Consideraciones para implementar y dar seguridad en redes inalámbrica WiFi

Autor: Asdrubal Vega Alvarez

Tesina presentada para obtener el título de:
Lic. En Sistemas computarizados [sic]

Nombre del asesor:
Tomas Navarrete Gutierrez

UNIVERSIDAD VASCO DE QUIROGA

ESCUELA DE SISTEMAS COMPUTARIZADOS

No. de acuerdo: 952006 **Clave: 16PSU0014Q**

"CONSIDERACIONES PARA IMPLEMENTAR Y DAR SEGURIDAD EN REDES INALAMBRICAS WIFI"

TESINA

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA

ASDRUBAL VEGA ALVAREZ

ASESOR

I.S.C. TOMAS NAVARRETE GUTIERREZ

MORELIA, MICH., MEXICO **OCTUBRE 2005**

AGRADECIMIENTO

A mis padres: por el apoyo moral y económico durante la carrera.

INDICE

ANTECEDENTES

Los tres últimos siglos han sido marcados por la tecnología. En el siglo XVIII los grandes sistemas mecánicos. En el siglo XIX fue la maquina de vapor. Durante el siglo XX una de las mas importantes tecnologías, los sistemas de computo como herramientas para la obtención, procesamiento y distribución de información. También hemos visto avances como la instalación de redes mundiales de telefonía, la invención de la radio y la televisión, satélites de comunicaciones, así como el crecimiento de la industria de la computación.

La industria de la computación ha progresado espectacularmente, en sus primeras dos décadas de existencia los sistemas eran altamente centralizados. Un número muy reducido de computadoras eran con las que las universidades o empresas medianas contaban, en tanto que las instituciones grandes tenían cuando mucho una docena.

Nunca se imaginó que en 20 años se producirían en masa millones de computadoras con el mismo potencial pero de mucho menor tamaño. Hoy en día el modelo antiguo donde una sola computadora realiza todas las tareas computacionales de una empresa ha sido reemplazado por otro en el que un gran número de computadoras separadas pero interconectadas hacen el trabajo. Estos sistemas se les conocen como redes de computadoras.

Cuando más de dos computadoras pueden transferir información podemos decir que están interconectadas. No es necesario que la conexión se realice por medio de un cable de cobre. Para la interconexión se pueden utilizar; fibras ópticas, las microondas, los rayos infrarrojos, los satélites de comunicaciones y señales de radio frecuencia. Este trabajo se enfoca en esta última tecnología generalmente llamadas “redes inalámbricas”. Son redes basadas en emisiones de radio, principalmente orientadas a cubrir segmentos de redes de área local (LAN) y comúnmente también a redes de área personal (PAN).

Las primeras experiencias con redes inalámbricas datan de 1979 cuando científicos de IBM en Suiza despliegan la primera red de importancia con tecnología infrarroja. No es hasta 1985 cuando se comienzan los desarrollos comerciales de redes con esta tecnología, momento en el que el órgano regulador del espectro electromagnético americano, la FCC (Federal Communications Comisión), asigna un conjunto de estrechas bandas de frecuencia para libre uso en las bandas de los 2,4 y los 5 giga hercios. Inmediatamente, la asociación de ingenieros electrónicos (IEEE), asigna una comisión de trabajo para desarrollar una tecnología de red en dichas bandas: la 802.11. A partir de ese momento se liberan una serie de estándares, los cuales se analizan en esta investigación.

El primer estándar que surge es el 802.11 (1997), el cual sienta las bases tecnológicas para el resto de la familia. No tuvo mucha relevancia debido a su baja velocidad alcanzada, cerca de 2 Mbps. Muy poco después se publica el 802.11b, el cual es recibido con un gran éxito comercial. Opera en la banda de los 2,4 GHz y permite alcanzar velocidades teóricas de 11 Mbps mediante el empleo de mecanismos de modulación de canal y protección frente a errores bastante robustos. Para complementar su funcionamiento, este estándar incorpora un protocolo de seguridad para comunicaciones, el WEP Wired Equivalent Privacy (Privacidad Equivalente al Cable). Desafortunadamente, el pretencioso nombre no corresponde a la realidad, pues muy poco después de su publicación se descubrieron importantes defectos que permitían la intrusión en las comunicaciones con escaso esfuerzo y un equipo convencional.

Pese a lo anterior, el éxito fue de tal magnitud que aceleró la aparición de nuevos estándares y reclamó una especial atención por entidades de regulación, que empezaron a valorar la ampliación del espectro para este tipo de usos. El siguiente estándar fue el 802.11a, el cual tiene la particularidad de operar a una mayor velocidad, teóricamente hasta 54 Mbps mediante unos

esquemas de codificación de canal más sofisticados y sobre bandas en los 5 GHz, cuyo uso es permitido en nuestro país.

El estándar más reciente, el 802.11g, mejora varios aspectos: mantiene el rango de los 2,4 Ghz pero amplia su velocidad de transmisión hasta los 54 Mbps teóricos, en la práctica se obtiene un tasa efectiva menor que la mitad, mantiene la compatibilidad con el 11b y propone un protocolo de seguridad más robusto denominado WPA (Wi-Fi Protected Access). Dichas mejoras han relanzado más la confianza del mercado en la tecnología y como consecuencia de ello las implementaciones de redes inalámbricas y la venta de productos inalámbricos.

Una de las claves del éxito comercial ha sido la buena interoperabilidad existente entre equipos de diferentes fabricantes, labor que ha llevado a cabo la Wi-Fi Alliance. Este organismo, con cientos de empresas entre sus miembros y una gran variedad de productos certificados que han fomentado la tecnología y garantizado su genérico buen uso.

OBJETIVOS

Objetivo general

Conocer la tecnología inalámbrica WiFi 802.11 así como aspectos de implementación y seguridad de redes basadas en este estándar.

Objetivos específicos

Primero, hacer un breve análisis sobre las más recientes tecnologías inalámbricas y reunir todos los aspectos relevantes en esta investigación.

Segundo, analizar el estándar 802.11 y conocer las ventajas y desventajas que presentan el 802.11a, 11b y 11g.

Tercero, tener el conocimiento de las consideraciones básicas para implementar redes inalámbricas WiFi.

Cuarto, conocer los métodos para asegurar una red inalámbrica WiFi según las distintas situaciones de uso y tipos de red.

CAPITULO 1

INTRODUCCIÓN A REDES INALÁMBRICAS

En este primer capítulo se analizan los puntos básicos por los cuales las redes inalámbricas han logrado revolucionar el mundo de las redes de computadoras. Se verá la diferencia existente entre lo inalámbrico fijo y lo inalámbrico móvil así como la estandarización de redes inalámbricas, ya que los dispositivos inalámbricos están restringidos a operar en cierta banda de frecuencia. También se analiza a la IEEE que es una asociación internacional formada por profesionales de las nuevas tecnologías, como ingenieros de telecomunicaciones, ingenieros electrónicos e Ingenieros en informática y que se ha encargado de crear estándares para regular el uso de frecuencias, anchos de banda, entre otros, con el fin de normalizar los productos de fabricantes distintos. Por ultimo se analizan las principales aplicaciones de las redes inalámbricas, sus ventajas y desventajas.

1.- INTRODUCCIÓN A REDES INALÁMBRICAS

1.1.- Redes inalámbricas

En la actualidad muchas compañías tienen un gran número de computadoras. El interés por las redes nace cuando las compañías deciden conectarlas para extraer y correlacionar información acerca de su compañía. Lo esencial aquí es la compartición de los recursos y el objetivo es hacer que todos los programas, el equipo y, en particular los datos estén disponibles para todos los que se conectan a la red, independientemente de la ubicación física del recurso y del usuario.

Un ejemplo claro y muy común es el de un grupo de trabajo que comparten una impresora, sin embargo compartir información es tal vez más importante que compartir recursos físicos como las impresoras, escáners, quemadores, etc. Para las compañías en general, la información computarizada es vital. Poder tener acceso a recursos de una red inalámbrica desde cualquier parte de un edificio o de un campus ahora es una posibilidad que promete convertirse en una necesidad debido a que esta nueva manera de trabajar es realmente una comodidad.

Gracias a los dispositivos móviles, la información la podemos manejar en cualquier momento y en cualquier lugar, sin embargo, al igual que sucedió con la llegada de las redes alambradas de computadoras, esto nos parecerá en un par de años de lo mas normal y participaremos en esta forma de comunicación que será algo muy común.

1.1.1.- Diferencia entre inalámbrica fija e inalámbrica móvil

La conectividad inalámbrica y la computación portátil se relacionan frecuentemente, pero no son idénticas, como se muestra en la Tabla 1.1 en la que vemos una diferencia entre inalámbrica fija e inalámbrica móvil. En muchas ocasiones las computadoras portátiles son conectadas a la red por medio de cable. Por ejemplo, cuando se conecta una computadora portátil a una toma telefónica en una habitación de hotel u oficina, se tiene movilidad sin una red inalámbrica. También existen las aplicaciones inalámbricas móviles, que van desde la oficina portátil hasta las personas que pasean por una tienda con un PDA realizando un inventario. [3]

Para dejar en claro esta diferencia entre inalámbrica fija e inalámbrica móvil de la tabla 1.1 es necesario tener en cuenta que las aplicaciones mencionadas no necesariamente tienen que ser inalámbricas fijas o inalámbricas móviles, todo dependerá de la situación de uso en que se encuentre.

Aplicaciones	Inalámbrica	Móvil
Computadoras de escritorio en oficinas sin cableado	Si	No
Una computadora portátil conectada por medio de cable a la red en un cuarto de hotel	No	Sí
Redes en construcciones antiguas sin cableado, donde instalar cables es complicado	***Sí***	***No***
Oficina portátil; PDA para inventario de almacén	Sí	Sí

Tabla 1.1 Combinaciones de redes inalámbricas y computación móvil.

1.1.2.- Auge de las redes inalámbricas

Según la firma estadounidense Cahners In-Stat de investigación de mercado, la industria de las redes inalámbricas de área local es el segmento de la industria de las comunicaciones que más rápido ha crecido. Las ventas de

productos de redes inalámbricas en Estados Unidos fueron de cerca de 3.6 millones de unidades en el año 2003, se prevé que la cantidad crecerá de 3.9 billones de dólares en el 2003 a aproximadamente 5.2 billones de dólares para este año 2005. Este crecimiento es en gran parte debido a la introducción de productos de redes inalámbricas basados en estándares. Estos productos basados en estándares son más rápidos, baratos y simples de configurar y usar que productos generaciones anteriores.

La conectividad inalámbrica en las redes de área local (LANs) son sistemas en los que cada computadora cuenta con una tarjeta de red inalámbrica y una antena mediante la cual se puede comunicar con otros sistemas. Si los sistemas están lo suficientemente cerca, se pueden comunicar de manera directa entre sí en una configuración de igual a igual. Las redes inalámbricas de área local se están haciendo cada vez más comunes en casas, oficinas, universidades, cafeterías, salas de conferencias, edificios antiguos, donde instalar Ethernet[1] se considera muy problemático y costoso.

Casi al mismo tiempo que aparecieron las computadoras portátiles, muchas personas tuvieron el sueño de andar por la oficina y poder conectar a Internet su computadora, en consecuencia varios grupos empezaron a trabajar para cumplir esta meta. El método más práctico fue el que se mencionó anteriormente, equipar las computadoras de la oficina y las portátiles con transmisores y receptores inalámbricos que les permitieran comunicarse. Esto llevó a que varias empresas comenzaran a comercializar las LANs inalámbricas. El estándar para las LANs inalámbricas lo estandarizo la IEEE[2] y se llama 802.11, que la mayoría de los sistemas implementa y que se ha extendido ampliamente. Comúnmente se le conoce como WiFi[3] (Wireless Fidelity). Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero en la actualidad también se utiliza para acceder a Internet.

[1] Ethernet. Estándar más utilizado en redes de área local
[2] IEEE. Institute of Electrical and Electronics Engineers
[3] WiFi. Wireless Fidelity (Fidelidad Inalámbrica). Es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11

1.2.- Estandarización de redes inalámbricas

1.2.1.- El espectro electromagnético

Los dispositivos inalámbricos están restringidos a operar en cierta banda de frecuencia. Cada banda tiene asociado un *ancho de banda*, que es simplemente la cantidad de espacio de frecuencia en la banda. El ancho de banda ha adquirido la connotación de ser una medida de la capacidad de información de una liga.

El uso del espectro electromagnético es controlado rigurosamente por autoridades reguladoras a través de procesos de licenciamiento. En México, la regulación esta a cargo de la Secretaria de Comunicaciones y Transportes (SCT), sin embargo, las reglas para redes inalámbricas son copiadas del vecino país del norte. En Estados Unidos, la regulación esta a cargo de la Comisión Federal de Comunicaciones (FCC[4]). Algunas otras reglas son hechas por la Unión Internacional de Telecomunicaciones (ITU[5]). Para prevenir la sobreposición de los usos de las ondas de radio, la frecuencia es dividida en bandas, que son simples rangos de las frecuencias disponibles para aplicaciones específicas.

1.2.2.- Bandas ISM

Es una abreviación de Industrial, Científico y Médico[6]. Estas bandas son reservadas para equipo que esta relacionado a procesos industriales o científicos, o usada por el equipo medico. La banda ISM mas conocida es la de los hornos de microondas, el cual opera en la banda de los 2.4 gigahertz (GHz) debido a que la radiación electromagnética a esa frecuencia es particularmente efectiva para calentar agua. Es precisamente en esa banda donde los dispositivos WLAN más comunes hoy en día trabajan. Las bandas ISM son

[4] FCC de Federal Comunications Comission
[5] ITU International Telecomunications Union

generalmente libres de licencia debido a que estos dispositivos son de bajo consumo de energía. [1]

En mayo de 1985, y tras cuatro años de estudios, la FCC (Federal Communications Comission), asignó las bandas ISM 902-928MHz, 2.400-2.4835GHz y 5.725-5.850GHz a las redes inalámbricas basadas en espectro disperso. El espectro disperso también es llamado espectro esparcido, spread spectrum o SS. Es una técnica por la cual la señal transmitida se ensancha a lo largo de una banda muy ancha de frecuencias, mucho más amplia, de hecho, que el ancho de banda mínimo requerido para transmitir la información que se quiere enviar. No se puede decir que las comunicaciones mediante espectro disperso son medios eficientes de utilización del ancho de banda. Sin embargo, rinden al máximo cuando se les combina con sistemas existentes que hacen uso de la frecuencia.

Estas bandas son para uso comercial sin licencia: Es decir, la FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda. En 1996, un grupo de empresas del sector de informática móvil (mobile computing) y de servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de una amplia línea de productos y servicios interoperativos.

El NOM-121-SCT1-1994: Se refiere al proyecto de Norma Oficial Mexicana de Sistemas de Radiocomunicación que emplean la técnica de espectro disperso en las bandas de 902-928MHz, 2450-2483.5MHz y 5725-5850MHz. Esta norma dice que los sistemas de radiocomunicación que utilicen la técnica espectro disperso podrán operar en las bandas 902-928MHz, 2450-2483.5MHz y 5725-5850MHz, y están condicionados a no causar interferencia a los equipos ICM (Industriales, Científicos y Médicos), estaciones de radiocomunicación de voz y datos con frecuencia específica asignada. Además estarán expuestos a recibir las interferencias que aquéllas les puedan causar sin que tales sistemas de espectro disperso reclamen protección.

[6] ISM de Industrial, Scientifc and Medical radio frequency

1.2.3.- IEEE

IEEE corresponde a las siglas del Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos, una asociación estadounidense de alcance mundial dedicada a la estandarización. Es una asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros de telecomunicaciones, ingenieros electrónicos e Ingenieros en informática.

Se creó en EE.UU. en 1963 a partir de otras asociaciones como el AIEE (American Institute of Electrical Engineers) y el IRE (Institute of Radio Engineers).

Según el mismo IEEE, su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.

Algunos de sus estándares son:

- **POSIX**

Estándar de funciones POSIX. Estas funciones permiten introducir una interacción completa con el sistema para mejorar la escritura de scripts.

- **IEEE 1394 FireWire**

El IEEE 1394 o FireWire es un estándar multiplataforma para entrada/salida de datos en serie a gran velocidad. Suele utilizarse para la interconexión de dispositivos digitales como cámaras digitales y videocámaras a ordenadores.

- **IEEE 488**

Es un estándar bus de datos digital de corto rango desarrollado por Hewlett-Packard en los años 1970 para conectar dispositivos de prueba y medida (por ejemplo multímetros, osciloscopios, etc) con dispositivos que los controlen como un ordenador.

- **Familia IEEE 802**

Fue formado a principios de los 80's para desarrollar estándares para las tecnologías emergentes, de manera que el equipo de redes de diferentes fabricantes pudiera trabajar junto e integrarse sin problemas.

- **IEEE 802.11**

Estándar para redes inalámbricas IEEE 802.11 ratificado en 1997 por la IEEE.

El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) se ha encargado de crear estándares para regular el uso de frecuencias, anchos de banda, etc., de esta manera se logra un mejor aprovechamiento de recursos tecnológicos y se normalizan los productos de fabricantes distintos. Gracias a esto podemos comprar y utilizar productos de diferentes marcas que sigan un mismo estándar con la seguridad de que van a funcionar en el mismo ambiente y a trabajar juntos.

1.3.- Ventajas y desventajas de las redes inalámbricas

Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. En una red inalámbrica, las computadoras en un edificio, oficinas o hasta en el hogar, se comunican a través de señales de radio. Esto puede hacer que el proceso de crear una red sea relativamente fácil, especialmente si hay computadoras en todo el edificio. También hace más fácil el cambiar la ubicación de una computadora.

1.3.1.- Ventajas

- **Instalación más sencilla**
  Sin cablear, perforar, etc.

- **Flexibilidad**
  Alternativa para aplicaciones de cable

- **Movilidad**
  Aplicaciones móviles portátiles

- **Edificio a Edificio**
  Aplicaciones de Campus

1.3.2.- Desventajas

- Su ancho de banda es menor al de los sistemas cableados
  - Espectro limitado
  - Potencia limitada
  - Nivel de ruido alto
- El ruido y la interferencia les afectan
- Necesitan cierta asignación de frecuencias
- Importancia considerable con la seguridad
- Las paredes y muros pueden obstruir la señal de la red inalámbrica
- Los costos en la implementación pueden sen elevados

1.4.- Aplicaciones de redes inalámbricas

1.4.1 Oficina

- Movilidad inmediata
- Uso más eficiente del espacio
- Instalaciones de de redes temporales

1.4.2 Educación

- Acceso a la red en cualquier lugar del campus
- Acceso a diversos servicios escolares y recursos educativos (biblioteca electrónica, Internet, portales)
- Proyectos de e-learning

1.4.3 Salud

- Estaciones móviles de enfermeras
- Acceso a expedientes, tratamientos, datos de laboratorio, etc., de cada paciente.
- Registros al alcance de los doctores
- Consulta de datos externos

1.4.4 Almacenes y puntos de venta

- Inventarios
- Terminales punto de venta móviles
- Generación de órdenes de compra, embarques, guías en movimiento.

CAPITULO 2

TECNOLOGÍAS INALÁMBRICAS PARA REDES DE AREA LOCAL

Las redes inalámbricas de área local generalmente son clasificadas de acuerdo a la técnica que usen para transmitir. Todos los productos inalámbricos caen en alguna de las categorías siguientes;

- ⇒ Infrared LANs (Redes de Area Local Infrarrojas).
- ⇒ Spread spectrum LANs (Redes de Area Local de espectro disperso).
- ⇒ Narrowband microwave LANs (Redes de Area Lacal por microondas de banda angosta).

En este capitulo se analizan brevemente estas tecnologías, haciendo énfasis en las bandas en que operan así como sus características básicas.

TECNOLOGÍAS INALÁMBRICAS PARA REDES DE AREA LOCAL

2.1.- Radio Frecuencia

2.1.1.- Redes de radiofrecuencia (RF)

Una red de área local de radio frecuencia puede definirse como una red local que utiliza tecnología de radio frecuencia para enlazar los equipos conectados a la red en lugar de los medios utilizados en las LAN[1] convencionales cableadas.

Sus inicios son de los años ochenta. Surgieron por la necesidad de tener interconectividad dentro de espacios abiertos en los que no se podía llegar con cables tan fácilmente, como edificios antiguos donde además cablear es complicado y el costo por tender cables es elevado.

2.1.2.- Beneficios

Movilidad: Proveen a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar donde exista señal de radiofrecuencia dentro de una oficina u organización.

Simplicidad: Es rápida y fácil de instalar y además elimina o minimiza la necesidad de tirar cables.

Flexibilidad en la instalación: Permite a la red ir donde la alambrada no puede ir.

Inversión rentable: Tiene un costo de inversión inicial alto, pero los beneficios y costos a largo plazo son superiores en ambientes dinámicos que

[1] LAN Local Area Network. Por sus siglas en inglés, Red de Area Local.

requieren acciones y movimientos frecuentes, como los salones improvisados para juntas o reuniones temporales donde solo se requiere conectividad por un corto periodo de tiempo.

Escalabilidad: Pueden ser configurados en una amplia variedad de topologías. Las configuraciones son fáciles de cambiar y además es sencilla la incorporación de nuevos usuarios a la red.

Existen varias tecnologías utilizadas en redes inalámbricas. El empleo de cada una de ellas depende mucho de la aplicación. Cada tecnología tiene sus ventajas y desventajas. A continuación se listan las más importantes en este género.

- Infrarrojo (Infrared)
- Banda Ancha (Spread Spectrum)
- Banda Angosta (Narrowband)

2.2.- Redes de Área Local Infrarrojas (Infrared LANs)

Utilizan muy altas frecuencias, justo abajo del espectro de la luz visible para transportar datos. La tecnología reflectiva no requiere línea de vista pero se limita a cuartos individuales en zonas cercanas.

2.2.1- Fortaleza y debilidad

La comunicación inalámbrica infrarroja es comúnmente utilizada en el hogar, donde es utilizada por una gran variedad de artículos de control remoto. Recientemente esta tecnología ha sido aplicada para construir redes inalámbricas de área local. A continuación se analizan algunas características básicas.

Para comenzar, el espectro para red infrarroja es virtualmente ilimitado, el cual tiene la posibilidad de alcanzar altos niveles de transmisión de datos. El espectro infrarrojo no esta regulado en ninguna parte del mundo.

Una de sus desventajas es que no puede penetrar objetos opacos, ya sea directamente o indirectamente (reflectiva). Se reduce a conectar dos redes fijas. Pero esto tiene dos ventajas:

1. La comunicación infrarroja puede ser por mucho, más segura para evitar que personas con malas intensiones escuchen nuestra información.
2. Una instalación infrarroja por separado puede ser operada en cualquier lugar de un edificio sin causar interferencia con otra.

Otro aspecto importante para considerar es que el equipo infrarrojo es relativamente económico y sencillo.

El medio infrarrojo también nos muestra aspectos negativos para considerar. En muchos ambientes interiores se experimenta una intensa radiación infrarroja de la luz solar y luz interior. El ambiente de radiación se presenta como ruido en el receptor infrarrojo, requiriendo el uso de transmisores de más alta potencia. Sin embargo, incrementar el poder de transmisión está limitado por razones de seguridad para los ojos y excesivo consumo de energía.

2.2.2.- Técnicas de transmisión

Existen tres técnicas de transmisión comúnmente usadas para la transmisión de datos infrarroja: la señal transmitida puede ser enfocada y dirigida como en un control remoto de Tv; puede ser radiada omnidireccionalmente; o puede ser reflejada desde el techo.

- *Rayo de Luz directa (IR)* puede ser aplicado para crear conexiones punto a punto. En este modo la amplitud depende del poder emitido y del grado de enfoque del rayo de luz. Con un buen enfoque del rayo de luz la amplitud puede ser de kilómetros.

- *Configuración omnidireccional* consiste en una estación base que esta dentro la línea de visión de todas las demás estaciones de la red LAN. Típicamente estas estaciones son montadas en el techo del lugar. La estación base trabaja como un repetidor multipuerto. El transmisor del techo emite una señal omnidireccional que puede ser recibida por todos los demás transmisores (IR) en el área. Estos otros transmisores (IR) transmiten un rayo direccional dirigido hacia la unidad base del techo.

- *Configuración en modo difusión* todos los transmisores (IR) están enfocados y dirigidos hacia un punto en la difusión reflejada desde el dispositivo en el techo. La radiación (IR) desde el techo es retransmitida omnidireccionalmente y recogida por todos los receptores en el área. [2]

2.3.- Redes de Área Local de Espectro disperso (Spread spectrum LANs)

Hoy en día el tipo de red inalámbrica más usado utiliza técnicas de Spread Spectrum.

2.3.1.- Configuración

Excepto las pequeñas oficinas, una red inalámbrica de área local Spread Spectrum hace uso de un arreglo de múltiples celdas[2]. Las celdas adyacentes hacen uso de diferente centro de frecuencias dentro de la misma banda para evitar interferencia.

Dentro de una celda determinada, la topología pude ser cualquiera, ya sea por concentrador o punto a punto. En la topología de concentrador, el

[2] Área de influencia o cobertura inalámbrica.

concentrador es instalado en una ubicación adecuada y conectado a la red LAN alambrada para proveer conectividad a estaciones conectadas a la red alambrada de área local y a las estaciones que son parte también de la red inalámbrica de área local en otras celdas. El concentrador puede controlar también el acceso, función de punto de coordinación. También podría controlar el acceso actuando como un repetidor multipuerto con funcionalidad similar como los repetidores multipuerto de 10 Mbps y 100 Mbps Ethernet. En este caso todas las estaciones en la celda transmiten solo hacia el concentrador y reciben solo del concentrador.

2.3.2.- Cuestiones clave de transmisión

Una de las características de las redes inalámbricas de área local es que son utilizables sin tener que ir a un procedimiento de licencia para usar una porción del espectro electromagnético. Las regulaciones de licencia difieren de un país a otro. Dentro de los Estados Unidos, la FCC ha autorizado dos aplicaciones dentro de la banda ISM: el sistema de espectro disperso (spread spectrum) el cual puede operar al máximo de 1 watt de potencia, y sistemas de muy bajo poder los cuales pueden operar al máximo de 0.5 watts. Desde que la FCC abrió esta banda, las redes inalámbricas de área local se han hecho muy populares.

En Estados Unidos, tres bandas de microondas han sido puestas al lado del uso sin licencia del espectro disperso:

- ⇒ 902-928 MHz (915-MHz band)
- ⇒ 2.4-2.4835 GHz (2.4-GHz band)
- ⇒ 5.725-5.825 GHz(5.8-GHz band)

Entre más alta sea la frecuencia, se incrementa la potencia de la banda. Un gran número de dispositivos operan en la banda de 900 MHz como los teléfonos inalámbricos, micrófonos inalámbricos y radios sencillos. Operando en la banda de los 2.4 GHz solo hay unos cuantos dispositivos, como ejemplo tenemos a los hornos de microondas, los cuales tienden a tener una gran

emisión de radiación. En el presente hay una leve competencia con la banda de los 5.8 GHz; sin embargo, entre más alta sea la banda de frecuencia, en general el equipo será más costoso. [2]

2.4.- Redes de Área Local por Microondas de Banda Angosta (Narrowband Microwave LANs)

El término de microondas de banda angosta se refiere al uso de microondas de radiofrecuencia, con relativamente reducido ancho de banda, solo lo suficientemente ancha para alojar la señal. Hasta hace poco todos los dispositivos para LANs de microondas de banda angosta habían usado licencia.

2.4.1.- Licencia para banda angosta (RF)

Las microondas por radiofrecuencias, utilizadas para voz, datos y transmisión de video son autorizadas y coordinadas dentro de áreas geográficas específicas para evitar interferencias potenciales entre sistemas. Dentro de Estados Unidos las licencias son controladas por la FCC. Cada área geográfica tiene un radio de 28 km y puede contener 5 licencias, con cada licencia cubre dos frecuencias. Motorota tiene 600 licencias (1200 frecuencias) en el rango de 18 GHz que cubre todas las áreas metropolitanas con población de 30,000 o más.

Ya que en Estados Unidos la empresa Motorola controla la banda de frecuencia, puede asegurar que LANs independientes en locaciones cercanas geográficamente no interferirán una con otra. Para proveer seguridad, todas las transmisiones están encriptadas.

2.4.2.- Banda angosta sin licencia (RF)

En 1995, RadioLAN se convirtió en el primer distribuidor en introducir una red LAN inalámbrica de banda angosta utilizando el espectro sin licencia ISM. Este espectro puede ser usado para trasmisión de banda recta a bajo

poder (0.5 watts o menos). Los productos RadioLAN operan a 10 Mbps en la banda de los 5.8-GHz.

Los productos RadioLAN hacen uso de la configuración punto a punto con una interesante característica. Como un sustituto de hub estacionario, los productos de RadioLAN automáticamente seleccionan un nodo como maestro dinámico, basado en parámetros como ubicación, interferencia y potencia de la señal. La identidad del maestro puede cambiar automáticamente como las condiciones cambien. [2]

2.5.- Bluetooth

En 1994 la empresa L.M. Ericsson se interesó en conectar sus teléfonos móviles y otros dispositivos como los PDA's sin necesidad de cables. En conjunto con IBM, Intel, Nokia y Toshiba formaron un SIG (grupo de interés especial, es decir un consorcio) con el propósito de desarrollar un estándar inalámbrico para interconectar computadoras, dispositivos de comunicaciones y accesorios a través de radios inalámbricos de bajo consumo de energía, corto alcance y económicos. Al proyecto se le dio el nombre de Bluetooth. Aunque la idea original era tan solo prescindir de cables entre dispositivos, su alcance se expandió rápidamente al área de las LAN's inalámbricas. Aunque esta expansión le dio más utilidad al estándar, también provocó el surgimiento de competencia con el 802.11. Los dos sistemas interfieren entre si en ámbito eléctrico. [5]

El SIG de Bluetooth en julio de 1999 dio una especificación de 1500 páginas V1.0. Un poco después el grupo de estándares del IEEE que se encarga de las redes de área personal inalámbricas, 802.15, adoptó como base el documento sobre Bluetooth y empezó a trabajar en el. A pesar de que podría parecer extraño estandarizar algo que ya cuenta con una especificación bien detallada, sin implementaciones incompatibles que tengan que armonizarse, la historia demuestra que al existir un estándar abierto manejado por un cuerpo neutral como el IEEE con frecuencia se estimula el uso de una tecnología.

Bluetooth permite la interconexión de todo tipo de dispositivos electrónicos sin necesidad de cables, es una tecnología hasta cierto punto desconocida por el público pese a estar respaldada por casi 2000 empresas. La celebración del Congreso Bluetooth en Montecarlo y la aparición en el mercado de sus primeras aplicaciones comerciales pueden hacer que como sucede con el nacimiento del último hijo todos los ojos se vuelvan hacia ella.

2.5.1.- Arquitectura de Bluetooth

Bluetooth permite conectar cámaras digitales, auriculares, escáneres y otros dispositivos a una computadora con el único requisito de que se encuentren dentro del alcance de la red. Sin cables, sin instalación de controladores, simplemente se colocan, se encienden y funcionan. Para la mayoría de las personas esta facilidad de operación es algo muy importante.

La unidad básica de un sistema Bluetooth es una piconet[3], que consta de un nodo maestro y hasta 7 nodos esclavos activos a una distancia de 10 metros. En una misma sala pueden conectarse varias piconets y se pueden conectar mediante un nodo puente. Un conjunto de piconets interconectadas se denomina sacatnet.

Además de los 7 nodos esclavos activos de una piconet, puede haber hasta 255 nodos estacionados en la red. Estos son dispositivos que el nodo maestro ha cambiado a un estado de bajo consumo de energía para reducir el desgaste innecesario de sus pilas. Lo único que un dispositivo en estado estacionado puede hacer es responder a una señal de activación por parte del maestro.

La razón para el diseño maestro/esclavo es que los diseñadores pretendían facilitar la implementación de chips Bluetooth completos por debajo

[3] Piconet. Una piconet esta formada por al menos dos dispositivos, como puede ser un teléfono cellular con una computadora.

de 5 dólares. La consecuencia de esta decisión es que los esclavos son sumamente pasivos y realizan todo lo que los maestros indican. En esencia, una *piconet* es un sistema TDM[4] centralizado, en el cual el maestro controla el reloj y determina que dispositivo se comunica en un momento determinado. Todas las comunicaciones se realizan entre el maestro y el esclavo; no existe comunicación directa de esclavo a esclavo. [3]

Para que la tecnología Bluetooth pueda operar en todo el mundo es necesaria una banda de frecuencia abierta a cualquier sistema de radio independientemente del lugar del planeta donde se encuentre el equipo; para ello, sólo la banda ISM de 2,4 Ghz cumple con éste requisito, con rangos que van de los 2.400 Mhz a los 2.500 Mhz, y solo con algunas restricciones en países como Francia, España y Japón.

La velocidad máxima de transferencia de datos es de aproximadamente 720 kbps. Al encender los aparatos bluetooth, estos buscan e identifican automáticamente cualquier otro dispositivo que e encuentre dentro de su campo de alcance. Cuando estén conectados simultáneamente hasta siete aparatos al dispositivo maestro, los usuarios estarán creando una red personal.

Cada dispositivo equipado con bluetooth está exclusivamente identificado con una dirección, contraseña y nombre especificado por el usuario. Los usuarios pueden configurar sus aparatos bluetooth para que estén disponible a un grupo selecto o a múltiples dispositivos en el campo de alcance, dependiendo de sus preferencias personales. Por ejemplo, si un usuario desea conectarse al aparato de otro usuario equipado con Bluetooth, este obtendrá todos los nombres especificados por los usuarios dentro de su campo de alcance, para poder escoger así el aparato correcto.

[4] TDM. La **Multiplexación por división de tiempo** (**MDT**) o (**TDM**), del inglés *Time Division Multiplexing*, es la más utilizada en la actualidad, especialmente en los sistemas de transmisión digitales. En ella, la anchura de banda total del medio de transmisión es asignada a cada canal durante una fracción del tiempo total (intervalo de tiempo).

2.5.2.- Interferencia y solución

Bluetooth trata de superar las desventajas de dispositivos cableados y la tecnología infrarroja. Opera en la frecuencia de los 2.4 GHz, que es la misma que usan los estándares IEEE 802.11b y 802.11g, así como hornos de microondas y teléfonos inalámbricos.

Una de las maneras en que Bluetooth evita la interferencia con otros dispositivos es enviando señales muy débiles de 1 mW. (Watt = unidad de potencia). En comparación con los teléfonos inalámbricos que usan 3 W [6]. El poco poder limita el rango del dispositivo Bluetooth a aproximadamente 10 metros evitando así las posibilidades de interferencia. Aun con este bajo poder, las paredes de un edificio no detienen la señal, haciendo este estándar útil para controlar dispositivos en diferentes cuartos.

Se podría pensar en un área con múltiples dispositivos Bluetooth, se crearía interferencia entre ellos, pero los dispositivos no usan la misma frecuencia al mismo tiempo, ya que se emplea la técnica FHSS[5], que implica que un dispositivo usa una frecuencia de 79 disponibles, escogida en forma aleatoria y la cambia en forma regular. En el caso de Bluetooth, los transmisores cambian de frecuencia 1600 veces cada segundo, lo que implica que más dispositivos pueden hacer uso del espectro de radio. Esto implica también que otros dispositivos propios de una casa interrumpan con la transmisión, ya que cualquier interferencia en una frecuencia en particular solo durará una pequeña fracción de segundo.

2.5.3.- Aplicación Bluetooth

Esta tecnología tiene un sin número de aplicaciones, aplicaciones que van desde ambientes de trabajo (oficinas), en el hogar, el en ámbito comercial y no solo busca la interconexión de distintos dispositivos que estén dentro de una misma zona sino que en esencia, lo que más busca esta tecnología es que

[5] FHSS de Frecuency Hopping Spread Spectrum. Transmisión de ensanchamiento del espectro por saltos de frecuencia.

diversos dispositivos (sin importar el fabricante) puedan sincronizarse al entrar a una misma zona de interconexión ó piconet, manteniendo de esta manera actualizados a todos los dispositivos que estén bajo su dominio.

Así pues, solo por mencionar algunas de las importantes prestaciones que la tecnología Bluetooth puede ofrecer son:

a) Validación de boletos.
b) La automatización de un sin número de actividades en el hogar, en la oficina, en el auto.
c) Transferencia de información.
d) Se pueden recibir boletines de ofertas que ofrece alguna tienda de manera inmediata al pasar cerca de ella.
e) El conectarse con la red de redes de forma inalámbrica.

2.5.4.- Ventajas e Inconvenientes de Bluetooth

La ventaja más evidente es que permite conectar entre sí todo tipo de dispositivos electrónicos (teléfonos, computadoras personales, impresoras, faxes, etc) situados dentro de un radio limitado de 10 metros sin necesidad de utilizar cables.

Bajo costo y corto alcance, proporcionando conexiones instantáneas para entornos de comunicaciones tanto móviles como estáticos.

El espectro de radiofrecuencia en el que opera no está abierto al público en todos los países. En lugares como Francia o España el uso del espectro está restringido y se requiere la aprobación explícita del gobierno para poder usarlo. La interoperabilidad, pilar sobre el que se sustenta Bluetooth, es uno de los factores que se someterán a tensiones en el largo plazo. Con miles de compañías diseñando productos y aplicaciones Bluetooth, será difícil mantenerlas a todas bajo el mismo manto. [7]

CAPITULO 3

ESTANDAR DE REDES INALAMBRICAS DE AREA LOCAL WiFi

En este capítulo se analiza el estándar de comunicaciones 802.11 de la IEEE, haciendo énfasis en las diferencias que existen entre los estándares 802.11, 802.11a, 802.11b y 802.11g ya que estos definen la tecnología de redes inalámbricas de área local. También se analiza brevemente el tipo de redes en las que trabaja este estándar, así como los servicios que ofrece.

3.- ESTANDAR DE REDES INALAMBRICAS DE AREA LOCAL WiFi

3.1.- IEEE 802.11

3.1.1.- Aspectos del estándar 802.11

Muchas personas llaman al estándar 802.11 "Ethernet inalámbrico" para enfatizar su descendencia compartida con el Ethernet tradicional (802.3). Recientemente la Alianza de Compatibilidad de Ethernet Inalámbrico (WECA[1]) ha estado introduciendo su programa de certificación de fidelidad inalámbrica (Wi-Fi[2]). Cualquier vendedor de productos 802.11 puede hacer que sus productos sean probados para la interoperabilidad.

El producto que pase el conjunto de pruebas puede usar la marca Wi-Fi. Para los productos 802.11a, la WECA autoriza el uso de la marca Wi-Fi5, el número 5 refleja que el producto usa otra frecuencia, alrededor de los 5 GHz.

La tabla 3.1 es una comparación básica de los diferentes estándares 802.11. Los productos basados en el estándar 802.11 salieron en 1997. Al principio los productos 802.11 estaban limitados a 2 Mbps, que es bastante poco para estos días. El grupo de trabajo del IEEE 802.11 empezó a trabajar rápidamente en capas de radio frecuencias más veloces.

Estándar	Velocidad	Banda de Frecuencia	Comentarios
802.11	1 y 2 Mbps	2.4 GHz	Primer estándar (1997)
802.11a	Hasta 54 Mbps	5 GHz	Segundo estándar (1999), pero sus productos no se vendieron hasta el 2000
802.11b	5.5 y 11 Mbps	2.4 GHz	Tercer estándar, el mas común hoy en día.
802.11g	Hasta 54 Mbps	2.4 GHz	Conveniente y barato, compatible con 802.11b

Tabla 3.1 Primeros estándares IEEE 802.11

[1] WECA Wireless Ethernet Compatibility Alliance
[2] Wi-Fi Wireless Fidelity

A las tarjetas de red inalámbrica, se les asigna un número de control de acceso al medio (MAC[3], por sus siglas en inglés) de 48 bits, y para propósitos prácticos parecen tarjetas de red Ethernet. De hecho, la asignación de direcciones MAC es regulada por la misma fuente, así que las tarjetas 802.11 tienen una dirección MAC única aun si se mezclan con tarjetas de red convencionales. Para los demás dispositivos de la red, la MAC de una tarjeta inalámbrica es como cualquier otra, también se almacena en las tablas del Protocolo de Resolución de Direcciones (ARP[4]). Hay muchas diferencias entre dispositivos inalámbricos y dispositivos Ethernet, pero la más obvia es que los dispositivos inalámbricos son móviles; se pueden mover fácilmente de un lugar a otro dentro de la red pero a diferencia de dispositivos Ethernet (red alambrada) los dispositivos inalámbricos requieren de una antena para lograr tener buena señal inalámbrica.

El estándar 802.11 permite accesos móviles a la red; para lograr esta meta, un número de características adicionales se agregaron a la MAC. Como resultado, la MAC 802.11 puede verse un poco mas complicada comparada con MAC de otras especificaciones IEEE 802.

3.1.2.- Operaciones de red 802.11

A simple vista, 802.11 fue diseñado para ser simplemente otra capa de enlace para protocolos de capas superiores. Los administradores de redes familiarizados con Ethernet lo están inmediatamente con 802.11.

Los elementos principales presentes en Ethernet están presentes en 802.11. Las estaciones son identificadas por una dirección MAC IEEE 802 de 48 bits. Conceptualmente, los marcos de las tramas de datos son entregados basándose en la dirección MAC. La entrega de marcos no es muy confiable,

[3]MAC. Media Access Control; es un identificador físico, un número único en el mundo de 48 bits, almacenado en fábrica dentro de una tarjeta de red. Las direcciones MAC son asignadas por el IEEE y son utilizadas en varias tecnologías incluyendo: ethernet, token ring, 802.11 (WiFi).
[4] ARP de Address Resolution Protocol.

aun cuando 802.11 incorpora algunos mecanismos de confiabilidad para compensar la transmisión de datos importantes en forma omnidireccional característica del canal de radio que usa.

3.2.- Diseño 802.11

Las redes 802.11 constan de cuatro principales componentes físicos, que están resumidos en la figura 3.1.

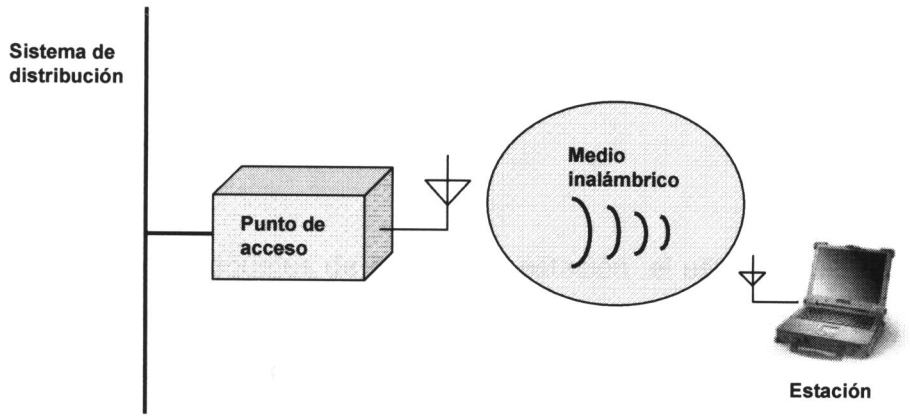


Figura 3.1 Componentes de una WLAN

3.2.1.- Sistema de distribución

Cuando varios puntos de acceso están conectados para formar un área grande de cobertura, se deben comunicar unos con otros para rastrear los movimientos de las estaciones móviles. El sistema de distribución es el componente lógico de 802.11 usado para retransmitir paquetes a su destino. 802.11 no especifica una tecnología en particular para el sistema de distribución. En los productos comerciales, el sistema de distribución es implementado como una combinación de un puente y un medio del sistema de distribución, que es el troncal de la red usado para enviar paquetes entre

puntos de acceso, a menudo es llamado simplemente el troncal de la red. En la mayoría de las soluciones actuales, Ethernet es usado como troncal de red.

3.2.2.- Puntos de acceso

Los paquetes de una red 802.11 deben ser convertidos a paquetes de otro tipo de red para que puedan llegar al resto del mundo. Los dispositivos llamados puntos de acceso hacen la función de puente de una red inalámbrica a una red alambrada. Los puntos de acceso también realizan muchas otras funciones, pero la función de puente es por mucho la más importante.

3.2.3.- Medio inalámbrico

Para mover paquetes de estación a estación, el estándar usa un medio inalámbrico. Diferentes capas físicas son definidas, la arquitectura permite que capas físicas sean desarrolladas para soportar la MAC 802.11. Inicialmente, dos capas físicas de radio frecuencia y una capa física de luz infrarroja fueron estandarizadas, aunque las primeras son más populares.

3.2.4.- Estaciones

Las redes están hechas para transmitir información entre estaciones. Las estaciones son dispositivos computacionales con interfaces de red inalámbrica. Generalmente, las estaciones son computadoras portátiles o dispositivos personales tipo PDA (Personal Digital Assistant) como las Palms[5] o iPaqs[6]. No hay razón por la cual las estaciones deban ser dispositivos portátiles. En algunos ambientes, las redes inalámbricas son usadas para evitar tender cable, y las estaciones de trabajo se conectan por medios inalámbricos.

[5] Palms. Asistente digital personal de tamaño reducido y portátil.
[6] El iPAQ. es la PDA (Personal Data Assistant) para PocketPC de HP

3.3.- Tipos de redes

La pieza básica de una red 802.11 es el conjunto de servicio básico (BSS[7]), que es simplemente un grupo de estaciones que se comunican entre ellas. La comunicación toma lugar en un área irregular, llamada área de servicio básico, definida por las características de propagación del medio inalámbrico. Cuando una estación está en el área de servicio básico, se puede comunicar con los otros miembros del BSS. El BSS viene en dos maneras, las cuales se muestran en la figura 3.2.

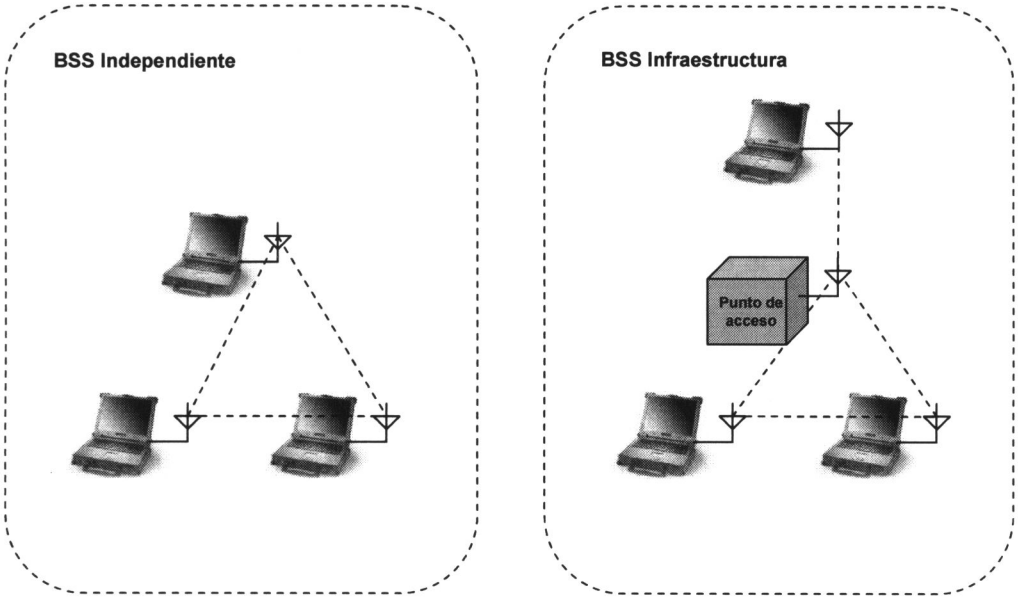


Figura. 3.2 BSS Ad-Hoc y de tipo infraestructura.

3.3.1.- Redes Ad-Hoc

A la izquierda en la figura 3.2 se muestra un BSS independiente. Las estaciones en una red Ad-Hoc se comunican directamente con las demás, y de esa manera deben estar dentro de un rango de comunicación directa. La red

[7] BSS de Basic Service Set

ad-hoc mas pequeña posible es de dos estaciones. Usualmente, las redes ad-hoc están compuestas por pocas estaciones configuradas para propósitos específicos o por periodos cortos de tiempo. Un uso común es crear una red temporal para cubrir las necesidades de una junta en un salón de conferencias. Cuando la junta comienza, los participantes crean la red para compartir información. Una vez que la junta termina, la red se disuelve.

3.3.2.- Redes tipo infraestructura

En la parte derecha de la figura 3.2 hay un BSS infraestructura. Se distinguen por el uso de un punto de acceso. Los puntos de acceso son usados para todas las comunicaciones en las redes infraestructura, incluyendo la comunicación entre nodos móviles en la misma área de servicio. Si una estación móvil en una red infraestructura necesita comunicarse con una segunda estación, la comunicación debe tomar dos saltos. Primero, la estación origen transfiere el paquete al punto de acceso, segundo, el punto de acceso transfiere el paquete a la estación destino. Con todas las comunicaciones llevadas a cabo a través de un punto de acceso, el área básica de servicio que corresponde a un BSS infraestructura esta definida por los puntos en los cuales las transmisiones del punto de acceso pueden ser recibidas.

⇒ Un BSS infraestructura esta definido por el alcance del punto de acceso. Todas las estaciones requieren estar dentro del alcance del punto de acceso, pero no hay restricción en cuanto a la distancia entre las estaciones. Permitir comunicación directa entre las estaciones ahorra capacidad de transmisión, pero a costo de incrementar la complejidad de la capa física debido a que las estaciones móviles deberán mantener relaciones de vecinos con todas las otras estaciones móviles del área de servicio para encaminar los paquetes entre todos ellos.

⇒ Los puntos de acceso en modo infraestructura pueden ayudar a las estaciones a ahorrar energía. Los puntos de acceso pueden notar cuando una estación entra en modo de ahorro de energía y guarda los paquetes para ella. Las estaciones que dependen de una batería pueden apagar el receptor / emisor inalámbrico y solo prenderlo para recibir y transmitir paquetes guardados en el punto de acceso.

En una red tipo infraestructura, las estaciones se deben asociar con el punto de acceso para obtener los servicios de red. La asociación es el proceso mediante el cual una estación móvil se une a una red 802.11; es lógicamente equivalente a conectar el cable en una red Ethernet. Las estaciones móviles siempre inician el proceso de asociación, y los puntos de acceso pueden escoger entre darles o denegarles el acceso basándose en el contenido de la petición de asociación. Las asociaciones también son exclusivas en la parte de la estación móvil, una estación solo puede estar asociada a un punto de acceso. El estándar 802.11 no pone limite en el número de estaciones móviles que un punto de acceso puede dar servicio. Las consideraciones en la implementación, por supuesto, limitan el número de estaciones móviles por punto de acceso. En la práctica, por otra parte, el bajo ancho de banda de las redes inalámbricas tiende a limitar el número de estaciones móviles por red.

3.4.- Áreas de servicio extendidas

Las BSSs pueden crear una cobertura en casa u oficinas pequeñas, pero no pueden proveer cobertura a áreas más extensas. El estándar 802.11 permite crear redes inalámbricas de un gran tamaño arbitrario ligando BSSs en un *conjunto de servicio extendido* (ESS[8]). Un ESS es creado encadenando BSSs juntas con un troncal de red. El estándar 802.11 no especifica una tecnología de troncal en particular; requiere solamente que el troncal ofrezca un conjunto de servicios. En la figura 3.3 el ESS es la unión de los cuatro BSSs (asumiendo que todos los puntos de acceso están configurados para ser parte

[8] ESS de Extended Service Set

del mismo ESS). En las soluciones del mundo real, el grado de sobreposición sería probablemente mayor al que se muestra en la figura 3.3.

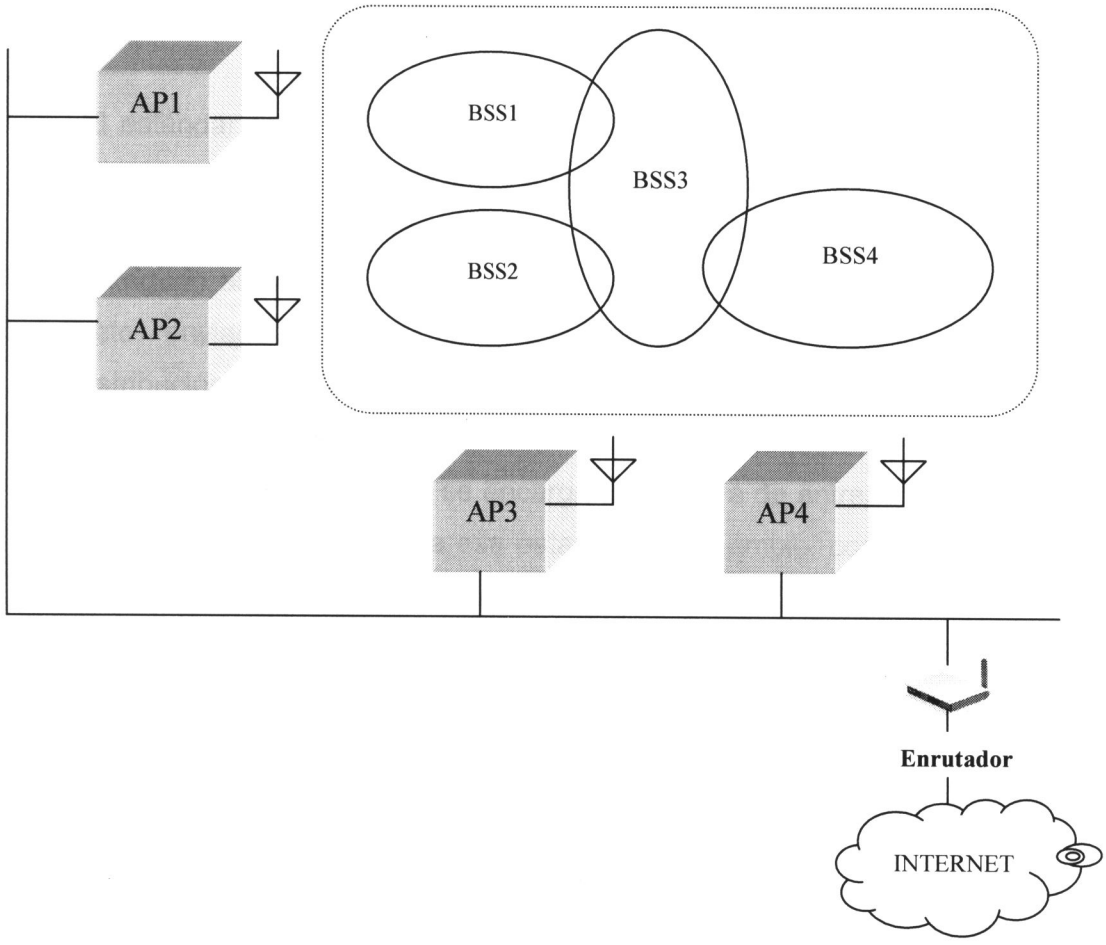


Figura 3.3. Conjunto de servicio extendido

Las estaciones dentro de un mismo ESS pueden comunicarse entre ellas, aun cuando puedan estar en diferentes áreas de servicio básico y aun más si se están moviendo entre diferentes áreas de servicio básico. Para que las estaciones en un ESS se puedan comunicar entre ellas, el medio inalámbrico debe actuar como si fuera una sola conexión de la capa de enlace de datos. Los puntos de acceso actúan como puentes, así la comunicación directa entre estaciones en un ESS requiere que el troncal también sea una conexión de capa de enlace de datos. Cualquier conexión de capa de enlace será suficiente. Varios puntos de acceso en un área pueden estar conectados a

un solo switch o concentrador, o pueden usar redes virtuales si la conexión de capa de enlace debe cubrir un área grande.

3.5.- El sistema de distribución

El estándar 802.11 describe al sistema de distribución en términos del servicio que provee a las estaciones inalámbricas. El sistema de distribución provee movilidad al conectarse a los puntos de acceso. Cuando un paquete es entregado al sistema de distribución, es entregado al punto de acceso correcto enviado por el punto de acceso a la estación deseada. El sistema de distribución es responsable de saber donde esta una estación dada y entregar los paquetes apropiadamente. Cuando un paquete es enviado a una estación móvil, el sistema se encarga de la tarea de entregarlo al punto de acceso que le da servicio a esa estación. Por ejemplo, consideremos el enrutador de la figura 3.3. El enrutador simplemente usa la dirección MAC de una estación móvil como destino. El sistema de distribución de ESS debe entregar el paquete al punto de acceso correcto. Obviamente, una parte del mecanismo de entrega es el troncal Ethernet, pero el troncal no puede ser el sistema de distribución completo porque no tiene manera de saber escoger el punto de acceso correcto.

Para encontrar el resto del sistema de distribución, se necesita voltear a los mismos puntos de acceso. La mayoría de los puntos de acceso actuales operan como puentes. Tienen por lo menos una interfaz inalámbrica y otra Ethernet. El lado Ethernet puede ser conectado a una red existente, y el lado inalámbrico se convierte en una extensión de esa red. El manejo de paquetes entre los dos medios de red es controlado por un puente.

La figura 3.4 ilustra la relación entre el punto de acceso, troncal de red y el sistema de distribución. El punto de acceso tiene dos interfaces conectadas por un puente. Las flechas indican las rutas potenciales desde y hacia el puente. Los paquetes pueden ser enviados por el puente a la red inalámbrica; cualquier paquete enviado por el puerto inalámbrico del puente es transmitido a todas las estaciones asociadas. Cada estación asociada

puede transmitir paquetes al punto de acceso. Finalmente, el puerto del troncal en el puente puede interactuar directamente con el troncal de red. El sistema de distribución en la figura 3.4 esta compuesto por el puente más el troncal de red.

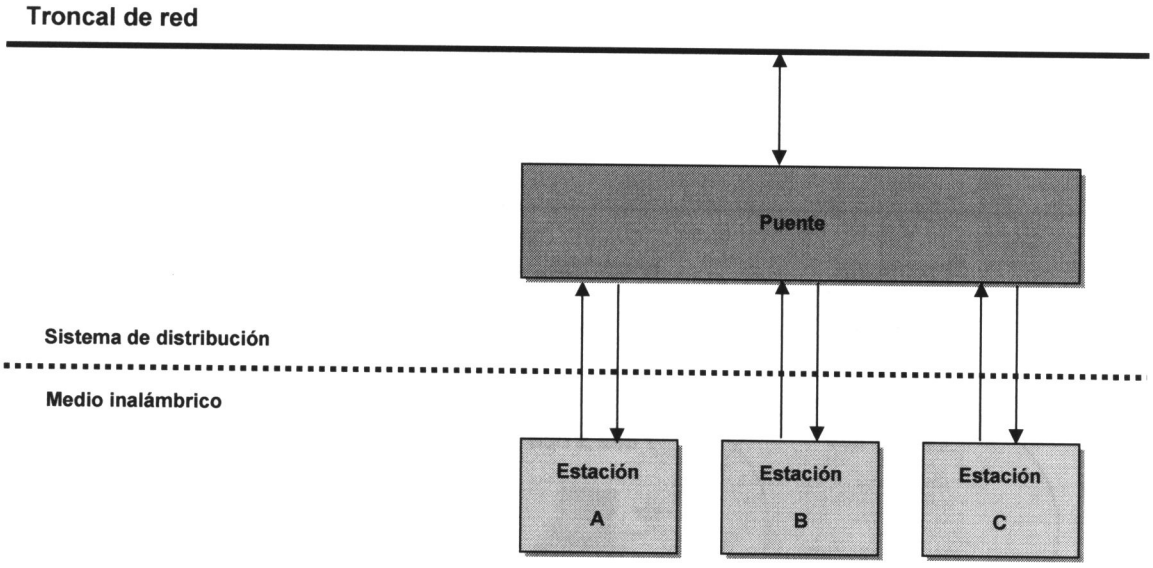


Figura 3.4 Sistema de distribución en implementaciones de puntos de acceso 802.11

3.6.- Soporte de movilidad

La movilidad es la mayor motivación para implementar una red 802.11 las estaciones se pueden mover mientras permanecen conectadas a la red. La movilidad puede causar una de tres tipos de transiciones:

Sin transición: cuando las estaciones no se mueven fuera del área de servicio de su punto de acceso actual, no es necesaria ninguna transición. Este estado ocurre debido a que la estación no se mueve o se mueve dentro del área de servicio básico de su punto de acceso actual.

Transición BSS: La figura 3.5 ilustra una transición BSS. Los tres puntos de acceso en la figura están todos asignados al mismo ESS. Al principio, denotado por *t=1*, la computadora con una tarjeta de red 802.11 esta dentro del área de servicio básico del punto de acceso AP1 asociada al BSS 1. Cuando la

computadora se mueve fuera del BSS 1 y entra al BSS2 en *t*=2, ocurre una transición BSS. La estación móvil usa el servicio de reasociación para asociarse con el punto de acceso AP2, que entonces empieza a mandar marcos a la estación móvil.

Las transiciones BSS requieren la cooperación de los puntos de acceso. En este ejemplo, el punto de acceso AP2 necesita informar al punto de acceso AP1 que la estación móvil esta ahora asociada con él. 802.11 no especifica los detalles de la comunicación entre puntos de acceso entre transiciones BSS.

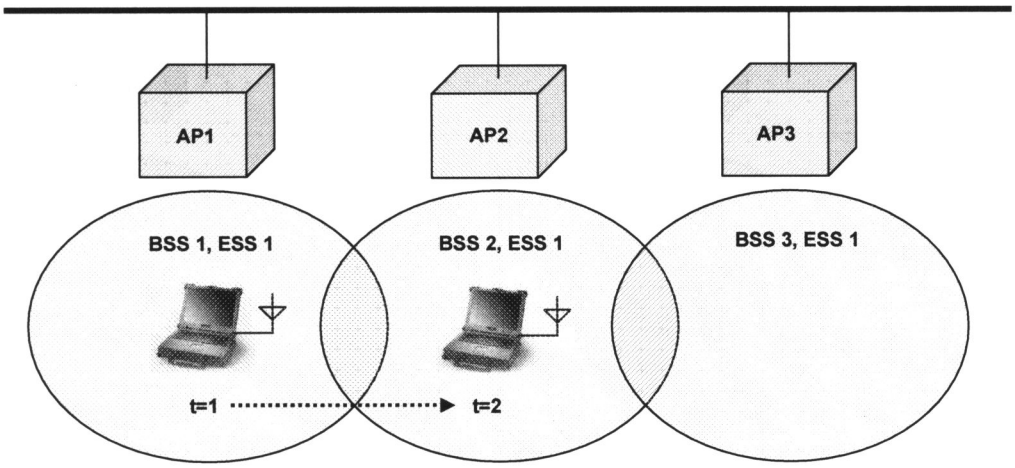


Figura 3.5 Transición BSS

Transición ESS: se refiere al movimiento desde un ESS hacia otro distinto. 802.11 no soporta este tipo de transición, excepto para permitir a la estación móvil asociarse con un punto de acceso en otro ESS una vez que deja el primero. Las conexiones de capas superiores son interrumpidas casi en forma garantizada. Es bueno decir que 802.11 acepta transiciones ESS solo porque es relativamente fácil tratar de asociarse con un punto de acceso en el nuevo ESS. El mantener conexiones de más alto nivel requiere soporte del conjunto de protocolos en cuestión. En el caso de TCP/IP, IP móvil[9] es requerido para tratar de soportar la transición ESS.

[9] El protocolo IP móvil permite que ordenadores configurados para funcionar en una subred determinada cambien de subred y sigan funcionando exactamente como lo harían si estuviesen en su subred original.

La figura 3.6 ilustra una transición ESS. Cuatro áreas de servicio básico están organizadas en dos áreas de servicio extendido. Transiciones limpias y sin problemas desde el ESS 1 hacia el ESS 2 no están soportadas. Las transiciones ESS son soportadas únicamente porque la estación móvil se asociará rápidamente con el punto de acceso en el segundo ESS. Cualquier conexión de red activa se caerá cuando la estación móvil deje el primer ESS. [4]

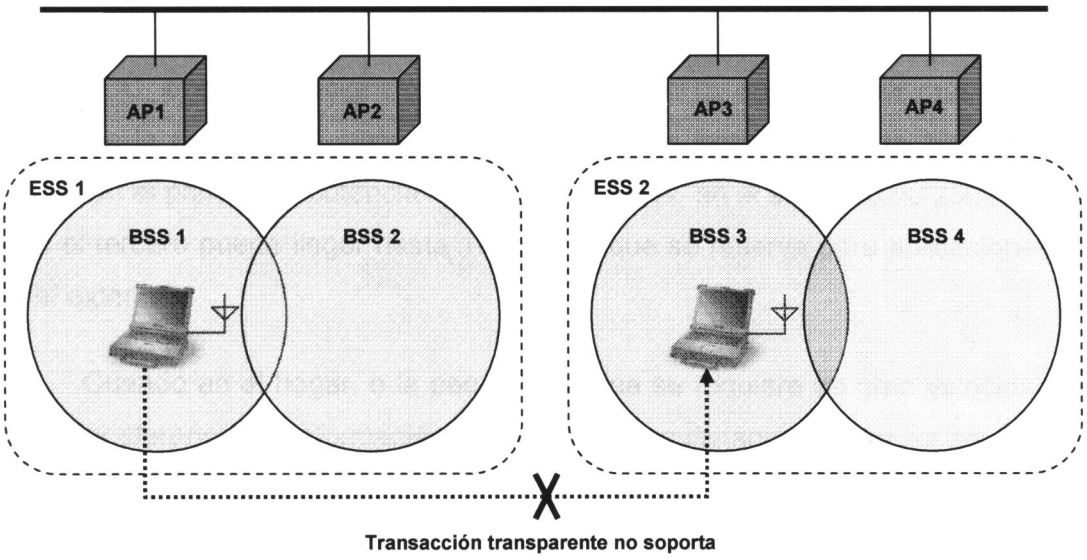


Figura 3.6 Transición ESS

3.7.- Estándar 802.11

En 1997 el IEEE creó el primer estándar de redes inalámbricas. Fue llamado 802.11, desafortunadamente solo soportaba un máximo de 2 Mbps, demasiado lento para la mayoría de las aplicaciones. Por esta razón, los productos del estándar 802.11 ya no son fabricados.

3.8.- IEEE 802.11a

3.8.1.- Aspectos del estándar IEEE 802.11a

La primera de las LANs inalámbricas de alta velocidad. El IEEE ratificó en julio de 1999 el estándar en 802.11a (los productos comerciales comenzaron a aparecer a mediados del 2002), que con una modulación QAM-64[10] y la codificación OFDM (Orthogonal Frequency Division Multiplexing) alcanza una velocidad de hasta 54 Mbit/s en la banda de 5 GHz, menos congestionada y por ahora, con menos interferencias, pero con un alcance limitado.

La banda de 5 GHz que utiliza se denomina UNII (Infraestructura de Información Nacional sin Licencia), que en los Estados Unidos está regulada por la FCC, el cual ha asignado un total de 300 MHz, cuatro veces más de lo que tiene la banda ISM, para uso sin licencia, en tres bloques de 100 MHz, siendo en el primero la potencia máxima de 50 mW, en el segundo de 250 mW, y en el tercero puede llegar hasta 1W, por lo que se reserva para aplicaciones en el exterior.

Cuando en el hogar, o la pequeña oficina se requiere de gran velocidad en la transferencia de información inalámbrica y las distancias entre los equipos inalámbricos son cortas este estándar es el adecuado.

3.8.2.- Ventajas

- Lo que hace que la red 802.11a sea única entre las redes Wi-Fi es que se ejecuta a una velocidad de 5.0 mega hercios (MHz) en lugar de a 2.4 MHz que utiliza tanto el estándar 802.11b como el 802.11g. De este modo se evitan problemas de interferencia con la mayoría de los teléfonos inalámbricos que por lo general operan en la banda de 2.4 MHz.
- Su máxima velocidad es la más alta en comparación con el estándar 802.11b y el 802.11g.
- Soporta más usuarios simultáneos.

[10] QAM-64 Modulación de Amplitud en Cuadratura. Ofrece la posibilidad de transmitir dos señales en la misma frecuencia, de forma que favorece el aprovechamiento del ancho de banda disponible.

- Las frecuencias reguladas previenen de interferir con otros aparatos.

3.8.3.- Desventajas

- Alto costo debido a que opera en una frecuencia más alta, entre más alta sea la frecuencia de operación mayor será el costo de los dispositivos.
- Señal de cobertura limitada dado que sus ondas son más fácilmente absorbidas y en comparación con los otros estándares es fácilmente obstruida.
- Si se pretende utilizar en combinación con estándares 802.11b y/o 802.11g se requeriría de un adaptador que incrementaría considerablemente el costo.

3.8.4.- Costos

El costo de los dispositivos con este estándar es el más alto en comparación con los estándares 802.11b y 802.11g, esto se debe principalmente a que trabaja en una frecuencia más alta (5.0 GHz). Un punto de acceso para hogar o pequeña oficina con este estándar oscila entre $120 y $160 dólares y las tarjetas de red alrededor de $80 y $100 dólares.

3.9.- IEEE 802.11b

3.9.1.- Aspectos del estándar 802.11b

HR-DSSS (Espectro Disperso de Secuencia Directa de Alta Velocidad), otra técnica de espectro disperso. El 802.11b no es la continuación del 802.11a. De hecho su estándar se aprobó primero y apareció primero en el mercado. Las tasas de datos soportadas por 802.11b son 1, 2, 5.5 y 11 Mbps en la banda de 2.4 GHz.

En la práctica, la velocidad de operación de 802.11b siempre es aproximadamente 11Mbps. Aunque 802.11b es más lento que 802.11a su rango es aproximadamente 7 veces mayor, lo que es más importante en muchas situaciones. Por ejemplo, cuando se requiere comunicación entre edificios y/o oficinas grandes.

Trabaja a buena velocidad y alcance, pero presenta una menor seguridad como se verá en el siguiente capítulo. El alcance puede llegar a los 100 metros, suficientes para un entorno de oficina o residencial.

3.9.2.- Ventajas

- Menor costo, ya que esta banda es ampliamente usada y en el mercado podemos encontrar una gran variedad de artículos.
- La señal es mejor que 802.11a en cuestión de alcance y no es obstruida tan fácilmente.

3.9.3.- Desventajas

- Su máxima velocidad es baja en comparación con el estándar 802.11a y 802.11g.
- Soporta pocos usuarios simultáneos y aparatos electrodomésticos que trabajan en la misma banda de 2.4 GHz como teléfonos inalámbricos y hornos microondas pueden causar interferencia.

3.9.4.- Costos

Actualmente los costos varían mucho dependiendo de las características y marcas de los dispositivos. Para el estándar 802.11b hay una gran variedad de marcas, el costo aproximado de un Punto de Acceso con este estándar oscila entre $60 y $100 dólares y el costo de las tarjetas de red inalámbricas ya sea por puerto USB, PCMCIA o para puerto PCI, oscila entre $35 y $65 dólares.

3.10.- IEEE 802.11g

3.10.1.- Aspectos del estándar 802.11g

En noviembre de 2001, el IEEE aprobó una versión mejorada de 802.11b que es el 802.11g, después de mucha discusión por cuál tecnología patentada podría utilizar. Utiliza el método de modulación OFDM de 802.11a pero opera en la banda ISM más estrecha (2.4 GHz) junto con 802.11b. En teoría puede operar hasta 54 Mbps. Aún no se ha decidido si esta velocidad se va a alcanzar en la práctica.

3.10.2.- Ventajas

- Su máxima velocidad es más alta que el estándar 802.11b.
- Soporta más usuarios simultáneos y la señal de cobertura es la mejor y no es fácilmente obstruida.

3.10.3.- Desventajas

- Los productos 802.11g son más caros que los productos 802.11b.
- Otros aparatos electrodomésticos que trabajan en la misma banda de frecuencia de 2.4 GHz pueden causar interferencia.

3.10.4.- Costos

Al igual que con el estándar 802.11b los costos varían dependiendo de las marcas de los fabricantes. El costo por dispositivos con el estándar 802.11g es mayor al 802.11b aproximadamente un Punto de Acceso inalámbrico para casa u oficina con este estándar va de los $75 a los $150 dólares, mientras que las tarjetas de red inalámbricas 802.11g van de los $60 a los $100 dólares aproximadamente.

La tabla 3.2 muestra características importantes con las que se pueden comparar las tres tecnologías existentes de redes inalámbricas de una mejor manera.

Estándar	802.11a	802.11b	802.11g
Frecuencia	5 GHZ Puede coexistir con redes de la banda de 2.4 GHz sin interferir	2.4 GHz esta banda está ampliamente usada y pueden interferir otros aparatos como electrodomésticos	2.4 GHz esta banda está ampliamente usada y pueden interferir otros aparatos como electrodomésticos
Velocidad	54 Mbps 5 veces mayor que 802.11b	11 Mbps Comparable con Ethernet (10 Mbps)	54 Mbps 5 veces mayor que 802.11b
Promedio de Transferencia Real	27 Mbps	4 - 5 Mbps	20 – 25 Mbps
Canales / sin Sobreponerse	12 / 8	11 /3	11 / 3
Cobertura (depende de la antena, poder de transmisión, sensibilidad de la tarjeta receptora y de los obstáculos)	Mas corta que 802.11b y 802.11g debido a que opera en una frecuencia mas alta	Mejor que 802.11a. La señal viaja mas lejos y puede atravesar paredes y pisos mejor que las señales de 5 GHZ	Mejor que 802.11a. La señal viaja mas lejos y puede atravesar paredes y pisos mejor que las señales de 5 GHZ
Compatibilidad	Incompatible con 802.11 b y 802.11g	Ampliamente adoptada. Puede trabajar en redes 802.11g	Compatible con 802.11b. Incompatible con 802.11a
Popularidad	Uso relativamente bajo todavía. Hay pocos productos para escoger	Su uso es el mas amplio, es usado actualmente en aeropuertos, hoteles, cafés. Amplia gama de productos para escoger	Recién salido al mercado. Se espera que sustituya al estándar 802.11b
Costo	El mas caro	Barato	Precio relativamente bajo. Puede competir con 802.11b. Más barato que 802.11a
Beneficios	Excelente velocidad. No es afectado por dispositivos 2.4 GHz. Puede coexistir con redes 802.11b y 802.11g, ya que no causa interferencia.	Ampliamente usado, es usado en cafés, aeropuertos, hoteles para uso publico. Amplia gama de productos para escoger.	La velocidad de 802.11a con la cobertura de 802.11b. Puede ser el sustituto de 802.11b.
Aprobación del estándar	Septiembre de 1999	Septiembre de 1999	Junio de 2003
Ancho de banda disponible	300 MHz	83.5 MHz	83.5 MHz
Frecuencia de operación sin licencia	5.15 – 5.35 GHz OFDM 5.725 – 5.825 GHz OFDM	2.4 – 2.4835 GHz DSSS	2.4 – 2.4835 GHz DSSS, OFDM
Tasa por canal	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2, 1 Mbps
Tipo de modulación	BPSK (6 y 9 Mbps) QPSK (12 y 18 Mbps) 16-QAM (24 y 36 Mbps) 64-QAM (48 y 54 Mbps)	DQPSK/CCK (11 y 5.5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)	OFDM/CCK (6, 9, 12, 18, 24, 36, 48, 54 Mbps) OFDM (6, 9, 12, 18, 24, 36, 48 y 54 Mbps) DQPSK/CCK (22, 33, 11 y 5.5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)

Tabla 3.2 Características de tecnologías 802.11a, 802.11b y 802.11g [5]

3.11.- COMPATIBILIDAD Wi-Fi

El comité 802.11 ha producido 3 LANs inalámbricas diferentes de alta velocidad: 802.11a, 802.11b y 802.11g.

A finales de la década de los 90, los líderes de la industria inalámbrica (3Com, Aironet, Lucent, Nokia, etc.) crean la WECA (Wireless Ethernet Compatibility Alliance), una alianza para la Compatibilidad Ethernet Inalámbrica, cuya misión es la de certificar la interfuncionalidad y compatibilidad de los productos de redes inalámbricas 802.11b y promover este estándar para la empresa y el hogar. Para indicar la compatibilidad entre dispositivos inalámbricos, tarjetas de red o puntos de acceso de cualquier fabricante, se les incorpora el logo "Wi-Fi" (estándar de Fidelidad Inalámbrica), y así los equipos con esta marca, soportada por más de 150 empresas, se pueden incorporar en las redes sin ningún problema.

CAPITULO 4

SEGURIDAD EN REDES INALAMBRICAS WIFI

Las redes inalámbricas son inseguras aunque sólo sea porque el medio de transporte que emplean es el aire; por tanto, un elemento esencial a tener en cuenta en este tipo de redes al utilizarse la radio frecuencia, es la encriptación para mantenerla segura. En general se utiliza WEP (Wired Equivalent Privacy), que es un mecanismo de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso, pero se muestra en este capítulo que no es suficiente. En el capitulo también se presentan diversas técnicas y alternativas para asegurar una red inalámbrica como lo es el filtrado de direcciones MAC, WPA, VPN y 802.1x.

4.- SEGURIDAD EN REDES INALAMBRICAS WIFI

4.1.- El problema de la seguridad

El acceso a la red sin necesidad de cables es la razón que ha hecho tan populares a las redes inalámbricas. Pero esto a la vez se convierte en el problema más grande en este tipo de redes en cuanto a seguridad se refiere.

Cualquier equipo que se encuentre en el área de influencia de un punto de acceso, podría tener acceso a la red inalámbrica. Por ejemplo, si varias empresas están juntas en un mismo edificio y todas ellas poseen una red inalámbrica, el equipo de un empleado podría conectarse en cierto momento en el área de influencia de dos o más redes diferentes, y dicho empleado podría conectarse intencionalmente o no, a la red de una compañía que no es la suya. Aún peor, como las ondas de radio pueden salir del edificio, cualquier persona que tenga un equipo móvil y entre en el área de influencia de la red podría conectarse a la red de la empresa.

La mala configuración (en cuestiones de seguridad) de un punto de acceso inalámbrico es desgraciadamente algo muy común. Algunos administradores no se dan cuenta de las implicaciones negativas de poseer puntos de acceso inalámbricos mal configurados en la red de una empresa. Es muy común encontrar redes en las que el acceso a Internet se protege adecuadamente con un Firewall[1] bien configurado, pero al interior de la red existen puntos de acceso inalámbricos totalmente desprotegidos e irradiando señal hacia el exterior del edificio. Desde el exterior cualquier persona que capte la señal del punto de acceso, podría tener acceso a la red de la compañía, logrando navegar gratis en Internet, usar la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software, borrar información, introducir virus o software maligno, entre muchas otras cosas. Un punto de acceso mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía.

[1] FIREWALL. Pared de fuego. Dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra.

Siendo esto tan común (la mala configuración como consecuencia de la sencillez para instalar una WLAN) se han popularizado varias técnicas para encontrar WLANs sin seguridad.

Para localizar una red inalámbrica existen algunas prácticas muy bien conocidas.

4.1.1.- Wardriving

La formalización del concepto wardriving data de 1999 y es atribuido a Peter Shipley. Su experiencia con wardriving fue posteriormente introducida a la comunidad hacker DEFCON 9 en las Vegas en Julio de 2001. Wardriving es una extensión del concepto wardialing[2].

La idea básica consiste en localizar puntos de acceso inalámbricos desde un automóvil. Para lograr esto se necesita de un equipo portátil equipado con una tarje de red WLAN configurada en modo monitor, una antena adecuada (que se puede hacer fácilmente con una lata de papas fritas), un dispositivo GPS[3] para localizar los puntos de acceso en un mapa y software para detección de redes inalámbricas que se puede conseguir libremente en Internet, como AirSnort o Kismet para Linux y el NetStumbler para sistemas Windows.

La práctica del wardriving ha demostrado que la tecnología inalámbrica tiene abierto el más grande agujero en cuestiones de seguridad en las redes de computadoras.

[2] War dialing. Práctica que consiste en scanear listas de números telefónicos de manera ilegal.
[3] GPS. Sistema de Posicionamiento Global.

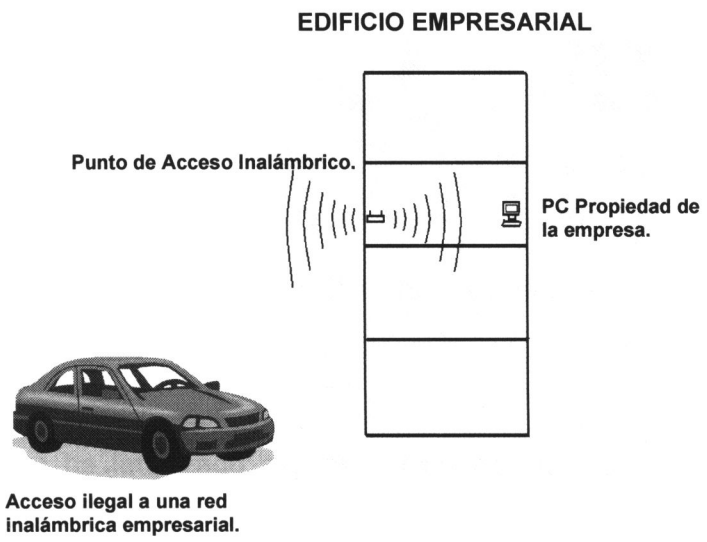


Figura 4.1 Wardriving. Acceso ilegal a una red inalámbrica.

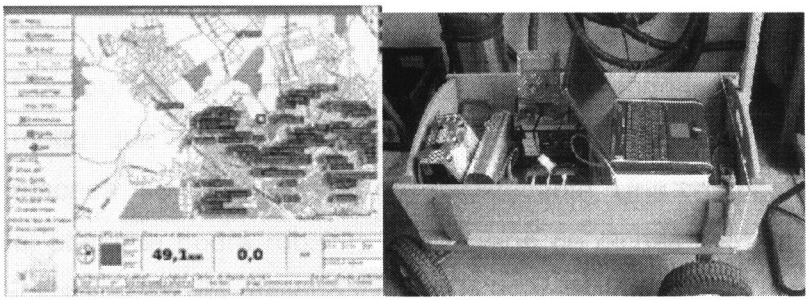
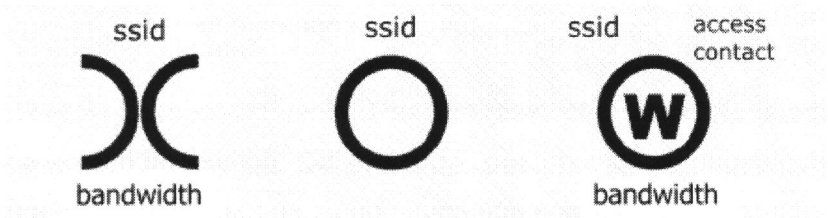


Figura 4.2 Wardriving. Equipo necesario como Lap Top, GPS y Antena.

4.1.2.- Warchalking

La práctica de warchalking consiste en caminar por la calle con un equipo portátil equipado con una tarjeta de red WLAN, buscando la señal de puntos de acceso. La gente que ha realizado este tipo de prácticas pinta con un gis o tiza un símbolo especial en la banqueta o en el muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. La figura 4.2 muestra los símbolos usados en esta práctica.



Open node Close Node WEP Node

Figura 4.3 Warchalking y su simbología

4.1.3.- Ataques

Ya que se ha localizado alguna red inalámbrica, una persona podría llevar a cabo varios tipos de ataques, entre ellos:

- Navegar gratuitamente en Internet.
- Escuchar la información que es transmitida en la red.
- Ingresar a la red y hacer uso ilegítimo de sus recursos informáticos.
- Configurar un punto de acceso propio, orientando la antena de tal modo que los equipos que son clientes legítimos de la red atacada, se conecten a la red del atacante. Una vez hecho esto, el atacante podrá robar la información de dichas computadoras, instalar software maligno y dañar la información.
- Usar la red como punto de ataque hacia otras redes.
- Escuchar la información que es transmitida y hacer mal uso de ella.

4.2.- Filtrado de direcciones MAC

Consiste en la creación de una base de datos, la cual es una tabla con la dirección MAC[4] de cada una de las tarjetas de red inalámbricas que se podrán conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Una dirección MAC podría ser E1:B1:CF:3D:4A:AA. Normalmente viene impresa en la tarjeta de red, aunque también se puede consultar mediante el comando ipconfig /all en ms-dos.

[4] MAC. (**Media Access Control address).** Número que identifica a cada una las tarjetas de red.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impractico para el uso de redes medianas o grandes:

4.2.1.- Desventajas

- Cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso (en el caso de un ESS). La situación se torna inmanejable después de cierto número de puntos de acceso y equipos.
- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de listas.
- Un aspecto negativo muy importante es que las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas registradas en la base de datos que sí pueden usar la red, empleando un sniffer[5]. De este modo el atacante puede hacerse pasar como un cliente válido, forzando a su tarjeta de red a usar una MAC de las capturadas.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema se torna más serio, ya que el punto de acceso puede contener toda la base de datos de direcciones válidas.

Este método no garantiza la confidencialidad de la información transmitida ya que no prevé ningún mecanismo de cifrado.

[5] Sniffer. Programa de para monitorear y analizar el trafico en una red de computadoras, detectando los cuellos de botella y problemas que existan en ella. Un sniffer puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red.

4.3.- WEP (Wire Equivalent Privacy)

El algoritmo WEP forma parte de la especificación 802.11 y se diseño con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP es soportado por la mayoría de los fabricantes de soluciones inalámbricas.

4.3.1.- Algoritmo

El algoritmo WEP cifra de la siguiente manera:

1	A la trama en claro se le calcula un código de integridad (Integrity Check Value, ICV) mediante el algoritomo CRC-32[6]. Dicho ICV se concatena con la trama y es empleado mas tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.
2	Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede ser de 40 ó 128 bits.
3	Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.
4	La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4[7] de números seudo-aleatorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.
5	El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).
6	Se hace un XOR[8] bit por bit de la trama con la secuencia de clave. Obteniéndose como resultado la trama cifrada.
7	El IV y la trama se transmiten juntos.

Tabla 4.1 Algoritmo de cifrado WEP

[6] CRC-32. Algoritmo de Chequeo de Redundancia Cíclica de 32 bits. El objetivo del algoritmo es garantizar la integridad de los datos enviados.
[7] RC4. Algoritmo de Cifrado de flujo (no de bloques), creado en 1987.
[8] XOR. Operación "or" exclusivo.

El proceso de descifrado en el receptor se lleva a cabo como se muestra en la tabla 4.2.

1	Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
2	Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.
3	Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.
4	A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.
5	Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

Tabla 4.2 Proceso de descifrado en el receptor.

4.3.2.- Debilidades

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre el emisor y receptor. Sin embargo, existen algunas situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de las aplicaciones:

- En la mayoría de las instalaciones se emplea WEP con claves de cifrado estáticas, se configura una clave en el punto de acceso y no se le cambia nunca, o muy esporádicamente. Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque de fuerza bruta[9].
- El IV (vector de inicialización) que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2^{24} IV distintos. Esto no es problema en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de

[9] Fuerza Bruta. Consiste en probar todo el abanico de posibles claves hasta descubrir la que realmente funcione.

ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

- WEP no ofrece servicio de autenticación[10]. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Gratuitamente en Internet se pueden encontrar herramientas para identificar redes inalámbricas así como para romper la clave secreta de enlaces protegidos con WEP.

[10] Autenticar. Legalizar o autorizar

4.3.3.- Herramientas de identificación de redes inalámbricas

Herramienta	Sitio Web	Descripciones
NetStumbler	www.netstumbler.com	Identificador de APs, escucha los SSID y manda señales buscando APs
Kismet	www.kismetwireless.net	Sniffer y monitor de WLANs- de forma pasiva monitorea el trafico inalámbrico, orden la información para identificar SSIDs, direcciones MAC, canales y velocidades de conexión.
Wellenreiter	http://packetstormsecurity.nl	Herramienta para descubrir WLANs. Usa la fuerza bruta para identificar APS de bajo tráfico, oculta su verdadera MAC y se integra con GPS.
THC-RUT	www.thehackerschoice.com	Herramienta para descubrir WLANs. Usa la fuerza bruta para identificar APS de bajo tráfico. Su primera herramienta en una red desconocida.
Ethereal	www.ethereal.com	Analiza WLANs. Permite surfear de forma interactiva la información capturada, observando información detallada de todo el tráfico inalámbrico.
WepCrack	http://sourceforge.net/projects/wepcrack	Rompe la encriptación. Hace un crack de WEP utilizando las vulnerabilidades en la programación de RC4.
AirSnort	http://airsnort.shmoo.com	Rompe la encriptación, monitorea de forma pasiva las transmisiones, computando la llave de encriptación cuando se han capturado suficientes paquetes.
Hostal	http://hostap.epitest.fi	Convierte una estación WLAN para funcionar como un AP.

Tabla 4.3 Herramientas para identificar redes inalámbricas.

4.4.- VPN

Una red privada virtual (VPN[11]) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

4.4.1.- Implementación

Muchas compañías han instalado redes privadas virtuales (VPNs) como una manera de proveer acceso remoto seguro a los usuarios de la información de la empresa vía Internet. Al implementar una solución VPN para asegurar la transmisión inalámbrica, la red inalámbrica es tratada como una red intrusa como Internet. Los servidores VPN actúan como puertas de enlace de la red empresarial proporcionando autenticación y encriptación completa a la red inalámbrica.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN[12] si se emplea conmutación. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente solo cuando este ha sido debidamente autorizado y autenticado. Los usuarios son autenticados usando un servicio centralizado de autenticación como un servidor RADIUS[13].

---

[11] VPN. Red Privada Virtual
[12] VLAN. Rede Virtual de Área Local
[13] RADIUS (Romote Autentication Dial-In User Service). Servidor remoto que autentica y autorizará el acceso a una red.

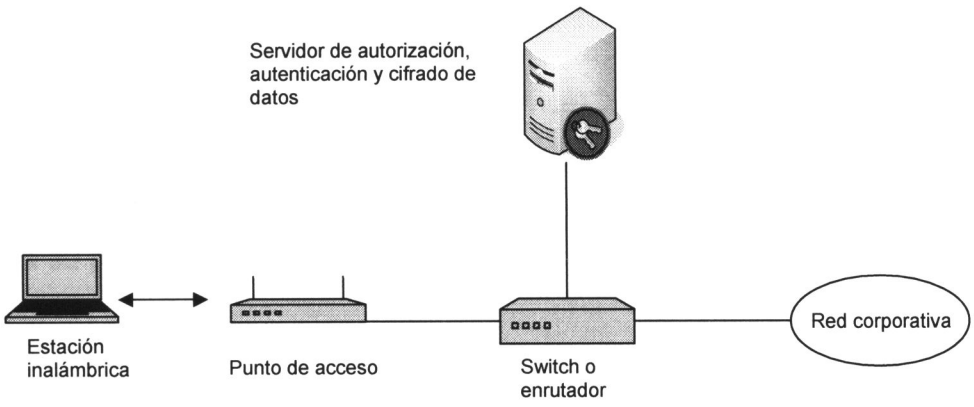


Figura 4.4 Estructura de una VPN para acceso inalámbrico seguro

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

4.4.2.- Desventajas

⇒ Alto costo

⇒ No es rápido

4.5.- 802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para el uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

El protocolo 802.1x involucra tres participantes:

1.- El suplicante o equipo del cliente que desea conectarse con la red.

2.- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS[14] (Romote Autentication Dial-In User Service), cuya especificación se puede consultar en el RFC[15] 2058 [8]. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se opto por emplearlos también para autenticación en las LAN.

3.- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo confirma.

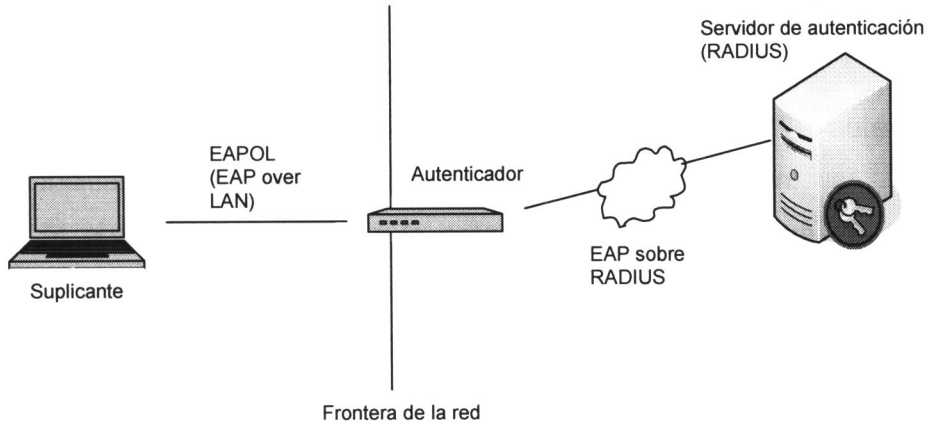


Figura 4.5 Arquitectura de un sistema de autenticación 802.1x

[14] RADIUS (Romote Autentication Dial-In User Service). Servidor remoto que autentica y autorizará el acceso a una red.
[15] RFC (Request For Comments). En esta serie de documentos se detalla prácticamente todo lo relacionado con la tecnología de la que se sirve Internet: protocolos, recomendaciones, comunicaciones.

4.5.1.- Implementación

Una de las principales preocupaciones de las empresas es lograr que sus sistemas de seguridad para acceder a los recursos de la compañía sean algo más que teclear un nombre de usuario y una contraseña, por lo que se ha diseñado un nuevo protocolo de autenticación llamado EAP (Extensible Authentication Protocol). EAP se encuentra dentro del protocolo de autenticación PPP[16] (Point-to-Point Protocol) y proporciona un marco general compatible con diversos métodos de autenticación.

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol[17]) y el servicio RADIUS, de la siguiente manera:

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.
- La estación de trabajo envía un mensaje "EAPOL-Start" al autenticador, indicando que desea iniciar el protocolo de autenticación.
- El autenticador solicita a la estación que se identifique mediante un mensaje "EAP-Request/Identity."
- La estación se identifica mediante un mensaje "EAP-Response/Identity".
- Una vez recibida la información de identidad, el autenticador envía un mensaje "Radius-Access-Request" al servidor de autenticación y le pasa los datos básicos de identificación del cliente.
- El servidor de autenticación responde con un mensaje "RADIUS-Access-Challenge", en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso.

[16] PPP (Point-to-Point Protocol) Es uno de los protocolos más utilizados en los sistemas de acceso a Internet por marcación.
[17] (EAP - RFC 2284). Uno de los elementos básicos del 802.1x y desarrollado como mejora del Point to Point Protocol (PPP - RFC 1661). PPP utiliza como método de autenticación "username" y "password".

Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafía al cliente en un mensaje "EAP-Request".

- El cliente da respuesta al desafío mediante un mensaje EAP-Response dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje "RADIUS-Access-Response".
- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje "RADIUS-Access-Accept", que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red, como en el protocolo DHCP.
- El autenticador envía un mensaje "EAP-Success" al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje "RADIUS-Access-Accept" un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada 5 minutos), para evitar el ataque de rompimiento de la clave descrito anteriormente en la parte de WEP.

4.5.2.- Variantes del protocolo EAP

Existen variantes del protocolo EAP. Según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad y las que utilizan contraseñas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

- EAP-TLS: Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte, el servidor autentica al cliente y viceversa, soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).

- EAP-TTLS: desarrollada por Funk Software y Certicom. Proporciona servcios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP[18], CHAP[19], MS-CHAP ó MS-CHAP v2.
- PEAP: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAP-TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

Desventajas del empleo de certificados

⇒ La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida o montar una CA propia.

⇒ El diálogo de autenticación es largo. Esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que reautenticarse con mucha frecuencia, por ejemplo los usuarios en movimiento que cambien de un punto de acceso a otro.

⇒ La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tarjeta inteligente (smart card) lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

---

[18] PAP. Password Authentication Protocol. Protocolo de autenticación simple usado para autenticar un usuario a un servidor de acceso remoto.

[19] CHAP. Challenge-Handshake Authentication Protocol. Es usado para verificar periódicamente la identidad del cliente.

⇒ Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

Las variantes de EAP que utilizan contraseñas son las siguientes

- EAP-MD5: Emplea un nombre de usuario y una contraseña para autenticación. La contraseña se transmite cifrada con el algoritmo MD5.
- LEAP: Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP.
- EAP-SPEKE: Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta, en este caso una contraseña, a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

Desventajas de EAP que utilizan contraseñas

⇒ Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se esta conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

4.6.- WPA (WiFi Protected Access)

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación. En la tabla 4.4 se hace una comparación de las características de seguridad proporcionadas por IEEE 802.11 y WPA.

Características			802.11	WPA
Cifrado	Sistema (Algoritmo) de Cifrado		WEP (RC4)	TKIP(RC4)
		Longitud	40 bits	128 bits
	Gestión Claves	Generación clave	Estática, la misma para todos los dispositivos	Dinámica, por usuario, sesión y por paquete
		Distribución clave	Manual, en cada dispositivo	Automática, gestionada por 802.1x/EAP
Autenticación		Entorno	Definido por 802.11	802.1x/EAP
		Método	Abierta/Clave compartida (autentifica el equipo).	EAP-TLS, PEAP, EAP-TLS (autentificación al usuario).

Tabla 4.4 Comparación de características se seguridad proporcionadas por IEEE 802.11 y WPA.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). TKIP amplía la longitud de la clave de 40 a 128 bits. Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoran los algoritmos de cifrado de trama y generación de los IVs pasando de 24 a 48 bits minimizando la reutilización de claves.

TKIP utiliza el algoritmo Michael[20] para garantizar la integridad, generando un bloque de 4 bytes (MIC Control de Integridad de Mensajes) a partir de la dirección MAC de origen, de destino y de los datos, añadiendo el MIC calculado a la unidad de datos a enviar. Posteriormente los datos (que incluyen el MIC) se fragmentan y se les asigna un número de secuencia. La mezcla del número de secuencia con la clave temporal genera la clave que se utilizará para el cifrado de cada fragmento.

4.6.1.- Implementación

Para soportar WPA, en caso de que los productos no estén certificados por Wi-Fi WPA, debe actualizarse el Firmware de los puntos de acceso y de los adaptadores de red inalámbricos. En las estaciones debe actualizarse el sistema operativo para soportar 802.1x y el método EAP elegido. Windows XP soporta WPA mediante una actualización.

Según el método EAP elegido se define la configuración del servidor RADIUS y su posible integración con un servicio de directorio empresarial. También es posible que se requiera utilizar o implementar los servicios de una autoridad de certificación.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP. Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- Modalidad de red empresarial

Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usaran para cifrar los datos.

---

[20] Algoritmo Michael. Hace un chequeo de integridad del mensaje (MIC - *Message Integrity Check*).

- Modalidad de red casera

También llamada PSK (Pre-Shared Key): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso.

La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la WiFi Alliance a partir de finales de 2003. Según la WiFi Alliance, todo equipo de red inalámbrica que posea el sello "WiFi Cretified" podrá ser actualizado por software para que cumpla con la especificación WPA.

4.6.2.-WPA y el uso de AES

Las directrices del estándar final IEEE 802.11i denominado RSN (Robust Security Network) marcan como algoritmo de cifrado a AES (Advanced Encription Standard), basado en el algoritmo Rijndael[21] para proporcionar privacidad y en claves de 128 bits o más. Parece que la implementación más probable es el modo Cipher Block Chaining Counter Mode (CBC-CTR) con Cipher Block Chaining Message Authenticity Check (CBC-MAC), conocido el conjunto como CBC-CCM. AES ya ha sido adoptado como estándar para cifrado en sistemas de computación y comunicaciones.

WPA indica el soporte de AES como opcional, existiendo dispositivos que ya implementan AES.

4.6.3.- Desventajas

- Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), por que ya se ha comprobado que WPA es

[21] Algoritmo Rijndael. Fue elegido por el NIST (Nacional Institute of Standards and Technology) para ser el estándar de cifrado simétrico de los próximos 20 años y es llamado AES (Advanced Encription Standard). [13]

vulnerable a ataques de diccionario si se utiliza una contraseña corta.

- La carga útil de datos enviados se reduce debido al uso del algoritmo que usa WPA.
- La implementación de WPA implica que los usuarios deberán estar siempre acordes con las contraseñas de acceso.

4.7.- WPA2

El IEEE aprobó en julio de 2004 la norma 802.11i una extensión de 802.11 para mejorar la seguridad. La norma WPA tiene como objetivo solucionar todas las deficiencias de WEP.

En el año 2004 aparece WPA2 que es la segunda generación de WPA. Este ya proporciona encriptación con un fuerte algoritmo llamado AES[22] (Norma de Encriptación Avanzada) y esta contemplado por el estándar IEEE 802.11i.

También en el 2004 la Wi-Fi Alliance anunció la salida al mercado de los primeros productos con certificación Wi-Fi para WPA2. WPA y WPA2 ofrecen un nivel alto de seguridad para usuarios finales y administradores de red. Ambos utilizan 802.1x y EAP (Extensible Authentication Protocol) para la autenticación. Cuentan con dos modos de operación para las distintas necesidades de los usuarios; ambiente casero (SOHO[23]) y ambiente empresarial. En modo de operación SOHO la autenticación es llevada a cabo por PSK (pre-share key), mientras que en el modo de operación empresarial la autenticación es lograda por 802.1x y EAP. En modo SOHO solo se requiere de una estación o cliente y un punto de acceso, mientras que en modo empresarial típicamente se requiere además un servidor de autenticación RADIUS.

WPA2 cuenta con un mecanismo de encriptación (AES) de información más poderoso que el TKIP (Temporal Key Integrity Protocol) de WPA, el cual

[22] AES. Advanced Encryption Standard
[23] SOHO. Small Office Home Office

es requerido por las empresas y usuarios gubernamentales que exigen un nivel alto de seguridad para su información.

Los productos con certificación Wi-Fi WPA2 son interoperables con los productos con certificación WPA. Solo algunos productos WPA pueden actualizarse a WPA2 por medio de software. En otros casos el cambio de hardware será necesario ya que WPA2 y la naturaleza de encriptación de AES así lo requiere. [9]

CAPITULO 5

CONSIDERACIONES PARA IMPLEMENTAR REDES INALÁMBRICAS WI-FI SEGURAS

En este capítulo se analizan las consideraciones básicas que se deben tomar en cuenta para implementar una red inalámbrica de área local WiFi. Básicamente se tratan los siguientes aspectos; el lugar donde se implementará la WLAN, colocación adecuada para los AP (Puntos de acceso), factores para el buen funcionamiento, consideraciones para evitar interferencias de radio frecuencia, selección de antenas para extender la señal inalámbrica y varias técnicas para implementar la red inalámbrica Wi-Fi de forma segura.

5.- CONSIDERACIONES PARA IMPLEMENTAR REDES INALÁMBRICAS WI-FI SEGURAS

De acuerdo a esta investigación, se propone una serie de consideraciones que se deben tomar en cuenta para la implementación de redes inalámbricas de área local WiFi. Estas consideraciones son las siguientes y serán tratadas con profundidad en este capítulo:

1. selección adecuada de la topología de red inalámbrica
2. planificación
3. consideraciones para el desempeño
4. áreas de influencia
5. penetración de señal
6. selección adecuada del estándar
7. antenas
8. administración de la red inalámbrica
9. aseguramiento de la red inalámbrica
10. niveles de seguridad (según la situación de uso)

5.1.- Topologías de redes inalámbricas de área local

Las redes inalámbricas se construyen utilizando dos topologías básicas. Estas topologías se llaman de "ad-hoc" e "infraestructura". Aquí se usan estos términos.

Una topología ad-hoc es en la cual se crea una red LAN únicamente por los dispositivos inalámbricos mismos, sin controlador central o punto de acceso. Cada dispositivo se comunica directamente con los demás dispositivos en la red, en lugar de que sea a través de un controlador central. Esto es útil en lugares en donde pequeños grupos de computadoras pueden congregarse y no se necesita acceso a otra red. Por ejemplo, un hogar sin una red cableada o un cuarto de conferencia en donde se reúnen regularmente equipos para intercambiar información, son ejemplos en los que puede ser útil una red inalámbrica ad-hoc.

Por ejemplo, cuando se combinan la nueva generación de software y las soluciones inteligentes de punto a punto, estas redes inalámbricas ad-hoc pueden permitir a los usuarios que viajan colaborar, disfrutar de juegos con varios participantes, transferir archivos o comunicarse de alguna otra forma entre sí, utilizando sus PCs o dispositivos inteligentes de manera inalámbrica.

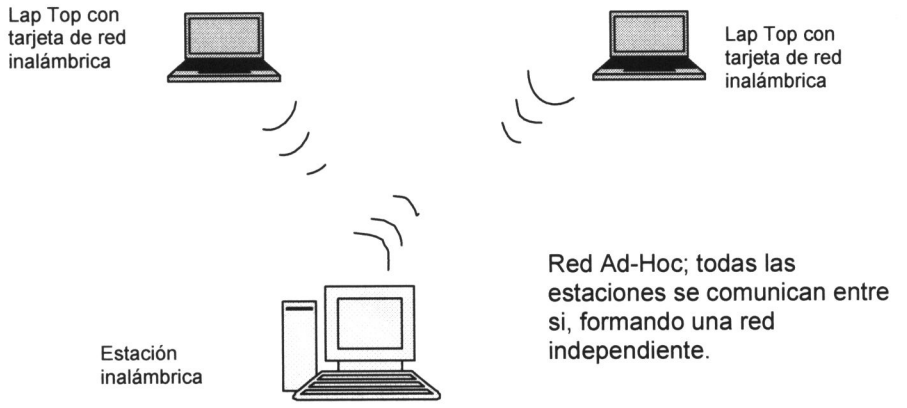


Figura 5.1 Red Ad Hoc

El costo por una red de este tipo, se reduce al costo por tarjeta de red inalámbrica por equipo. Como se vio en el capitulo 3 los costos varían dependiendo de la marca y características de estas. Una característica que puede influir en este costo mencionado es precisamente la versatilidad que tienen algunos dispositivos inalámbricos (tarjetas de red inalámbricas) para ser conectados en este modo ad-Hoc.

Una topología de infraestructura es la que amplía una red cableada existente a dispositivos inalámbricos, proporcionando una estación base (llamada punto de acceso). El punto de acceso se une a las redes inalámbricas y cableadas, actuando como un controlador central para la red inalámbrica. El punto de acceso coordina la transmisión y la recepción de múltiples dispositivos inalámbricos dentro de un rango específico. El rango y cantidad de dispositivos dependen del estándar inalámbrico que se utilice, así como las características del producto del proveedor.

En la infraestructura puede haber varios puntos de acceso para cubrir una gran área o sólo un punto único de acceso para un área pequeña, como por ejemplo una casa o un edificio pequeño.

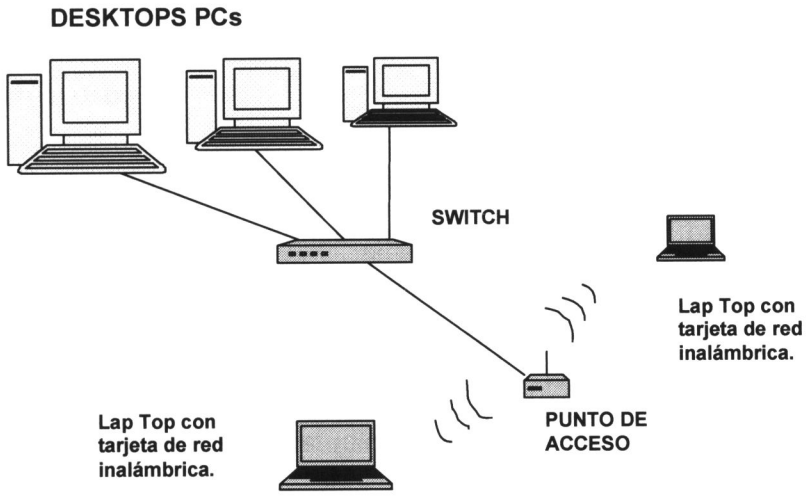


Figura 5.2 Red tipo infraestructura

La topología de infraestructura es la más utilizada en la actualidad, en redes caseras, oficinas, industria donde se requiere de una conexión a la red pero también necesita movilidad para supervisión de labores o procesos en una fábrica, las universidades para tener conectividad (sin depender de cables) desde diferentes lugares dentro del campus, hospitales que requieren tener acceso desde un lugar determinado dentro del edificio a su base de datos para conocer la historia clínica de algún paciente, entre otros.

5.2.- Planificación

La instalación de una red inalámbrica 802.11a, .11b, o .11g es relativamente fácil. De hecho, el uso de equipo certificado WiFi tiene la sencillez de no requerir ningún tipo de configuración al momento de adquirirlo y extraerlo de su caja. Simplemente se conecta y con la configuración de fábrica en unos cuantos minutos estará trabajando. Sin embargo trabajar y trabajar óptimamente son cosas muy diferentes.

La instalación de una red inalámbrica para la mayoría de las empresas, requiere de un gran número de factores que tienen que considerarse. El diseño e implementación de una red inalámbrica de área local esta en función del ambiente físico del lugar donde se implementara y el ámbito de uso de la red.

Aunque la funcionalidad deseada dependa de la configuración física de los equipos, el ambiente físico del lugar donde se implementara impone limitaciones en el uso.

El primer paso para estas cuestiones mencionadas es verificar que el lugar físico de implementación cumpla con los requerimientos básicos para el buen funcionamiento, como lo es el material, grosor y la textura de los muros. Determinar el área o áreas que se quieran cubrir así como las que no se quieren cubrir. Una vez bien definidos estos puntos, acerca del lugar de implementación, se emprende el estudio del lugar interior. Este estudio incluye la supervisión de artículos que puedan afectar la propagación de la señal de radio, tales como los materiales con los que esta construido el interior del edificio así como todas las fuentes potenciales de interferencia (hornos microondas, teléfonos inalámbricos que trabajan en la banda de 2.4 Ghz). También es importante identificar áreas donde las señales de radio están prohibidas o no son recomendables. Por ejemplo es común que en los hospitales tengan estrictas regulaciones en las transmisiones de radio ya que muchos equipos médicos se pueden ver afectados por este tipo de señales.

Después de conocer el ambiente físico, deben ser establecidos los requerimientos para el uso de la red WLAN. Lo que incluye; el número total usuarios, el número de usuarios conectados a la red simultáneamente y cuales áreas tienen alta concentración de usuarios que tienen acceso de manera simultanea (por ejemplo los lugares destinados para conferencias).

Considerando estos puntos importantes como la distancia, el poder de transmisión y posibles generadores de interferencia, se puede determinar las expectativas que se pretendan para una WLAN. Así se puede escoger el equipo y el lugar propio para la implementación.

5.3.- Consideraciones para el desempeño WLAN

Hoy en día, las empresas están implementando redes inalámbricas para un gran número de usuarios con necesidades de aplicaciones corporativas,

como el correo electrónico, navegación en Internet, y acceder a servidores de bases de datos. La necesidad de altas tasas de transferencia y técnicas para mejorar el desempeño de las WLANs se esta volviendo crucial para dar soporte a este tipo de aplicaciones. A continuación se enlistan consideraciones para lograr un mejor desempeño WLAN.

⇒ **Escoger el estándar adecuado.** Un elemento importante que impacta el desempeño de la WLAN es la selección del estándar adecuado. 802.11a ofrece una tasa alta de transferencia de 54 Mbps para cada canal no encimable de los 12 que maneja y casi no le afecta la interferencia (debido a que la banda de frecuencia en la que opera es muy poco usada). 802.11b provee tasas de transferencia de 11 Mbps con solo 3 canales no encimables. 802.11g ofrece una tasa alta de transferencia de 54 Mbps, pero existe la limitante de que solo hay 3 canales no encimables. Claro esta que los requerimientos dictan la necesidad de desempeño, lo cual permite guiarse hacia un estándar particular. Si lo que se quiere es una tasa alta de transferencia, el estándar 802.11a sería el adecuado, sin embargo los productos de este estándar son muy caros.

⇒ **Ajustar adecuadamente los canales.** Los estándares 802.11b y g definen once canales que se sobreponen, dejando solo tres canales que no se sobreponen entre ellos. Para puntos de acceso que están dentro de un rango muy cercano, es conveniente configurarlos en canales diferentes (por ejemplo en los canales 1, 6 y 11) para evitar interferencias entre ellos. También se puede aprovechar la ventaja de la selección automática de canal que algunos puntos de acceso implementan. Es una práctica común configurar los puntos de acceso en el mismo canal, el problema con esto es que el concepto de movilidad no funciona cuando un usuario se desplaza por el edificio de la empresa, debido a que la transmisión a un punto de acceso único bloquea a otros que están en la misma área. Como resultado, el desempeño se degrada

significativamente. Con 802.11a esto no es un problema porque este estándar define canales que no se sobreponen, además cuenta con un mayor número de ellos (8 en total).

⇒ **Proveer cobertura de RF adecuada.** Si los puntos de acceso están muy apartados, entonces algunos usuarios se estarán asociando con la red inalámbrica a una tasa de transferencia un poco menor. Por ejemplo, los usuarios que se encuentren cerca de un punto de acceso 802.11b estarán operando a 11 Mbps, sin embargo usuarios que estén alejados del punto de acceso, estarán operando a 2 Mbps. Para poder maximizar el desempeño, hay que asegurarse que la cobertura de RF esté distribuida de la mejor manera posible en todas las áreas, especialmente donde la mayor cantidad de usuarios estén operando. La configuración correcta de poder de transmisión y selección de antenas ayudará a decidir el posicionamiento de los puntos de acceso para un desempeño optimo.

⇒ **Evitar interferencia de RF.** Teléfonos inalámbricos y otras redes inalámbricas cercanas pueden causar señales de interferencia considerables que degradan la operación de una red 802.11b o g. Estas fuentes externas de energía de RF en la banda de 2.4 GHz bloquea periódicamente a los usuarios y puntos de acceso para acceder al medio aéreo. Como resultado, el desempeño de la WLAN sufre cuando hay interferencia presente. Así que obviamente se debe tratar de minimizar las fuentes de interferencia y configurar los puntos de acceso en canales adecuados para evitar señales de interferencia. Si no es posible reducir la interferencia potencial a un nivel aceptable, entonces se debe considerar implementar redes 802.11a de la banda de 5 GHz.

⇒ **Considerar RTS / CTS.** El protocolo opcional del estándar 802.11 petición para enviar / listo para enviar (RTS / CTS, por sus siglas

en inglés) requiere que una estación se contenga de enviar un marco de datos hasta que complete la negociación con otra estación, como puede ser un punto de acceso. RTS / CTS reduce las colisiones asociadas con nodos escondidos y puede mejorar el desempeño. Las colisiones pueden ocurrir cuando nodos escondidos transmiten "ciegamente" cuando otra estación esta transmitiendo. Esto causa una colisión y da como resultado que cada estación se vea en la necesidad de transmitir sus marcos, con la posibilidad de que de nuevo vuelva a haber una colisión debido al nodo escondido. El resultado es un menor desempeño. Si se sospecha que nodos escondidos están causando colisiones / retransmisiones, entonces hay que tratar de configurar un umbral menor para mejorar el desempeño y detectar el error.

Los dispositivos 802.11b y g operan en la banda de los 2.4 GHz y esta banda es usada también por otros aparatos electrodomésticos, como teléfonos inalámbricos y hornos de microondas. La especificación 802.11b provee un ancho de banda de 11 Mbps, lo cual es solo una máxima teórica. Las redes inalámbricas, así como las alambradas, nunca dan el nivel de desempeño óptimo, ni siquiera cercano a él. El ancho de banda real que se puede obtener de una red 802.11b es de 4 a 5 Mbps; de una red 802.11a es de 27 Mbps; y el de una red 802.11g es de 20 a 22 Mbps. [1].

Este nivel de rendimiento es más que suficiente para las tareas más rudimentarias. Cuando se considera que una conexión típica por cable o DSL puede proveer de 256 Kbps a 1.6 Mbps de ancho de banda, se puede ver que la velocidad de una red 802.11b no será un impedimento para actividades como navegación por Internet, correo electrónico, descargas de archivos, correr aplicaciones, etc.

Por otra parte, no es difícil ver escenarios donde el ancho de banda si necesita ser mas grande, cuando se quiere hacer una transferencia rápida de archivos grandes, como imágenes, video, etc; o simplemente una colección de

MP3 o películas. Si se experimenta la necesidad de mayor velocidad, hay que considerar 802.11g u 802.11a.

5.4.- Áreas de influencia

El desempeño de las redes inalámbricas decrece mientras la distancia hasta la antena aumente. La degradación no es lineal; en otras palabras, no se pierde la mitad del desempeño cuando la distancia se duplica, y el desempeño no decrece en pequeñas porciones mientras la estación se mueve más lejos.

Cada especificación tiene un conjunto de niveles de ancho de banda predefinidos en los cuales puede operar (802.11b tiene 4, 802.11a tiene 8 y 802.11g tiene 12). Los niveles de ancho de banda se van hacia abajo mientras la estación se aleja, y al momento de encontrarse en los rangos extremos, el ancho de banda disponible es solo una pequeña fracción del máximo.

Cuando se encuentra dentro del edificio, las señales 802.11b y g pueden viajar hasta 150 metros. Al aire libre el área es casi 3 veces mayor, esto es 500 metros. Los rangos al aire libre son mayores porque hay menos obstáculos, como paredes, que absorban o bloqueen la señal de radio. En cualquiera de los extremos de rangos, el ancho de banda disponible es de 1 Mbps, lo cual se acerca a la velocidad de la conexión de banda ancha. El bajo nivel de transmisión puede afectar a las actividades de red.

Por otra parte, para que 802.11b y g operen a su máximo ancho de banda, la distancia dentro del edificio debe ser no mayor de 50 metros, y al aire libre puede ser hasta de 250 metros. Cuando se analiza la relación entre desempeño y área, 802.11a se comporta de la misma manera que los otros 2 estándares. Así que el desempeño decrementa mientras la distancia aumenta.

802.11a ofrece un área pequeña. Dentro del edificio, se permite un rango de aproximadamente de solo 100 metros. Al aire libre, el rango aumenta a 350 metros. Cuando se usa equipo 802.11a en el extremo del rango, se puede comunicar únicamente a la velocidad mas baja soportada, que en este

caso son 6 Mbps. Si se desea el ancho de banda de 54 Mbps, el rango dentro de edificio esta limitado a 18 metros, y al aire libre aproximadamente 30 metros.

Con cualquier tecnología se pierde alrededor de 50% del rango para poder disfrutar de transferencias de información con la mayor tasa posible.

5.5.- Penetración

Además de las diferencias obvias en el área, otro factor diferenciador entre 802.11b y g con 802.11a es la calidad, o robustez de la señal. Debido a la alta frecuencia (y por lo mismo longitud de onda mas corta) que se usan, las señales 802.11a tienen mas resistencia a la penetración en objetos sólidos como paredes, pisos y techos. Como resultado, el precio de la alta velocidad de 802.11a no es solo el rango más corto, sino también una señal más débil e inconsistente.

5.6.- Selección del estándar.

802.11g opera en la banda de 2.4 GHz, así que es compatible con los dispositivos 802.11b. Pero cuando productos de ambas tecnologías se encuentren en una red, los productos 802.11g tendrán que bajar su velocidad a una común con los productos 802.11b existentes en la red. Además, si ya se tiene una red 802.11b, la compatibilidad con 802.11g protegerá la inversión del hardware existente. Esto en contraste con la situación cuando 802.11a apareció, debido a que usa otra frecuencia y tipo de modulación que 802.11b, los usuarios que quisieran actualizar su red a 802.11a tenían que cambiar todo el hardware.

5.7.- Antenas

Para ampliar y optimizar el área de influencia inalámbrica existen dos tipos de antenas que se pueden implementar en conjunto con el equipo inalámbrico, ya sea directamente en los puntos de acceso o en las tarjetas inalámbricas Wi-Fi instaladas en las estaciones[1].

La característica más importante de una antena es la ganancia. Esto viene a ser la potencia de amplificación de la señal. La ganancia representa la relación entre la intensidad de campo que produce una antena en un punto determinado, y la intensidad de campo que produce una antena omnidireccional (llamada isotrópica), en el mismo punto y en las mismas condiciones. Cuanto mayor es la ganancia, mejor es la antena. La unidad que sirve para medir esta ganancia es el decibelio (dB).

Relación señal/ruido. Siempre que se emite o se recibe una señal de radio, lleva acoplada una señal de ruido. Obviamente, cuanto menor sea la relación de ruido con respecto a la señal, más óptima se considerará la señal "valida". Incluso en las transmisiones digitales, se tienen que usar métodos de modulación que reduzcan el ruido y amplifiquen la señal de radio.

El resultado de dividir el valor de la señal de datos, por la señal de ruido es lo que se conoce como relación señal/ruido. Cuanto mayor es, mejor es la comunicación.

Se expresa en decibelios (dB), y en escala exponencial, lo que quiere decir que una relación señal ruido de 10 dB, indica que la señal es 10 veces mayor que la de ruido, mientras que 20 dB indica 100 veces más potencia.

Antenas omnidireccionales

En las antenas onmidireccionales de 2.4 GHz la señal se dispersa en todas las direcciones (360^0) y ofrecen una solución de rango extendido para el hardware de la red inalámbrica. Estas antenas se clasifican por la potencia en decibles, a mayor número de decibeles la potencia de la señal incrementará.

[1] Estaciones. Computadoras con una interfaz de red inalámbrica.

La mayoría de las antenas omnidireccionales de 6dBi, 7dBi, 9bBi, 14dBi que son las mas comerciales soportan todos los estándares Wi-Fi de 2.4 GHz, incluyendo IEEE 802.11b y el estándar 802.11g. Al añadir una antena omnidireccional a un punto de acceso (AP) con antenas extraíbles o a una tarjeta PCI inalámbrica con antena extraíble, se mejora substancialmente la fuerza de la señal mientras se incrementa la cobertura de un 20% hasta un 60% dependiendo de los decibeles de la antena. Soportando una instalación rápida (Plug & Play) se puede instalar en un par de minutos.

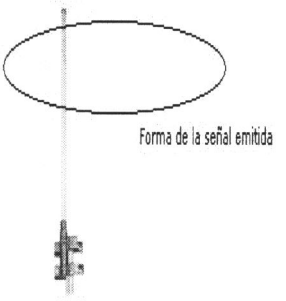


Figura 5.3 Antena Omnidireccional. Se les llama también antenas de fuste vertical. Se utilizan principalmente para emitir la señal en todas las direcciones. En realidad la señal que emite es en forma de óvalo, y sólo emite en plano (no hacia arriba ni hacia abajo).

Antenas direccionales

En las antenas direccionales se orientan la señal en una dirección determinada, se suelen utilizar para unir dos puntos a largas distancias, trabajan en la frecuencia de 2.4 GHz y soportan los estándares 802.11b y el 802.11g. La señal que emiten es direccional y proporciona una ganancia que oscila entre los 15 y los 21 dBi. Como todas las antenas exteriores hay que protegerla ante posibles descargas eléctricas.

Figura 5.4 Antena direccional (o yagui). Tienen forma de tubo. En su interior tienen unas barras de metal que cruzan el interior de ese tubo.

5.8.-Administración de la WLAN

El software de administración de la WLAN puede producir reportes con detalles, dando al administrador una perspectiva amplia del desempeño de la red. Muchas compañías ofrecen herramientas de administración WLAN, como son Airwave, Computer Associates, Cisco, Symbol y Wavelink, entre otras. Cuando se evalúa software de administración WLAN, hay ciertos atributos que distinguen a una solución superior:

⇒ **Centralización.** El software debe permitir controlar todo desde un lugar. Un administrador de red debe ser capaz de realizar actividades como configuración y monitoreo de la infraestructura, haciendo cambios de configuración del punto de acceso y actualizando el software del mismo.

⇒ **Soporte multi producto.** El software debe soportar puntos de acceso de distintos fabricantes para asegurar la flexibilidad del diseño del sistema.

⇒ **Flexibilidad.** Un software que sea actualizable fácilmente es una gran ventaja. En el caso contrario sería una inversión no conveniente.

⇒ **Facilidad de uso.** El software debe tener un ambiente operativo amigable, fácil de navegación y proveer ayuda adecuada cuando se necesite.

⇒ **Facilidad de integración.** Siempre es bueno cuando un producto se puede integrar a un sistema sin problemas, debido a que no se pierde la inversión existente. El software también debe ser capaz de integrarse con otro software de administración de red.

⇒ **Automatización.** Cuando se necesitan cambios en la configuración, el software debe ser capaz de implementar esos cambios automáticamente sobre múltiples puntos de acceso. Esto elimina las posibilidades de que haya un error humano y se asegura una implementación uniforme de los cambios.

5.9.- Asegurando la red inalámbrica

Si se tiene en mente implementar una red inalámbrica, se tiene que planear muy bien para asegurarse que la red este segura. Como todas las frecuencias de radio, cualquiera con un receptor inalámbrico (tarjeta de red inalámbrica) puede unirse a un canal de WLAN, así que se necesitan implementar precauciones extra para prevenir que los datos de red puedan ser escuchados.

La primera razón para construir una WLAN es incrementar la movilidad, así una estación se puede mover de una habitación a otra sin la necesidad de estar conectado a una roseta por medio de un cable. Otra razón por la cual se prefiere una WLAN es que no se tienen que tender cables dentro de las paredes o canaletas, por ello es que implementar una red inalámbrica es mucho mas fácil.

Hay un sinnúmero de tipos de productos de protocolos inalámbricos. Cuando se esta configurando una red inalámbrica, básicamente lo que se hace es configurar un transmisor (punto de acceso). Cualquier punto de acceso de algún proveedor de prestigio (LinkSys, 3Com, SMC) tiene una interfaz TCP/IP por la cual se configura, que es algo que se debe tener en cuenta cuando se compra uno. Cuando se configura un punto de acceso, se conecta primero al concentrador o switch por medio de un cable (Ethernet, en la mayoría de los casos), luego se configura la interfaz inalámbrica, después la interfaz de cable, y después la seguridad. Los tipos de cosas que se deben configurar incluyen la frecuencia de radio, la distancia entre puntos de acceso y la dirección IP del punto de acceso.

Después hay que configurar las estaciones. Las tarjetas de red inalámbrica tienen una dirección MAC de 48 bits que es el identificador único de ellas. Se necesitará configurar el SSID asociado con el punto de acceso.

Aun cuando se ha descubierto que WEP no ofrece una fuerte seguridad, al menos ofrece un nivel de seguridad, que ya es más que no tener algún mecanismo de seguridad. Por lo mismo, se debe tener habilitado WEP sin importar si es confiable o no.

WEP es usado para autenticar usuarios en la red y esto se necesita configurar en la interfaz de red de la estación, así como en el punto de acceso. WEP puede ser usado en modo de 40, 64 y 128 bits, obviamente en el modo de 128 bits hay mas seguridad.

También se puede agregar más seguridad, por ejemplo el protocolo de integridad de la llave temporal (TKIP[2]). TKIP ofrece nuevos algoritmos de encriptación, y constantemente cambia las llaves de encriptación haciendo más difícil el trabajo de ataque. Debido a que las llaves están cambiando constantemente, si una de ellas es capturada, no le servirá mucho a un atacante malicioso porque para el momento en que trate de utilizarla, la WLAN estará utilizando una llave de encriptación diferente. Con TKIP las llaves de encriptación son también encriptadas ellas mismas, así que se necesitaría primero desencriptarlas para poder usarlas para desencriptar el tráfico de la red.

El filtro por direcciones MAC es usado para limitar las tarjetas de red que pueden acceder a la red inalámbrica. En una red grande, filtrar las direcciones MAC puede ser una gran tarea administrativa y es conveniente usar tarjetas con direcciones MAC secuenciales para poder hacer el trabajo más fácil.

[2] TKIP de Temporal Keying Integrity Protocol

Para implementar aun mayor seguridad, se puede instalar una red privada virtual (VPN) en la red inalámbrica. Aunque se tenga información sumamente importante y confidencial, probablemente no sea conveniente el tiempo y el esfuerzo para hacer esto. Al usar una VPN, se genera un "túnel" a través de una puerta de enlace. Al usar WEP, TKIP y una VPN se creará una barrera de seguridad muy buena en la red inalámbrica. Si se usa una VPN puede causar cuellos de botella en el desempeño, así que no es conveniente implementar una si no se ocupa.

Implementar una red inalámbrica segura no es tan complicado. Teniendo la información adecuada acerca de las capacidades de los productos y seguir las instrucciones de instalación con las recomendaciones básicas. La ventaja de no usar cables es mucha, y mientras algunas personas están renuentes a usar redes inalámbricas, con el tiempo se convertirán en indispensables y las redes con cables serán obsoletas [10].

5.9.1.- Niveles de seguridad

Como se vio en el capítulo 4 algunos métodos para la seguridad de redes inalámbricas WiFi como lo es WEP y el Filtrado MAC son deficientes o no cumplen con las expectativas que alguna empresa con información importante requiere. También existen métodos muy convenientes para dichas empresas, es importante poner en diferentes niveles los distintos métodos de seguridad.

Si la red inalámbrica es de tipo casero o de pequeña oficina, la información no es de relevancia y el tráfico de la red es ligero, los métodos adecuados pueden ser el cifrado WEP y el Filtrado MAC. Aunque se vio que no son seguros, se pueden seguir algunas recomendaciones para contrarrestar las debilidades de estos métodos.

En el Punto de Acceso

- Cambiar la contraseña por defecto; todos los fabricantes de puntos de acceso establecen un password por defecto para el acceso de la administración y/o configuración. Al usar un fabricante la misma contraseña para todos sus equipos es fácil o posible que un observador con malas intensiones la conozca.
- Evitar contraseñas como fechas de nacimiento, nombres personales, preferiblemente intercalar letras con números.
- Activar en el punto de acceso la encriptación WEP de 128 bits.
- Los puntos de acceso mas recientes permiten escribir una frase a partir de la cual se generan automáticamente las claves. Es importante que esta frase intercales mayúsculas con minúsculas y numeros, evitar palabras usadas en el diccionario y secuencias contiguas en el teclado como "zxcvbn", o "012345".
- Cambiar el SSID[3] por de defecto; por defecto siempre son como "default", "Wireless", "SMC", Linksys" o "SSID". Debemos cambiarlo por un nombre menos atractivo.
- Desactivar el broadcasting SSID. El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red WiFi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual. Al desactivarlo se tendrá que introducir manualmente el SSID en la configuración de cada nuevo equipo que se quiera conectar.
- Si el punto de acceso lo permite, es recomendable establecer el número máximo de dispositivos que pueden conectarse al mismo tiempo al punto de acceso.
- Desactivar DHCP en el ruteador y/o punto de acceso. En la configuración de los dispositivos/accesorios WiFi tendrás que introducir a mano la dirección IP, la puerta de enlace, la mascara de subred y el DNS primario y secundario.

[3] SSID. Service Set Identifier; nombre que se le da a la red inalámbrica para que todos los dispositivos la reconozcan.

- Cambiar las claves WEP regularmente. Se recomienda semanalmente o mínimo dos veces al mes, esto dependerá del tráfico generado en la red inalámbrica. Entre mas sea la carga de tráfico, será recomendable cambiar las claves con mayor frecuencia.

5.9.2.- Métodos para asegurar redes inalámbricas Wi-Fi según la situación de uso

En el caso de las redes inalámbricas donde se maneja información de gran trascendencia para las empresas, es de vital importancia el uso de un método que brinde seguridad a la información que es transmitida. Como se vio en el capítulo 4 existen varios métodos que son confiables para lograr este objetivo. En orden de menor a mayor seguridad se enlistan a continuación los distintos métodos:

SITUACION	METODOS PARA ASEGURAR LA RED INALAMBRICA WiFi
Redes caseras y/o pequeñas oficinas (SOHO)	Cifrado "WEP". Aunque se vio que este método no es seguro, siguiendo algunas consideraciones en la configuración de los AP y en las estaciones, se logra tener la seguridad necesaria para este tipo de redes donde el tráfico de información es ligero.
	Filtrado "MAC". Seguridad mínima ya que la dirección MAC es fácilmente detectable y replicable. Pero en este tipo de redes y en conjunto con WEP puede ser de gran ayuda.
	"VPN". Resultan atractivas para proteger este tipo de redes inalámbricas. Funcionan sobre cualquier tipo de hardware inalámbrico. Los servidores VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. No es necesario emplear WEP. Su gran desventaja son el costo, el tráfico de red es lento y cuando el volumen de usuarios es alto no escala bien.

Redes empresariales (Manejo de información sensible para la empresa)	"802.1x". Este protocolo controla el acceso y autenticación basado en la arquitectura cliente servidor, que restringe la conexión de equipos no autorizados a la red. Se ha comprobado que el método es muy seguro aun con contraseñas cortas. Ofrece protección contra ataques de diccionario así como el servicio de autenticación mutua sin necesidad de certificados. Es un método de autenticación robusto y sencillo, el cual es ampliamente recomendado para este tipo de redes inalámbricas.
	"WPA". Este método usa el protocolo de cifrado TKIP el cual cambia la clave compartida entre el punto de acceso y el cliente cada cierto tiempo, con esto se evitan ataques que permitan revelar la clave. El mecanismo de autenticación que emplea es 802.1x y EAP. En modalidad empresarial trabaja con un servidor RADIUS en la red, el cual suministra claves compartidas que cifran los datos. Este método es una de las mejores soluciones para las empresas que manejan información sensible y trascendente. Como otra alternativa, ya existe la nueva versión de WPA que es llamado WPA2, el cual provee encriptación de datos vía AES, y opera en los mismos modos que WPA, modo SOHO y empresarial.

Tabla 5.1 Lista de métodos para asegurar redes inalámbricas Wi-Fi según la situación de uso.

Actualmente en el mercado podemos encontrar dispositivos inalámbricos como Access Pionts y tarjetas de red inalámbricas 802.11b y g que cuentan con soporte para los distintos mecanismos de seguridad. La mayoría de estos dispositivos tiene una interfaz de configuración tipo Web a la que se puede tener acceso mediante el navegador.

Para ejemplificarlo, en las siguientes figuras se analiza la manera en que la mayoría de los AP son configurados para autenticar usuarios y dar seguridad a la información que se transmite, auque cabe mencionar que en esta interfaz también se puede monitorear la actividad en la red. Para tener acceso se requiere saber la dirección IP del punto de acceso, que siempre es proporcionada en el manual de usuario de los AP. Para este caso el fabricante

SMC tiene asignada la dirección IP 192.168.2.1 solo se requiere teclearla en el navegador y entrar.

Por cuestiones de seguridad el fabricante solicita una contraseña para tener acceso a la interfaz de configuración. Como se vio anteriormente, es importante cambiar esta contraseña, ya que fácilmente puede ser descubierta por el observador con malas intensiones. Por default, dependiendo del fabricante estas contraseñas suelen ser, "SMCADMIM", "LINKSYS", "ADMIN".

Figura 5.3 Contraseña de acceso a interfaz web

En la figura 5.4 se observan las opciones de configuración básicas para el AP como el nombre del SSID, habilitar o deshabilitar el broadcast del SSID, el estándar con el que se desea trabajar (11b, 11g o ambos) y el rango de transmisión.

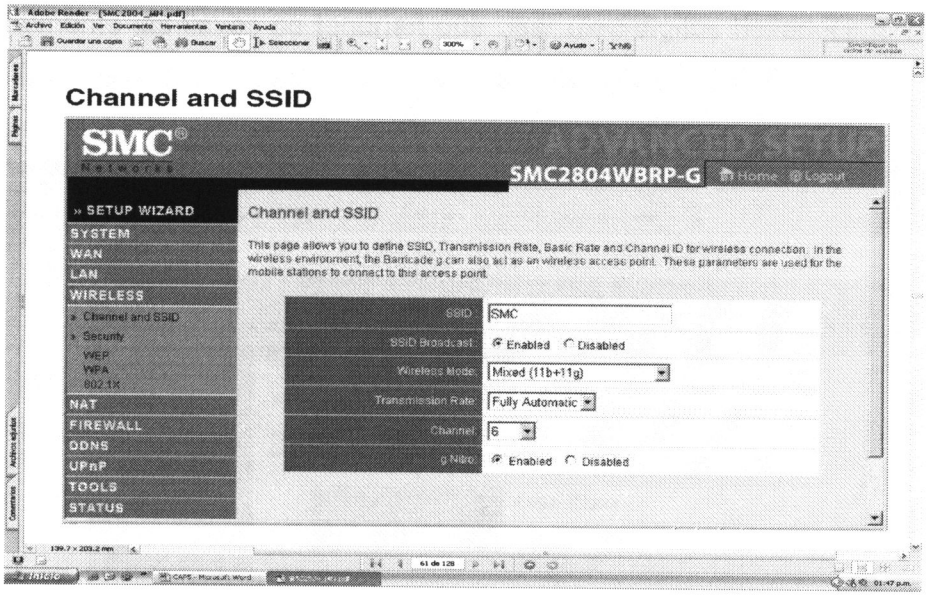


Figura 5.4 Configuración de AP

En la figura 5.5 se presentan las opciones de los diferentes mecanismos de seguridad; autenticación y cifrado que se desea habilitar.

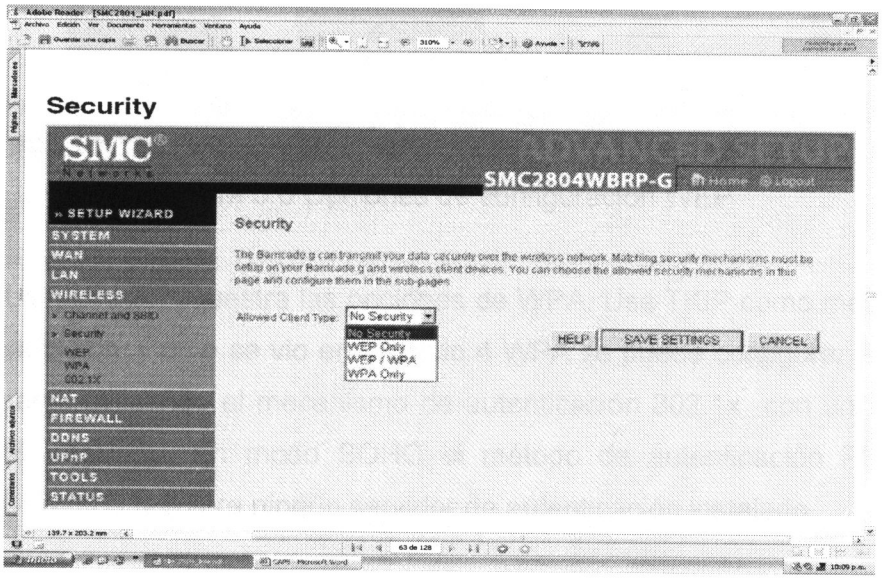


Figura 5.5 Selección de mecanismos de seguridad.

En la figura 5.6 se presentan las opciones para habilitar el cifrado WEP. Se presentan dos modos, 64 bits y 128 bits. Como se vio en el capítulo 4 el modo de 128 bits es más seguro que el de 64 bits. Para configurar

manualmente las llaves se tendrían que usar diez dígitos hexadecimales[4] por cada llave de 64 bits o 26 dígitos para la llave única de 128 bits.

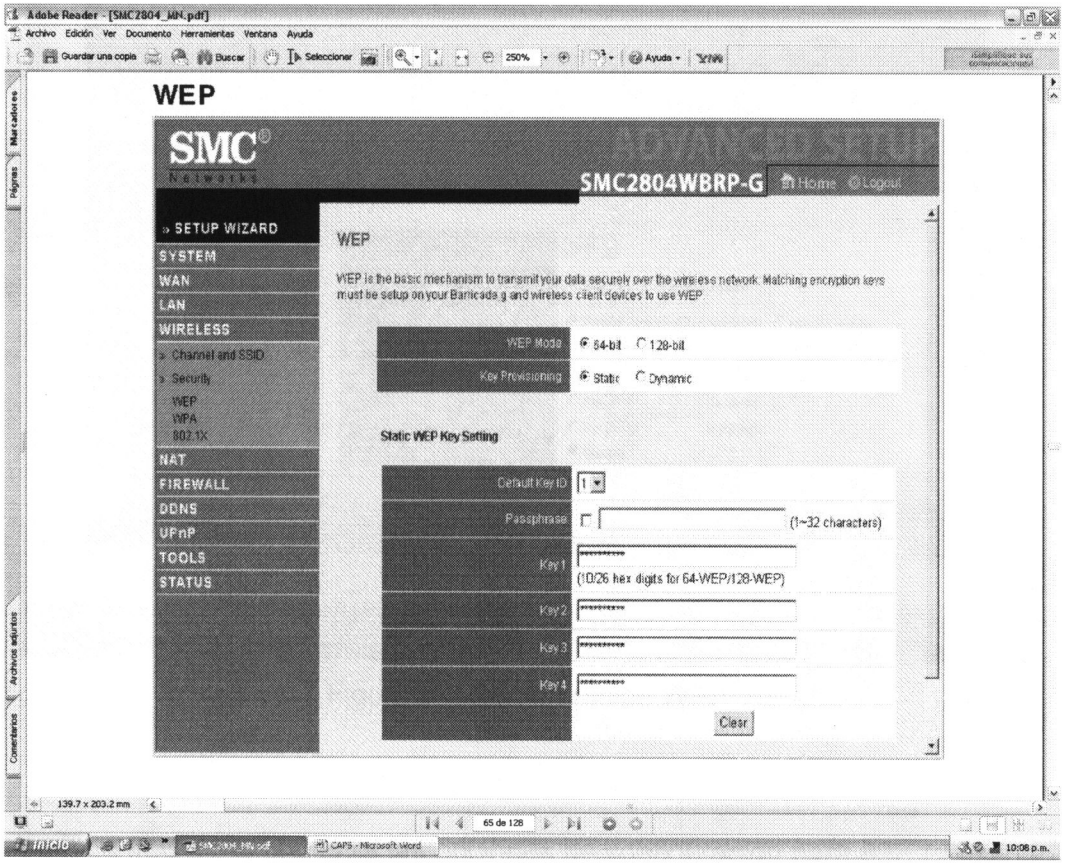


Figura 5.6 Opciones de configuración WEP

La figura 5.7 muestra las opciones de WPA. Usa TKIP como mecanismo de encriptación. Como se vio en capítulo 4 WPA se puede configurar en modo empresarial utilizando el mecanismo de autenticación 802.1x con un servidor RADIUS instalado. En modo SOHO el método de autenticación PSK (Pre Shared-Key) no requiere ningún servidor de autenticación instalado.

[4] Hexadecimal. Número o letra en el rango de 0-9 o A-F.

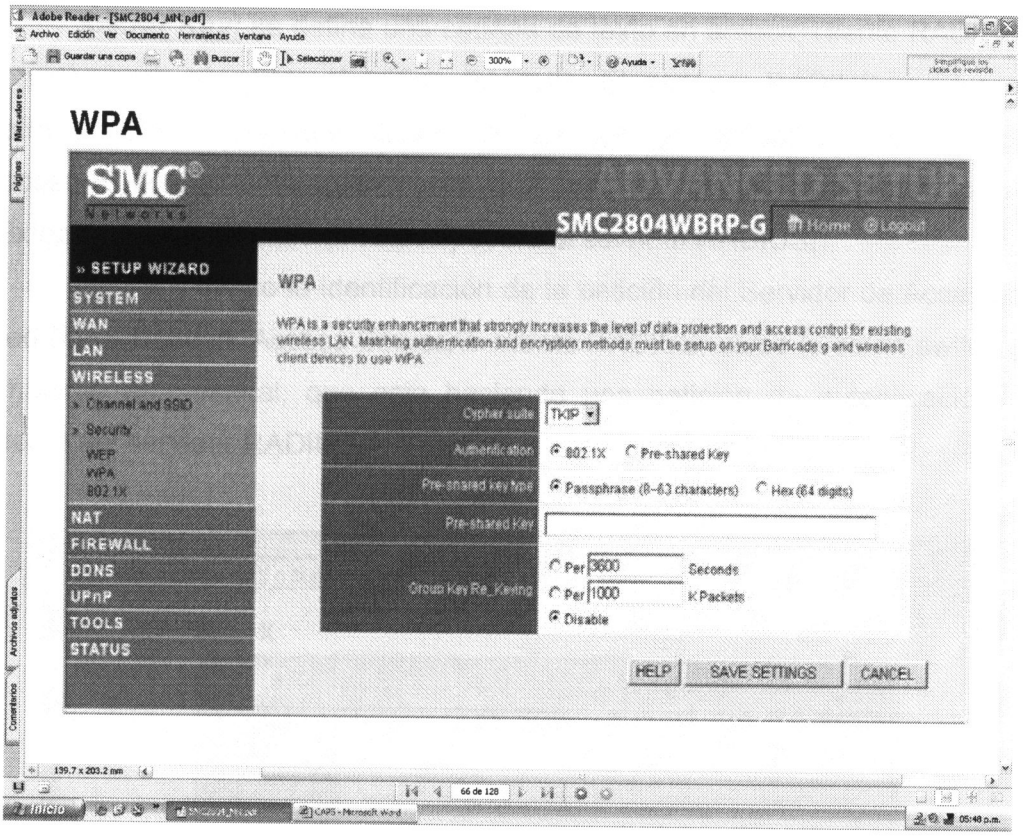


Figura 5.7 Configuración WPA

La figura 5.8 muestra las opciones de configuración para 802.1x usando un servidor de autenticación RADIUS.

Session Idle timeout; aquí se configuran parámetros como el tiempo máximo de conexión durante inactividad.

Re-Authentication Period; el periodo máximo de tiempo en el cual el servidor RADIUS reasignará una llave de sesión a la estación de un cliente conectado.

Quiet Period; El tiempo máximo que el AP esperará entre cada fallo de la autenticación.

Server Type; se selecciona el tipo de servidor.

Server IP; seleccionando el servidor RADIUS se configuran los parámetros, dirección IP del servidor (Default 192.168.2.1).

Server Port; el puerto por default UDP 1812 es usado para los mensajes de autenticación RADIUS.

Secret Key; se define una cadena de texto en ambos, cliente RADIUS y servidor para asegurar el tráfico RADIUS. El servidor RADIUS requiere el atributo MD5 mensaje-autenticador para todos los mensajes de solicitud de acceso. El esquema de autenticación 802.1x es soportado por el protocolo EAP (Extensible Authentication Protocol) sobre el servidor RADIUS.

NAS-ID; define la identificación de la petición del Servidor de Acceso de Red (NAS Network Access Server) o cliente RADIUS, como lo es un switch en ambiente empresarial, que esta haciendo una petición de autenticación de cliente del servidor RADIUS.

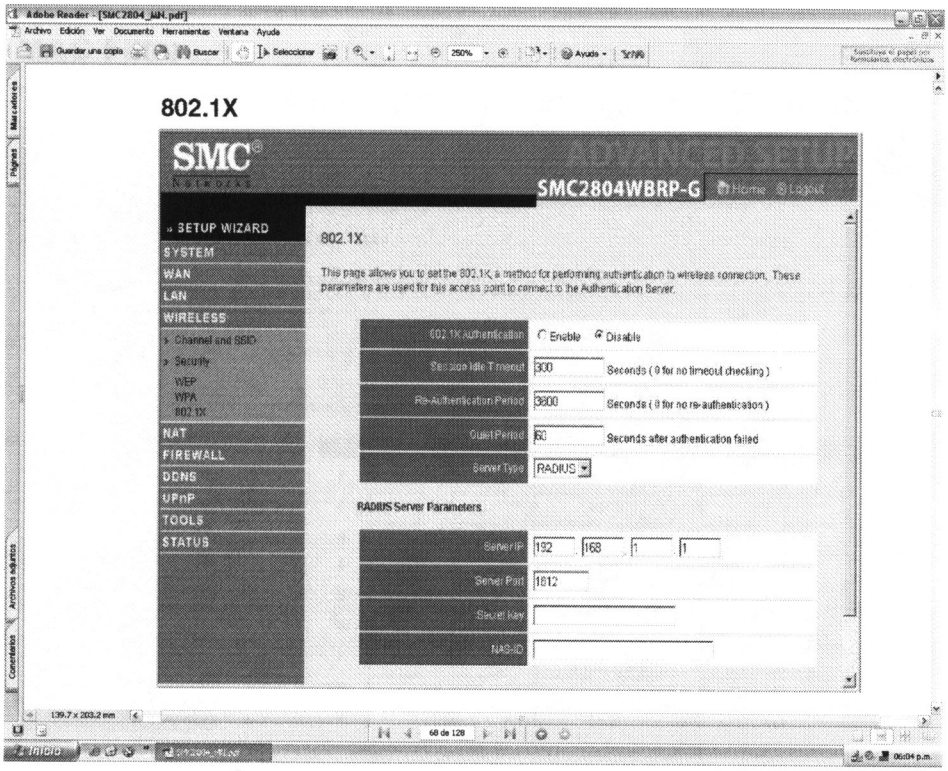


Figura 5.8 Configuración 802.1x con servidor RADIUS

Dentro de las opciones de Firewall en la figura 5.9 están algunos mecanismos para el control de acceso. El filtrado MAC es una opción útil para los ambientes SOHO pero no para los ambientes empresariales, como se vio en el capítulo 4 el filtrado MAC no es seguro y cuenta con algunas desventajas para tomar en cuenta. Para obtener la dirección MAC de las tarjetas de red podemos ejecutar en msdos de Windows el comando ipconfig/all. En esta tabla podemos enlistar 32 direcciones MAC y solo las enlistadas podrán tener acceso a la red.

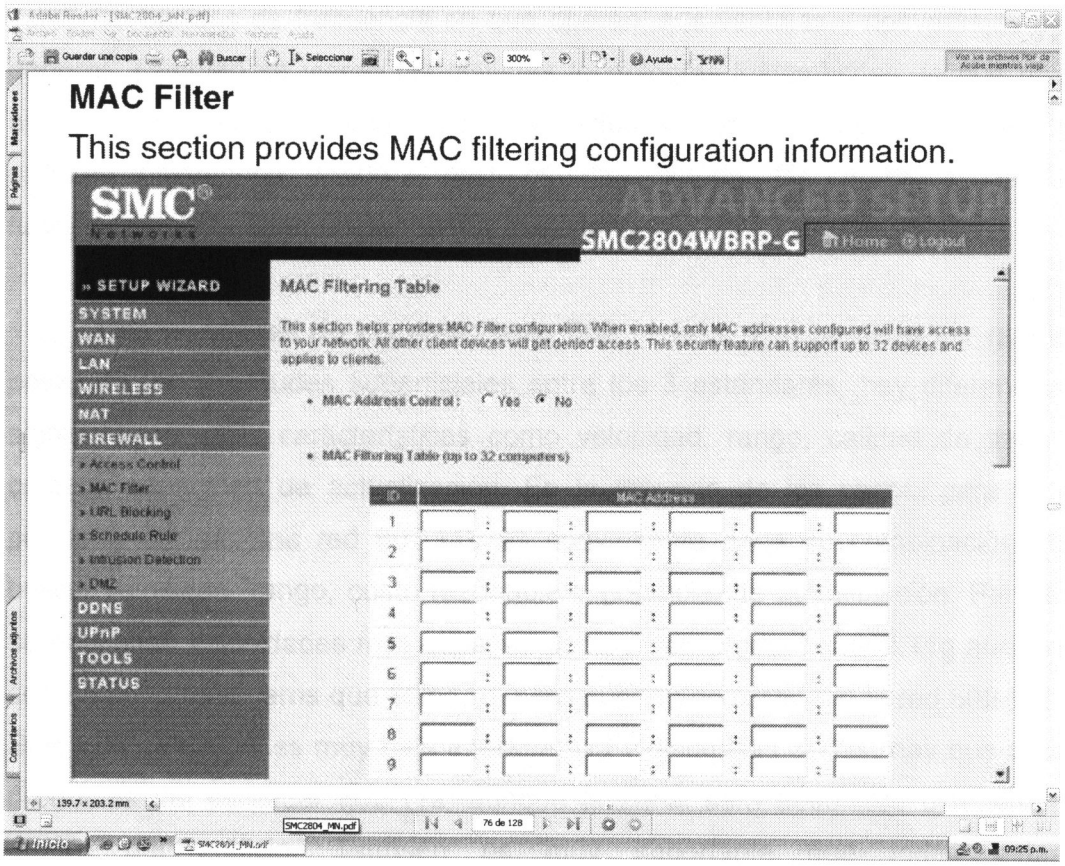


Figura 5.9 Configuración de filtrado MAC

[12]

CONCLUSIONES Y RECOMENDACIONES

Las redes inalámbricas han avanzado a pasos agigantados. En este trabajo se vio la evolución que en los últimos años ha tenido el estándar 802.11 y algunos de los problemas con los que se ha enfrentado.

En los primeros capítulos se vieron cuestiones como las aplicaciones que se le pueden dar a este tipo de redes y los beneficios que se obtienen, así como las bandas de frecuencia en que operan, sus ventajas y desventajas en general. También se vieron las distintas tecnologías inalámbricas, lo que nos aporta conocimiento para la toma de decisiones al momento de implementar una red inalámbrica, donde el costo-beneficio y todas las características de funcionamiento juegan un papel muy importante.

Con el análisis de los estándares 802.11 (a, b y g) se pudo ver que a pesar de las similitudes superficiales entre los 3 estándares, hay diferencias significativas entre características como velocidad, rango, calidad de señal, costo y capacidad de actualización. En la mayoría de los casos, para una pequeña oficina, una red 802.11b es conveniente dada su combinación de buena velocidad, rango, costo razonable y potencial de actualización. Pero si se necesitan velocidades más altas, se deben usar productos 802.11g aunque son un poco más caros que 802.11b, pero pueden coexistir con la red 802.11b. Si lo que se desea es muy baja interferencia y distancias cortas, hay que usar productos del estándar 802.11a, aunque la señal será absorbida o reflejada dentro del edificio. También es muy importante que todas estas consideraciones sean analizadas en función del ambiente físico donde se quiera implementar una red de este tipo, como se vio en esta investigación, ya que existen factores que pueden afectar el funcionamiento como los muros y algunos aparatos electrodomésticos como hornos de microondas, teléfonos inalámbricos, etc. Es por esto la importancia de una buena planeación tanto interior como exterior para lograr el funcionamiento óptimo y elección adecuada de los estándares propios para la red inalámbrica en cuestión.

Las redes inalámbricas envían los datos a través del aire, en forma de ondas de radio, y pueden ser accesibles desde fuera de los límites físicos de una empresa. Es por estos motivos que la importancia de la seguridad en este tipo de redes es de vital importancia. Como se analizó, hoy en día existen varios mecanismos de seguridad que podemos implementar según el ámbito de red y nivel de seguridad que se le quiera dar. En la tabla 5.1 del capítulo 5 se vio el tipo de mecanismo de seguridad conveniente según la situación de uso de una red WLAN. Se vio que el método de seguridad WEP ha sido vulnerado fácilmente, pero como método de seguridad básico y para ambientes caseros y de pequeñas oficinas donde no existe gran flujo de información, es una solución rápida y sencilla para este tipo de redes. El filtrado de direcciones MAC también puede ser una solución bastante accesible, aunque también, al igual que WEP, hay que considerar que es un método poco seguro y además impractico para redes con un gran número de estaciones. Los métodos 802.1x y WPA son métodos que brindan buena seguridad a redes que así lo requieran, son robustos y sencillos. La nueva versión WPA2 provee un buen sistema de encriptación de datos y tiene la versatilidad de configuración en modo casero (o de oficina pequeña) y empresarial, siendo los métodos más recomendables para lograr una buena seguridad en las redes inalámbricas.

Siguiendo estas consideraciones se logrará mantener un buen nivel de seguridad para las redes inalámbricas. Pero día con día la tecnología avanza, al igual que las malas intensiones de la gente que trata de violar la seguridad de estas. Por estos motivos es importante que los administradores de redes WLAN se mantengan al día en las nuevas mejoras de los mecanismos de seguridad.

GLOSARIO DE TERMINOS

Algoritmo: Conjunto de instrucciones concretas y detalladas mediante el cual se consigue una acción determinada.

Ancho de banda: Es común denominar así a la cantidad de datos que se pueden transmitir en una unidad de tiempo.

Cortafuegos (firewall): Programa que protege a una red de otra red.

Encriptar: Mezclar los datos para protegerlos como medida de seguridad, es decir, convertir texto normal a texto cifrado, que es ininteligible hasta que no se desencripta.

Explorador (Navegador): Aplicación mediante la cual podemos visualizar páginas Web de Internet (en inglés browser). Los más conocidos son Internet Explorer y Netscape Navigator.

Firewall: Dispositivos de seguridad a entradas no autorizadas.

Hacker: Informáticos que utilizan sus grandes conocimientos para traspasar cualquier barrera informática.

Hardware: Partes duras de una computadora o componentes de ésta.

Interfaz: Aspecto que presentan los programas tras su ejecución mediante el cual ejercemos la comunicación con éstos.

LAN (Red de Area Local): Grupo de equipos conectados en la misma ubicación.

Paquete de datos: Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras modernas. El término datagrama es usado a veces como sinónimo. Un paquete está generalmente compuesto de tres elementos: una cabecera (header en inglés) que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos (payload en inglés) que contiene los datos que se desean trasladar, y la cola (trailer en inglés), que comúnmente incluye código de detección de errores.

Puente: Un puente o bridge es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete.

PCI: Bus local de 32 bits cuyas ranuras conectan tarjetas que requieren transferencias rápidas.

PCMCIA: Una tarjeta PCMCIA es un dispositivo normalmente utilizado en computadoras portátiles para expandir las capacidades de este. Estas tarjetas reciben su nombre del estándar PCMCIA (estándar) (Personal Computer Memory Card International Association, asociación de la industria de fabricantes de hardware para computadoras portátiles encargada de la elaboración de estándares) y pueden ser de muy distintos tipos: memoria, disco duro, tarjeta de red, etc.

Tarjeta de red: Hardware que se inserta en un equipo para conectarlo a una red.

USB (Universal Serial Bus): Conector de dispositivos externos que hace de vía de ampliación de los nuevos sistemas de cómputo.

BIBLIOGRAFÍA

[1]	802.11 DEMYSTIFIED. James Larocca Ed. Mc Graw Hill 2002.
[2]	Data and Computer Communications. William S. Stallings. Seventh Edition.
[3]	Redes de computadora. Andrew S. Tanenbaum. Cuarta Edición. 2003 Ed. Pearson.
[4]	802.11 Wireless Networks. The definitive Guide. Matthew S. Gast. Ed. O'Reilly. 2002.
[5]	http://www.ieee.org
[6]	http://www.csr.com
[7]	http://spanish.bluetooth.com
[8]	http://www.faqs.org/rfcs/rfc2058.html
[9]	http://www.weca.net/OpenSection/index.asp
[10]	www.fortresstech.com
[12]	http://www.smc.com
[13]	http://computacion.cs.cinvestav.mx/~jjangel/aes/AES_v2005_jjaa.pdf