manejo apropiado del tráfico de datos. El punto de acceso dirige datos entre las estaciones y otras estaciones inalámbricas y/o el servidor de la red. Típicamente las WLAN controladas por un punto de acceso central proporcionará un rendimiento mucho mayor.

Los estándares aparecen en las faces intermedias o finales de vida de una tecnología, en lugar de la fase de introducción en la que llega una tecnología al mercado. El orden en el que surge un estándar creado por IEEE 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 provedores de tecnología.
5. Establecimiento del estándar por una entidad de estándares.
6. Ratificación del estándar por los provedores de la tecnología.

El comité de estándares IEEE 802 formó el grupo de trabajo de estándares de redes LAN inalámbricas 802.11 en 1990. El Grupo de trabajo 802.11 asumió la tarea de desarrollar una norma global para equipos de radio y redes que operaban en la banda de frecuencia de 2.4GHz, para tasas de datos de 1 y 2Mbps.

La norma no especifica tecnologías ni aplicaciones, sino simplemente las especificaciones para la capa física y la capa de control de acceso al medio (MAC). La norma permite a los fabricantes de equipos inalámbricos de radio LAN construir equipos interoperables de red.

Los socios del comité son individuos de varias compañías y universidades que investigan, fabrican, instalan y utilizan productos en aplicaciones de redes LAN inalámbricas. Fabricantes de semiconductores, computadoras, equipos de radio, proveedores de soluciones de sistemas WLAN, laboratorios universitarios de investigación y usuarios finales constituyen el grupo. El grupo es representado globalmente por compañías de los Estados Unidos, Canadá, Europa, Israel y algunas del Pacífico.

Según el diseño requerido se tienen distintas tecnologías aplicables:[15,28]

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, confiable 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)

b) Secuencia directa (DSSS: Direct-Sequence Spread Spectrum)

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. La capa física de cualquier red define la modulación y la señalización características de la transmisión de datos. En la capa física, se definen dos métodos de transmisión radio frecuencia y un infrarrojo. El funcionamiento de la WLAN en bandas RF, requiere la modulación en banda ancha para reunir los requisitos de funcionamiento en la mayoría de los países.

Un error muy cometido, es la confusión que aparece entre las técnicas de modulación y propagación. La diferencia entre una y otra, es que la técnica de propagación distribuye la información a través de una variedad de canales, en tanto que una técnica de modulación modula la información a través de cada uno de los canales. El espectro extendido de secuencia directa (DSSS), el espectro extendido de saltos de frecuencia (FHSS), el acceso multiplexado de división de código (CDMA) y al multiplexión por división ortognal de frecuencia (OFDM), son ejemplos de técnicas de propagación.

La multiplexión por división ortogonal de frecuencia codificada (COFDM) es la técnica de propagación que se usa en 802.11a y 802.11g.

Los estándares de transmisión RF en el estándar, son la frecuencia de saltos FHSS (Frecuency Hopping Spread Spectrum) y la secuencia directa DSSS (Direct Séquense Spread Spectrum)[4].

Ambas arquitecturas se definen para operar en la banda de frecuencia de 2.4 GHz, ocupando típicamente los 83 MHz de banda desde los 2.400 GHz hasta 2.483 GHz.

DBPSK (Differential BPSK) y DQPSK es la modulación para la secuencia directa. La frecuencia de saltos utiliza los niveles 2-4 Gaussian FSK como el método de señalización de modulación.

La tasa de datos de la capa física para sistemas FHSS es de 1Mbps. Para DSSS se soportan tanto tasas de datos de 1 Mbps como de 2 Mbps. La elección entre FHSS y DSSS dependerá de diversos factores relacionados con la aplicación de los usuarios y el entorno en el que el sistema esté operando.

Capa fisica infrarroja

Se soporta un estándar infrarroja, que opera en la banda 850nM a 950nM, con un poder máximo de 2 W. La modulación para el infrarrojo se logra usando o 4 o 16 niveles de modulación "posicionamiento por pulsos". La capa física soporta dos tasas de datos: 1 y 2Mbps.[4]

La Capa Física DSSS

Se genera un bit redundante por cada bit transmitido. Estos bits redundantes son llamados çhipping code". Cuanto mayor sea esta secuencia mayor es la

probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda). 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.[34]

La Capa Física FHSS

La capa física FHSS tiene 22 modelos de espera para escoger. La capa física frecuencia de saltos se exige para saltar por la banda ISM 2.4GHz cubriendo 79 canales. Cada canal ocupa un ancho de banda de 1Mhz y debe brincar a la tasa mínima especificada por los cuerpos reguladores del país pretendido. Para los Estados Unidos se define una tasa de salto mínima de 2.5 saltos por segundo.

Cada una de las capas físicas utiliza su propio encabezado único para sincronizar al receptor y determinar el formato de la señal de modulación y la longitud del paquete de datos. Los encabezamientos de las capas físicas siempre se transmiten a 1Mbps. Los campos predefinidos en los títulos proporcionan la opción para aumentar la tasa de datos a 2 Mbps para el paquete de los datos existente.[4]

La capa MAC

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 protocolo conocido como CSMA/CA (Multiple acceso por detección de portadora evitando colisiones). Este protocolo 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 es un subconjunto de la capa de enlace, que a su vez es adyacente a la capa fisica en una red basada en IP. La capa 1 en una red 802.11 realiza por lo menos tres funciones esenciales:[15,28]

- Funciona como interfaz entre la capa MAC en dos o más ubicaciones geográficas. Estas ubicaciones normalmente sólo estan a pocos cientos de metros de distancia.

- Realizan la detección real de los sucesos CSMA/C, mismos que ocurren dentro de la capa MAC.

- Efetúan la modulación y demodulación de la señal entre dos puntos geográficos en los que reciden equipos 802.11. Este esquema de modulación puede ser DSSS o FHSS.

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 (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía RF de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente 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 CCA que puede estar sola o con la medida RSSI. 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 operativo. 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.[4]

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. Las estaciones receptoras 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.

Una limitación común de los sistemas LAN inalámbricos es el problema del nodo oculto. Esto puede romper un 40 o más de las comunicaciones en un ambiente LAN muy cargado. Ocurre cuando hay una estación en un grupo de servicio que no puede detectar la transmisión de otra estación, y así descubrir que el medio está ocupado.

La capa de control de acceso a los medios (MAC) la cual controla el flujo de paquetes entre dos o más puntos de la red y sus funciones principales son:

- Exploración.
- Autenticación.
- Asociación.
- Seguridad.
- Modo de ahorro de energía.
- Fragmentación.

En la figura 3.1, las estaciones A y B se pueden comunicar. Sin embargo, una obstrucción impide a la estación C recibir de la estación receptora A y no puede determinar cuándo está ocupado el canal.Por lo tanto, ambas estaciones A y C podrían intentar transmitir a la vez a la estación B. El uso de las secuencias RTS, CTS.

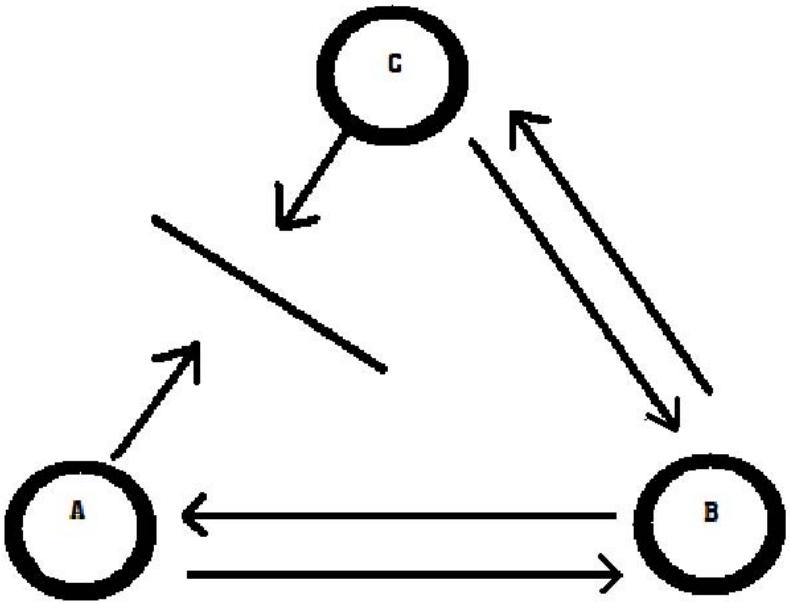

Figura 3.1: Capa MAC.

3.2. Estándar 802.11a

Fue la primera aproximación a las WLAN y llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de velocidad ofrecidas por diferentes fabricantes, pero que no están (a día de hoy) estandarizadas por el IEEE. Esta variante opera dentro del rango de los 5 Ghz.

802.11a, la cual nunca llegó realmente al mercado, lo que suponía una serie de problemas técnicos y legales.

Inicialmente se soportan hasta 64 usuarios por punto de acceso. Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y g, la no incorporación a la misma de QoS (Calidad de Servicio), la no disponibilidad de esta frecuencia en Europa dado que esta frecuencia está reservada a la HyperLAN2 y la parcial disponibilidad de la misma en Japón. El hecho de no estar disponible en Europa prácticamente la descarta de nuestras posibilidades de elección para instalaciones en nuestro pais.[14,24]

En 1997 la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) crea el Estándar 802.11 con velocidades de transmisión de 2Mbps. En 1999, el IEEE aprobó ambos estándares:

* 802.11a.

* 802.11b.

En 2001 hizo su aparición en el mercado los productos del estándar 802.11a. La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza los protocolos de base que el estándar original, opera en la banda de 5 Ghz utilizando la técnica OFDM (orthogonal frequency-division multiplexing).

Esta técnica permite dividir una portadora de datos de alta velocidad en 52 subportadoras de baja velocidad que se transmiten en paralelo con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s.

La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2.4 Ghz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias.Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

Transmisión exteriores valor máximo A 30 metros 54 Mbps valor mínimo A 300 metros 6 Mbps.

Interiores valor máximo a 12 metros 54 Mbps valor mínimo A 90 metros 6 Mbps.

3.3. Estándar 802.11b

Es la segunda aproximación de las WLAN. Alcanza una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por la velocidad que ofrecen algunos fabricantes pero sin la estandarización (a día de hoy) del IEEE. Opera dentro de la frecuencia de los 2.4 Ghz. Inicialmente se soportan hasta 32 usuarios por PA.

Cambia en varios de los inconvenientes que tiene el 802.11a como son la falta de QoS, además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues en los 2.4 Ghz funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos bluetooth, lo cual puede provocar interferencias. En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo. Está estandarizado por el IEEE.

Aprobado en 1997 y conocido como Wi-Fi, forma parte de una familia de los estándares del IEEE. Básicamente se diferencian en el uso exclusivo de la modulación DSSS con el sistema de codificación CCK (Complementary Code

Keying) que solo funciona con esta modulación. Esto le permite ofrecer hasta 11 Mbps, las velocidades de transmisión que es capaz de ofrecer podrían variar desde 1,2, 5.5 y 11 Mbps, dependiendo de diferentes factores.[14,24]

Otros datos que hay que tomar en cuenta sobre este estándar es el soporte para tres canales sin soplamiento y su reducido nivel de consumo que le hace perfectamente válido para su uso en PCs portátiles o PDAs.

En cuanto a las distancias a cubrir ,dependerá de las velocidades aplicadas , del número de usuarios conectados y del tipo de antenas y amplificadores que se pueden utilizar. Aún asi,se pueden dar cifras alrededor de entre 120m(a 11 Mbps) y 460m(a 1 Mbps)en espacios abiertos y entre 30m(a 11 Mbps) y 90m(a 1 Mbps) en interiores, dependiendo lógicamente del tipo de materiales que sea necesario atravesar.[10]

3.4. Estándar 802.11g

Es la tercera aproximación a las WLAN, y se basa en la compatibilidad con los dispositivos 802.11b y en el ofrecer unas velocidades de hasta 54 Mbps o de 24.7 Mbit/s de velocidad real de transferencia. Funciona dentro de la frecuencia de 2.4 Ghz. Dispone de los mismos inconvenientes que el 802.11b.Las ventajas de las que dispone son las mismas que las del 802.11b además de su mayor velocidad.

En el año 2003 se aprobó el nuevo estándar, trabaja sobre la frecuencia de 2.4Ghz y es capaz de utilizar dos métodos de modulación DSSS y OFDM, lo que la hace compatible con el estándar de facto en esta industria.

Al soportar ambas codificaciones este estándar es capaz de incrementar notablemente la velocidad de transmisión asi pudiendo llegar hasta los 54 Mbps, manteniendo asi las caracteristicas del estándar 802.11b en cuanto distancia, niveles de consumo y frecuencia.[11]

La tabla 3.1 muestra las características de los estándares en las redes inalámbricas.[10,11]

Estándar WLAN	**802.11a**	**802.11b**	**802.11g**	**HiperLAN2**	**Bluetooth**
Organismo	IEEE	IEEE	IEEE	ETSI	Bluetooth SIG
Finalización	2002	1999	2003	2003	2002
Denominación	Wi-Fi5	Wi-Fi	-	-	-
Frecuencias	5 Ghz	2.4 Ghz	2.4 Ghz	5 Ghz	2.4 Ghz
Velocidad máx	54 Mbps	11 Mbps	54 Mbps	54 Mbps	.721Mbit/s
Interface de aire	OFDM	DSSS	OFDM/DSSS	OFDM	DSSS/FHSS

Tabla 3.1: Estándares de redes inalámbricas.

3.5. Tecnología inalámbrica

La tecnología inalámbrica se ha ido convirtiendo poco a poco en la solución a muchos problemas o incomodidades que representaban tantos cables. El término "inalámbrico"hace referencia a la tecnología sin cables que permite conectar varias máquinas entre sí. Se mide en Mbps, un Mbps es un millón de bits por segundo, o la octava parte de un MegaByte por segundo - MBps (Recordemos que un byte son 8 bits.) Existen principalmente dos tecnologías inalámbricas certificadas. Una es la tecnología 802.11b y la otra 802.11g (ésta última tecnología es más reciente ha sido aprobada a finales de 2003- y más rápida).

Los teléfonos portátiles(móviles o celulares)utilizan esta tecnología inalámbrica. Son redes de área amplia (WAN) y ejemplifican a la perfección lo efectivo y práctico de la tecnología inalámbrica. La tecnología inalámbrica de banda ancha revolucionará la vida de los usuarios permitiendo conectarse directamente con las personas y la información mediante una conexión a alta velocidad desde cualquier parte. Intel cree que las tecnologías inalámbricas como 3G, Wi-Fi, WiMAX y UWB funcionaran de forma comjunta para cubrir las necesidades de los usuarios. Es probable que ninguna de las tecnologías inalámbricas de banda ancha llegue a dominar.

* WiMAX: Las redes metropolitanas inalámbricas (por sus siglas en inglés WMAN) cubren una distancia mucho mayor que las WLAN, conectando edificios entre sí dentro de una amplia área geográfica.La emergente tecnología WiMAX (802.16d hoy día y 802.16e en un futuro próximo) permitirán mayor movilidad y reducirán la dependencia de las conexiones con cable.

* Wi-Fi: Las redes locales inalámbricas (por sus siglas en inglés WLAN) disponen de un alcance más amplio que las WPAN, normalmente se ubican en edificios de oficinas, restaurantes, tiendas, casas, etc.Las WLAN van ganando popularidad, alimentada en parte por la disponibilidad de dispositivos optimizados para la informática inalámbrica como la tecnología móvil Intel Centrino.

* 3G: Redes amplias inalámbricas (por sus siglas en inglés WWAN) son las redes inalámbricas de mayor alcance, así como las más utilizadas hoy día en la infraestructura de telefonía móvil, aunque también disponen de la capacidad de transmitir datos.Los servicios de próxima generación de telefonía móvil basados en las diversas tecnologías 3G mejorarán significativamente las comunicaciones WWAN.

Muchas veces se confunde lo que es la tecnología inalámbrica con tecnología movíl, vamos a dar la diferencia entre ellas, la tecnología móvil hace referencia a la posibilidad de trasladar el trabajo de un sitio a otro, es decir, de llevar a cabo unas tareas determinadas fuera del campo de trabajo; en cambio, la tecnología inalámbrica hace referencia a la posibilidad de conectar varios dispositivos entre sí o a una red sin necesidad de cables, se puede emplear estas conexiones inalámbricas para transferir la información entre un sistema de empresa, donde un grupo de personas necesitan estar comunicados entre si.

3.5.1. Tecnologías inalámbricas

Bluetooth: Bluetooth es una frecuencia de radio de disponibilidad universal que conecta entre sí los dispositivos habilitados para bluetooth situados a una distancia de hasta 10 metros. Permite conectar un ordenador portátil o un dispositivo de bolsillo con otros ordenadores portátiles, teléfonos móviles, cámaras, impresoras, teclados, altavoces.

IrDA: Esta tecnología, basada en rayos luminosos que se mueven en el espectro infrarrojo. Los estándares IrDA soportan una amplia gama de dispositivos eléctricos, informáticos y de comunicaciones, permite la comunicación bidireccional entre dos extremos a velocidades que oscilan entre los 9.600 bps y los 4 Mbps. Esta tecnología se encuentra en muchos ordenadores portátiles, y en un creciente número de teléfonos celulares, sobre todo en los de fabricantes líderes como Nokia y Ericsson.

Wi-Fi: Wi-Fi o red de área local inalámbrica (WLAN) es una red de TI de tamaño medio que utiliza la frecuencia de radio 802.11a, 802.11b o 802.11g en

lugar de cables y permite realizar diversas conexiones inalámbricas a internet.Si sabe dónde se encuentra una red Wi-Fi o WLAN, puede navegar por internet, utilizar el correo electrónico y acceder a la red privada de una empresa. Esta es una buena opción para un empleado móvil que pasa fuera de su compañía.

Tecnología Wi-Max: Específicamente, la tecnología 802.16, a menudo denominada WiMAX, complementa la WLAN conectando hotspots con tecnología 802.11 a internet y ofrece una alternativa inalámbrica para la conectividad de banda ancha de última generación a empresas y hogares. Esta es una red muy costosa que aplica Microsoft, una red Wi-Fi, red ad hoc puede ser establecida por cualquiera para conectar la casa con la oficina, mientras que Wimax está diseñado para cubrir una ciudad entera a través de estaciones base dispersas alrededor del área metropolitana.

Tecnología GPRS: GPRS es la sigla de General Packet Radio Services (servicios generales de paquetes por radio). A menudo se describe como 2.5 G, es decir, una tecnología entre la segunda (2G) y la tercera (3G) generación de tecnología móvil digital.Se transmite a través de redes de telefonía móvil y envía datos a una velocidad de hasta 114 Kbps. El usuario puede utilizar el teléfono móvil y el ordenador de bolsillo para navegar por internet, enviar y recibir correo, y descargar datos y soportes. Permite realizar videoconferencias con sus colegas y utilizar mensajes instantáneos para charlar con sus familiares y amigos, esté donde esté. Además, puede emplearse como conexión para el ordenador portátil u otros dispositivos móviles.

Tecnología 3G: Al igual que GPRS, la tecnología 3G (tecnología inalámbrica de tercera generación) es un servicio de comunicaciones inalámbricas que le permite estar conectado permanentemente a internet a través del teléfono móvil, el ordenador de bolsillo, el tablet PC o el ordenador portátil. La tecnología 3G promete una mejor calidad y fiabilidad, una mayor velocidad de transmisión de datos y un ancho de banda superior (que incluye la posibilidad de ejecutar aplicaciones multimedia). Con velocidades de datos de hasta 384 Kbps, es casi siete veces más rápida que una conexión telefónica estándar.

Tecnología GSM: Global system for mobile communications, es la tecnología inalámbrica de más rápido crecimiento. Es el sistema de comunicaciones móviles más universal, que garantiza, mediante itinerancia, una cobertura mundial y que permite realizar llamadas de voz, datos o enviar mensajes de texto. GSM es el primer paso en la transformación de network TDMA a la nueva generación o 3G network y nos abre el camino para el desarrollo de funcionalidades avanzadas tales como GPRS. GSM se construye en la plataforma existente de TDMA. Avances

en tecnología permiten un uso más efectivo y eficiente en GSM. 3/4 partes del total del mercado de telefonía celular es GSM, el cual es el sistema utilizado. En más de 174 países del mundo. Lo más innovador que ofrece este sistema es el Smartchip, una pequeña tarjeta que se inserta en el teléfono GSM de Cingular Wireless y que almacena la información personal o de negocios de cada cliente.Al ser totalmente portátil le permite al usuario mover la información de un teléfono a otro con tal sólo colocar el SmartChip en otro teléfono GSM de Cingular Wireless.

Tecnología CDMA: CDMA2000 es la solución de 3era generación basada en IS-95. A diferencia de otros estándares de 3G, CDMA2000 es una evolución de un estándar inalámbrico existente. CDMA 2000 provee servicios de tercera generación como está definido por la ITU (International Telecommunications Union) en la IMT-2000. Las redes 3G proporcionarán servicios inalámbricos con mejor desempeño, gran rentabilidad y más contenido. La meta es acceder a cualquier servicio, en cualquier lugar, a cualquier hora desde una terminal.

3.5.2. Comunicaciones móviles

Según la UIT,se habla de comunicaciones móviles cuando existe al menos un terminal cuya ubicación se desplaza, requiriéndose servicio durante ese desplazamiento.

Una posible clasificación, puede ser la siguiente:

- Sistemas vía satélite (INMARSAT, IRIDIUM).
- Redes de área extensa de transmisión de datos (WATM).
- Redes móviles privadas (Wireless Ethernet).
- Redes de telefonía celular públicos (GSM, GPRS, UMTS).
- Redes de telefonía sin hilos (DECT).
- Redes domésticas (Home RF).
- Redes de área personal (Bluetooth).

Elementos de un sistema móvil.

- Estación base (BS): Son estaciones fijas que pueden ser controladas por una unidad de control.

- Estación de control (CS): Son estaciones también fijas que controlan automáticamente las emisiones o el funcionamiento de otra estación fija.
- Estación repetidora (RS): Son estaciones que retransmiten señales recibidas y permiten la cobertura en una zona no accesible por la estación base.
- Estación móvil (MS): Es una estación dotada de movilidad.

3.5.3. Redes celulares

La licencia de explotación del espectro radioeléctrico es uno de los principales costes que debe soportar un operador de telefonía móvil.

En estos casos, la reducción del número de frecuencias en el diseño de una red puede suponer un ahorro considerable. Igualmente, una vez contratada la licencia y determinado el número máximo de frecuencias disponibles, la capacidad de tráfico de la red puede ser incrementada mediante un mejor aprovechamiento del espectro, en el sentido de reutilizar frecuencias en distintas celdas de la red y poder transmitir simultáneamente desde distintos puntos con una misma portadora. Analizar las técnicas de modulación y los protocolos de acceso al medio (MAC) utilizados en redes celulares inalámbricas de 3ra Generación, así como en redes multimedia de banda ancha, (W-LAN's) y las llamadas redes de área personal (PAN's).

Niveles celulares:

- Pico celdas: De 20 a 400 m. Usualmente, internas a edificios.

- Micro celdas De 400m a 2 Km. Usualmente, zonas urbanas.

- Macro celdas De 2 a 20 Km.

- Comunidad global, Todo el mundo

Presente y Futuro (Wireless):

1G: Red celular analógica - Conmutación de circuitos.

2G: Red celular digital (GSM) - Conmutación de circuitos.

2,5 G: Red celular digital (GPRS) - Conmutación de paquetes.

3G: Red celular digital UMTS - Conmutación de paquetes.

4G: Red celular digital multimedia: - Todo IP (VoIP).

3.6. Antenas

Todos los estándares aseguran su funcionamiento mediante la utilización de dos factores, cuando estamos conectados a una red mediante un cable, sea del tipo que sea, disponemos de una velocidad fija y constante. Sin embargo cuando estamos hablando de redes inalámbricas aparece un factor añadido que puede afectar a la velocidad de transmisión, que es la distancia entre los interlocutores. Así pues cuando un TR se conecta a un PA se ve afectado principalmente por los siguientes parámetros:

- Velocidad máxima del PA (normalmente en 802.11g será de 54Mbps o dependiendo del estándar.)

- Distancia al PA (a mayor distancia menor velocidad.)

- Elementos intermedios entre el TR y el PA (las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el PA y el TR modifican la velocidad de transmisión a la baja.)

- Saturación del espectro e interferencias (cuantos más usuarios inalámbricos haya en las cercanías más colisiones habrá en las transmisiones por lo que la velocidad se reducirá, esto también es aplicable para las interferencias.)

Normalmente los fabricantes de PAs presentan un alcance teórico de los mismos que suele andar alrededor de los 250 metros. Esto obviamente es sólo alcanzable en condiciones de laboratorio, pues realmente en condiciones objetivas el rango de alcance de una conexión varía y siempre a menos por la infinidad de condiciones que le afectan.

Cuando ponemos un TR cerca de un PA disponemos de la velocidad máxima teórica del PA, 54 Mbps por ejemplo, y conforme nos vamos alejando del PA, tanto él mismo como el TR van disminuyendo la velocidad de la transmisión/recepción para acomodarse a las condiciones puntuales del momento y la distancia. Actualmente ya hay fabricantes que ofrecen antenas que aumentan la capacidad de TX/RX (transmisión y recepción) de los dispositivos wireless. Dentro de los PAs se puede modificar enormemente la capacidad de TX/RX gracias al uso de antenas especiales.

Estas antenas se pueden dividir en: direccionales, omnidireccionales,sectoriales.

A continuación se definen.

Antenas para redes inalámbricas WiFi disponemos de tres tipos de antenas para redes inalámbricas :

Antenas direccionales (o directivas)

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz de luz concreto y estrecho pero de forma intensa (más alcance).

Las antenas direccionales envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se escucha nada, no se puede establecer comunicación entre los interlocutores.

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor (fig 3.3).

Antena omnidireccionales

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance.Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir,con menor alcance (fig 3.2).

Las antenas omnidireccionales envían la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contra el alcance de estas antenas es menor que el de las antenas direccionales.

El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

Antenas sectoriales

Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con

un haz de luz más ancho de lo normal. Para tener una cobertura de 360 grados (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120 grados ó 4 antenas sectoriales de 80 grados. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales (fig 3.4).

Las antenas, pese a ser un elemento al cual se le presta escasa atención a la hora de realizar una instalación, es sin embargo uno de los pilares fundamentales de todo diseño. Una inadecuada selección de antenas puede suponer una deficiente cobertura en la zona de operación, con áreas de sombra con imposibilidad de recepción y otras con escasa señal que fuerzan a trabajar a un ratio de bits muy bajo, degradando las prestaciones de todo el conjunto. Por contra, uno de los principales defectos de los diseñadores un exceso de potencia de señal conlleva la cobertura de zonas más alejadas de lo deseado, pudiendo interferir con otras celdas (con lo que de nuevo baja el rendimiento del sistema por múltiples conexiones), además de permitir que equipos alejados puedan recibir las emisiones, facilitando notablemente la tarea de hackers. También a la hora de realizar la selección y ubicación física de las antenas (techos, paredes, esquinas, azoteas) pueden primar factores como la estética, precio o simple desconocimiento, agravando el error de diseño.

3.6.1. Apertura vertical y apertura horizontal

La apertura es cuanto se abre el haz de la antena. El haz emitido o recibido por una antena tiene una abertura determinada verticalmente y otra apertura determinada horizontalmente. En lo que respecta a la apertura horizontal, una antena omnidireccional trabajará horizontalmente en todas direcciones, es decir, su apertura será de 360 grados. Una antena direccional oscilará entre los 4 grados y los 40 grados y una antena sectorial oscilará entre los 90 grados y los 180 grados. La apertura vertical debe ser tenida en cuenta si existe mucho desnivel entre los puntos a unir inalámbricamente. Si el desnivel es importante, la antena deberá tener mucha apertura vertical. Por lo general las antenas, a más ganancia (potencia por decirlo de algún modo) menos apertura vertical. En las antenas direccionales, por lo general, suelen tener las mismas aperturas verticales y horizontales.

¿Qué antenas debemos instalar?

Las antenas direccionales se suelen utilizar para unir dos puntos a largas distancias mientras que las antenas omnidireccionales se suelen utilizar para dar señal extensa en los alrededores.

Las antenas sectoriales se suelen utilizar cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa. Si necesita dar cobertura de red inalámbrica en toda un área próxima (una planta de un edificio o un parque por ejemplo) lo más probable es que utilice una antena omnidireccional. Si tiene que dar cobertura de red inalámbrica en un punto muy concreto (por ejemplo un PC que está bastante lejos) utilizará una antena direccional, finalmente, si necesita dar cobertura amplia y a la vez a larga distancia, utilizará antenas sectoriales.

Figura 3.2: Antenas omnidireccionales.

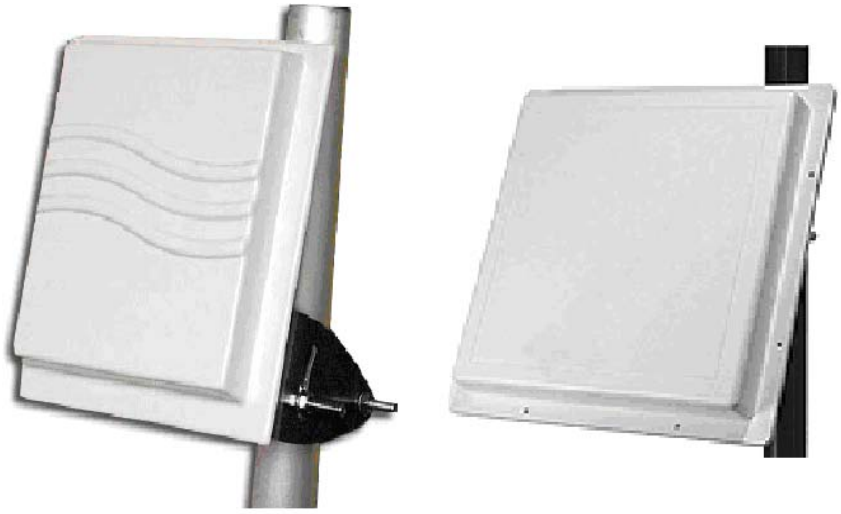

Figura 3.3: Antenas direccionales.

Figura 3.4: Antenas sectoriales.

Figura 3.5: Antenas compuestas, sectoriales, direccionales.

3.7. Puntos de acceso

Del inglés access point. En redes de computadoras, un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar roaming.(Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso - se convierten en una red ad-hoc).

Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) 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. Este o

su antena son normalmente colocados 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, mediante una antena.

3.7.1. Configurar access point

La configuración de estos equipos es muy sencilla, apenas necesitando la introducción de su dirección IP (en la mayoría de ellos se puede activar el cliente DHCP que poseen y de esta forma la capturan automáticamente), la del gateway por defecto, los parámetros de la parte inalámbrica y su seguridad (fig 3.6).

Esta es una guía paso a paso para configurar tu accesspoint para dar acceso a la gente a una red, cada marca de accesspoint es distinta pero parecida.

Revisa la version del Firmware: Antes de empezar a configurar el accesspoint, deberias mirar si la versión del firmware del accesspoint es la última o la más adecuada para el dispositivo.

Programas de Configuración: Una vez que tengas el accesspoint, necesitas cambiar las opciones por defecto para ser compatibles con la red. En la mayoria de los casos, los fabricantes proveen herramientas de configuración muy poco versatiles que permiten al usuario cambiar unos pocos parámetros (Por ejemplo, la que viene con el OrinocoRG1000 o Trendet). Hay varios programas realizados por terceras personas que pueden ser usados en vez de los oficiales.

Las opciones que debes cambiar son las siguientes:

SSID: Cambialo por el nombre de la red (sin mayusculas, ni espacios, ni comillas).

WEP: si lo desactivamos, lo hacemos por ampliar la compatibilidad del hardware en la red. Una red con el WEP activado supone que todas las tarjetas deben funcionar al mismo nivel de cifrado. Esto es útil en una empresa donde todos los empleados usen el mismo hardware, pero en una empresa donde cada uno tendrá el hardware que quiera hay que desactivarlo.

Nombre: Aquí se pone el nombre de tu nodo.

Situación: Pon tu dirección si lo deseas.

Canal: Observa los nodos mas cercanos a ti y escoge el canal menos usado.

Password: Muchos access point tienen passwords para cambiar las opciones de configuración. Escoge uno adecuado para que nadie pueda entrar en el access point y modificar las opciones.

DHCP: Tu access point o la red en la que este conectado debe correr un servidor DHCP para proporcionar direcciones IP adecuadas. Mira en la página direccionamiento ip para saber que rango de direcciones debes usar. Ahora tu access point forma parte de la red.

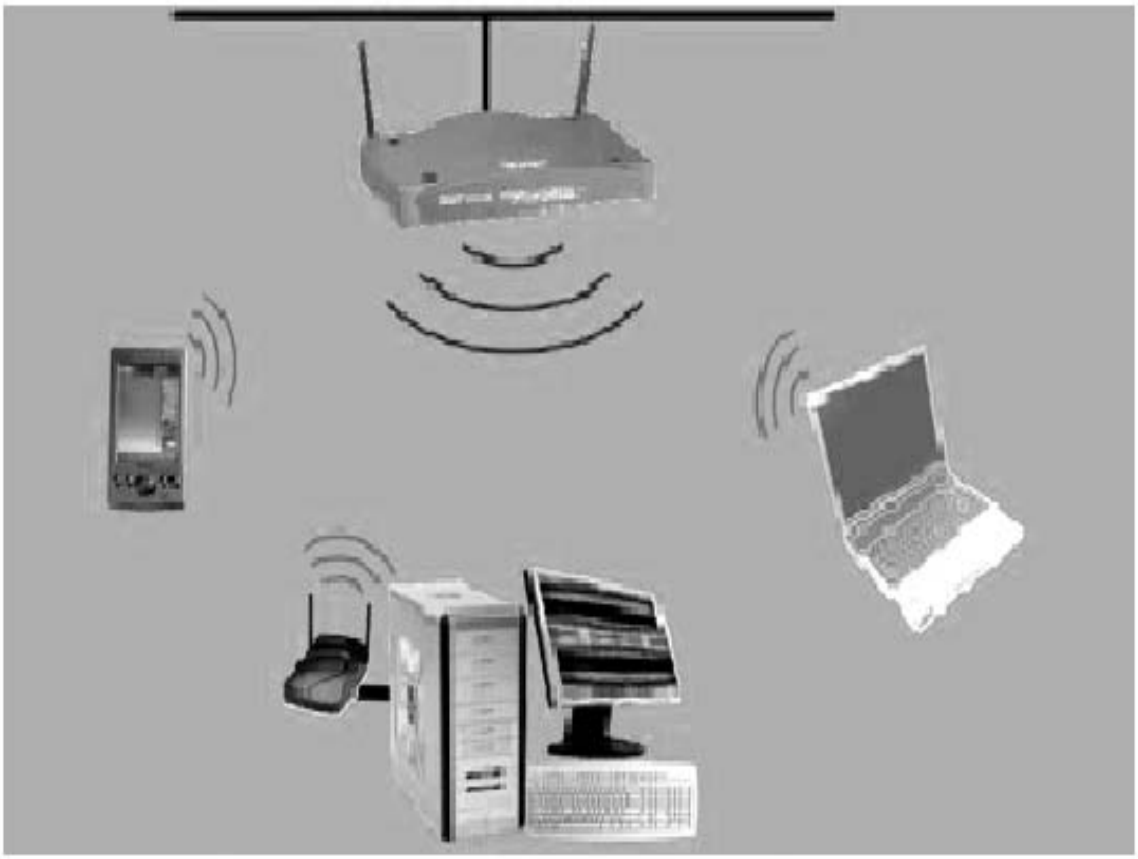

Figura 3.6: Puntos de acceso.[15]

3.8. Bridges

Son elementos que interconectan dos o más redes locales (a nivel 2 OSI). En el mundo wireless el concepto se matiza: deben interconectar redes locales fijas.

Esta definición expone su principal uso, la interconexión de redes fijas separadas por una distancia física la cual se ha cubierto mediante un segmento inalámbrico. Poseen dos interfaces, uno ethernet y otro inalámbrico. En cada red fija se ubica un bridge inalámbrico, orientando las antenas de ambos equipos para la mejor recepción. En caso de redes en edificios distantes, se suelen instalar antenas directivas de alta ganancia en los tejados lo que permite cubrir distancias en visión directa de hasta unos pocos kilómetros. Los parámetros inalámbricos de ambos extremos deben ser idénticos para posibilitar la comunicación (fig 3.7).

Virtualmente se pueden encadenar un número ilimitado de parejas de bridges para enlazar infraestructuras muy distantes o con obstáculos entre si. La configuración de estos dispositivos suele ser también bastante simple, requiriendo adicionalmente a los parámetros indicados para un AP poco más que la introducción de la dirección ip del bridge del otro extremo.[15,28]

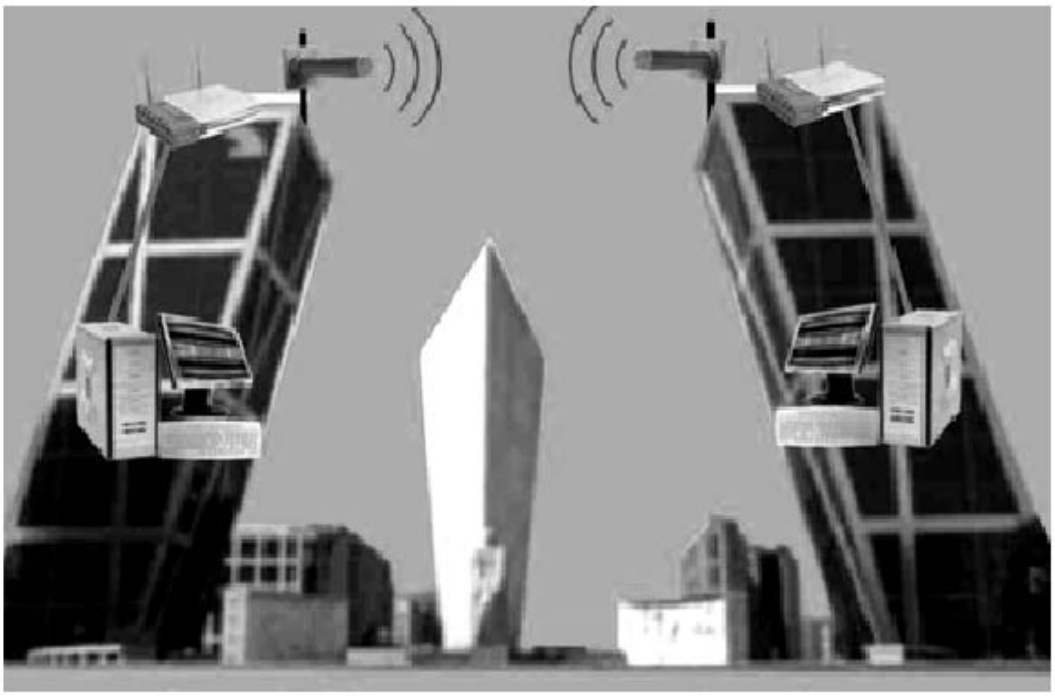

Figura 3.7: Bridges.[15]

3.9. Routers y Gateways

Poseen capacidad de enrutamiento (niveles 3 y 4 OSI) de los paquetes de información que los atraviesan. Una de sus interfaces es inalámbrica, existiendo al menos otra fija ethernet a la cual se suele denominar puerto WAN. La mayoría de modelos existentes en el mercado no posee funcionalidades puras de router, sino que están especialmente diseñados para actuar como pasarela entre la red inalámbrica directamente gestionada por el equipo (genéricamente llamada LAN) y las redes externas (red local de empresa, red de acceso a internet u otras). Por ello con frecuencia se les denomina gateway (pasarela). Su complejidad interna es superior al resto de los otros equipos. No sólo realizan labores de mayor procesamiento de la información como el enrutamiento, sino que además han sido enriquecidos con funcionalidades avanzadas en networking (traducción de direcciones por NAT y PAT o servidor DHCP de direccionamiento propio) y seguridad (firewall interno avanzado, listas de acceso por dirección MAC ethernet, bloqueo de acceso a urls para control paterno, restricción de uso por franja horaria). Además de lo anterior, suelen proporcionar en la parte LAN, además del interfaz Wireless, un conmutador Ethernet integrado de varios puertos. Ya menos frecuente, también algunos modelos poseen un servidor interno de impresión junto a un puerto serie, paralelo o USB para conectar una impresora. Igualmente existen modelos que poseen un interfaz para interconectarse directamente con redes ADSL (fig 3.8).

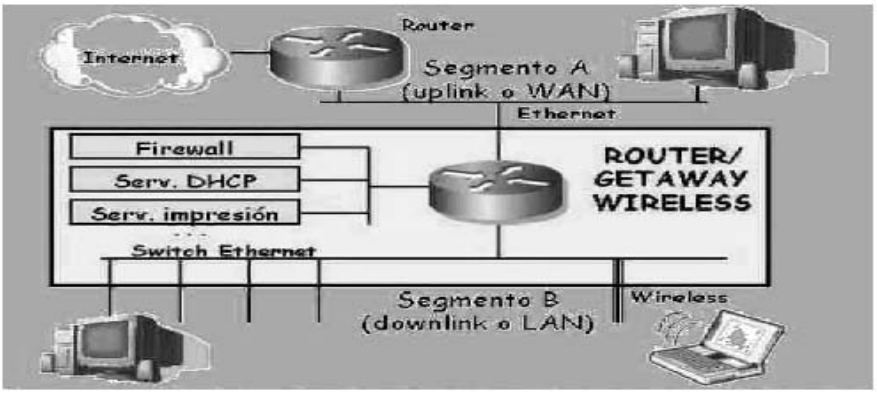

Figura 3.8: Routers y Gateways[15]

3.10. Conclusiones

En este capítulo se estudiaron los 3 tipos de estándares de la IEEE para las redes inalámbricas(a, b, g), se explico su manera de funcionar, sus ventajas, desventajas, y interoperatividad. Tambien se explico cada uno de los instrumentos que se necesitan para crear una red inalámbrica como son access point, router, punte, antenas.

Capítulo 4

Protocolos de seguridad

4.1. Introducción

En este capítulo se describen los problemas de seguridad más comunes en las redes inalámbricas asi como las recomendaciones y protocolos más recomendados para la seguridad de estas.

Las amenazas a la seguridad de la información atentan contra su confidencialidad, integridad y disponibilidad. Existen amenazas relacionadas con fallas humanas, con ataques malintencionados. Mediante la materialización de una amenaza podria ocurrir el acceso, modificación o eliminación de información no autorizada; la interrupción de un servicio o el procesamiento de un sistema; daños físicos o robo del equipamiento y medios de almacenamiento de información.

Hoy en día no basta que un experto en computadoras sea un pirata informático. Existen demasiados sitios en internet orientados hacia la piratería que ofrecen programas y scripts de piratería fáciles de descargar con tan solo pulsar el botón derecho del mouse. Estas herramientas de fácil acceso han dejado las puertas abiertas a una gran cantidad de nuevos ataques. A medida que las redes inalámbricas han ido ganando popularidad, se hace más necesario fortalecer la seguridad de las mismas es asombroso ver como empresas o personas que instalan su red inalámbrica no cifran la señal.

Esto es equivalente a dejar abierta la puerta para que cualquier persona con una computadora portátil debidamente equipada y cerca a su organización pueda leer todo lo que pasa por la red interceptando las ondas de radio.

Es responsabilidad de los diseñadores y administradores de los sistemas computacionales, proveer la suficiente garantía y confiabilidad que nos permita operar en las mejores condiciones y lograr un funcionamiento continuo de los sistemas bajo el mejor clima de confianza de nuestros usuarios, garantizando el respeto por niveles adecuados de confidencialidad e integridad de la información que procesamos.

Incidentes como el robo de información, espionaje industrial, estafas, extorsión, daño de sistemas son los objetivos de ataques a nuestros sistemas. Definitivamente si queremos minimizar los riesgos (nunca hay un sistema totalmente protegido), debemos tomar conciencia del problema y adoptar una metodología o guías para enfrentarlo. Esto comienza con el conocimiento profundo de nuestra red, un análisis de amenazas y riesgos, la adoptación de políticas de seguridad y finalmente la utilización de las tegnologías adecuadas para implementar nuestro sistema de seguridad, el cual incorpora herramientas de criptografía, cortafuegos, monitoreo, auditoría y hasta esquemas proactivos que nos permitan adelantarnos a los ataques y prevenirlos.

4.2. Amenazas y ataques

Para analizar el contexto de la seguridad en redes inalámbricas, definiremos un sistema informático como un conjunto de elementos hardware, software, datos/información y personal que hacen posible el almacenamiento, proceso y transmisión de la información con el objetivo de realizar una determinada tarea. Todos estos elementos son susceptibles de ser atacados y sobre ellos tenemos una serie de amenazas.

Aunque son varios los elementos que conforman un sistema informático, será la información el recurso más preciado sober el cual enfocaremos todos los esfuerzos para asegurar un nivel aceptable de seguridad. Por esto se definen los objetivos básicos de la seguridad de la información:

1. **Confidencialidad:**Asegurar que la información no es expuesta a personas no autorizadas.

2. **Integridad:**Asegurar consistencia de los datos, en particular prevenir la creación, alteración o borrado de datos de entidades no autorizadas.

3. **Disponibilidad:**Asegurar que los usuarios legítimos no obtengan acceso denegado a su información y recursos.

4. **Uso legitimo:**Asegurar que los recursos no son usados por personas no autorizadas o en formas no autorizadas.

5. **Configurar los AP debidamente:**Esto nos permite tener mayor control en cuanto a los accesos se refiere con nuestras redes inalámbricas.

Para soportar estos objetivos necesitamos definir las políticas de seguridad que regirán en nuestro dominio de seguridad. Estas políticas deben ser definidas en varias categorías: acceso físico, seguridad en la comunicación, computadoras, sistemas operativos, bases de datos, aplicaciones, personal, ambiente natural, respaldos, planes de contingencias etc.

Las amenazas pueden ser clasificadas en **Intencionales y Accidentales** siendo las primeras las más peligrosas. Las amenazas intencionales lo cual se convierte en un ataque, puede ser **Pasivo o Activo**.

Un ataque pasivo es aquel que no causa modificación o cambio en la información o recurso, son los más peligrosos ya que los fines que se alcanzan son más letales y beneficiosos para el que los comete. Los ataques activos, son aquellos que producen cambios en la información o en el comportamiento del sistema.

4.2.1. Clasificación de las amenazas

Podemos clasificar las amenazas en:

1. Amenazas fundamentales: Afectan directamente los cuatro objetivos básicos de la seguridad: fugas de información, violación a la integridad, negación de servicios y uso ilegítimo.

2. Amenazas habilitadoras de las primarias: Son importantes porque la realización de cualquiera de estas amenazas puede conducir directamente a la realización de las amenazas fundamentales. Estas son:

   a) Suplantación: Una persona pretende ser otra diferente. Es la forma más común de penetración al perímetro de seguridad.

b) Violación con autorización: Una persona autorizada para usar un sistema o recurso, lo utiliza para lograr un propósito no autorizado. Es conocido como amenaza interna.

c) Caballo de troya: Un software que contiene una parte invisible de código, la cual cuando es ejecutada comprende la seguridad del sistema.

d) Virus: Son programas que se autoreplican y afectan principalmente los archivos ejecutables, llegan a afectar miles de computadoras.

4.2.2. Métodos de detección de Redes Inalámbricas

Existen métodos para la detección de una red inalámbrica, mencionaremos algunos de ellos:[9]

4.2.2.1 Wardriving

Propio para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas o de papas fritas) un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas(AirSnort para Linux, NetStunbler para windows), que se consigue libremente en la internet (fig 4.1, 4.2).[9]

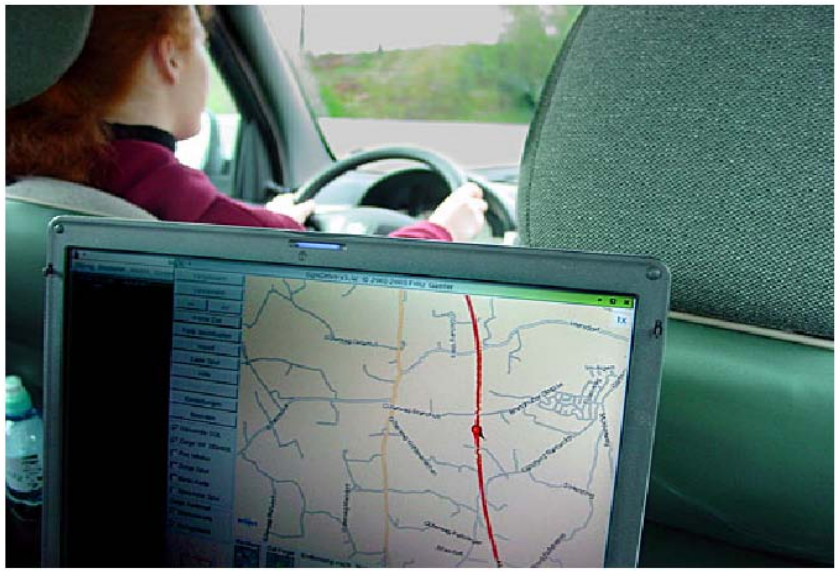

Figura 4.1: Wardriving [9]

Figura 4.2: Wardriving [9]

4.2.2.2 Warchalking

Consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial con sus caracteristicas en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red y utilizarla si es que pasan por allí.

Por ejemplo:

Xarxa

)(

1.5

Indicaría un nodo abierto o sea red de acceso libre, que utiliza el SSID Xarxa y esta es la contraseña para acceder a le red y que dispone de u ancho de banda de 1.5Mbps. Esta simbología permite disponer de un mapa donde se constan los puntos de acceso con sus datos(SSID, WEP, direcciones MAC)(fig 4.3).

Figura 4.3: Warchalking y su simbología [9]

4.2.2.3 Sniffing

Monitorización de redes, análisis de tráfico o detección de intrusos, son desde algún punto de vista, más o menos el objetivo de la diferentes técnicas que usan los administradores de red o los hackers basadas en el arte del sniffing para comprobar la seguridad intrínseca de una red.

Un sniffer o más concretamente un sniffer de paquetes, se define como una pieza de software o hardware que se conecta a una red informática y supervisa todo el tráfico que pasa por el cable. Al igual que los dispositivos de intervención de teléfonos que usan las autoridades para escuchar conversaciones de otras personas, un programa sniffing permite a alguien escuchar las conversaciones entre computadoras que fluyen por las redes.

Las conversaciones entre ordenadores consisten en aparentemente, datos binarios aleatorios. Por lo tanto los programas de intervención necesitan disponer de una caracteristica denominada **análisis de protocolo**, la cual permite decodificar el tráfico enviado y darle sentido para hacerlo de alguna manera legible.

El arte de sniffing tiene una gran ventaja sobre las intervenciones telefonicas:la mayoría de las redes aún usan topologías de red compartidas. Esto quiere decir que no es necesario que el ordenador al cual se quiere monitorizar deba estar situado en las proximidades, simplemente si está conectado al mismo cable será susceptible de ser interveido. Esto se conoce como un sniffer en modo promiscuo.

En cambio, la tecnología compartida (usan hubs) está rápidamente desplazándose a tecnología conmutada (switches), donde estas tácticas ya no son posibles, aún así, existen varias técnicas de sniffing usadas en redes conmutadas que pueden servir para saber si sus datos viajan de una manera segura.

4.2.2.4 Eavesdropping

La interceptación o eavesdropping, también conocida por passive wiretapping es un proceso mediante el cual un agente capta información -en claro o cifrada- que lo le iba dirigida; esta captación puede realizarse por muchísimos medios (por ejemplo, capturando las radiaciones electromagnéticas.)

Aunque es en principio un ataque completamente pasivo, lo más peligroso del eavesdropping es que es muy difícil de detectar mientras que se produce, de forma que un atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta hasta que dicho atacante utiliza la información capturada, convirtiendo el ataque en activo.[6]

4.2.2.5 Snooping y Downloading

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes ,además de interceptar el tráfico de red ,el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en a mayoría de los casos un downloading de esa información a su propia computadora.

El snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataque fueron:el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa y la difusión ilegal de reportes oficiales reservados de la naciones unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.[11]

4.2.2.6 Tampering o Data Dibbling

Esta categoría se refiere a la modificación desautorizada de los datos o al software instalado en un sistema, incluyendo borrado de archivos.

Este tipo de ataques son particularmente serios cuando el que los realiza ha obtenido derechos de administrador o supervisor, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada, o aún si no hubo intenciones de ello, el administrador posiblemente necesite darse de baja por horas o dias hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders o outsiders, generalmente con el propósito de fraude o dejar fuera de servicio a un competidor.

Son innumerables los casos de este tipo como empleados(o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes o contribuyentes que pagan para que se les anule la deuda por impuesto en el sistema municipal.

Múltiples web sites han sido víctimas del cambio de sus home pages por imágenes terroristas o humorísticas o el reemplazo de versiones de software para download por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos esta dentro de esta categoría y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de internet como el caso de Back Orifice y NetBus de reciente aparición.

4.2.2.7 Honeypots

Consiste en activar un servidor y llenarlo de archivos tentadores y hacer que sea difícil, pero no imposible penetrarlo y sentarce a esperar que aparezcan los intrusos. Los honeynets(conjunto de honeypots) dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos, ellos juegan con los archivos y conversan animadamente entre ellos sobre todos los fascinantes programas que encuentren,mientras el personal de seguridad observa con deliete cada movimiento que hacen.

Un honeypot es un sistema diseñado para analizar cómo los intrusos emplean sus armas para intentar entrar en un sistema (analizan la vulnerabilidades) y alterar, copiar o destruir sus datos o la totalidad de estos (por ejemplo borrando el disco duro del servidor). Por medio del aprendizaje de sus herramientas y métodos se puede, entonces, proteger mejor los sistemas.

Pueden constar de diferentes aplicaciones ,una de ellas sirve para capturar al intruso o aprender como actúan sin que ellos sepan que estan siendo vigilados.

También existe el honeynet que es un conjunto de honeypots, asi abarca más información para su estudio. Incluso hace más emocionante el ataque al intruso, lo cual incrementa el número de ataques.

4.2.2.8 Dirección MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica, dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única,se logra autentificar el equipo.

Debido a que numerosas máquinas pueden tener acceso a un mismo segmento de una red ethernet, cada una de ellas debe disponer de un identificador único. Esto se lleva a cabo usando un número de 12 dígitos representado normalmente en forma hexadecimal, o lo que es igual, un número de 48 bits.

Las siglas MAC hacen referencia a Media Access Control (control de Acceso del medio) y es básicamente la dirección Ethernet de un adaptador en concreto.

Los primeros 24 bits del número MAC hacen referencia al fabricante de la tarjeta de red y los siguientes 24 bits representan una tarjeta única asignada por el fabricante. La identificación del fabricante se llama OUI (Organizationally Unique Identifier). De esta forma se asegura que no existan dos tarjetas de red con las mismas direcciones MAC.

A continuación en la tabla 4.1 se mencionan los tipos de amenazas que existen y en la tabla 4.2 se da un resumen de los métodos de detección de redes inalámbricas.

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

Tabla 4.1: Principales amenazas de las redes inalámbricas

	Definición	**Acciones y Componentes**
Wardriving	Paseo por una ciudad o centro de negocios para verificar puntos de acceso donde imaginemos se esta utilizando una red inalámbrica.	• Tarjeta de red inalámbrica • Computadora portátil • Software • Mapas • Antenas
Warchalking	Es un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de redes inalámbricas.	• Gis • Lenguaje de símbolos.
Sniffing	Monitorización de redes, análisis de trafico o detección de intrusos.	• Análisis de trafico a través de ondas de radio. • Uso para detección de intrusos o para hachear una red. • Decodifica el trafico capturado que recibe,es solo de escucha.
Snooping o Downloading	Mismo objetivo que el sniffing además de interceptar el tráfico de red, el atacante ingresa a los documentos.	• Realiza en la mayoría de los casos downloading de información a su propia computadora.
Tampering o Data Diddling	Mismo objetivo que el sniffing solo que refiere a la modificación desautorizada de los datos.	• Ejecución de cualquier comando en la computadora atacada. • Propósito, dejar fuera de servicio la computadora • Los troyanos están incluidos en esta categoría
Honeypots	Es una trampa para los saboteadores solo que ellos no se dan cuenta. El administrador de la red tiene el control.	• Activa un servidor para llenarlo de archivos tentadores • Son trampas para posibles saboteadores • El administrador de la red observa cada movimiento del intruso • Captura al intruso y aprende como actúa sin que ellos sepan que están siendo vigilados.

Tabla 4.2: Principales métodos de detección de redes inalámbricas

4.3. Inseguridad en las redes inalámbricas

Desafotunadamente por simple omisión. La seguridad en muchas organizaciones, inclusive organizaciones muy grandes, es relegada dándole muy baja prioridad o hasta ignorándola por completo. Es desafortunadamente demasiado común ver grandes organizaciones en las que no se ha tomado ni las mas básicas precauciones relativas a la seguridad y a nadie sorprende cuando reportan pérdidas millonarias por un ataque.

¿Por que es tan común que siendo tan importante y tan simple la seguridad es relegada? En mi opinión, esto no puede calificarse más que de negligencia, si bien no me es posible justificar que una organización no invierta en la seguridad adecuada para su red, si puedo entender que hasta que no tengan un primer incidente importante no contraten a un equipo dedicado a seguridad.

Sin embargo, el no configurar los aspectos más básicos de seguridad en una red inalámbrica, los cuales pueden ser implementados sin costo adicional, no puede calificarse más que de negligencia.

4.4. Seguridad y privacidad de las redes inalámbricas

Si usted escoge una solución con sofisticadas tecnologías de seguridad, sus comunicaciones inalámbricas serán muy seguras.Las soluciones líderes ofrecen encriptación de 128 bits y para los niveles más altos de seguridad, los sistemas más avanzados generarán automáticamente una clave de 128 bits para cada sesión de red inalámbrica. Estos sistemas tambien ofrecerán autentificación de usuarios, requiriendo que cada usuario ingrese con una contraseña.

El cliente y el punto de acceso deben establecer una relación antes de poder intercambiar datos .Esta relación puede utilizar tres estados diferentes:

1. Sin autentificación y desasociado.

2. Con autenticación y desasociado.

3. Con autenticación y asociado.

El intercambio de datos reales sólo es posible en el tercer estado. El AP transmite tramas con señales de gestión en periodos de tiempos regulares. Las STA reciben estas tramas e inician la autenticación mediante el envío de una trama de autenticación.Una vez realizada satisfactoriamente la autenticación, la STA envía la trama asociada y el AP responde con otra trama asociada.

4.5. Mecanismos de seguridad

4.5.1. WEB(Wired Equivalent Protocol)

WEB(Wired Equivalent Privacy,privacidad equivalente a cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEB, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes inalámbricas.

WEB utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no completa ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios incovenientes. Por un lado, la clave esta almacenada en todas las estaciones, aumentando las posibilidades de que sea comprendida.Y por otro lado, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva en mayoría de ocasiones, que la clave se cambie poco o nunca.[29]

El algoritmo de encriptación utilizado es RC4 con claves(seed), según el estándar de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente.El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama.

El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que esta almacenado en la configuración de cada elemento de red. El IV en cambio se genera en un extremo y se envía en la propia trama al otro extremo, por lo que tambien será conocido.Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEB es el siguiente:

1. Se calcula un CRC de 32 bits de los datos.Este CRC-32 es el método que propone WEB para garantizar la integridad de los mensajes (ICV,integrity Check Value).
2. Se concatena la clave secreta a continuación del IV formado el seed.
3. El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorio(keystrem), a partir del seed, de la misma longitud que loos bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3.El resultado es el mensaje cifrado.
5. Se envía el IV(sin cifrar)y el mensaje cifrado dentro del campo de datos (frame body) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el seed y con ello podra generar el keystream. Realizando el XOR entre los datos recibidos y el keystream se obtendra el mensaje sin cifrar (datos y CRC-32). A continuación se comprobará que el CRC-32 es correcto.

4.5.1.1 Debilidad del vector de inicialización

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la clave (seed) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica cómo manejar el IV. Según se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello.Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos.La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama.Y esto ocasiona que los primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de IVs diferentes no es demasiado elevado, por lo que terminarán repitiéndose en cuestión de minutos u horas [6]. El tiempo será menor

cuanto mayor sea la carga de la red.Lo ideal sería que el IV no se repitiese nunca, pero como vemos, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red. Observemos que es trivial saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática.

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

¿Qué podemos hacer una vez hemos capturado varias tramas con igual IV, es decir, con igual keystream? necesitamos conocer el mensaje sin cifrar de una de ellas.Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV.Conociendo el keystream asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráficos predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.).

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los IVs de los que sabemos su keystream, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla.

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP [7] permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar suficientes IVs y sus keystreams asociados obtenidos por el procedimiento anterior.

4.5.1.2 Otras debilidades de WEP

WEP también adolece de otros problemas además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos más arriba, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado

que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que el destino se percatará de ello. En lugar del algoritmo de CRC se recomienda como ICV (Integrity Check Value) un algoritmo diseñado para tal fin como SHA1-HMAC.

El estándar IEEE 802.11 incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación. Una estación que quiere unirse a una red, solicita al punto de acceso autentificación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de autentificación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas más arriba.

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso tendríamos una autentificación de sistema abierto, es decir, sin autentificación.

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (replay). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica. El estudio de N. Borisov, I. Goldberg y D. Wagner explica razonadamente que ninguno de los objetivos planteados por WEP se cumplen.

4.5.1.3 Alternativas a WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como WEP2. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera.WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada enquad algunas implementaciones es WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP/ RADIUS. Requiere un servidor de autentificación (RADIUS normalmente) funcionando en la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP. Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperatibilidad entre dispositivos de distintos fabricantes.[30]

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA y WPA2 (IEEE 802.11i). El primero es de 2003 y el segundo se espera para 2004. Se estudian a continuación.

4.5.2. WAP(Wi-Fi Protected Access, Acceso Protegido Wi-Fi)

Es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar. El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la

norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales. WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

4.5.2.1 Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación. WPA incluye las siguientes tecnologías:

o IEEE 802.1X. Estándar del IEEE [10] para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP [11] y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service) [12]. Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

o EAP. EAP, [11], Es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol) [13], aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN) [10].

o TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama [4].

o MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas [4].

4.5.2.2 Modos de funcionamiento de WPA

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay). Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP. Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

4.5.2.3 Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

- **Con servidor AAA, RADIUS normalmente.** Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

- **Con clave inicial compartida (PSK).** Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

4.5.3. WPA2 (IEEE 802.11i)

802.11i [3] es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mediados de 2004. Wi-Fi [4] está haciendo una implementación completa del estándar en la especificación WPA2. Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa. WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS [14]. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC. Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

4.5.4. OSA(Open System Authentication)

Es otro sistema de autentificación definido por el estándar 802.11 para autentificar todas las peticiones que rebibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente,además las tramas de gestión son enviadas sin encriptar,aún activando WEP, por lo tanto es un mecanismo poco confiable

4.5.5. ACL(Access Control List)

Este mecanismo de de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autentificación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la lista de control de acceso.

4.5.6. CNAC(Closed Network Access Control)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID)actuando este como contraseña.[6]

Mecanismos de seguridad	Descripción
Especificación original 802.11	Utiliza tres mecanismos para proteger las redes WLAN: - SSID (Identificador de Servicio):Es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para accesar a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía (beacon). - Filtrado con dirección MAC (Control de Acceso al Medio):Restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico. -WEP (Privacidad Equivalente a Cable):Es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.
802.11X	Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autenticación remota de usuarios entrantes RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes).

Tabla 4.3: Mecanismos de seguridad de las redes inalámbricas

Mecanismos de seguridad	Descripción
WAP(Wi-Fi Protected Access)	Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de llaves integras -Seguras-Temporales). TKIP fue construido tomando como base el estándar WEP, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles.EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación. Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi. Esta especificación proporciona una mayor encriptación de datos para corregir las vulnerabilidades de seguridad WEP, además de añadir autenticación de usuarios que no se habían contemplado.

Tabla 4.4: Continuación, Mecanismos de seguridad de las redes inalámbricas

4.6. Encriptación

Toda encriptación se encuentra basada en un algoritmo, la función de este algoritmo es básicamente codificar la información para que sea indescifrable a simple vista, de manera que una letra A pueda equivaler a:"5x5mBwE"ó bien a "xQE9fq", el trabajo del algoritmo es precisamente determinar como será transformada la información de su estado original a otro que sea muy difícil de descifrar. Una vez que la información arrive a su destino final, se aplica el algoritmo al contenido codificado "5x5mBwE"ó bien a "xQE9fq [2]resulta en la letra A ó según sea el caso, en otra letra. Hoy en día los algoritmos de encriptación son ampliamente conocidos,es por esto que para prevenir a otro usuario "no autorizado"descifrar información encriptada, el algoritmo utiliza lo que es denominado llave ("key") para controlar la encriptación y decriptación de información. Algunos algoritmos son DES (algoritmo simétrico) AES que posiblemente suplantará a DES y uno de los más conocidos RSA (algoritmo asimétrico).[6]

Existen dos tipos de llaves (keys) , pero la de mayor uso en internet es denominada "public key.º algoritmo asimétrico. El nombre public proviene de su funcionamiento: existe una llave pública que es dada a conocer a cualquier persona que así lo desee (todo internet), esta llave pública es utilizada por los emisores de mensajes para encriptar información, sin embargo, existe otra llave (su pareja por llamarla de alguna manera) única que es conocida exclusivamente por el destinatario del mensaje, y es mediante esta llave única secreta que el destinatario descifra (decripta) los mensajes encriptados por el emisor.

4.6.1. Firmas digitales(Digital Signatures)

Una firma digital utiliza el mismo funcionamiento del public key ó algoritmo asimétrico mencionado anteriormente. Como se mencionó, existe una llave pública y una llave secreta, en el caso de firmas digitales la llave pública que es ampliamente conocida es capaz de identificar si la información proviene de una fuente fidedigna. En otras palabras, la llave pública será capaz de reconocer si la información realmente proviene de la llave secreta en cuestión. Ejemplo: El departamento de compras posee las llaves públicas de todos los empleados de la compañía, si llega un pedimento con la dirección de email del director de finanzas, ¿como puede asegurarse el departamento de compras que en realidad esta persona realizó el pedimento y no alguna otra que sobrepuso el email ?. La llave secreta del director de finanzas debe de encontrarse solo en su computadora, por lo tanto al enviar el mensaje electrónico esta llave pública se añadió al email,y por lo tanto las llave publicas determinarán si la llave secreta coincide con la del director.

4.6.2. Firmas digitales en Internet

En el caso anterior de un Intranet, todas las llaves públicas provienen de una fuente fidedigna, esto es, las llaves "publicas"que posee el departamento de compras son autenticas ya que TODAS pertenecen sólo a empleados dentro de la compañía, la única posibilidad de fraude que existe, es si alguien trata de forjar la "llave secreta"de un empleado para hacerse pasar por otro.

4.6.3. Encriptación de 40-bits y 128-bits

Existen varios niveles de encriptación, pero las combinaciones más comunes son 40-512 bits ("llave secreta–llave pública") y 128-1024 bits ("llave secreta–llave pública"). La versión 128-1024 bits es el tipo de encriptación más fuerte que existe en el mercado. Actualmente U.S.A prohibe la exportación de productos con este tipo de tecnología, pero cabe mencionar que ya existen varios productos producidos en Europa con esta Tecnología que no poseen tales restricciones de exportación.

La gran mayoría de los sitios en internet utilizan la encriptación 40-512 bits, la encriptación 128-1024 bits es utilizada generalmente en transacciones de alto riesgo, como las bancarias.

4.7. Algunas técnicas para encriptar los datos

Mientras un administrador de redes puede emplear mucho tiempo en consegir que su red sea difícil de ser atacada mediante sniffers utilizando firewalls, switches, detectores de modo promiscuo,etc, lo cierto es que la mejor forma de protegerse ante estos ataques es la de encriptar el tráfico de red.

Algunas técnicas son las siguientes:

Secure Sockets Laser(SSL) Está presente en todos los Web populares así como en los servidores HTTP más conocidos. Sus ventajas ya han sido discutidas en numerosos artículos, pero para resumir diremos que permite una navegación encriptada no vulnerable a los sniffers.

Por ello, este tipo de seguridad es utilizada en internet para transmitir información privada de los usuarios, como por ejemplo el número de la tarjeta de crédito.

PGP y S/MIME El correo puede ser interceptado de muchas formas alternativas. Tenga en cuenta que un correo electrónico necesita para llegar a su destino atravesar distintos servidores de red, firewalls y routers. Por ello, la posibilidad de que alguien pueda leer el correo es muy elevada si se envía sin ningún sistema de encriptación.

Los métodos más comunes para realizar esto son PGP(Pretty Good Privacy) y S/MIME(segure MIME). PGP puede usarse como un añadido a diferentes productos y S/MIME esta incluido en la mayoría de los nuevos gestores de correo como Outlook o Netscape, aunque dentro de internet puede encontrar ambos productos para implementarlos en sus clientes(en páginas dedicadas a encriptación).

Secure Shell(Ssh) se ha convertido en el estándar de facto para acceder remotamente a servidores UNIX a través de internet.

Si aún sigue utilizando el protocolo telnet, debería remplazarlo inmediatamente con este servicio. El producto fue diseñado por una compañia filandesa pero se puede encontrar en muchas implementaciones freeware.

4.8. Políticas de seguridad

Aparte de las medidas que se tomen en el diseño de la red inalámbrica, debemos aplicar ciertas normas y políticas de seguridad que nos ayudarían a mantener una red más segura:

1. Utilizar WEP,aunque sea rompible con herramientas como AirSnort ó WEPCrack, como un mínimo de seguridad.
2. Utilizar mecanismos de intercambio de clave dinámica aportado por los diferentes productos comerciales hasta que el comité 802.11i, encargado de mejorar la seguridad en las redes inalámbricas, publique una revisión del estándar 802.11 con características avanzadas de seguridad, incluyendo AES (Advanced Encryption Standar) e intercambio dinámico de claves.
3. Inhabilitar DHCP para la red inalámbrica. Las IPs deben ser fijas.
4. Actualizar el firmware de los puntos de acceso para cubrir los posibles agujeros en las diferentes soluciones wireless .
5. Proporcionar un entorno físicamente seguro a los puntos de acceso y desactivarlos cuando se pretenda un periodo de inactividad largo (ej, ausencia por vacaciones).

6. Cambiar el SSID(server set ID) por defecto de los puntos de acceso, conocidos por todos. El SSID es una identificación configurable que permite la configuración de los clientes con un determinado punto de acceso.
   Actúa como un password compartido entre la estación cliente y el punto de acceso. Ejemplos de SSID por defecto son "tsunami"para cisco, "101"para 3com,"intel"para intel.
7. Inhabilitar la emisión broadcast del SSID.
8. Reducir la popagación de las ondas de radio fuera del edificio con pintura metálica.
9. Utilizar IPSec, VPN, firewalls y monitorizar los accesos a los puntos de acceso.

4.9. Problemas típicos de seguridad y soluciones recomendadas

La rápida expansión de las redes inalámbricas (wireless) basadas en los estándares 802.11 han añadido un nivel adicional de complejidad al problema de la seguridad de redes. Aunque los mencionados estándares incorporan ciertas funciones de seguridad y que los diferentes fabricantes de equipos inalámbricos han añadido diferentes mecanismos de protección, las redes inalámbricas representan un punto extremadamente vulnerable en la seguridad de una red.

Problema 1: Puntos de Acceso Vulnerables: Las redes inalámbricas son fáciles de detectar. Con el objetivo de facilitar la conexión a los usuarios las redes emiten gran cantidad de información acerca de su configuración. Esta información es exactamente lo que un hacker necesita para lanzar un ataque. Las redes 802.11 no utilizan ninguna función de seguridad para proteger esta información. Por tanto cualquier usuario con tarjeta inalámbrica estándar 80.11 puede acceder a estos datos. Atacantes con antenas amplificadoras pueden hackear a redes ubicadas en otros edificios y a algunas calles de distancia.

Solución: La solución ideal sería aislar la red inalámbrica de forma que las emisiones electromagnéticas de la red no salieran fuera del perímetro de la empresa o fuera de las habitaciones en las que se utilice la red. Sin embargo para la mayoría de las empresas esta no es una solución factible.

En muchos casos una solución eficiente es utilizar VPNs en la comunicación con los usuarios (para proteger el contenido de las transmisiones y poder contar con el sistema de autentificación del servidor de VPNs).

Otra medida de seguridad adicional es autentificar el acceso de los usuarios a través de la red inalámbrica con un servidor de autentificación. Por ejemplo, el estándar 802.1x soporta nuevos tipos de autentificación para integraciones con servidores RADIUS.

Problema 2: Puntos de Acceso no Autorizados: Las redes inalámbricas son fáciles de implementar y su precio está al alcance de cualquier usuario. Es relativamente sencillo comprar e instalar un punto de acceso inalámbrico sin que este sea advertido por los administradores de la red. En algunas ocaciones un departamento dentro de la empresa puede decidir instalar sus propios puntos de acceso sin coordinar dicha instalación con los responsables de seguridad.

Al funcionar prácticamente tan pronto se conecta, la mayoría de puntos de acceso inalámbrico instalados sin supervisión utilizan la configuración por defecto. El problema principal es que esta configuración normalmente carece de todas las medidas de seguridad aplicables.

Solución: Auditar las oficinas de la empresa de forma regular con un detector de redes inalámbricas o un wireless Analyzer. Por ejemplo esto puede implicar asignar de forma regular un técnico para que se pasee por las oficinas con un ordenador portátil o una agenda personal PDA, equipada con una herramienta para la detección de puntos de acceso wireless.

Existen varias herramientas en el mercado para el escaneo de redes inalámbricas. Algunas funcionan de forma pasiva detectando fuentes de emisión y analizando los datos tranmitidos, mientras que otras intentan interrogar a los puntos de acceso que encuentran buscando información sobre los mismos.

Problema 3: Accesos a la Red no Autorizados: Muchas instalaciones de redes inalámbricas utilizan la configuración por defecto de los equipos realizando los cambios mínimos para que funcionen. Por lo general estas configuraciones no hacen uso de la encriptación WEP(incluida en el estándar 802.11).

Sin WEP es prácticamente inmediato acceder a la red 802.11 aunque se haya restringido el acceso mediante listas de códigos MAC autorizados. Un hacker equipado con un sniffer puede obtener direcciones MAC válidas en cuestión de segundos, realizar un spoof (falcificación) de la dirección MAC de su tarjeta wireless utilizando la de una tarjeta con acceso autorizado y entrar en la red.

Solución: La mejor forma para impedir los accesos no autorizados es utilizar un mecanismo de autentificación fuerte protegido mediante encriptación. Por ejemplo, Transport Layer Security (TLS), Protected EAP (PEAP)o Tunneled TLS (TTLS).

Problema 4: Análisis de Tráfico y Sniffing: Nada impide a un atacante el "escuchar"el tráfico de radio de una red wireless y observar el tráfico de forma pasiva. Armandon con esta información o utilizando un analizador de redes,un hacker puede averiguar toda la información necesaria para realizar el ataque.

El protocolo 802.11 no dispone de ningún mecanismo para evitar que los datos transmitidos sean interceptados. Desafortunadamente el Wired Equivalente Privacy (WEP), que inicialmente tenía que prevenir estos problemas, solamente encripta una parte de los paquetes. Los paquetes de datos para el control y gestión de las transmisiones no son encriptados ni autentificados. Además, el sistema de encriptación utilizado por WEP tiene fallos y es fácilmente descifrable.

Las implementaciones actuales de WEB han corregido muchos de los fallos originales que permitían a un usuario equipado con las herramientas WEBcrack o AirSnort calcular las claves criptográficas en unos pocos minutos. Algunos fabricantes tambien han implementado un sistema para cambiar las claves WEP cada 15 minutos. De esta manera aunque la red genere grandes cantidades de datos, estos no son suficientes para poder descifrar las claves WEP antes de que éstas sean cambiadas.

Solución: Al igual que en el punto anterior, la mejor solución es emplear protocolos seguros como el SSH, SSL que son para encriptar datos o el protocolo IPSec. Solamente el uso de estos protocolos seguros puede garantizar la seguridad contra escuchas e interceptación del tráfico.

4.10. Consejos de seguridad

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

1. Cambiar las claves por defecto cuando instalemos el software del Punto De Acceso.

2. Control de acceso seguro con autentificación bidireccional.

3. Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.

4. Configuración WEP (muy importante), la seguridad del cifrado de paquetes que se transmiten es fundamental en la redes inalámbricas, la codificación puede ser mas o menos segura dependiendo del tamaño de la clave creada y su nivel, la mas recomendable es de 128 Bits.

5. Crear varias claves WEP ,para el punto de acceso y los clientes y que varíen cada día.

6. Utilizar opciones no compatibles, si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro.

7. Radio de transmisión o extensión de cobertura, este punto no es muy común en todo los modelos, resulta mas caro, pero si se puede controlar el radio de transmisión al circulo de nuestra red podemos conseguir un nivel de seguridad muy alto y bastante útil.

Todos estos puntos son consejos, las redes inalámbricas están en pleno expansión y se pueden añadir ideas nuevas sobre una mejora de nuestra seguridad.

4.11. Conclusiones

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite la seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información. Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), de si es una red

ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores.

La restricción de acceso mediante direcciones MAC es insuficiente para cualquier red, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta cualquiera. El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico. Tanto la especificación WPA como IEEE 802.11i solucionan todos los fallos conocidos de WEP y, en estos momentos, se consideran soluciones fiables. La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos.

El uso de las VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.La alternativa de 802.1x y EAP es la adecuada si los equipos de la red inalámbrica se pueden actualizar, o si se va a montar una red nueva.Puede usarse la solución de WEP con clave dinámica, o la de WPA; ambas ofrecen un excelente grado de protección.Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa.

Capítulo 5

Proyecto aplicado a Mercado Soriana(Tutelar 136)

5.1. Introducción

En este capítulo explicaremos el funcionamiento de la red alámbrica del centro comercial CECOSORI asi como sus funciones en cada una de sus áreas, y asi después implementaremos la tecnología inalámbrica.

Hoy en dia es clara la alta dependencia en las actividades empresariales e institucionales de las redes de comunicación, por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad. Así mismo la red puede ser más extensa sin tener que mover o instalar cables, respecto a la red tradicional la red sin cable ofrece muchas ventajas como lo mencionamos en el capítulo 2.

5.2. Consideraciones de desempeño para una red inalámbrica

Una vez que se ha decidido añadir un sistema inalámbrico a su red, necesita determinar como debe empezar y que productos necesita usar. En la mayor parte de las tecnologías de red, los fabricantes piensan en el desempeño e interoperatibilidad de sus productos. Los clientes buscan una solución que ofrezca un desempeño alto y una interoperatividad completa. Una de las mejores formas de hacer una red inalámbrica es tomando en cuenta el aspecto de la seguridad, es seleccionar un fabricante que tambien considere la seguridad.

El primer paso para diseñar cualquier red es determinar el objetivo de ella y las necesidades de los usuarios, para una WLAN esto es la definición del área de cobertura.Por lo tanto al principio e la etapa de planeación debe de determinar los puntos importantes en los que los usuarios estarán ubicados, además de las rutas más comunes entre la ubicaciones principales de reunión como por ejemplo, salas de junta, de conferencia, oficinas de personal importante, para esto se necesita contar con un diagrama adecuado de las instalaciones que muestre la cobertura que necesita tomarse en cuenta para la WLAN.

También se debe de determinar las velocidades mínimas que requieren los usuarios. En relación con este aspecto, debe tener una descripción de las aplicaciones que los usuarios ejecutan. Obiamemte que todos diran que se necesitan 100 Mbps, o que equivale a lo que ofrece una red de cables, pero la tecnología inalámbrica no usa un medio conmutado, usa un medio compartido, por lo tanto no todas las aplicaciones se ajustarán al sistema WLAN.

Es poco probable que todos los usuarios en una LAN usen el mismo dispositivo. Por lo tanto se debe derterminar si los usuarios necesitan dispositivos especiales en el sistema inalámbrico, por ejemplo, servidores de impresión, lectores de códigos de barras,tarjetas PCI, tarjetas PCMCIA, si es asi deberá de decidir si es necesario comprar todos los dispositivos del mismo fabricante o de fabricantes distintos.

Antes de tomar una decisión debemos de hacer una lista de preguntas y responderlas: (Las respuestas son conforme a nuestra aplicación)

- ¿Cuales son las aplicaciones actuales que se usarán y cual es su rendimiento de ancho de banda por usuario?

  Para aplicaciones normales de oficina(MS,office, correo electrónico, acceso a la base de datos.)El ancho de banda de un sistema 802.11g normal sera suficiente.

- ¿Cual es la cantidad promedio y maxima de los usuarios WLAN en un área de cobertura predeterminada? y ¿es posible que esta cantidad aumente con el tiempo?

  Alrededor de 40 usuarios en total tiempos diferentes, para un promedio de 10 usuarios por AP (4).

- ¿A que área físicas planea proporcionar el acceso WLAN?

  Cobertura máxima, cubrir áreas internas y externas.

- ¿Los puntos de acceso necesitan estar colocados en el techo o en ubicaciones seguras que no esten al alcance de la vista?

  En el techo por estética del lugar, tambien por que en el interior hay sistemas de calefeccion, aire acondicionado, líneas eléctricas, instalación de iluminación, y estos pueden afectar el funcionamiento del equipo.

- ¿Quien determinara al fabricante del radio de los clientes-los usuarios o los administradores?

  Hay que elegir un equipo con interoperatividad alta, para que no importando el estándar haya comunicación, en este caso nos decidimos a utilizar el AP cisco 1200, compatible con los 3 estandares de IEEE, es un AP de banda dual.

- ¿Que tipos de dispositivos de cliente se usarán en la WLAN?

  Lectores de códigos de barras, computadoras, terminales móviles, impresoras de etiquetas, interfaces PCMCIA y mini-PCI, de preferencia puras mini-PCI por que las interfaces PCMCIA no son lo suficientemente rápidas como para proporcionar velocidades de 54 Mbps.

- ¿Cuales son las regulaciones que rigen el uso de 802.11 IEEE en esta región?

  En Mexico si estan permitidos los estándares b, g.

- ¿Existe algún elemento en la construcción del edificio que interfiera con la señal RF?

  Se hicieron pruebas en el sitio con ambas tegnologías para verificar su desempeño en el entorno, y no hay ningún problema con la estructura del edificio.

- ¿Dentro de las instalaciones se emplea algún otro equipo de 2.4 o de 5 Ghz, como por ejemplo sistemas de bluetooth, teléfonos inalámbricos, hornos de microondas, cámaras y alarmas de seguridad inalámbricas o cosas parecidas?

Si lectores de barras inalámbricos, y el servidor de impresión inalámbrico (ambos por bluetooth).

5.3. Selección de hardware para la red inalámbrica

Los puntos de acceso de CISCO se conectan de forma transparente a las redes inalámbricas de Intermec a través de las CCX (Cisco's Compatible Extensions).

- 4 AP de Cisco 1200 series Aironet (fig 5.1).
- 20 Cisco Aironet 350 series client adapter(segun el número de máquinas a utilizar le red inalámbrica (fig 5.2, 5.3).
- 4 antenas Cisco AIR-ANT5959, o Cisco AIR-ANT2506.
- Terminales móviles Intermec 700 serie color, ck30,o 730 color (fig 5.20).
- Impresoras portátiles Intermec pw40a, 6820 (fig 5.4).
- Impresoras Lexmark E340 (fig 5.5).
- Servidor de impresión inalámbrico Lexmark N4050e 802.11g (fig 5.6).
- Lectores de barras inalámbricos Intermec SR60, SR61 (fig 5.7).

Figura 5.1: AP Cisco 1200[35]

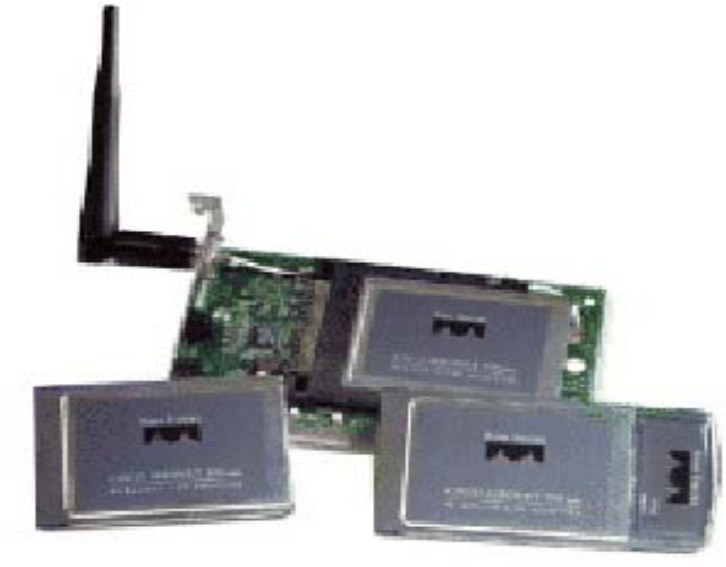

Figura 5.2: Cisco Aironet 350 series client adapter[35]

Figura 5.3: Cisco Aironet 350 series PCcard[35]

Figura 5.4: Impresora portátil Intermec[34]

Figura 5.5: Impresora Lexmark E340[36]

Figura 5.6: Servidor de impresión inalámbrico Lexmark[36]

Figura 5.7: Lector de códigos de barras inalámbrico Intermec[34]

5.4. Estructura de la red estructurada del centro comercial CECOSORI

Explicaremos el funcionamiento de la red del centro comercial CECOSORI, antes que nada diremos que es un espacio de $9000M^2$que tiene 33 computadoras en red, claro que de distinta manera, unas computadoras como las de linea de cajas estan en el sistema para punto de venta, el departamento de informes utiliza el sistema para devoluciones, el departamento de caja general el sistema de recolección de valores, el departamento de recibo utiliza el sistema de pedidos, el departamento de mesa de control como su nombre lo dice es el encargado de supervisar a todos los demás sistemas así como de realizar otras funciones como el control de mercancia que ingresa a tienda y trabajar conjuntamente con el departamento de recibo. Así todas las computadoras estan en red conectadas por medio de 3 rack de comunicaciones.

Antes que nada mencionaremos el trabajo que se realiza un cada uno de los departamentos donde se encuentran estaciones de trabajo. Primero hablaremos del departamento de mesa de control es aqui donde se controla la mayor parte del sistema. Este departamento cuenta con tres máquinas más la del administrador de sistemas,una es para controlar el acceso de los pedidos, llevar el inventario de toda la mercancia que entra y toda la mercancia que sale, otra maquina es la que se encarga de llevar el manejo de todos los departamentos, como por ejemplo sus pedidos, balances sus presupuestos, promociones, en esta maquina se controlan los precios de toda la tienda, tambien esta monitorea las terminales móviles.

Otra maquina es la que se utiliza para realizar cualquier documento, imprimir etiquetas, imprimir compares, dar copias de tickets, etc.

La maquina del administrador de sistemas es la maquina principal es la base de la tienda en esta se encuentra la mayor parte de información respecto al manejo de la tienda, asi como es el punto de enlace principal de la red, como a nivel tienda como a nivel corporativo. A esta maquina le envían todas las ofertas, correos electrónicos, avisos, noticas, cambios de todo tipo, mecanicas, actualizaciones. Así como tambien desde aqui se puede ingresar a cualquier maquina de la red y monitorearla y controlarla a la vez.

Otro departamento importante y que trabaja conjuntamente con mesa de control es el departamento de recibo que tiene a cargo el área de mesa de pedidos aqui es donde los jefes de departamento piden a los proveedores la mercancia necesarea para la tienda. Tenemos que tener en claro que cuando es un pedido de provedores

como coca, pepsi, sabritas, gamesa, lacteos, huevo, bimbo, etc; Estos llegan a la tienda provenientes de la misma ciudad por que estas empresas tienen distibuidoras en la mayor parte de las ciudades y tardan en llegar un dia. Cuando es un pedido a los CEDIS (centros de distribución, actualmente se cuenta con tres en todo el pais). se tarda segun sea los pedidos de la zona éste se refiere que si en la zona en la que se encuentra esta sucursal no hay pedidos se espera hasta que haya para aprovechar el viaje y sea un costo menor.

En resumen este departamento se encarga de pedir la mercancia.Una vez que llega la mercancia es recibido por mesa de control este autoriza el pedido y lo almacena en la base de datos, y se le entrega al departamento de recibo para que lo verifique que venga completo y aqui ellos dan la liberación de el pedido a mesa de control.

Todas estas máquinas estan en red por medio del primer rack que se denomina rack MC(rack de mesa de control).

La segunda área de trabajo es la más importante es la parte monetaria es aqui donde tenemos que tener la mayor seguridad en todos los aspectos, este rack se encuentra bajo llave aqui esta toda la información respecto el área de operaciones. El rack A que es como se le denomina tiene en red a los departamentos de atención al cliente, caja general, gerencia, y parte de la linea de cajas, esto por que por políticas de empresa que desconozco el cable utp debe de ser menor a 90mts de la parte de a tras del patch panel a roceta checkout, y las ultimas máquinas de linea de cajas se encuentran a más de 90mts.

En la maquina de gerencia o más bien dicho de la secretaria de gerencia es donde el administrador de sistemas manda todos los correo que le mandan de diferentes lados al gerente de tienda y aqui se tienen programas básicos.

En el departamento de caja general es donde se euncuentran dos máquinas que llevan el control total monetario de toda la tienda aqui se puede ver en tiempo real lo que uno hace en una maquina de cajas, ver el cobro, ver si ya retiro una caja o si no lo ha hecho, ver cuanto dinero se tienen en toda la linea o por caja, checar si el servidor de banco esta funcionando correctamente además de otras funciones.

En el departamento de atención al cliente cuenta con en sistema de punto de venta pero alrevez, aqui es donde se hacen las devoluciones y se lleva el control de datos de tarjetas de tienda asi como facturación, apartados, y transferencias de dinero.Por ultimo es el departamento de cajas es aqui donde se cobra todo y todo se va transfiriendo a caja general por el caso que comentabamos arriba la mitad de la line de cajas esta con el rack A, y la otra mitad esta con un tercer rack.

En la figura 5.8 podemos observar que se tiene 3 rack de comunicaciones el primero de mesa de control otro es el de caja general y un tercero que es para parte de la linea de cajas.

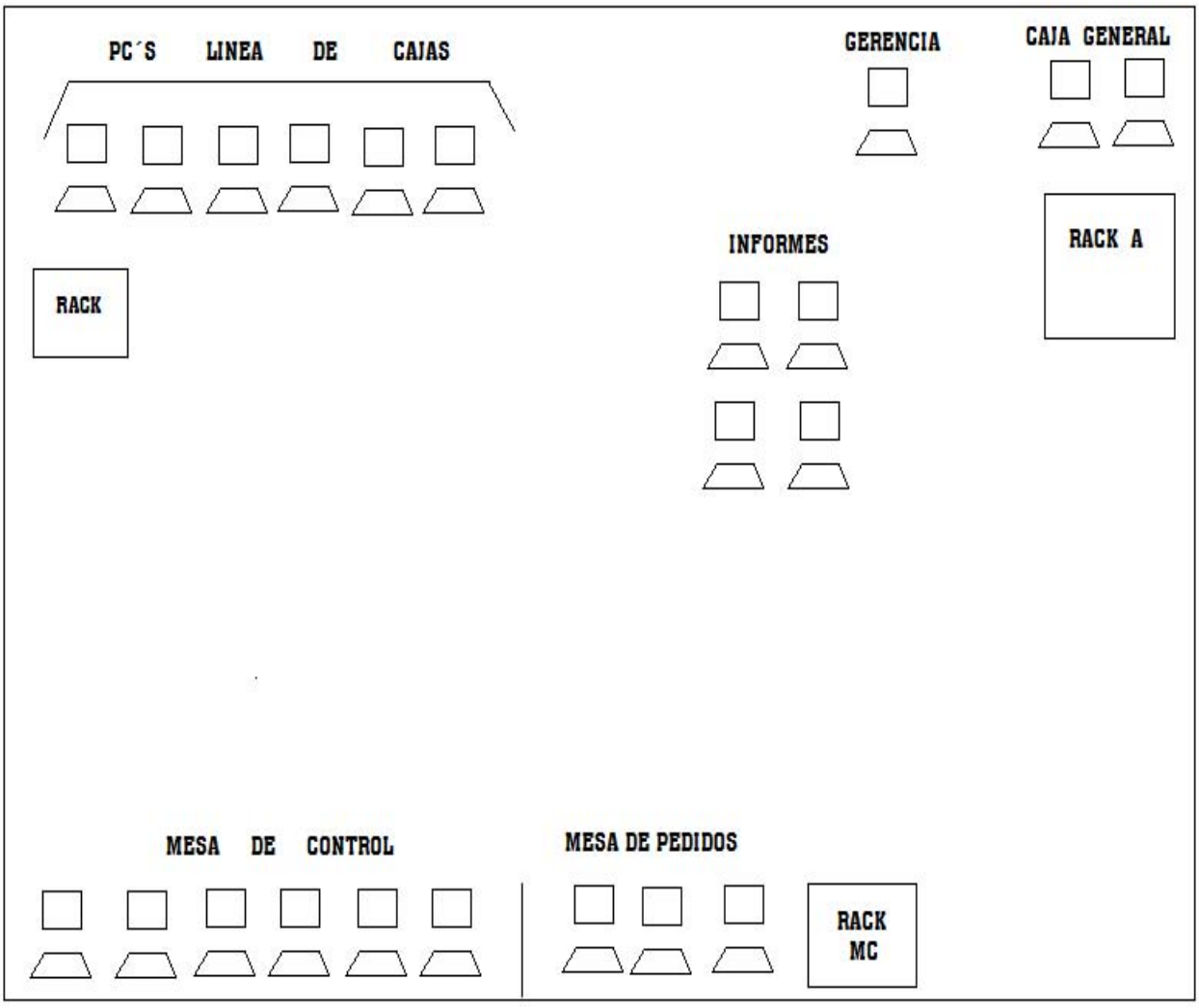

Figura 5.8: Mapa de tienda

En las imágenes 5.9 y 5.10 se ilustra el departamento de mesa de control :

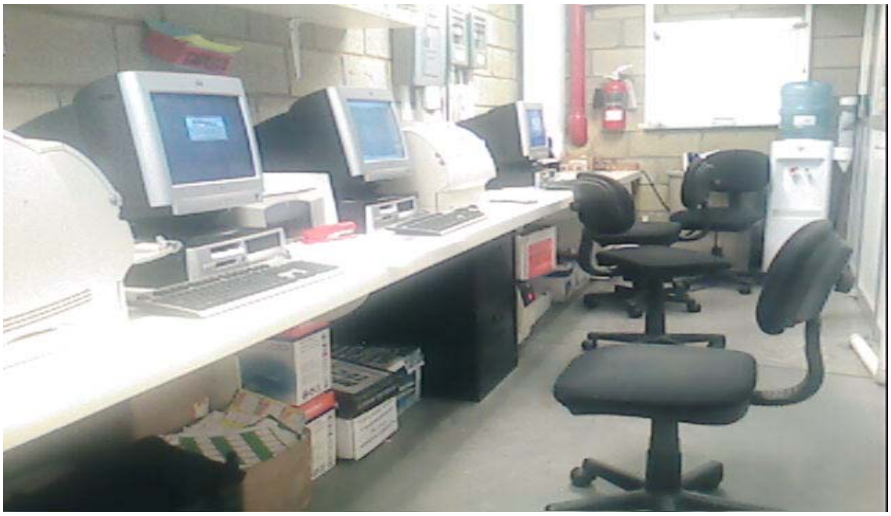

Figura 5.9: Mesa de control, maquina para controlar pedidos y departamentos

Figura 5.10: Mesa de control, maquina para etiquetas y máquina del administrador

En la figura 5.11 se muestra el rack de mesa de control y como esta intregrado.

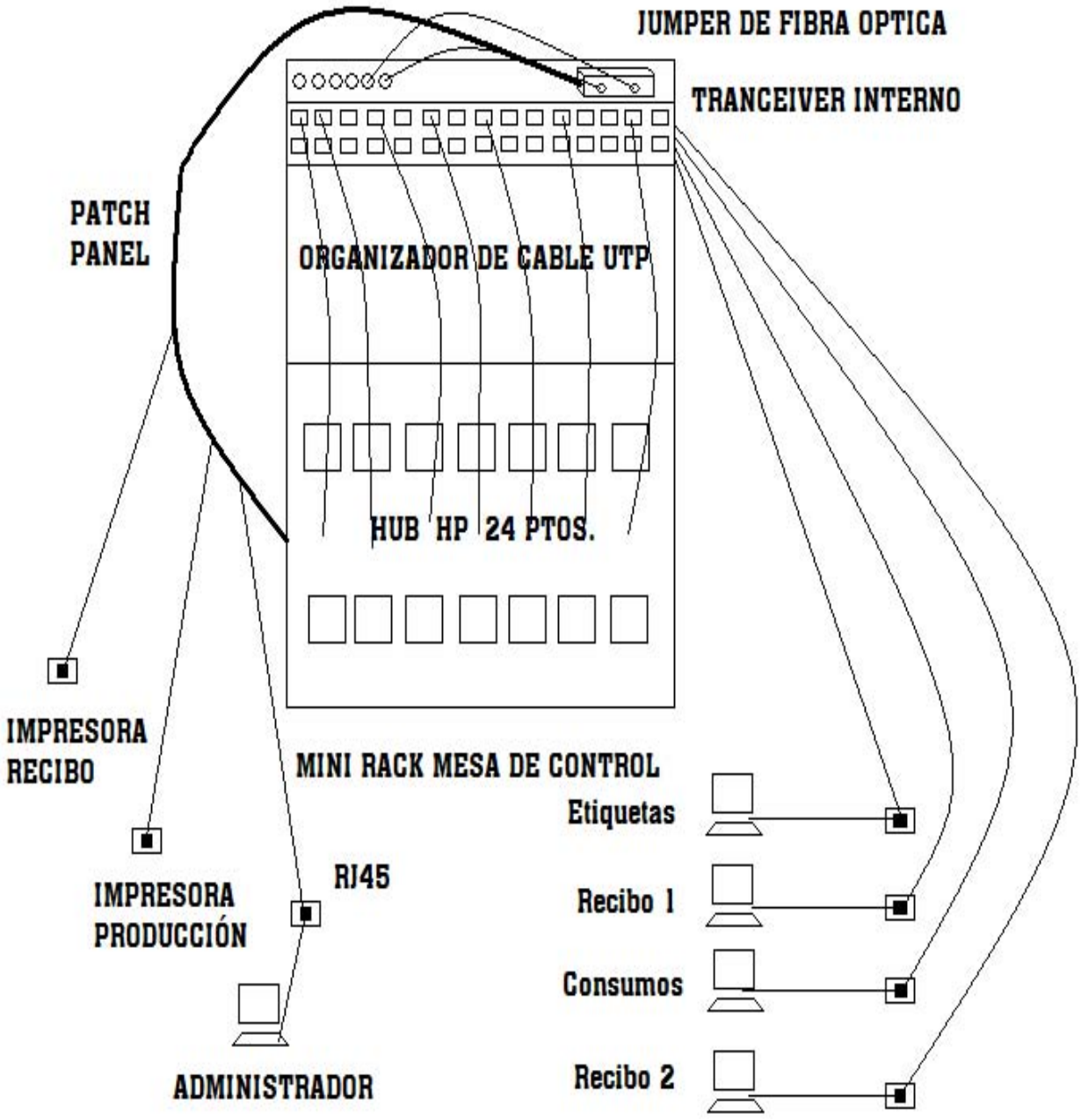

Figura 5.11: Rack de MC

Como podemos ver en la fig 5.12 el rack utiliza un switch 3com y el enlace de red a nivel corporativo es a través de fibra óptica, el rack cuenta con un tranceiver que es un enlace de fibra óptica. Para conectar el switch con las máquinas se utiliza cable utp. Del patch panel sale el cable a las distintas máquinas e impresoras. Para provar que funciona el switch hay que hacer ping de una de las PC a otra del mismo segmento, ej. ping de Pc de consumos a la Pc de recibo,si contesta el ping el hub esta en ok de lo contrario no funciona el hub y seguramente el problema es el tranceiver.

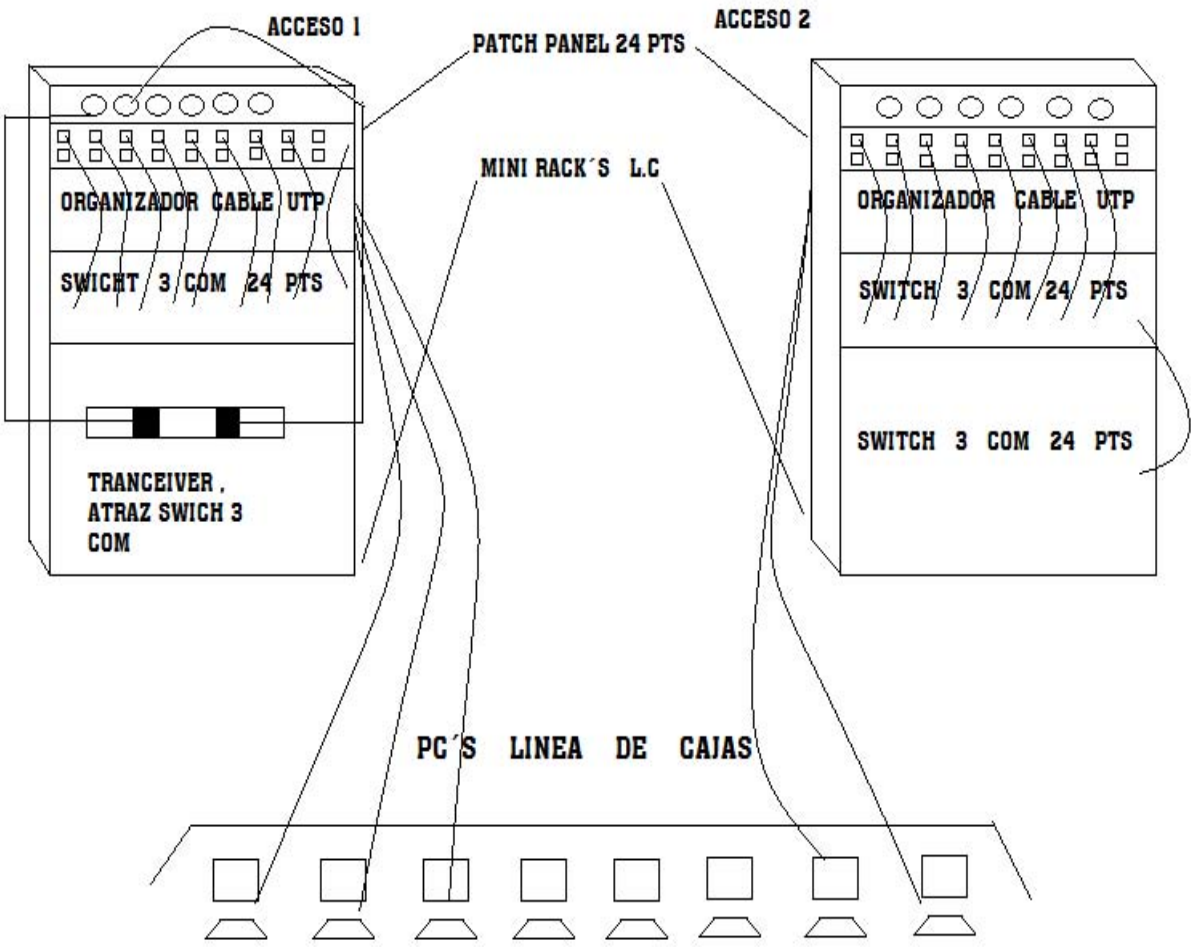

Figura 5.12: Enlace de red UTP típico en PCs L.C

En la figura 5.13 podemos observar como estan dos accesos de L.C como aviamos dicho anteriormente el cable utp debe ser menor a 90mts de la parte de a tras del patch panel a roceta checkout.

Si el distribuidor de F.O recibe la comunicación en el 1 y 2 es por que el distribuidor de F.O ubicado en conmutador tambien lo envía por el 1 y 2.

Figura 5.13: Rack A de línea de cajas

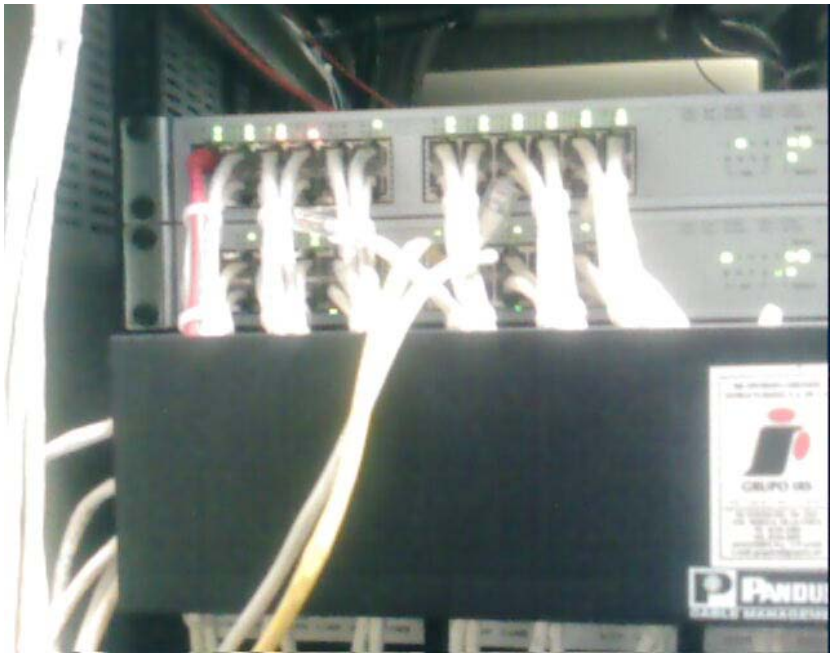

Figura 5.14: Switch 3com

Figura 5.15: Switch 3com

Figura 5.16: Patch Panel

Figura 5.17: Router cisco

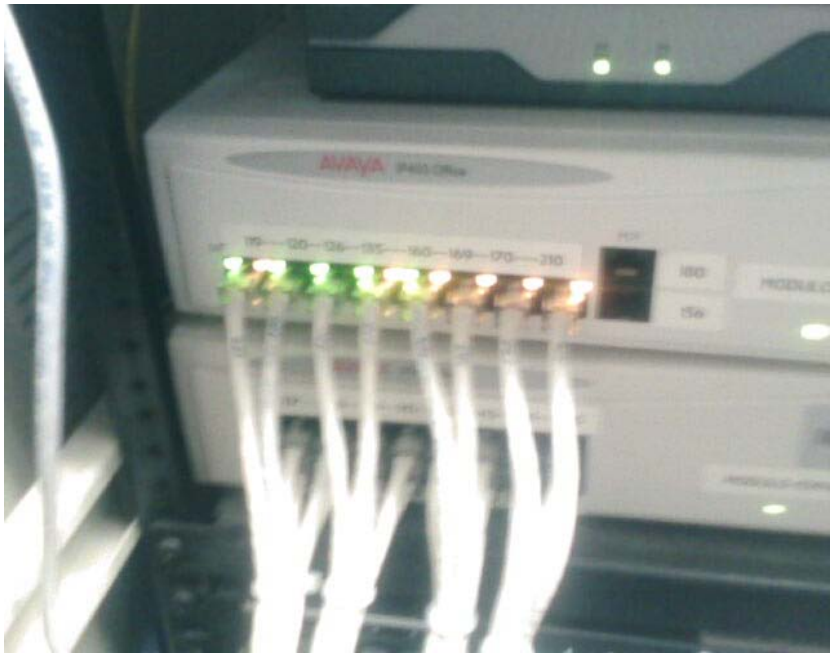

Figura 5.18: Switch 24 puertos

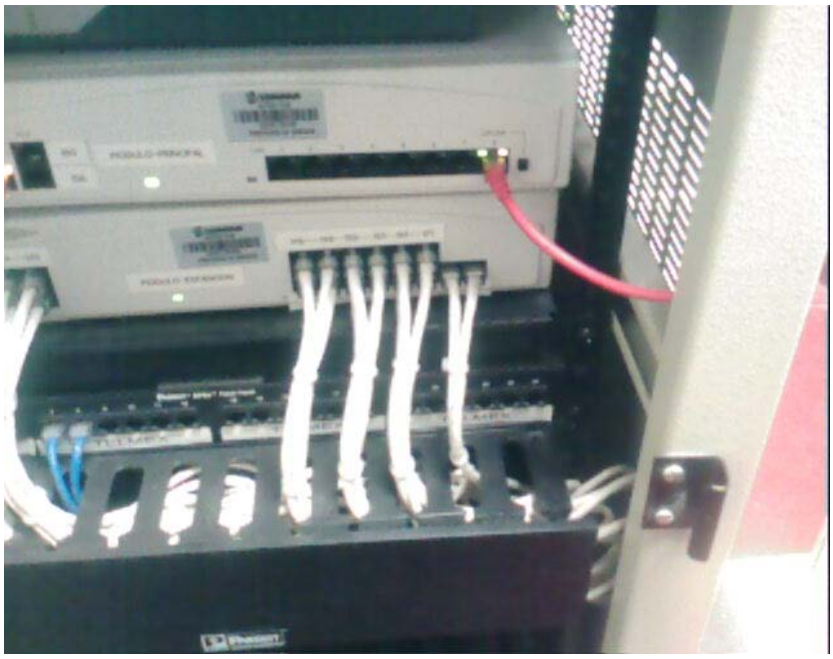

Figura 5.19: Switch 24 puertos

Una de las tecnologías inalámbricas con las que cuenta las sucursales de la empresa es la de las terminales móviles. Sabemos que la empresa lider en redes LAN es Cisco y en terminales móviles es intermec, en nuestra sucursal se utiliza la tecnología cisco y las terminales móviles de intermec ya que estan son compatibles. Mencionaremos lo que es una terminal móvil.

Una terminal móvil es una computadora portátil que realiza funciones de movilidad. Los terminales móviles son los elementos fundamentales para realizar la prestación de los servicios de movilidad. La evolución de la tecnología hace que los operadores puedan ofrecer nuevas modalidades de servicios que impulsen una mejora de los beneficios (fig 5.13).

Figura 5.20: Terminales móviles[34]

En los terminales móviles se incorporan dos tipos de procesadores:

1. **El procesador de banda base**.Este procesador funciona de manera conjunta con la circuitería de radiofrecuencia (RF), encargándose de realizar los protocolos de comunicaciones de bajo nivel (modulación/desmodulación, codificación, gestión de la pila de protocolos especificados en GSM/GPRS/UMTS, etc.).

2. **El procesador de aplicaciones**.Este procesador, similar al de los PCs, es el responsable de gestionar la interfaz (conocida como MMI, Man Machine Interface) con el usuario teclado, pantalla y puntero. También se encarga de proporcionar los nuevos servicios ofrecidos por el terminal, ejecutando un sistema operativo polivalente (Symbian, Microsoft, Palm, etc.) y las correspondientes aplicaciones.

Desde un punto de vista funcional, el procesador de aplicaciones es el que se puede considerar como un nuevo dispositivo. Ello se debe a que su aumento de capacidad de proceso (junto con el aumento de memoria) ha hecho posible que las terminales móviles se acerquen a la versatilidad y prestaciones de los PCs, ejecutando aplicaciones cada vez más complejas que incluyen manejo, intercambio y almacenamiento de información multimedia en tiempo real.

Intermec es una de las compañías líderes a nivel mundial en el diseño y fabricación de escáneres de código de barras, impresoras de código de barras, computadoras móviles de uso robusto (terminales de mano, PDAs industriales y computadoras para vehículos), así como sistemas RFID (etiquetas, tags, lectores y antenas).

Los sistemas de intermec permiten a las compañías capturar de manera automática y eficiente datos críticos de su operación diaria, ya sea en procesos de manufactura, almacenes, distribución, rutas, etc., y transmitirlos vía alámbrica o inalámbrica a sus sistemas corporativos, a fin de obtener visibilidad total en su cadena de suministros, incrementando así el aprovechamiento de sus recursos, la administración de sus inventarios y líneas de producción, mejorar los niveles de respuesta a sus clientes, y aumentar sus niveles de productividad y eficiencia, desde la entrada de los insumos hasta la entrega de sus productos al cliente final.

En la cadena de centros comerciales soriana se utiliza la intermec compatible con los estándares cisco, y se tienen de 5 terminales móviles y 4 access point de cisco modelo 1200. Estos access point estan colocados de manera exacta segun el diametro de alcanze en el techo de la sucursual (alcance 100m interiores y 220m en exteriores), como se muestra en la figura 5.21:

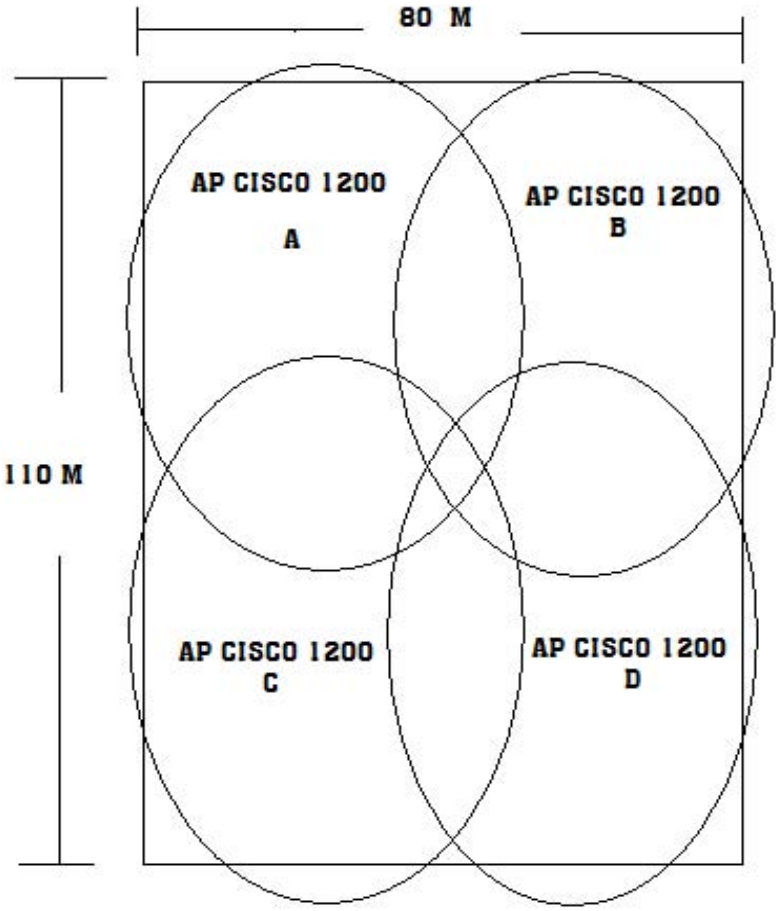

Figura 5.21: Access point en la tienda.

5.5. Implementacíón de tecnología inalámbrica a la red estructurada de CECOSORI

Hasta el momento hemos explicado como se encuentra toda la red cableada del centro comercial, ahora implementaremos nueva tecnología inalámbrica para mejorar su funcionabilidad.

Lo primero y más sencillo es adaptar todas las computadoras una tarjeta de red inalámbrica Cisco Aironet 350 series, por ahora lo haremos solo en el departamento de mesa de control.

Como habiamos mencionado antes este conforma de tres computadoras y la del administrador de sistemas, todas estas junto con las máquinas de mesa de pedidos estan en red y todas necesitan imprimir lo cual nos lleva a que la primera parte es cambiar las impresoras comunes que se tienen y colocar unas que se comuniquen con las máquinas y asi ahorar espacio y tiempo, se utilizarian impresoras Lermark E340 que son las mejores para el uso duro e industrial, tambien el servidor de impresión inalámbrico Lexmark N4050e 802.11g. Todas las máquinas deberan estar en red, esto lo hacemos posible con un access point cisco 1200 con power injector este es un access point compatible con las tecnologías que se van a ocupar.

Lo mismo se haría en la maquina de gerencia que necesita imprimir cambiar su impresora actual por una de marca lermark, y lo mismo con informes y caja general y por ende estas deben estar en red por otro access point de marca cisco 1200 con power injector.

Hasta el momento tendríamos 2 access point estos a su vez tendrán que tener un WAP, e encriptar la señal, poner una SSID. La seguridad es un tema importante por que en estos departamentos se trabaja con información valiosa, en tanto que la comunicación entre cajas y caja general debe de seguir asi por ovias razones es una información completamente confidencial e importante y valiosa.

En tanto a tecnologías puede haber varios cambios uno seria sustituir las terminales móviles por unas más modernas como por ejemplo la 700 serie color o la ck30, 761B, IP4 todas estas compatibles con la tecnología Cisco, tambien impresoras portátiles de intermec como la pw40a, 6820.

Se puede contar tambien en cada caja con un lector de barras totalmente inalámbrico como puede ser la SR60 o SR61, estos lectores de barras inalámbricos tienen alcance de hasta 30 metros metros.

Tambien se puede acortar tambien el tiempo de imprimir etiquetas , ya no mandando hasta mesa de control el número de etiquetas que se requiran, sino contando cada departamento con una impresora móvil cocectada en red con la terminal móvil. Quedando de la siguiente manera(fig 5.22):

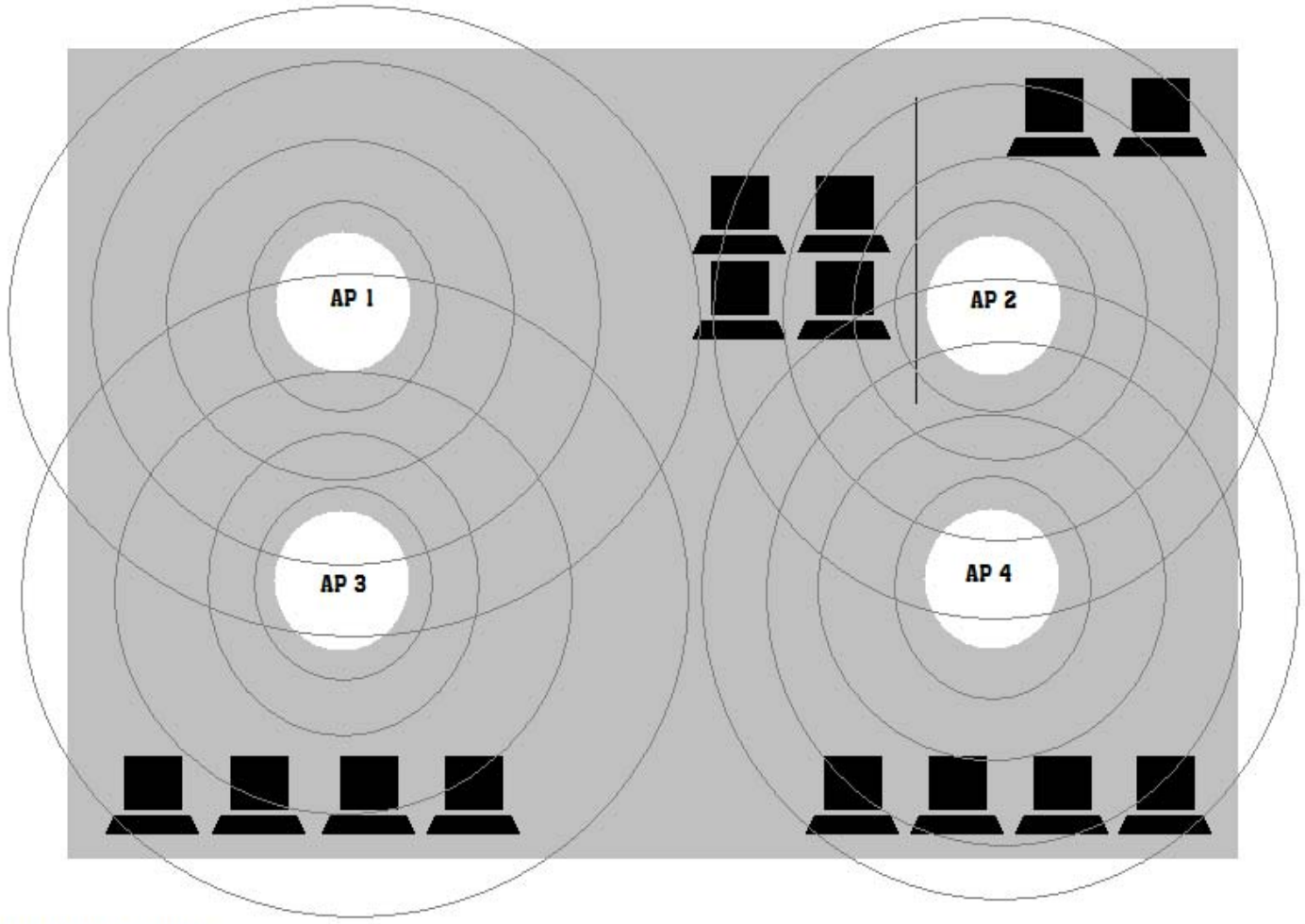

Figura 5.22: Ubicación de access point dentro de la tienda.

5.6. Conclusiones

Se colocaran 4 access point Cisco 1200 series Aironet, y a cada maquina que estará en la red se le colocara una tarjeta de red Cisco Aironet 350 series, las antenas se colocaron estrategicamente para que todo el espacio quedara con señal.

Se recomienda cambiar las terminales móviles por unas mas recientes, y estas a su vez con impresoras portátiles para impresión de etiquetas de anaquel, compares, y cada departamento tener un par de juegos.

Colocar impresoras Lexmark en puntos donde se tenga que imprimir documentos, como informes, mesa de control, gerencia, y caja general y con su respectivo servidor de impresión.

En cada caja tener un lector de código de barras inalámbrico.

CONCLUSIONES

Aprendí todo lo relacionado con las redes inalámbricas, su arquitectura, los tipos de estándares, los diferentes tipos de redes inalámbricas, su manera de operar con otras tecnologías inalámbricas en este caso con Intermec y Lexmark.

El funcionamiento del sistema y de la red de la tienda departamental Mercado Soriana Tutelar 136, fueron otras de las cosas que aprendí, esta tienda departamental pertenece a una de las cadenas más grandes de tiendas de autoservicio CECOSORI (centros comerciales soriana).

Todas las tiendas de esta cadena tienen el mismo sistema y el mismo tipo de red de datos, lo cual significa que este estudio que se hizo se puede dar a conocer en cualquier tienda del pais de esta cadena.

Se mejoró la tecnología inalámbrica ya existente y se coloco nueva, para a cortar tiempos del personal al realizar sus actividades diarias, y cabe destacar que en tiempos de navidad, de inventarios y cambios drasticos como cambios de lugar o cambios de provedores, la tecnología inalámbrica facilitó muchísimas actividades.

También se mantuvieron las mismas marcas de servicio como Intermec que es el lider en tecnología inalámbrica en terminales móviles, Cisco lider en redes, Lexmark lider en impresoras para uso industrial, ya que la cadena CECOSORI tiene un contrato con estas empresas.

GLOSARIO

802.11
802.11 o IEEE 802.11, es un grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local(LAN). 802.11 se compone de distintas normas que operan a diferentes frecuencias, con distintas velocidades y capacidades.

Access Point (AP, Punto de Acceso).
Estación base o "base station"que conecta una red cableada con uno o más dispositivos wireless.
Existen muchos tipos de Access Point en el mercado,con diferentes capacidades:bridge, hubs, gateway, router, y las diferencias entre ellos muchas veces no estan claras, por que las caracteristicas de uno se pueden incluir en otro.Por ejemplo,un router puede hacer bridge y un hub puede hacer switch.
Además los access points pueden mejorar las caracteristicas de la WLAN permitiendo a un cliente realizar roaming entre distintos AP de la misma red o compartiendo una conexión a internet entre los clientes wireless.

Ad-Hoc, modo.
Un tipo de topología de WLAN en la que solo existen dispositivos clientes, sin la participación de ningún access point, de forma que los clientes se comunican de forma independiente punto a punto, peer-to-peer.

Dado que no existe un dispositivo central, las señales pueden ocasionar mayores interferencias reduciendo las prestaciones de la red.

Asociación, servicio de.
Servicio del protocolo 802.11 que asocia a un cliente wireless a un Punto de Acceso.

Autentificación
Proceso de identificación de un equipo o usuario. El estándar 802.11 define dos métodos de autentificación:open system y shared key.

Bluetooth.
Tecnología desarrollada para la interconexión de portátiles, PDAs, teléfonos móviles y similares a corta distancia (menos de 10 metros) con una velocidad máxima de 11mbps a al frecuencia ISM de 2.4Ghz.

Bandwidth
El ancho de banda de una red sobre la que se construye cualquier comunicación.

BSSID, Basic Sercvice Set Identification.
Uno de loos tipos de SSID, el que se emplea en redes wireless en modo Ad-Hoc.

CEPT, Conferencia Europea de Administraciones de Correos y Telecomunicaciones.
Organismo internacional que agrupa a las entidades responsables en la administración pública de cada país europeo de las políticas y la regulación de las comunicaciones, tanto postales como de telecomunicaciones. Fue fundada el 26 de junio de 1959.

Cifrado.
Técnicas utilizadas para hacer inaccesible la información a personas no autorizadas. Se suele basar en una clave, sin la cual la información no puede ser descifrada.

Clave de encriptación.
Conjunto de caracteres que se utilizan para encriptar y desencriptar la información que se quiere mantener en privado.El tipo de clave y la forma de emplearla depende del algoritmo de encriptación que se utilice.

Cliente, o dispositivo cliente.
Cualquier equipo conectado a una red y que solicita servicios (ficheros, impresión, etc) de otro miembro de la red. En el caso de las WLAN, se suelen emplear para referirse a los adaptadores que proporcionan conectividad a través de la red inalámbrica, como tarjetas PCMCIA, PCI o USB, que permiten al equipo acceder a la red.

Eavesdropping.
Es un proceso mediante el cual un agente capta información-en claro o cifrada- que no le iba dirigida; lo más peligroso del eavesdropping es que es muy difícil de detectar mientras se produce.

Espectro radioeléctrico
El espectro radioeléctrico es toda la escala de frecuencias d las ondas electromagnéticas. Considerando como un dominio de uso público, su división y utilización esta regularizando internacionalmente.

ESSID, Extended Service Set Identification.
Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

Ethernet.
Ethernet es el nombre común del estándar IEEE 802.3, que define las redes locales con cable coaxial o par trenzado de cobre.

ETSI, European Telecommunications Standard Institute.
Organización europea sin ánimo de lucro para el desarrollo de estándares de telecomunicación, agrupa 699 miembros de 55 países.

FHSS, Frequency Hopping Spread Sprectrum.
Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en cambios sincronizados entre emisor y receptor de la frecuencia empleada.

Honeypots
Es un método de detección de intrusos que consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarce a esperar que aparezcan los intrusos.

Hub.
Dispositivo de red multipuerto para la interconexión de equipos via Ethernet o Wireless. Los concentradores mediante cables alcanzan mayores velocidades que los concentradores wireless (Access Points), pero éstos suelen dar cobertura a un mayor número de clientes que los primeros.

IEEE, Institute of Electrical and Electronics Engineers
Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para,entre otros campos, las comunicaciones.
esta organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas.Así el subgrupo 802 se encarga de las redes LAN y WAN y cuenta con la subsección 802.11 para las redes WLAN.

IP. Dirección.
Un número de 32 bits que identifica a un equipo a nivel de protocolo de red en el modelo OSI. Se compone de dos partes:la dirección de red,común a todos los equipos de la red, la dirección el equipo, única en dicha red.

IrDA.
(Infrared Data Association):Organización fundada para crear las normas internacionales para el hardware y el software usados en enlaces de comunicación por rayos infrarrojos. La tecnología de rayos infrarrojos juega un importante papel en las comunicaciones

inalámbricas.

ISM, Industrial Scientific and Medical dand
Bandas de frecuencias reservadas originalmente para uso no comercial con fines industriales, científicos y médicos. Posteriormente, se empezaron a usar para sistema de comunicación tolerantes a fallos que no necesitaran licencias para la emisión de ondas. 802.11b y 802.11g operan en la ISM de los 2.4Ghz, asi como otros dispositivos como teléfonos inalámbricos y hornos microondas, por ejemplo.

MAC, Media Access Control.
En las redes wireless, el MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2)en el modelo OSI. Cada dispositivo wireless posee una dirección par este protocolo,denominada dirección MAC, que consiste en un número de 48 bits:los primeros 24 bits identifican al fabricante de la tarjeta ,mientras que los restantes 24,a la tarjeta.Este modelo de direccionamiento es común con las redes Ethernet (802.3).

Modulación
Técnicas de tratamiento d la señal que consiste en combinar la señal de información con una señal portadora, para obtener algún beneficio de calidad, eficiencia o aprovechamiento del ancho de banda.

Network name,nombre de red.
Identificador de la red para su diferenciación del resto de las redes. Durante el proceso de instalación y configuración de dispositivos wireless, se requiere introducir un nombre de red o SSID para poder acceder a la red en cuestión.

Open System, autentificación.
Método de autentificación por defecto del estándard 802.11, en la que no se realiza ningún proceso de comprobación de identidad; simplemente, se declaran, por lo que no ofrece ninguna seguridad ni control de acceso.

Router.
Dispositivo de red que translada los paquetes de una red a otra. Basándose en las tablas y protocolos de enrutamiento y en el origen y destino, un router decide hacia dónde enviar un paquete de información.

Sniffing
Un sniffing o más concretamente,un sniffer de paquetes, se define como una pieza de software o hardware que se conecta a una red informática y supervisa todo el tráfico que pasa por el cable.Los sniffers comerciales se usan para mantener redes y los sniffers ündergroud"se usan para asaltar a los ordenadores de una red.

Snooping y Downloading
Puede ser realizado por simple curiosidad,pero también es realizado con fines de espionaje y robo de información o software. Obtiene la información sin modificarla. Sin embargo los métodos a diferencia del sniffing son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

SSID, Service Set Identification.
Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deben tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.
Dependiendo de si la red wireless funciona en modo Ad-hoc o en modo Infraestructura,el SSID se denomina ESSID o BSSID.

TCP/IP.
Transport Control Protocol/Internet Protocol, protocolo estándar desarrollado por la agencia de investigación de la defensa de USA como base para la red ARPANET y que es utilizado por defecto en sistemas operativos abiertos y en la red Internet. Se utilizan para el intercambio de información entre ordenadores conectados a una red.

Tampering o Data Diddling.
Es un tipo de ataque a la modificación desautorizada de los datos, son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada.

Warchalking.
Proceso de realizar marcas en superficies (paredes, suelos, señales de tráfico)para indicar la existencia de redes wireless y alguna de sus caracteristicas .

Wardriving.
Localización y posible introducción en redes wireless de forma no autorizada. Sólo se necesita un portátil, un adaptador wireless,el software adecuado y un medio e transporte.

WAP
Wireless Access Protocol, protocolo de acceso sin hilos,utilizado para la transmisión de datos a través de internet desde un teléfono movíl a un servidor internet. Es un protocolo que se puede utilizar siempre que se trate de acceso de ordenadores a internet a través de redes inalámbricas.

WEP, Wired Equivalent Privacy.
Algoritmo de seguridad, de uso opcional,definido en el estandard 802.11 basado en el algoritmo criptográfico RC4, utiliza una clave simétrica que debe configurarse en todos los equipos que participan en la red. Emplea claves de 40 y 104 bits, con un vector de inicialización de 24 bits.
Se ha demostrado su vulnerabilidad y que su clave es fácilmente obtenible con software de libre distribución a partir de cierta cantidad de tráfico recogido de la red.

Wi-Fi, Wireless Fidelity.
Nombre dado al protocolo 802.11b. Los dispositivos certificados como Wi-Fi son interoperables entre si, como garantía para el usuario.
Wi-Fi Alliance, también llamada Wireless Ethernet Compability Alliance (WECA). Asociación internacional formada en 1999 para certificar la interoperatibilidad de los dispositivos wireless basados en el estándar 802.11, con el objetivo de promover la utilización de dicha tecnología.

Wi-MAX, WMAN Redes Metropolitanas Inalámbricas.
Redes inalámbricas que cubren una amplia área geográfica, más que una WLAN.

WPA, Wi-Fi Protected Access.
Protocolo de seguridad desarrollado por la Wi-Fi para mejorar la seguridad de la información en las redes wireless y permitir la autentificación de usuario, puntos débiles del WEP.

WWAN, 3G Redes Amplias Inalámbricas.
Son redes inalámbricas de mucho alcance en la actualidad son las más utilizadas en la telefonía móvil y tambien disponen de la capacidad de transmitir datos.

ACRÓNIMOS

Notacion empleada	Significado
ACL	Access Control List
AP	Access Point
ARP	Address Resolution Protocol
ATM	Asynchronus Transfer Mode
BSS	Basic Service Set
CCK	Complementary Code Keying
CDMA	Code Division Multiple Access
DDS	Digital Data Service
DHCP	Dynamic Host Configuration Protocol
DLS	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EAS	Extended Area Service
EDGE	Enhanced Data Rates for GSM Evolution
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FDD	Frequency Division Duplexing
FDMA	Frequency Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HiperLAN	High Performance Radio Local Area Network
IEEE	Institute of electrical and Electronics Engineers,Inc
IM	Intensity Modulation
IP	Internet Protocol
ISM	Industrial ,Scientific and Medical
ISDN	Integrated Services Digital Network
ISN	Information Systems Network
ISSN	Integrated Special Services Network
ITU	International Telecommunications Union
LAN	Local Area Network
MAC	Medium Access Control

Notacion empleada	Significado
NIC	Network Interface Card
PCS	Personal Communications Service
PDA	Personal Digital Assistant
PIN	Personal Identification Number
QoS	Quality of service
$SSDS/FH$	Spread Sprectrum Direct Sequence/Frequency Hopping
$SSID$	Service Set Identifier
$SWAP$	Shared Wireless Access Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Protocol
$Wi-Fi$	Wireless Fidelity
$WLAN$	Wireless Local Area Network

BIBLIOGRÁFIA

REFERENCIAS BIBLIOGRAFICAS

[1] Redes y Comunicación de Datos para los Negocios
Jerry Fitzgerald y Associates.
Editorial Omega.

[2] Systems Analysis and Desig.
Alan Dennis.
Indiana University.

[3] Redes de Área Local Inalámbricas segun el Estándar IEEE 802.11.
Miquel Oliver, Ana Escudero.
Universidad Politécnica de Catalunya.1997

[4] REDES INALÁMBRICAS WIRELESS.
Instituto Nacional de Estadistica e Informatica (sub-jefatura de Informatica).

[5] Arquitectura Basada en Comportamiento Aplicada al Ruteo de Redes AD-HOC.
Griselda Patricia Cervantes Casiilas, Instituto Tecnologíco de Estudios Superiores de Monterrey Campus Monterrey Division de Electrónica, Computación, Informatica y Comunicaciones.2002

[6] Protocolos se seguridad en redes inalámbricas.
Saulo Barajas
Doctorado en Tecnologías de las Comunicaciones.
Universidad Carlos III de Madrid.

[7] Manual de mantenimiento de red mercado CECOSORI.

[8] Servicios de Valor Añadido en Redes Móviles Ad-hoc.
Iván Vidal, Carlos García, Ignacio Soto, José Ignacio Moreno
Departamento de Ingeniería Telemática Universidad Carlos III de Madrid.

[9] Seguridad en redes inalámbricas 802.11.
Juan Manuel Madrid Molina
Universidad Icesi jmadrid@icesi.edu.co SISTEMAS y TELEMÁTICA

[10] Redes Inalámbricas
Estándares y mecanismos de seguridad
Jaime Cuéllar Ruiz.
Publicado en la revista "muy interesante 2003").

[11] Estándares WLAN
Evelio Martinez
Publicado en la revista RED junio 2002.

[12] Grupo de Comunicaciones Móviles y de banda ancha.
Departamento de Matemática Aplicada y Telemática(DMAT).
Universidad Politécnica de Catalunya.
Miquel Oliver,Ana Escudero.

[13] Redes de acceso de Banda Ancha
Arquitectura,prestaciones,servicios y evolución.
Ministerio de Ciencia y tecnología.

[14] Bluetooth más que una conexión inalámbrica.
Lourdes Velázquez Pastrana.
Articulo.

[15] 802.11(WI-FI)
Manual de redes inalámbricas
Neil Reid y Ron Seide.

REFERENCIAS ELECTRÓNICAS

[16] http://microasist.com.mx/noticias/mo/acho060403.shtml

[17] http:eveliux.com/articulos/bluetooth.html

[18] http://microasist.com.mx/noticias/mo/gspmo2510.shtml

[19] http://www.monografias.com/especiales/comunicamov/

[20] http:www.zonagratuita.com/servicios/seguridad/wireless.html

[21] http://www.laneros.com/archive/index.php/t-39617.html

[22] http://www.wireless-nets.com

[23] http://maestrosdelweb.com/editorial/redeswlan/

[24] http://mailxmail.com/curso/informatica/wifi

[25] http://www.es.wikipedia.org/wiki/GSM

[26] http://www.wireless-station.com

[27] http://www.jiwire.com

[28] http://es.wikipedia.org/wiki/Enlaces Infrarojos

[29] http://www.wi-fiplanet.com/tutorials/article.php/1368661

[30] http://compnetworking.about.com/cs/wirelesssecurity/g.htm

[31] http://www.sincables.es

[32] http://www.glad.hu

[33] http://www.movitelia.com

[34] http://www.intermec.com.mx

[35] http://www.cisco.com

[36] hrrp://www.lexmark.com