UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

ESTUDIO Y EVALUACIÓN DE LA IMPLEMENTACIÓN DE UNA RED INALAMBRICA TIPO MAN

T É S I S

PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACIÓN

P R E S E N T Á N:

ALEJANDRO GARCÍA ZAVALA
HÉCTOR SANTIAGO GUTIERREZ REYES
PARIS GUZMÁN SANCHEZ
MARÍA LETICIA PÉREZ FUENTES

DIRECTORA: ING. LUCILA PATRICIA ARELLANO

CIUDAD UNIVERSITARIA SEPTIEMBRE 2005

AGRADECIMIENTOS

Alejandro García Zavala.

A mi Madre,
Por que eres una madre maravillosa y ejemplar, que gracias a tu esfuerzo, cariño y consejos, lograste darme las herramientas necesarias para enfrentar la vida, y gracias a eso pude cumplir una meta que me había trazado en la vida.
A mi Padre,
Que a través de tu imagen, respeto me inculcaste tus valores, tus conocimientos, tu experiencia y cariño, esto es para ti.
A Angélica, Gabriela y Erica,
Gracias por todo su cariño y su apoyo incondicional, por sus esfuerzos a concluir una etapa más en mi vida.
A Leslie,
Por tus palabras de aliento a concluir siempre lo que uno comienza y por estar a mi lado.
A la Universidad,
Por darme la oportunidad de entrar al mundo del conocimiento, a través de sus instalaciones y sus profesores.
A la Facultad,
Por darme la oportunidad de formar parte de ella.

Héctor Santiago Gutiérrez.

A Dios por haberme dado a los que son mi familia y amigos, en especial a mi madre quien nunca ha dejado de apoyarme ni de creer en mi en todo momento y que me dotó con la inteligencia y tenacidad suficiente para llegar hasta donde estoy ahora.

Al Ingeniero Lucila Patricia Arellano Mendoza por su dirección durante el desarrollo del presente trabajo y a cada uno de los sinodales por la paciente revisión del trabajo y los consejos para corregir el mismo.

A mi Universidad, la Universidad Nacional Autónoma de México, ¡Gracias!

Paris Guzmán.

A la Universidad por acogerme como miembro de su comunidad, tratarme como un hijo y darme la oportunidad de ser un profesionista.

A Dios, que en todo momento me ha guiado.

Y a aquellos que me permitieron llegar a este momento, por que si he hecho cosas grandes es por que siempre he estado en hombros de gigantes, mis padres, hermanos, maestros, amigos y en especial a TI, Estela.

María Leticia Pérez Fuentes.

Ahora estoy aquí plasmando la conclusión de una parte de mi vida, de un objetivo que me propuse y termino con gran gozo y satisfacción, agradeciéndote a ti mi vida por tu paciencia, confianza y apoyo, gracias ***Ing. Fidel SP*****.**

Así mismo doy gracias a Dios por permitirme estar aquí y poder disfrutar de esto, de igual manera les doy las gracias a cada uno de mis hermanos y mis padres por todo su apoyo.

Me es de un gran valor agradecer y tener siempre en mi memoria el apoyo que me ha brindado en esta parte de mi formación la máxima casa de estudios, nuestra **Universidad Nacional Autónoma de México**, profesores, académicos, empleados, estudiantes y amigos quienes en algún momento de mi vida contribuyeron a este logro. Por ultimo agradezco a mis compañeros de tesis así como a nuestra directora Ing. Lucila la oportunidad de haber trabajado con ustedes, fue un honor haberlo hecho.

ÍNDICE TEMÁTICO

1. Fundamentos Teóricos

1.1 Introducción a las redes y comunicaciones……. 3
1.1.1 Introducción a las comunicaciones……. 3
1.1.1.1 Concepto y definición de las comunicaciones…….. 3
1.1.1.2 Tipos de comunicación…….. 4
1.1.1.3 Comunicaciones inalámbricas…….. 5
1.1.2 Introducción a las redes……. 9
1.1.2.1 Concepto y definición de las redes…….. 9
1.1.2.2 Objetivo de las redes…… 10
1.1.2.3 Medios de transmisión……. 11
1.1.2.4 Topologías de las redes…… 13
1.1.2.5 Usos actuales y ejemplos……. 15
1.2 Sistemas de transmisión inalámbrica…….. 17
1.2.1 Microondas terrestres……. 17
1.2.2 Microondas por satélite……. 17
1.2.3 Ondas de radio…….. 18
1.2.4 Infrarrojos……. 19
1.3 Tipos de redes……. 19
1.3.1 Redes por cable……. 19
1.3.2 Redes inalámbricas……. 20
1.3.2.1 ¿Qué es una red inalámbrica?..... 20
1.3.2.2 Tipos de redes inalámbricas……. 23
1.3.2.3 Usos actuales y ejemplos……. 24

2. Análisis de Protocolos

2.1 Normas y estándares de comunicación inalámbrica……. 31
2.1.1 Protocolos de comunicación inalámbrica (802.11)…….. 31
2.1.1.1 Comparativa de la familia de estándares IEEE 802.11… 36
2.1.1.2 Acceso al medio…….. 37
2.1.1.2.1 Protocolos con arbitraje……. 38
2.1.1.2.2 Protocolos de acceso por contienda……. 38
2.1.1.2.3 Funcionamiento del protocolo CSMA/CA y MACA… 39
2.1.1.2.4 Nivel de acceso al medio MAC…….. 40
2.1.2 Estándar de redes inalámbricas de área metropolitana (802.16).. 43
2.1.2.1 Introducción a la modulación por espectro discreto…. … 46
2.1.2.2 Tecnología Direct Sequence (DSSS)…….. 47
2.1.2.3 Tecnología Frecuency Hopping……. 50
2.1.3 Velocidades de transmisión y cobertura……. 52

3. Seguridad de la comunicación

3.1 Elección de topología…….. 59
3.1.1 Enlace troncal entre edificios punto-punto…….. 59
3.1.2 Topología estrella…….. 59
3.1.3 Topología malla…… 60
3.2 DHCP…… 60
3.2.1 Asignación de direcciones IP…… 61
3.2.2 Parámetros configurables…… 62
3.3 NAT…… 64
3.3.1 Operación básica…… 65
3.4 Seguridad en las redes inalámbricas…… 66
3.4.1 El problema de la seguridad de una red inalámbrica…….. 67
3.4.2 Garantizando la seguridad de una red inalámbrica…… 69

4. Configuración y conectividad de puntos de acceso.

4.1 Tipo de hardware a utilizar…….. 81
4.1.1 Puntos de acceso…… 81
4.1.2 Antenas…… 82
4.1.2.1 Conectores de antena, cables de antena y adaptadores de red.. 84
4.1.3 Configuración y conexión de dispositivos…… 87
4.1.3.1 Arquitectura de configuración de puntos de acceso…….. 90
4.1.3.2 Aspectos básicos de cobertura en los punto de acceso… 92
4.2 Características…… 93
4.2.1 Características de puntos de acceso…… 93
4.2.2 Características de antenas externas…… 95

5. Configuración y conectividad de clientes.

5.1 Tipo de hardware a utilizar…… 105
5.2 Características…….. 106

6. Configuración y conectividad de servicios.

6.1 Tipo de hardware…….. 111
6.2 Características…… 111
6.3 Tipos de servicios…… 113

7. Resultados.

7.1 Comparación entre tecnologías de comunicación…… 119
7.2 Ventajas y desventajas de implementación…… 122
7.2.1 Razones de implementación…… .. 122

7.2.2 Requisitos de implementación……124
7.2.3 Seguridad en redes inalámbricas…… 128
7.3 Guía de implementación para redes WMAN…….. 129
7.3.1 ¿Qué es un Ckeck List?..... 130
7.3.2 Tecnología a ocupar…… 132
7.3.3 Distribución de antenas…… 133
7.3.4 Distribución de AP…… 134
7.3.5 Servicios a implementar…….. 136
7.3.6 Funcionalidad de la red inalámbrica…….. 137

Conclusión

Anexos

A1 – 1 Catalogo de antenas.
A2 – 1 Catalogo de AP.
A3 – 1 Catalogo de tarjetas y adaptadores de red inalámbricos.
A4 – 1 Check List.

Bibliografía

Prólogo

La investigación desarrollada en el presente trabajo nos proporciona una gran información en forma teórica acerca de las redes inalámbricas las cual se ha complementado relacionándola con las especificaciones de fabricantes actuales de Hardware y Software que nos pueden ayudar al objetivo de la implementación de la red inalámbrica de tipo MAN.

Objetivo

Realizar el estudio y evaluación de la factibilidad, en cuanto a la operación, económico, seguridad y técnico de la implementación de una red inalámbrica que proporcione conectividad y acceso a los recursos e información de una manera móvil y sencilla. Obteniendo las ventajas y desventajas de ésta.

Definición del problema

Hoy en día la mayoría de las aplicaciones de redes son por conexión física (cables) con la problemática que en la comunicación entre dos o más redes de este tipo se complica cuando no se encuentran en un sitio o lugar cercano, ya sea por la distancia a cubrir con cable o por las condiciones o circunstancias par tender el cable.

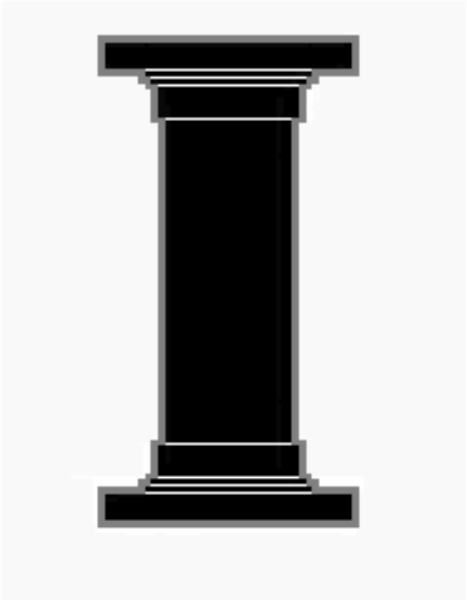
Con la incursión de las redes inalámbricas es posible compartir recursos e información sin tener la necesidad de una conexión física, permitiendo además mayor movilidad y facilidad, es decir hacer un enlace o comunicación no importando el sitio donde nos encontremos. Ofreciendo de esta forma un gran potencial con este tipo de comunicación, no solo en el área científica de investigación, sino también en las áreas didácticas, recreativas, medicas y empresariales, siendo en estas últimas donde se han desarrollado con gran auge el estudio, evaluación e implementación de este tipo de redes.

Así, la idea de hacer un estudio y evaluación para redes inalámbricas surge por los beneficios que se pueden obtener de esta en varios aspectos y con la gran variedad de aplicaciones y ambientes definidos en el área de computó y comunicaciones, algunas de las soluciones son:

- Movilidad: No estar sujeto aun lugar fijo de la empresa para obtener información en línea (tiempo real), obteniendo mayor productividad y ampliando las posibilidades de servicios.
- Facilidad de instalación: Evita las adecuaciones físicas grandes dentro de la edificación actual. (muros, techos paredes, zanjas, etcétera)
- Flexibilidad: Permite con una sencilla adecuación en diferentes circunstancias.
- Confiabilidad: Por a disponibilidad de acceso y seguridad de estas redes.
- Reducción de costos: AL representar menor gasto de instalación.
- Escalabilidad: Al poder incrementa los usuarios o cobertura además de poder cambiar de topología de forma sencilla.

Con lo anterior se puede llegar optimizar la operación de una empresa, incrementando el rendimiento y ahorrando los costos que un proyecto de red ofrece.

Capítulo



Fundamentos Teóricos

Introducción a las redes y comunicaciones
Sistemas de transmisión inalámbricas
Tipos de redes

1.1 INTRODUCCIÓN A LAS REDES Y COMUNICACIONES

1.1.1 Introducción a las comunicaciones

1.1.1.1 Concepto y definición de las comunicaciones

Todo proceso de comunicación requiere de componentes básicos, estos elementos son 3: un transmisor, un medio o canal y un receptor, este proceso comienza cuando alguien genera un mensaje el cual es transmitido (viaja) por el medio o canal y es recibido por el receptor, un modelo general que ilustra este proceso se muestra en la figura 1.1.

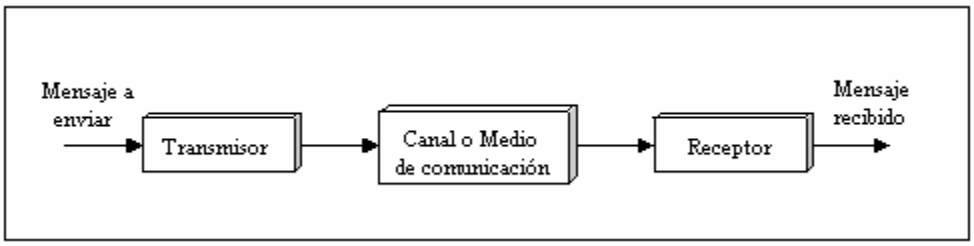


Figura 1.1 Modelo general de comunicación.

El transmisor es el componente que convierte en una forma adecuada el mensaje para ser enviado por el medio de comunicación determinado, en tanto el canal o el medio de comunicación es la forma de transporte (físico) por el cual se envía de un lugar a otro, por su parte el receptor es el componente que acepta el mensaje transmitido del canal y lo convierte en una forma entendible.

Durante todo el proceso anterior se consideran condiciones ideales donde el mensaje es claro e integro de inicio a fin, sin embargo cabe mencionar que en condiciones reales esto no es así debido a malas interpretaciones por el receptor o alteraciones que afectan al medio (producto de otros mensajes de otros transmisores o condiciones externas). A este conjunto de alteraciones se le conoce como *ruido*.

Puede darse el caso en donde la comunicación sea de dos vías, es decir que del lado del transmisor exista también un receptor y del lado del receptor exista un transmisor. Al componente que contiene un transmisor y un receptor se le conoce como Transreceptor.

Aquel proceso el cual utiliza específicamente señales generadas por electricidad en su transmisión se le conoce como comunicaciones electrónicas.

Así una definición de comunicación que aplica en nuestro estudio es:

El proceso mediante el cual se intercambian datos e información en forma de mensaje por medio de dispositivos electrónicos, conformados siempre por un emisor y un receptor, independientemente de la forma física por la cual se envíe el mensaje.

1.1.1.2 Tipos de comunicaciones

Las comunicaciones electrónicas se clasifican con base en:

1. Tipo de transmisión, si es un sentido o una vía (simplex) o si es en dos sentidos (Full-Duplex o Half-Duplex).
2. Tipo de señal, analógica o digital.

En una comunicación en un sentido (simplex), la información viaja en un sentido como lo muestra la figura 1.1, como ejemplo de esta forma de transmisión se tiene la radiodifusión de radio y televisión o en los mensajes beeper, para el caso Full-Duplex la comunicación es en dos sentidos con la capacidad de transmitir y recibir mensajes simultáneamente como por ejemplo en el teléfono donde se puede hablar y escuchar al mismo tiempo. Cuando la comunicación es en dos sentidos pero las direcciones se alternan a un tiempo es decir se turnan para transmitir y para recibir se le conoce como Half-Duplex este tipo de comunicación es utilizada por los militares, bomberos o policías por mencionar algunos ejemplos. En la figura 1.2 se muestran algunos ejemplos para las clasificaciones mencionadas.

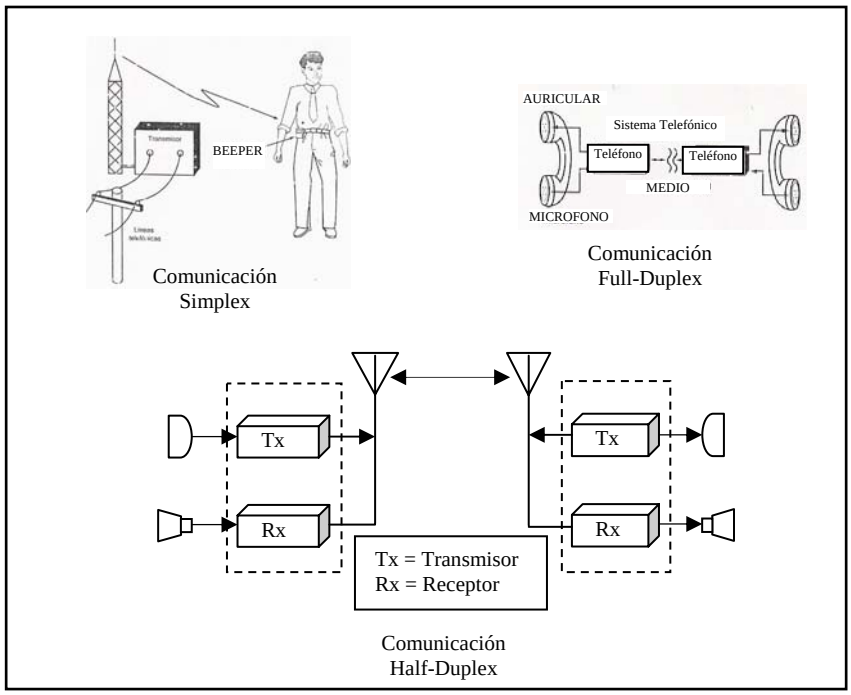


Figura 1.2 Clasificación con base a la forma de comunicación.

Las señales eléctricas usadas en el proceso de comunicación tienen diferente naturaleza, cuando esta señal es un voltaje o corriente que varía suave y continuamente en su forma con respecto al mensaje que es transmitido se le llama señal analógica, por otro lado cuando no varia su forma continua sino que cambia en pasos o incrementos discretos se les llama señales digitales. En la figura 1.3 se muestran ejemplos de señales analógicas y señales digitales.

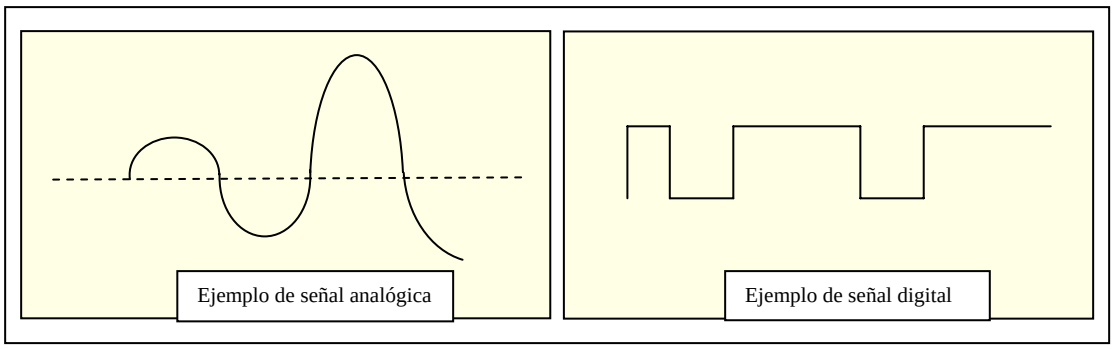


Figura 1.3 Ejemplo de una señal analógica y digital.

Ya sean señales analógicas o digitales éstas necesitan un medio de comunicación o "canal" para ser transmitidas es común mencionar como canal a los conductores eléctricos como el cable coaxial o un cable par trenzado utilizados en una red de computadoras o incluso medios no conductores como lo es la fibra óptica donde la señal eléctrica es enviada a un LED (Light Eminiting Diodo) y el mensaje es transmitido en forma de luz. Para el caso de las comunicaciones inalámbricas (sin cables) el medio usado es el espacio libre conocido mejor con el nombre de *radio*, en donde las señales eléctricas son enviadas en forma de señales electromagnéticas, las cuales pueden "viajar" por el radio a grandes distancias.

Cuando el mensaje que se desea enviar ya sea voz, video o datos es convertido a una señal eléctrica se le conoce como *señal en banda base*. Cuando esta señal es enviada por algún medio de comunicación se le conoce como transmisión en banda base.

1.1.1.3 Comunicaciones inalámbricas

Las comunicaciones inalámbricas son aquellas que no requieren como medio (canal) un cable o un medio físico tangible, por lo que a estas se les reconoce por que usan exclusivamente el espacio libre como medio de comunicación. El enviar mensajes por medio del espacio libre (radio) lleva consigo la necesidad de realizar una transmisión (envío) de la señal diferente a la señal en banda base, entre otras causas, para adecuarse al medio.

Las señales inalámbricas consisten en campos eléctricos y magnéticos[1]. A éstas también se les conoce como ondas de radio frecuencia (RF) o simplemente como ondas de radio. Para lograr la transmisión de RF es necesario el mencionar las técnicas electrónicas que hacen capaz el envío eficiente de estas señales de comunicación, estas técnicas son: modulación y multiplexado de la señal.

La Modulación Es el proceso de hacer que una señal en banda base modifique a otra señal conocida como portadora, esto se muestra en la figura 1.4, con el objetivo de

[1] Un campo eléctrico requerirá de una fuente de energía para ser producido, en tanto que un campo magnético no, ya que su naturaleza magnética actuará como tal.

que esa señal “modulada” con respecto al mensaje sea adecuada para que el transmisor pueda enviarla al medio, en este caso el espacio libre por medio de una antena. La antena como parte del transmisor requiere de un estudio adicional independiente a la comunicación misma, por tal motivo sólo mencionaremos el por qué elegir una longitud de antena determinada y por qué elegir una frecuencia portadora específica.

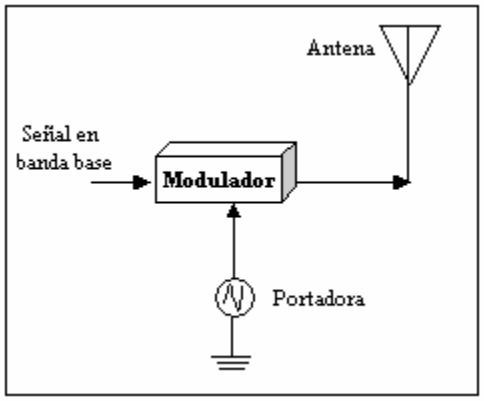


Figura 1.4 Proceso de modulación.

Las ondas de radio tienen la propiedad de propagarse en el espacio vació a una velocidad constante sin importar la frecuencia con la que son enviadas, esta velocidad se encuentra descrita en la ecuaciones de Maxwell[2] y representada por la constante c para cálculos prácticos ($c = 3x10^8$ Km/s), otra variable dentro de la relación de velocidad es la longitud de onda de la señal, la longitud se define para una señal periódica como la separación que existe entre dos puntos cuyo estado de movimiento es idéntico. Lo más sencillo para conocer esto es medir la separación entre dos crestas o dos valles de señal. Así la longitud de onda es representada por la letra griega lambda (**λ**) y la relación de lo anterior queda expresada como:

$$c = \lambda f = 3x10^8$$

Donde:

f = El valor de la frecuencia a enviar.

[2] Las ecuaciones de Maxwell, predicen la velocidad de propagación de las ondas electromagnéticas esta es 299.792 Km/s, así como su dirección (perpendiculares a las oscilaciones del campo eléctrico y magnético, que a su vez son perpendiculares entre sí).

La gran contribución de James Clerk Maxwell fue reunir en estas ecuaciones, los largos años de resultados experimentales, debidos a Coulomb, Gauss, Ampere, Faraday y otros, introduciendo los conceptos de campo y corriente de desplazamiento, y unificando los campos eléctricos y magnéticos en un solo concepto: el campo electromagnético, encontrando la relación:

$$c = \frac{1}{\sqrt{\varepsilon_0 \mu_0}}$$

Siendo ε_0 y μ_0 las permisividad eléctrica y la permeabilidad magnética del vacío respectivamente.

λ = Longitud de onda.
c = velocidad de la luz.

Ahora bien la longitud horizontal de una antena se encuentra dada por la teoría de la difracción la cual expresa en resultados prácticos:

l = 60 **λ.**

Donde: l es la longitud horizontal de la antena.

Así entonces si se deseará enviar una frecuencia de banda base de 1 MHz (Mega Hertz) = 1 000 000 Hz (Hertz), como lo puede ser una frecuencia de voz tendría primero que la longitud de onda sería de:

λ = 300 000 000/1 000 000 = 300 m.

Por lo tanto la longitud de antena sería de:

l = 60 **λ =** 60 * 300 = 18 000 m = 18 Km.

Que en la práctica no es factible, por lo tanto tenemos que a mayor frecuencia de envío la antena será más pequeña, así por ejemplo: para 1 GHz tendríamos una antena de 18 cm.

Resultado de lo anterior existe un margen de frecuencias que pueden ser enviadas como reglamentación para las comunicaciones. El intervalo de señales electromagnéticas que comprende todas las frecuencias se llama *espectro electromagnético*, así entonces este espectro se divide de la siguiente manera para usos prácticos (para frecuencias de 30 Hz a 300 GHz):

- Frecuencias extremadamente bajas (50 y 60 Hz). **ELF.** Se encuentran en frecuencias de líneas de energía y frecuencias de audio del oído humano.
- Frecuencias de voz (300 a 3 000 Hz). **VF.** Rango en el cual se genera la voz humana.
- Frecuencias muy bajas (15 a 20 KHz).**VLF.** Algunos instrumentos musicales y comunicaciones del gobierno como lo son las transmisiones submarino.
- Frecuencias bajas (30 a 300 KHz). **LF.** Usadas en servicios de navegación aeronáutica y marítima.
- Frecuencias medias (300 a 3000 KHz). **MF.** La mayor aplicación es en la radiodifusión de AM y comunicaciones aeronáutica y marítima.
- Frecuencias altas (3 a 30 MHz). **HF. C**onocida también como onda corta o banda corta.

- Frecuencias muy altas (30 a 300 MHz). **VHF.** Usadas en servicios de radio móvil, comunicaciones marítimas y radiodifusión por FM, así como los canales de televisión trabajan en estas frecuencias.
- Frecuencias ultra altas (300 a 3000 MHz). **UHF.** Se encuentran en canales de televisión, telefonía celular y servicios móviles de comunicación.
- Micro ondas y frecuencias súper altas (1 a 30 GHz). **SUHF.** Usadas en comunicaciones por satélite y el radar.
- Frecuencias extremadamente altas (30 a 300 GHz). **EHF.** En el presente hay un número limitado de actividades, ya que el equipo de comunicación para generar y recibir este tipo de señales es demasiado complejo así que solo se incluye algunas aplicaciones de satélite y radar especializado.
- Frecuencias mayores a 300 GHz. Son conocidas como frecuencias milimétricas tienen poco uso pero de los conocidos son los usos militares.

El Multiplexado El uso de la modulación permite utilizar la técnica de multiplexado, proceso mediante el cual dos o más señales pueden compartir el mismo medio o canal, es decir una o más señales en banda base se convierten en una señal compuestas para modular a una portadora, que se envía por el canal, el receptor remodula la señal y posteriormente la envía a un demultiplexor en donde se regresan las señales en banda base. Se mencionan como ejemplo dos tipos de multiplexores: por división de frecuencia y división de tiempo. En la figura 1.5 se puede observar el proceso de multiplexor.

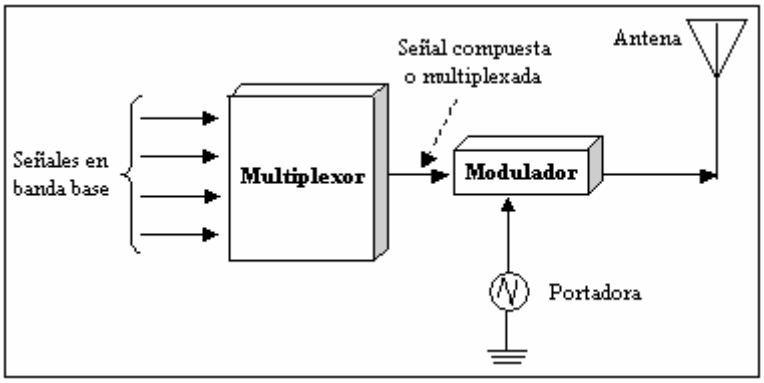


Figura 1.5 Proceso de multiplexado.

En el multiplexado por división de frecuencia, las señales en banda base modulan sub-portadoras que luego se suman y la señal compuesta se usa para modular la portadora. En el multiplexado por división de tiempo, las señales múltiples en banda bases se muestran consecutivamente y una pequeña parte de cada una se usa para modular la portadora.

Las telecomunicaciones es la materia que se dedica al estudio de éstas y otras comunicaciones a fondo (el termino “tele” significa en griego a gran distancia)

y usa los adelantos de cómputo, electrónica y eléctrica en sus técnicas y propiedades electromagnéticas para cumplir el objetivo de comunicar a puntos muy retirados incluso en distintos lugares fuera del planeta.

1.1.2 Introducción a las redes

1.1.2.1 Concepto y definición de las redes

Conforme las computadoras se van acoplando a nuestra vida diaria, cada vez las usamos más para resolver nuestros problemas. Una sola computadora resulta muy valiosa por su capacidad para procesar información sin necesidad de influencia externa. Las *redes* constan de dos o más computadoras conectadas entre sí y permiten compartir recursos e información.

Las redes están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información. La red de área local, representada en la parte izquierda, es un ejemplo de la configuración utilizada en muchas oficinas y empresas. Las diferentes computadoras se denominan computadoras de trabajo y se comunican entre sí a través de un cable o línea telefónica conectada a los servidores. Estos servidores son como las computadoras de trabajo, pero poseen funciones administrativas y están dedicados en exclusiva a supervisar y controlar el acceso de las computadoras de trabajo a la red y a los recursos compartidos (como las impresoras). La línea punteada representa una conexión principal entre servidores de red; la línea continua muestra las conexiones locales. Un módem (modulador/demodulador) permite a las computadoras transferir información a través de las líneas telefónicas normales. El módem convierte las señales digitales a analógicas y viceversa, y permite la comunicación entre computadoras muy distantes entre sí, como se muestra en la figura 1.6.

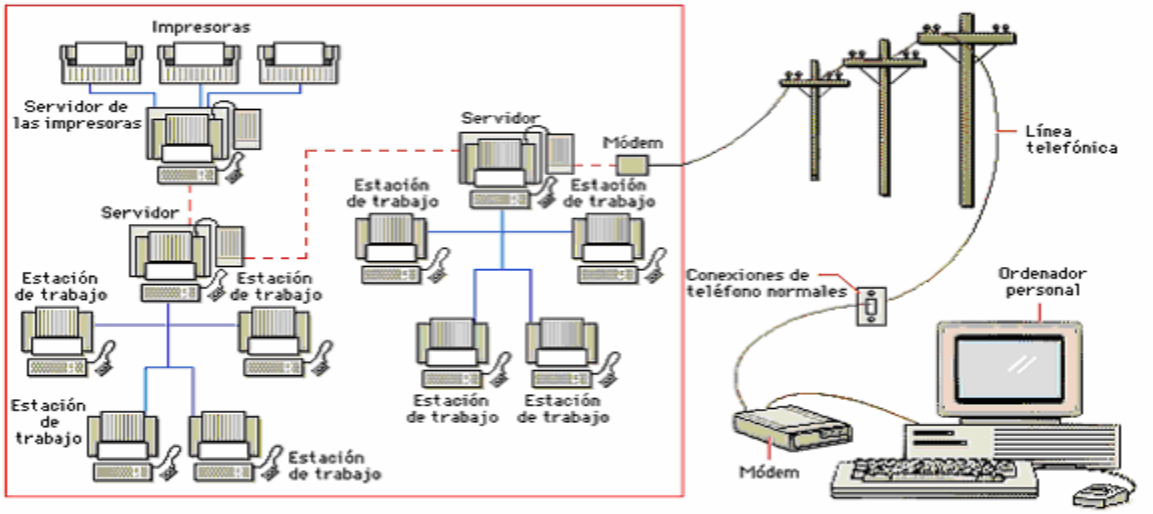


Figura 1.6 Estructura clásica de una red.

La generalización de la computadora personal (PC) y de la red de área local (LAN) ha dado lugar a la posibilidad de acceder a información en bases de datos remotas, cargar aplicaciones desde puntos de ultramar[3], enviar mensajes a otros países y compartir archivos, todo ello desde una computadora personal.

El origen de las redes inalámbricas (WLAN) se remonta a los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica, este tipo de redes se describen más adelante.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del Espectro Expandido (Spread Spectrum[4]), siempre a nivel de laboratorio. La FCC (Federal Comunications Comision, Comisión Federal de Comunicaciones), que es una agencia federal del Gobierno de los Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ICM (es una banda para uso comercial sin licencia) de uso Industrial Científico y Médico (Industrial Scientific and Medical) las frecuencias de 902-928 GHz, 5725–5850 GHz a las redes inalámbricas basadas en Espectro Expandido (Spread Spectrum).

La asignación de una banda de frecuencia propició una mayor actividad en el seno de la industria: ese respaldo hizo que las redes inalámbricas empezaran a dejar ya el laboratorio para iniciar el camino hacía el mercado. Hasta entonces, estas redes habían tenido una aceptación marginal en el mercado. Las razones eran varias:

- Gran cantidad de técnicas, tecnología y normas existentes en el ámbito de las comunicaciones móviles debido a que los diferentes fabricantes estaban desarrollando sus propias soluciones, utilizando frecuencias y tecnologías muy distintas y normalmente incompatibles. No existía una norma.
- Altos precios que reflejan los costos de investigación para desarrollar soluciones tecnológicas propietarias.
- Reducidas prestaciones si se comparan con sus homólogas las redes cableadas: las redes inalámbricas únicamente permiten el soporte de datos, mientras que por una red cableada se puede llevar a cabo una multitud de aplicaciones tanto de voz como de datos, video, etc. Y además las velocidades de transmisión en las redes inalámbricas son significativamente menores.

En conclusión, una red es un conjunto de computadoras conectadas entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos. Las computadoras suelen estar conectadas entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

[3] La manera más rápida de transmitir información entre continentes es mediante cables submarinos de fibra óptica. Algunos de estos cables pueden transmitir el equivalente a 62 500 páginas escritas por segundo.

[4] El espectro expandido es una técnica basada en señales de pseudoruido y señales de radiofrecuencia; el proceso comienza con la señal del dato digital y un generador de pseudoruido, los cuales se mezclan para formar un dato expandido.

Las computadoras conectadas a una red pueden ser grandes computadoras o bien computadoras personales, cada una de ellas con sus diversos tipos de periféricos. Cabe destacar que entre dichas computadoras pueden existir diferentes tipos de redes; sin embargo, entre ellas existen características comunes tales como:

1. Un medio de comunicación común a través del cual todos los dispositivos pueden compartir información, programas y equipo, independientemente del lugar físico donde se encuentre el usuario o el dispositivo. Las redes están contenidas en una reducida área física: un edificio, un campus, etc.
2. Una velocidad de transmisión muy elevada para que pueda adaptarse a las necesidades de los usuarios y del equipo. El equipo de la red puede transmitir datos a la velocidad máxima a la que puedan comunicarse las computadoras de la red, suele ser de un Mega bits por segundo (Mb/s).
3. Todos los dispositivos que están conectados a la red pueden comunicarse con el resto y algunos de ellos pueden funcionar independientemente.
4. Un sistema fiable, con un índice de errores muy bajo. Las redes disponen normalmente de su propio sistema de detección y corrección de errores de transmisión.
5. Flexibilidad, el usuario administra y controla su propio sistema.

Los dos tipos básicos de dispositivos que pueden conectarse a una red son las computadoras de trabajo y los servidores:

- Una computadora de trabajo es donde el usuario puede acceder a los recursos de la red.
- Un servidor es una computadora que permite a otras computadoras que accedan a los recursos de que disponen. Estos servidores pueden ser:

    - *Dedicados:* Son usados únicamente para ofrecer sus recursos a otros nodos[5].
    - *No dedicados:* Pueden trabajar simultáneamente como servidor y computadora de trabajo.

1.1.2.2 Objetivo de las redes

Las redes en general, consisten en compartir recursos, y uno de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera en la red que así lo solicite, sin importar la localización física del recurso y del usuario.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministros.

[5] Se denomina nodo a cada dispositivo activo conectado a la red. Un dispositivo activo es aquel que interviene en la comunicación de forma autónoma, sin estar controlado por otro dispositivo.

Otro objetivo es el ahorro económico. Las computadoras pequeñas tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las computadoras grandes. Éstas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosas computadoras personales, una por usuario. Este objetivo conduce al concepto de redes con varias computadoras en el mismo edificio. A este tipo de red se le denomina LAN (red de área local), en contraste con lo extenso de una WAN (red de área extendida), a la que también se le conoce como red de gran alcance y existe una que esta en medio de los dos tipos de redes mencionadas anteriormente que es conocida como MAN (red de área metropolitana).

Otro objetivo del establecimiento de una red de computadoras, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si.

1.1.2.3 Medios de trasmisión

Por medio de transmisión se entiende el soporte físico utilizado para el envío de información por la red. La mayor parte de las redes existentes en la actualidad utilizan como medio de transmisión cable coaxial, cable par trenzado y el cable de fibra óptica. También se utiliza el medio inalámbrico que usa ondas de radio, microondas o infrarrojos.

Cualquier medio físico o no, que pueda transportar información en forma de señales electromagnéticas se puede utilizar en redes locales como medio de transmisión. Las líneas de transmisión son la espina dorsal de la red, por ellas se transmite la información entre los distintos nodos. Para efectuar la transmisión de la información se utilizan varias técnicas, pero las más comunes son: la banda base y la banda ancha.

Cable coaxial Hasta hace poco, era el medio de transmisión más común en las redes. El cable coaxial consiste en dos conductores concéntricos, separados por un dieléctrico y protegido del exterior por un aislante (similar al de las antenas de TV). Existen dos tipos de cable coaxial:

- *Cable Thinck o Cable Grueso:* Es más voluminoso, caro y difícil de instalar, pero permite conectar un mayor número de nodos y alcanzar mayores distancias.
- *Cable Thinck o Cable Fino:* También es conocido como cheapernert por ser más económico y fácil de instalar. Sólo se utiliza para redes con un número reducido de nodos.

Ambos tipos de cable pueden ser usados simultáneamente en una red. La velocidad de transmisión de la señal por ambos es de 10 Mbps. La figura 1.7 muestra la estructura del cable coaxial.

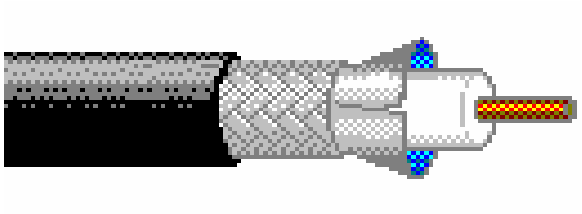


Figura 1.7 Estructura del cable coaxial.

Ventajas del cable coaxial:

- La protección de las señales contra interferencias eléctricas debida a otros equipos.
- Logra altas velocidades de transmisión en largas distancias (500 m).

Cable par trenzado El cable par trenzado consta como mínimo de dos aisladores trenzados entre ellos y protegidos con una cubierta aislante. Un cable de este tipo habitualmente contiene 1, 2, ó 4 u 8 hilos. Los cables trenzados constituyen el sistema de cableado en todo el mundo para telefonía. Es una tecnología bien conocida. El cable es bastante barato y fácil de instalar y las conexiones son fiables. Sus ventajas mayores son por tanto su disponibilidad y bajo costo.

Sin embargo es importante aclarar que habitualmente este tipo de cable no se maneja por unidades, sino por pares y grupos de pares, paquete conocido como cable multipar. Todos los cables del multipar están trenzados entre sí con el objeto de mejorar la resistencia de todo el grupo hacia diferentes tipos de interferencia electromagnética externa. La figura 1.8 muestra la estructura del cable par trenzado.



Figura 1.8 Estructura del cable par trenzado.

Por esta razón surge la necesidad de poder definir colores para los mismos que permitan al final de cada grupo de cables conocer qué cable va con cual otro. Los colores del aislante están normalizados a fin de su manipulación por grandes cantidades. Para las redes los colores estandarizados son:

- Naranja / Blanco → Naranja.
- Verde / Blanco → Verde.
- Blanco / Azul → Azul.
- Blanco / Marrón → Marrón.

En cuanto a las desventajas están la gran atenuación de la señal a medida que aumenta la distancia y que son muy susceptibles a interferencias eléctricas.

Por este motivo para evitar las interferencias, el conjunto de pares se apantalla con un conductor que hace de malla. Esto eleva el costo del cable en sí, pero su instalación y conexión continúa siendo más barato que en el caso del cable coaxial.

Fibra óptica Es el medio de transmisión más moderno y avanzado. Utilizado cada vez más para formar la espina dorsal de grandes redes. Las señales de información se transmiten a través de impulsos luminosos y pueden recorrer grandes distancias (del orden de kilómetros) sin que se tenga que amplificar la señal. Por su naturaleza, este tipo de señal y cableado es inmune a las interferencias electromagnéticas y por su gran ancho de banda (velocidad de transferencia), permite transmitir grandes volúmenes de información a alta velocidad.

Estas ventajas hacen de la fibra óptica la elección idónea para redes de alta velocidad a grandes distancias, con flujos de información considerables, así como en instalaciones en que la seguridad de la información sea un factor relevante. La figura 1.9 muestra la estructura de la fibra óptica.

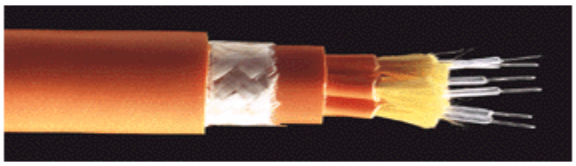


Figura 1.9 Estructura de la fibra óptica.

Como inconveniente, es que es el soporte físico más caro. De nuevo, no debido al costo del cable en sí, sino por el precio de los conectores, el equipo requerido para enviar y detectar las ondas luminosas y la necesidad de disponer de técnicos calificados para realizar la instalación y mantenimiento del sistema de cableado.

1.1.2.4 Topologías de las redes

Por topología de una red se entiende que es la forma en que se lleva a cabo la conexión entre equipos. Las topologías más utilizadas son: en bus (lineal), en estrella, en árbol y en anillo.

Bus (lineal) La topología en bus o lineal es un diseño sencillo en el que un solo cable, que es conocido como “bus”, es compartido por todos los dispositivos de la red. El cable va recorriendo cada una de las computadoras y se utiliza una terminación en cada uno de los extremos. Los dispositivos se conectan al bus utilizando generalmente un conector en T. En la figura 1.10 se muestra la topología de bus o lineal.

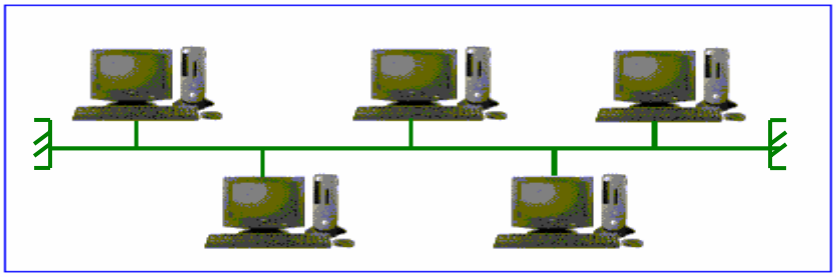


Figura 1.10 Topología de bus o lineal.

Las ventajas de las redes en bus son su sencillez y economía. El cableado pasa de una computadora a otra. Un inconveniente del bus es que si el cable falla en cualquier punto, toda la red deja de funcionar. Aunque existen diversos procedimientos de diagnóstico para detectar y solventar tales problemas, en grandes redes puede ser sumamente difícil localizar estas averías.

Estrella Los nodos de la red se conectan con cables dedicados a un punto que es una caja de conexiones, llamada *Hub o Switch*. En una topología en estrella cada computadora de trabajo tiene su propio cable dedicado, por lo que habitualmente se utilizan mayores longitudes de cable. La figura 1.11 muestra esta topología.

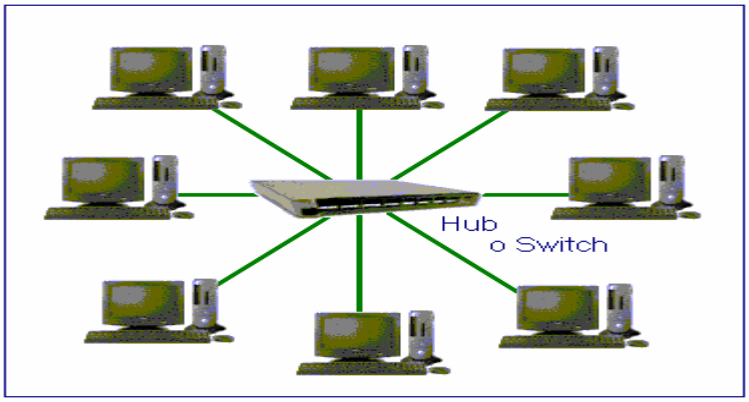


Figura 1.11 Topología estrella.

La detección de problemas de cableado en este sistema es muy simple al tener cada computadora de trabajo su propio cable. Por la misma razón, la resistencia a fallos es muy alta ya que un problema en un cable afectará solo a este usuario.

Árbol La topología en árbol se denomina también topología en *estrella distribuida*. Al igual que sucedía en la topología en estrella, los dispositivos de la red se conectan a un punto que es una caja de conexiones.

Éstos suelen soportar entre cuatro y doce computadoras de trabajo. Los hub's se conectan a una red en bus, formando así un árbol o pirámide de hub's y dispositivos. Esta topología reúne muchas de las ventajas de los sistemas en bus y en estrella. En la figura 1.12 muestra este tipo de topología.

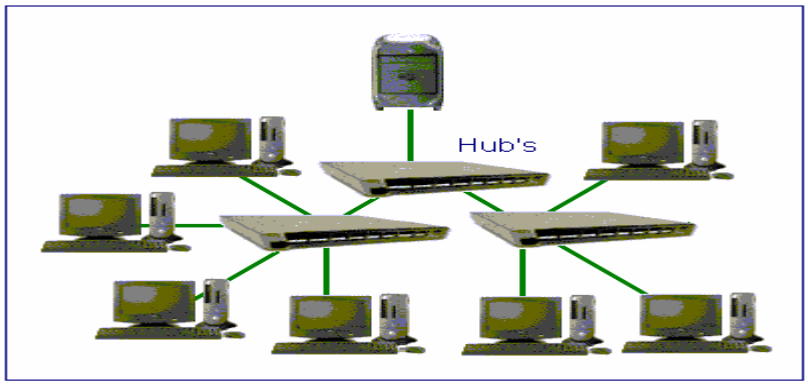


Figura 1.12 Topología en árbol.

Anillo En una red en anillo o *token ring* los nodos se conectan formando un círculo cerrado. El anillo es unidireccional, de tal manera que los paquetes que transportan datos o información circulan por el anillo en un solo sentido, como lo muestra la figura 1.13.

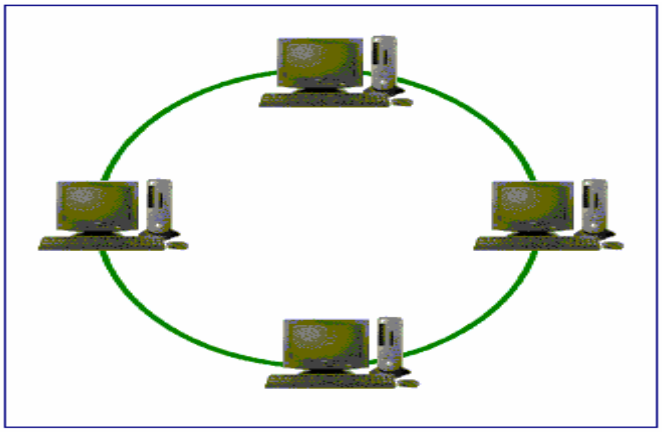


Figura 1.13 Topología de anillo o token ring.

En una red local en anillo simple, un corte del cable afecta a todas las estaciones, por lo que se han desarrollado sistemas en anillo doble o combinando topologías de anillo y estrella.

1.1.2.5 Usos actuales y ejemplos

La utilización de sistemas de comunicación surge como respuesta a las necesidades de flujo, distribución oportuna y eficaz de la información, que son soportadas a través de tecnologías de telecomunicaciones que se definen como la comunicación de información por medios electrónicos.

Un recuento de los usos actuales del Internet arroja un abanico de posibilidades. En México actualmente existen organizaciones que promueven y desarrollan proyectos

productivos usando Internet para comercializar sus productos. Es el caso de productores de café orgánico y exportadores de artesanía, por mencionar algunos. En otros casos es usado para solicitar voluntarios, presentar resultados de proyectos, realizar acciones urgentes. Por ejemplo, el adecuado manejo de una lista de correspondencia vía correo electrónico ayudó a mantener pendiente e informado a un vasto conjunto de grupos involucrados en el caso de Claudia Rodríguez, una mujer acusada de asesinato por haberse defendido de ser violada, quien es finalmente puesta en libertad gracias a la presión social. Cuando la situación lo amerita ocurren movilizaciones simultáneas en diversas ciudades del mundo, facilitadas por el intercambio de información a través de la red. El Internet cumple un eficiente papel informativo en estas circunstancias.

Aún cuando las posibilidades técnicas están al alcance de muchos grupos existen varios desafíos. Uno de ellos es la diferencia en el nivel de acceso a la tecnología de la comunidad usuaria. Accesibilidad telefónica y acceso a infraestructura marcan posibilidades básicas.

Algunas utilidades en los negocios en donde es clave la utilización de la tecnología son el correo electrónico, el correo de voz, el fax, las teléconferencias, las videoconferencias y el intercambio electrónico de datos.

Las comunicaciones son un elemento esencial en la vida de los negocios de hoy ya que permiten realizar operaciones de procesamiento en línea y crear accesos directos a los datos de la organización.

Algunos usos actuales de las tecnologías de redes y las telecomunicaciones, se pueden apreciar en la tabla 1.1, tomada del libro de Laudon.

Aplicación	Ejemplo	Requerimientos
Negocios		
Entrada de datos.	Control de inventarios.	Operaciones que ocurren cada tiempo/segundo, se requiere de respuesta directa.
Recuperación de texto en línea.	Sistema de información para hospitales. Sistemas de librerías.	Respuesta requerida en tiempo real; elevados volúmenes de caracteres.
Respuesta a solicitudes de información.	Sistema punto de venta. Sistema de reservación de líneas aéreas.	Operaciones varias veces (la segunda respuesta instantánea en cuestión de segundos).
Intercambio de datos entre computadoras.	Transferencias internacionales de fondos bancarios.	Elevados aunque poco frecuentes picos de información; transferencia de grandes bloques de datos; respuesta inmediata en línea.
Domésticos		
Respuesta a solicitudes de información.	Operaciones domésticas de bancos, compras pedidos.	Operaciones en línea, cobradas con alta frecuencia.
Recuperación de textos.	Educación en casa.	Elevado volumen, transmisión rápida.
Diversiones especiales.	Deportes, participación en encuestas y actividades políticas.	Elevada capacidad en las habilidades de video y voz.

Tabla 1.1 Usos actuales de las tecnologías de redes y las telecomunicaciones.

El papel del administrador en cuanto a telecomunicaciones consiste en mantenerse plenamente informado con respecto a las tecnologías existentes y su correspondiente aplicabilidad en la organización de la que hace parte.

1.2 SISTEMAS DE TRANSMISIÓN INALÁMBRICA

En las comunicaciones inalámbricas se consideran tres intervalos de frecuencia, donde el primer intervalo se define desde 1 GHz hasta 40 GHz, a este intervalo se denomina de frecuencias microondas y son adecuadas para enlaces punto a punto, estas también se ocupan en comunicaciones satelitales. A las frecuencias que van desde 30 MHz a 1 GHz se les denominan ondas de radio, otra frecuencia para aplicaciones de cobertura local, son la infrarroja las cuales comprenden de 20 y 30 MHz, estas conexiones son también punto a punto. En medios no guiados, la transmisión y la recepción se realiza mediante una antena.

1.2.1 Microondas Terrestres

La antena más común en microondas es la parabólica tipo plato con un diámetro de 3 m. La antena se fija de forma que el haz debe estar perfectamente enfocado siguiendo la trayectoria visual hacia la antena receptora. Para conseguir las transmisiones a larga distancia se concatenan distintos enlaces punto a punto entre antenas situadas en torres adyacentes, hasta cubrir la distancia deseada.

Los sistemas de microondas terrestres se usan principalmente en servicios de telecomunicaciones de larga distancia como alternativa al cable coaxial o a las fibras ópticas. Otro uso en conexiones punto a punto entre edificios con distancias cortas y las aplicaciones típicas son circuitos cerrados de TV o interconexiones entre redes locales. También las microondas a corta distancia se ocupan en aplicaciones denominadas bypass. Otro uso es en sistemas celulares. El rango de operaciones de las microondas cubre una parte sustancial del espectro electromagnético, su banda de frecuencia está comprendida entre 1 y 40 GHz. Entre más grande sea la frecuencia utilizada mayor es el ancho de banda potencial y por lo tanto es mayor la posible velocidad de transmisión.

1.2.2 Microondas por Satélite

Un satélite de comunicaciones es esencialmente una estación que transmite microondas, se usa como enlace entre dos o más receptores/transmisores terrestres, denominados estaciones base, como se muestra en la figura 1.14. El satélite recibe la señal en una banda de frecuencia (canal ascendente), la amplifica o repite y después la retransmite en otra banda de frecuencia (canal descendente). Cada satélite opera en una serie de bandas de frecuencias llamadas canales transpoders. Entre las aplicaciones más importantes de las comunicaciones satelitales son:

- La difusión de la TV.
- La transmisión telefónica a larga distancia.
- Las redes privadas.

Sus características de transmisión son: el rango de frecuencias óptimo está entre 1 y 10 GHz. Los satélites que proporcionan el servicio de enlace punto a punto operan en el intervalo entre 5925 y 6425 GHz para la transmisión desde el satélite (canal ascendente) hasta la tierra (canal descendente). Al intervalo de frecuencias se conoce como la banda 4/6 GHz.

Es importante mencionar que el retorno de propagación es aproximadamente del orden de un cuarto de segundo para una transmisión que vaya desde una estación terrestre hasta otra y que pase por el satélite.

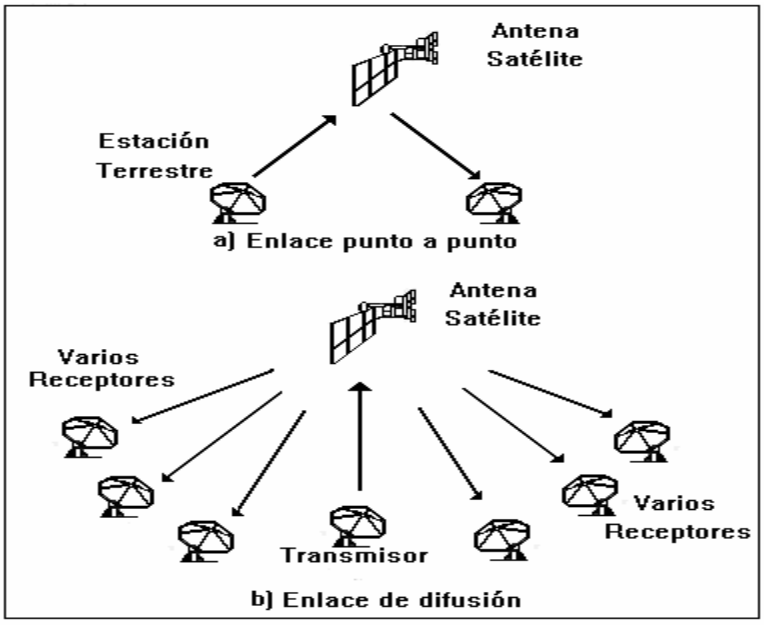


Figura 1.14 Microondas por satélite.

1.2.3 Ondas de Radio

La diferencia entre las microondas y las ondas de radio es que las de radio son omnidireccionales, mientras que las primeras tienen un diagrama de radiación mucho más direccional, esto hace que las ondas de radio no necesiten antenas parabólicas ni necesiten que las antenas estén instaladas sobre una plataforma rígida para estar alineadas.

El término ondas de radio por mencionar a la banda VHF y UHF: de 30 MHz a 1 GHz, este rango abarca a la radio comercial FM así como a la televisión UHF y VHF. Las características de transmisión y el rango están comprendidos entre 30 MHz y 1 GHz, son

adecuados para difusión simultánea a varios destinos. A diferencia de las ondas electromagnéticas con frecuencias menores, la ionosfera es transparente para las ondas con frecuencias superiores a 30 MHz.

La transmisión es solo posible cuando las antenas están alineadas. En esa banda no se producirán interferencias entre los transmisores debidas a las reflexiones en la atmósfera. Las ondas de radio son menos sensibles a la atenuación producida por la lluvia. Un factor muy importante en las ondas de radio son las interferencias por multitrayectorias.

1.2.4 Infrarrojos

La comunicación mediante infrarrojos se lleva a cabo mediante transmisores/receptores (transceivers) que modulan la luz infrarroja no coherente. Los transceptores deben estar alineados directamente, o bien deben estar accesibles a través de la reflexión en una superficie. Hay diferencias entre transmisión infrarroja y microondas es que los infrarrojos no pueden atravesar paredes, por lo que los problemas de seguridad y de interferencias que aparecen en las microondas no se presentan en este medio de transmisión.

1.3 TIPOS DE REDES

1.3.1 Redes por cable

Redes de Área Local (Local Area Network, LAN) Conjunto de computadoras que pueden compartir datos, aplicaciones y recursos (por ejemplo impresoras). Las computadoras de una red de área local están separadas por distancias de hasta unos pocos kilómetros, y se suelen usar en oficinas o campus universitarios. Una LAN permite la transferencia rápida y eficaz de información en el seno de un grupo de usuarios y reduce los costos de explotación.

Una LAN suele estar formada por un grupo de computadoras, pero también puede incluir impresoras o dispositivos de almacenamiento de datos como unidades de disco duro, etc. La conexión material entre los dispositivos de una LAN puede ser un cable coaxial, un cable par trenzado o una fibra óptica. También pueden efectuarse conexiones inalámbricas empleando transmisiones de infrarrojos o radiofrecuencia.

Un dispositivo de una LAN puede emitir y recibir señales de todos los demás dispositivos de la red. Otra posibilidad es que cada dispositivo esté conectado a un repetidor, un equipo especializado que transmite de forma selectiva la información desde un dispositivo hasta uno o varios destinos en la red.

Las redes emplean protocolos, o reglas, para intercambiar información a través de una única conexión compartida. Estos protocolos impiden una colisión de datos provocada por la transmisión simultánea entre dos o más computadoras. En la mayoría de las LAN, las computadoras emplean protocolos conocidos como Ethernet o Token Ring. Las computadoras conectadas por Ethernet comprueban si la conexión compartida está en uso; si no es así, la computadora transmite los datos. Como las computadoras pueden detectar si la conexión está ocupada al mismo tiempo que envían datos, continúan controlando la conexión compartida y dejan de transmitir si se produce una colisión. Los protocolos Token Ring transmiten a través de la red un mensaje especial. La computadora que recibe la contraseña obtiene permiso para enviar un paquete de información; si la computadora no tiene ningún paquete que enviar, pasa la contraseña a la siguiente computadora.

Redes de Área Metropolitana (Metropolitan Area Network, MAN) Una red de área metropolitana es un sistema de interconexión de equipos computacionales distribuidos en una zona que abarca diversos edificios por medios pertenecientes a la misma organización propietaria de los equipos. La red no abarca más de 100 Km. habitualmente, este tipo de redes se utiliza para interconectar redes de área local.

Redes de Área Extensa (Wide Area Network, WAN) Cuando se llega a un cierto punto deja de ser práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían las LAN hasta convertirla en una red de área extensa. Casi todos los operadores de redes nacionales ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como Frame Relay y SMDS, Synchronous Multimegabit Data Service) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Actualmente están proporcionando los enlaces necesarios entre las LAN para ser posible lo que han dado en llamarse autopistas de la información.

1.3.2 Redes inalámbricas

1.3.2.1 ¿Qué es una red inalámbrica?

El uso extendido de computadoras portátiles (laptops) y de asistentes personales de mano (PDA) ha impulsado avances en las redes inalámbricas. Las redes inalámbricas utilizan transmisiones de infrarrojos o radiofrecuencias para unir estos dispositivos portátiles a las redes.

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante ondas de radio o luz infrarroja, actualmente está siendo ampliamente investigado. 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. Pero la realidad es que esta tecnología está todavía en pañales y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

Los avances en la forma en que una red envía la información permitirán que los datos circulen directamente desde la computadora de origen hasta la de destino sin interferencia de otras computadoras. Esto mejorará la transmisión de flujos continuos de datos, como señales de audio o de vídeo. El uso generalizado de computadoras portátiles ha llevado a importantes avances en las redes inalámbricas.

Actualmente, la puesta en marcha de forma comercial de redes de fibra óptica y la mejora en los protocolos de Internet y un uso optimizado de líneas telefónicas estándar, al estilo de las ADSL[6], permite enviar de forma barata información masiva como vídeo o imágenes tridimensionales.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una “red híbrida” y poder resolver los últimos metros hacia la computadora. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica la que proporcione movilidad adicional al equipo y el operador para que se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de redes inalámbricas:

1. *De Larga Distancia:* Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como redes de área metropolitana).
2. *De Corta Distancia:* Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si (mejor conocidas como redes de área local).

Las redes inalámbricas permiten la comunicación de computadoras sin depender de los cables. Se utilizan en muchas aplicaciones y es una tecnología muy discutida en la actualidad, además facilita la operación en lugares donde la computadora no puede permanecer en un solo lugar.

[6] Es una técnica de modulación para la transmisión de datos a gran velocidad sobre el par de cobre. La primera diferencia entre esta técnica de modulación y las usadas por los módems en banda vocal (V.32 a V.90) es que éstos últimos sólo transmiten en la banda de frecuencia usada en telefonía (300 Hz a 3400 Hz), mientras que los módems ADSL operan en un margen de frecuencia mucho más amplio que va desde los 24 KHz hasta los 1104 KHz, aproximadamente.

1.3.2.2 Tipos de redes inalámbricas

Redes de Área Local Inalámbrica (Wireless Local Area Network, WLAN) Las redes inalámbricas de infrarrojos sólo funcionan dentro de una misma habitación, mientras que las redes inalámbricas de radiofrecuencias pueden funcionar a través de casi cualquier pared. Las redes inalámbricas tienen velocidades de transmisión que van desde menos de 1 Mbps hasta 8 Mbps, y funcionan a distancias de hasta unos cientos de metros.

Una WLAN es un tipo de red de área local que utiliza ondas de radio de alta frecuencia en lugar de cable para comunicar y transmitir datos entre los clientes de red y los dispositivos. Es un sistema de comunicación de datos flexible implementado como una extensión, o como una alternativa para una LAN conectada. Al igual que una LAN, la red permite que los usuarios de esa ubicación compartan archivos, impresoras y otros servicios. La mayoría de las redes WLAN utilizan tecnología de espectro distribuido. Su ancho de banda es limitado (generalmente inferior a 11 Mbps) y los usuarios comparten el ancho de banda con otros dispositivos del espectro.

Redes de Área Metropolitana Inalámbrica (Wireless Metropolitan Area Network, WMAN) Son a aquellas redes que tienen una cobertura desde unos cientos de metros hasta varios kilómetros. El objetivo es poder cubrir el área de una ciudad o entorno metropolitano. Los protocolos LMDS (Local Multipoint Distribution Service, Servicio Local de Distribución Multipunto) o MMDS (Multichannel Multipoint Distribution Service, Servicio Multicanal de distribución Multipunto) ofrecen soluciones de este tipo.

Existen dos topologías básicas: sistemas que facilitan una comunicación punto a punto a alta velocidad entre dos emplazamientos fijos y sistemas que permiten crear una red punto-multipunto entre emplazamientos fijos. En este último caso el ancho de banda utilizado es compartido entre todos los usuarios del sistema.

LMDS: Es una tecnología inalámbrica vía radio para comunicación entre puntos fijos. Esto quiere decir que no es una tecnología pensada para ser utilizada por terminales en movimiento. El rango de frecuencias utilizado varía entre 2 y 40 GHz dependiendo de la regulación del país en que se utilice. LMDS utiliza un transmisor central emitiendo su señal sobre un radio de hasta 5 Km. Las antenas de los receptores se sitúan generalmente en los tejados de los edificios para procurar una visibilidad directa con el transmisor central. Un inconveniente de los sistemas LMDS es que no existe un estándar que asegure la compatibilidad de los equipos de distintos fabricantes. En cualquier caso, en general, las soluciones LMDS no están teniendo una buena aceptación comercial.

IEEE 802.16: Este grupo de trabajo se creó con la idea de desarrollar un estándar de red inalámbrica metropolitana. El resultado publicado ha sido un sistema punto-multipunto que opera en la banda de frecuencias de 10 a 66 GHz. Posteriormente se hablará más de este protocolo.

Redes de Área Extensa Inalámbricas (Wireless Wide Area Network, WWAN) Son las redes inalámbricas de mayor alcance, así como las más utilizadas hoy día en la infraestructura de telefonía móvil, aunque también disponen de la capacidad de transmitir datos. Los servicios de próxima generación de telefonía móvil mejorarán significativamente las comunicaciones WWAN.

Las WWAN emplean redes de telefonía celular, transmisiones vía satélite o equipos específicos y proporcionan una cobertura regional o mundial, pero su velocidad de transmisión es de sólo 2000 a 19000 bps.

Con esta tecnología, los profesionales que viajan con asiduidad podrán disponer de "oficinas virtuales", conectarse de forma segura a las Intranets de sus empresas, enviar y responder su correo electrónico, navegar por Internet o descargar archivos: en definitiva, trabajar desde prácticamente cualquier sitio. Por si fuera poco, los usuarios tendrán siempre cobertura y, por consiguiente, acceso ininterrumpido a los mismos servicios de datos sobre IP. Con esta tecnología es posible trabajar con datos de facturación procedentes de redes distintas, para que así los clientes reciban del operador móvil una única factura en la que se refleje toda su actividad.

Algunas ventajas clave son:

- *Rendimiento:* Las soluciones inalámbricas proporcionan gran cantidad de ancho de banda de forma fiable y sin interrupción a gran distancia.
- *Fiabilidad:* Algunos productos empleados, utilizan la tecnología del espectro ensanchado por secuencia directa (Direct Sequence Spread Spectrum, DSSS). El ejército de EE.UU. inventó hace años la tecnología DSSS como medio seguro, sólido y fiable de comunicación a grandes distancias. La tecnología DSSS es intrínsecamente fiable, eficiente y segura.
- *Seguridad:* A diferencia de los populares estándares 802.11, basados en protocolos abiertos, algunas soluciones WWAN utilizan técnicas propias de los fabricantes para garantizar la seguridad durante las comunicaciones.

1.3.2.3 Usos actuales y ejemplos

Las redes de área local (LAN) inalámbricas, o WLAN, de la norma 802.11 operan en el espectro de radiofrecuencia sin licencia, lo que las hace que se implementen rápidamente y a un costo razonable. Las empresas y los consumidores disfrutan de libertad y economía conforme un variado grupo de dispositivos se prepara para Wi-Fi[7](Wireless Fidelity, Fidelidad Inalámbrica). Por ejemplo, las plataformas móviles con Intel Centrino incluyen un soporte integrado para la tecnología de inalámbricos de la norma 802.11. Las WLAN ofrecen varias ventajas en comparación con las redes tradicionales con cables:

- Los usuarios ya no están inmovilizados por los cables a un escritorio o pared. En vez de eso, pueden llevar su trabajo de un entorno a otro, por ejemplo, de un escritorio a un laboratorio o a una reunión, todo sin tener que desconectarse y volverse a conectar en cada cambio.
- Algunos estudios han demostrado que los usuarios de WLAN gozan de varios beneficios, que incluyen un incremento de la productividad, un ahorro de tiempo y la flexibilidad de poder acceder a redes casi en cualquier parte.
- También hay ventajas respecto al costo de la implantación de nuevas WLAN en comparación con las redes tradicionales con cables.

Diariamente, hay más usuarios y por lo tanto más dispositivos operando en el mismo espectro sin licencia, lo que produce más interferencia y ruido en un entorno dado de red. Las redes inalámbricas se están haciendo tan populares y se están implantando de forma tan generalizada que la demanda de los usuarios ha creado una cantidad de retos nuevos y complejos.

Las conexiones que aún existen no son rápidas ni imperceptibles entre los puntos de acceso y no hay formas efectivas de controlar la carga. Otro problema es que la repartición del ancho de banda no es equitativa: las soluciones de repartición actuales no se adaptan bien a los estados con vínculos agrupados. Finalmente, las WLAN no necesariamente funcionan bien con las redes celulares que usan otros métodos para administrar los recursos de radio.

Con el aumento tan dramático en su uso, las WLAN actuales están lejos de la optimización. Las experiencias de los usuarios pueden ser desiguales debido a que los entornos inalámbricos a menudo cambian significativamente en cortos periodos de tiempo. Una sola oficina u hogar puede incluir varios dispositivos que compitan por el mismo espectro de frecuencia sin licencia que utilizan las redes inalámbricas de la norma 802.11. Éstas incluyen los dispositivos Bluetooth[8], los hornos de microondas y los teléfonos inalámbricos; todos ellos pueden ocasionar interferencia en la red. Existe también una carencia de estándares industriales bien definidos para atender la necesidad de una administración eficaz de las redes inalámbricas.

[7] Se describe en el Capítulo II, Protocolos de comunicaciones inalámbricas (802.11), en la parte de estándar IEEE 802.11b.

[8] Es un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia.

Por ejemplo, en una cafetería concurrida, la densidad de usuario puede ocasionar cuellos de botella en los puntos de acceso a la red. Puede haber también dispositivos Bluetooth y hornos de microondas en uso, los cuales ocasionan interferencia a las señales de WLAN. Para el usuario, estos problemas aparecen como exploración y descargas lentas y una disminución general del funcionamiento. Se puede presentar otro problema, aunque es raro, cuando las señales que interfieren son lo suficientemente fuertes como para evitar que el cliente inalámbrico pueda acceder a la WLAN durante un periodo de tiempo indefinido.

Hasta ahora, la mayoría de las investigaciones encaminadas a mejorar los entornos inalámbricos se han enfocado en ajustar sólo un parámetro en la capa de MAC (control de acceso de medios). Sin embargo, un entorno inalámbrico puede estar saturado con todo tipo de elementos, desde interferencias y señales débiles hasta colisiones de paquetes, lo que puede ocasionar un aumento drástico en el número de retransmisiones necesarias para enviar un paquete. Un entorno dinámico presenta un problema de varias dimensiones que no se puede resolver ajustando sólo un valor.

Otro problema que no es trivial es la forma en la que un dispositivo inalámbrico selecciona su punto de acceso. En una red inalámbrica, cada dispositivo móvil se asocia a un punto de acceso a la red. Actualmente, los dispositivos seleccionan los puntos de acceso basándose en la potencia de la señal, un método que identifica el punto de acceso más cercano al dispositivo. Desafortunadamente, una señal potente no significa necesariamente un buen funcionamiento general. Por ejemplo, si la mayoría de los PC portátiles inalámbricos que se mueven hacia una sala de conferencias se conectan a la red mediante el punto de acceso sobre la puerta de entrada, podría haber docenas o cientos de PC portátiles usando el mismo punto de acceso. Al mismo tiempo, otros puntos de acceso en otros lugares de la sala podrían estar medianamente desocupados.

Los puntos de acceso con sobrecarga representan más que un problema de uso ineficaz de recursos. En las WLAN actuales, los dispositivos utilizan lo que se conoce como una función de coordinación distribuida (DFC) para acceder a la red. El buen funcionamiento de esta función depende en gran medida de la carga del canal y del número de usuarios que compitan por un punto de acceso. Cuando un punto de acceso está sobrecargado, se reduce la calidad del servicio individual a los usuarios. Esto se traduce en un peor funcionamiento para todos los usuarios, no sólo para los últimos que se conectaron.

Las nuevas tecnologías de LAN son más rápidas y permiten el empleo de aplicaciones multimedia y videoconferencia, al poder transferir sonido y vídeo. En la actualidad ya existen redes que utilizan el modo de transferencia asíncrono (Asyncronous Transfer Mode, ATM) y LAN con Ethernet que son entre 10 y 15 veces más rápidas que las LAN normales. Para aprovechar la mayor rapidez de las LAN, las computadoras deben aumentar su velocidad, en particular la del bus, la conexión que une la memoria de la computadora con la red. También influye en la velocidad de transmisión el soporte lógico que se utilice, que debe ser capaz de transferir eficientemente grandes cantidades de datos desde las redes a las aplicaciones computacionales.

Algunos beneficios principales de las redes de área local inalámbricas, son:

- *Extensión o alternativa de una solución de cableado:* Existen múltiples casos en que es más económico implementar una solución inalámbrica, en reemplazo a una cableada o como extensión de una red LAN: en lugares tales como edificios, oficinas, campamentos, etc.
- *Aumentar la productividad:* Una implementación de WLAN permite tener acceso a la información en cualquier lugar, con lo cual, se agiliza tiempo y obtiene en todo momento la información necesaria para la toma efectiva de decisiones.
- *Reutilización de infraestructura:* En algunas industrias es necesario reconfigurar la distribución física de una red, o incluso, cambiar de lugar las instalaciones frecuentemente, en estos casos, las WLAN proveen una solución eficiente en costo que permiten la reutilización de la inversión.

Conforme aumenta el número de usuarios y dispositivos conectados a redes inalámbricas, estos últimos necesitan estar al tanto de los factores del entorno que son críticos para la administración del funcionamiento. Esto incluye el número de puntos de acceso que están disponibles, la carga del canal, la potencia de la señal y la interferencia proveniente de otros dispositivos. Los dispositivos inalámbricos deben adaptarse a un entorno que cambia constantemente a fin de mantener un funcionamiento óptimo.

Capítulo II

Análisis de Protocolos

Normas y estándares de comunicación inalámbrica

2.1 NORMAS Y ESTÁNDARES DE COMUNICACIÓN INALÁMBRICA

En la actualidad, el mercado ofrece una gran cantidad de productos inalámbricos, cada uno de ellos creados por compañías distintas y que difieren significativamente entre sí. En su momento se reconoció la necesidad de desarrollar normas internacionales, para regular el uso de estas redes inalámbricas.

Existen dos normas internacionales: Una desarrollada en EEUU, patrocinada por la institución IEEE que es la norma 802.11, y por otro lado la europea, desarrollada por el Instituto de Estándares de Telecomunicaciones Europeo (ETSI), conocida como HiperLAN. En este capítulo solo se contemplará la norma o protocolo IEEE 802.11, ya que la norma o estándar HiperLAN está pensada para aplicaciones en la zona de Europa y no en América como lo es el estándar 802.11.

2.1.1 Protocolos de comunicaciones inalámbricas (802.11)

Un protocolo es el conjunto de normas para comunicar dos o más entidades (objetos que se intercambian información, por ejemplo las computadoras). Los elementos que definen un protocolo son:

- *Sintaxis:* Formato, codificación y niveles de señal de datos.
- *Semántica:* Información de control y gestión de errores.
- *Temporización:* Coordinación entre la velocidad y el orden secuencial de las señales.

Para establecer una buena comunicación entre computadoras de diferentes fabricantes es necesaria la implementación de un conjunto de convenciones comunes como estándares ya que promueven la interoperatividad entre las computadoras de distintos fabricantes. Una técnica muy aceptada y adoptada por ISO (Organización Internacional de Estandarización) es la división en capas. En esta técnica, las funciones de comunicación se distribuyen en un conjunto jerárquico en donde cada capa proporciona servicios a la capa inmediatamente superior. El modelo de referencia resultante tiene siete capas, las cuales son mostradas en la tabla 2.1.

Aplicación Proporciona el acceso al entorno OSI para los usuarios y también proporciona servicios de información distribuida.
Presentación Proporciona a los procesos de aplicación independencia con respecto a las diferencias en la representación de los datos (sintaxis).
Sesión Proporciona el control de la comunicación entre las aplicaciones; establece, gestiona y cierra las conexiones (sesiones) entre las aplicaciones cooperadoras.
Transporte Proporciona una transferencia transparente y fiable de datos entre los puntos finales; además

proporciona procedimientos de recuperación de errores y control de flujo origen-destino.
Red Proporciona independencia a los niveles superiores con respecto a las técnicas de conmutación y de transmisión utilizadas para conectar los sistemas; es responsable del establecimiento, mantenimiento y cierre de las conexiones.
Enlace de datos Proporciona un servicio de transferencia de datos fiable a través del enlace físico; envía bloques de datos (tramas) llevando a cabo la sincronización, el control de errores y el flujo.
Física Se encarga de la transmisión de cadenas de bits no estructurados sobre el medio físico; está relacionada con las características mecánicas, eléctricas, funcionales y de procedimiento para acceder al medio físico.

Tabla 2.1 Modelo de referencia OSI.

Todos los aparatos (tarjetas de red, puntos de acceso, etc.) que implementan esta tecnología se basa en un estándar de 1997, revisado en 1999. Si nos situamos en el modelo de referencia OSI, el estándar define a:

- *La capa física:* Se ocupa de definir los métodos por los que se difunde la señal. Para hacer esto, la capa física se divide en dos subcapas:

  - PLCP (Physical Layer Convergence Procedure, Procedimiento de Convergencia de la Capa Física). Se encarga de convertir los datos a un formato compatible con el medio físico.
  - PMD (Physical Médium Dependent, Dependiente del Medio Físico). Se encarga de la difusión de la señal.

  Esta capa define las transmisiones inalámbricas. Los medios físicos que soporta esta tecnología son 5 capas físicas basadas en 4 mecanismos diferentes: Espectro Expandido por Salto de Frecuencia (FHSS). Espectro Expandido por Secuencia Directa (DSSS el estándar más conocido es IEEE 802.11b por ser de alta velocidad). Infrarrojo (IR). Modulación por División de Frecuencia Ortogonal (OFDM definido en el estándar IEEE 802.11a).

- La capa de enlace: Dividida a su vez en:

  - Control de Acceso al Medio (Médium Access Control, MAC).
  - Control Lógico de Ligas (Logical Link Control, LLC), es la capa que se ocupa del control de enlace lógico. Define como pueden acceder múltiples usuarios a la capa MAC, como lo muestra la tabla 2.2.

MODELO ISO	**MODELO 802.11**	**TÉCNICAS DE DIFUSIÓN DE 802.11**				
Capa de enlace	LLC					
	MAC					
Capa física	PLCP	DSSS 802.11	FHSS 802.11	Infrarrojos 802.11	DSSS (Alta velocidad) 802.11b	OFDM 802.11a
	PMD					

Tabla 2.2 Capas física y de enlace del estándar IEEE802.11.

El estándar 802.11 para las redes inalámbrica fue desarrollado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Esta forma es equivalente a una Ethernet y puede ser comparada con el estándar 802.3 para redes cableadas. En la práctica. Las demás capas del modelo OSI, se basan en Ethernet facilitando así la interconexión entre redes heterogéneas basadas en estándares del IEEE.

Los productos de red inalámbrica son seguros no sólo respecto a otros productos electrónicos y de red, sino, lo que es más importante, respecto a las personas. Los productos de redes inalámbricas, estandarizados como IEEE 802.11, se han diseñado para usarse en la implementación de redes de área local inalámbrica tanto en edificios como en espacios abiertos con amplia cobertura y rendimiento. Por lo tanto, emiten un grado reducido de energía, lo cual es inofensivo. De hecho, los niveles de energía son significativamente más bajos que las emisiones de los teléfonos GSM[1] comunes, que funcionan a unos 2 Watts, en el caso de teléfonos de clase 2 GSM (el intervalo de frecuencia es de 880-960 MHz).

Después del estándar 802.11 surgieron complementos que definen dos nuevas capas físicas, el IEEE 802.11a y el IEEE 802.11b, este último es el que actualmente se vende, y por tanto el más conocido. A finales de 1999, el IEEE publicó dos suplementos al estándar 802.11: 802.11a y 802.11b. El estándar 802.11a es absolutamente diferente de su contraparte el estándar 802.11b. A continuación se detalla cada uno y también se describen otros estándares más.

Estándar IEEE 802.11a La especificación IEEE 802.11a hace uso de la banda de los 5 GHz. Al contrario que en el caso de las especificaciones en la banda de los 2.4 GHz, en IEEE 802.11a no se emplea un esquema de espectro expandido, sino multiplexación por división de frecuencia ortogonal (Orthogonal Frequency Division Multiplexing, OFDM). OFDM, también conocido como modulación multiportadora, utiliza varias señales portadoras con frecuencias diferentes, enviando algunos de los bits totales por cada canal. Se trata de un esquema similar a FDM. Sin embargo, en el caso de OFDM todos los subcanales están dedicados a una única fuente de datos. Las velocidades de datos posibles en IEEE 802.11a son: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

Así pues, una WLAN basada en el 802.11a puede admitir un mayor número de usuarios de alta velocidad simultáneos sin peligro de que surjan conflictos. Un inconveniente de utilizar la banda de 5 GHz es que las frecuencias utilizadas no están estandarizadas internacionalmente.

La frecuencia de funcionamiento más alta del estándar 802.11a tiene como consecuencia un alcance relativamente más corto. Se necesitarán más puntos de acceso 802.11a para cubrir la misma zona. Pero incluso con estos inconvenientes,

[1] La tecnología Europea GSM (Global System for Mobile Communications, Sistema Global para Comunicaciones Móviles) puede transmitir datos a 13 Kbps sin necesidad de utilizar módem. Para conectar una computadora a un teléfono GSM, sólo hace falta un cable adaptador y el software apropiado.

los productos 802.11a ofrecen un rendimiento casi tres veces superior al de los 802.11b en cuanto a alcances en interiores.

Estándar IEEE 802.11b El fundamento de muchas de las actuales redes inalámbricas se encuentra basado en el estándar IEEE 802.11, y más concretamente en la nueva especificación IEEE 802.11b, un consorcio, el Wíreless Ethernet Compatibility Alliance (WECA), formado por un nutrido grupo de relevantes empresas, ha creado una nueva línea de productos de mayores prestaciones y de plena compatibilidad. La especificación 802.11b fue concluida por IEEE en 1999.

Los productos acogidos a la norma IEEE 802.11b tienen garantizada la interoperatividad entre diferentes fabricantes, consiguiendo al mismo tiempo una significativa reducción de los costos y abaratamiento de los dispositivos para el usuario final.

Este consorcio ha establecido un estándar llamado Fidelidad Inalámbrica (Wi-Fi) que permite certificación de los productos acogidos a esta normativa para lograr que entre ellos existan una obligada compatibilidad y otros aspectos comunes de actuación como facilidad de configuración, unanimidad de protocolos, modos de funcionamiento, como las más elementales normas.

El nuevo estándar IEEE 802.11b que fue ratificado el 16 de septiembre de 1999, proporciona un cambio definitivo a la normativa estándar inicial, ya que permite operar a la velocidad de 1 Mbps y resuelve las carencias técnicas relativas a la falta de seguridad, escalabilidad, y de gestión, existentes hasta entonces. A su vez, los costos han bajado en cuanto a los productos que se han convertido en estándares, y de hecho, la relación precio/prestaciones de los productos de redes inalámbricas se ha multiplicado por diez en los últimos años.

Estándar IEEE 802.11g En este estándar la especificación de la capa física es de 2.4 GHz y pretende alcanzar tarifas de datos más rápidas que 802.11b (igual o exceder de 22 Mbps). La especificación está actualmente en desarrollo y no se ha autorizado.

Esta norma surgió con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2.4 GHz. Permite transmitir datos a 54 Mbps. Combina toda una gama de técnicas de codificación del medio físico utilizadas en 802.11a y 802.11b para proporcionar servicio a diversas velocidades. En la tabla 2.3 se describen las ventajas y desventajas inherentes a las tecnologías 802.11a y 802.11g.

	802.11a	**802.11g**
DESEMPEÑO	VENTAJA: Sólo OFDM, banda de 5 GHz y la ausencia de células[2] mixtas proporciona una mejor capacidad de	DESVENTAJA: Soporte para los estándares elevados, células mixtas y la operación en la banda de 2.4 GHz que

[2] La esencia de una red celular reside en el uso de múltiples transmisores. El área que necesita ser cubierta se divide en celdas siguiendo un patrón hexagonal que proporciona una cobertura total del área.

	salida.	podría estar potencialmente saturada, lo cual posiblemente daría como resultado una capacidad de salida ligeramente menor que la de 802.11a.
CAPACIDAD	VENTAJA: Con ocho canales, proporciona una capacidad agregada de 432 Mbps (54 Mbps multiplicados por ocho canales).	DESVENTAJA: Con sólo tres canales, proporciona una capacidad teórica agregada de 162 Mbps (54 Mbps multiplicado por 3 canales).
RANGO	DESVENTAJA: Una longitud de onda más corta y restricciones reguladoras en la potencia de transmisión y la ganancia de la antena que deterioran el rango de 802.11a.	VENTAJA: A pesar de que no proporcionará el mismo rango que 802.11b debido a las velocidades de datos más altas, la física y regulaciones en la banda de 2.4 GHz permiten un rango más grande que cuando se opera en la banda de 5 GHz.
INTERFERENCIA	VENTAJA: Las LAN 802.11a inalámbricas operan en las bandas de 5 GHz que son relativamente grandes, pero aún así están saturadas.	DESVENTAJA: Las bandas que no requieren de licencia de 2.4 GHz son relativamente pequeñas y se están saturando con las LAN inalámbricas, teléfonos inalámbricos y, potencialmente, dispositivos BlueTooth.
MIGRACIÓN	DESVENTAJA: Operando a 5 GHz y proporcionando soporte sólo para la transmisión OFDM, no proporciona compatibilidad con dispositivos anteriores de 802.11b.	VENTAJA: Al operar en la banda heredada de 2.4 GHz y soportar DSSS, proporciona la característica importante de la compatibilidad con productos anteriores de 802.11b.
FLEXIBILIDAD DE INSTALACIÓN	DESVENTAJA: Las regulaciones FCC que se aplican a los cuatro canales inferiores de 802.11a restringen a los fabricantes al uso exclusivo de antenas integradas que no se pueden desconectar.	VENTAJA: Al igual que 802.11b, permite antenas de 2.4 GHz auxiliares que pueden estar directamente conectadas o conectadas por cables.
OPERACIÓN A LO LARGO DE TODO EL MUNDO	DESVENTAJA: Operación en los países apegados a FCC y Japón, pero aún no se define en Europa.	VENTAJA: La operación libre de licencia en, prácticamente, todo el mundo.

Tabla 2.3 Comparación de los estándares IEEE 802.11a y IEEE 802.11g.

En resumen, las ventajas y desventajas de 802.11a y 802.11g son complementarias. Ambas tecnologías se pueden desplegar para alcanzar el máximo beneficio.

Estándar IEEE 802.11e Este grupo trabaja en los aspectos relacionados con la calidad de servicio (Quality of Services, QoS). En el mundo de las redes, calidad de servicio significa poder dar más prioridad de transmisión a unos datos que a otros, dependiendo de la naturaleza de la información (voz, video, imágenes, etc). Por ejemplo, la información de voz necesita ser transmitida en tiempo real, mientras que la información de datos originada por una transferencia de archivo da igual que llegue medio segundo antes o después.

IEEE 802.11e es un complemento de MAC que trabaja como el 802.11b y 802.11a en la capa física, así como la especificación próxima de la capa física del estándar 802.11g.

Estándar IEEE 802.11d En el mundo globalizado actual, los usuarios Wi-Fi a menudo transitan de un dominio regulador a otro. No es difícil encontrar a una persona de negocios que viaja de Cleveland, que se encuentra en el dominio regulador FCC, a París, que está dentro del dominio ETSI, y desde ahí a China y Japón, cada uno de los cuales tiene su conjunto de regulaciones particular. Este extenuante viaje de negocios es todavía peor debido a que el usuario Wi-Fi tendrá que llevar cuatro adaptadores Wi-Fi, uno para cada dominio regulador, e intercambiarlos dentro de su computadora portátil dependiendo del país en donde se encuentre.

Al observar esto, el grupo 802.11 del IEEE creó una fuerza de trabajo específica para desarrollar un medio mediante el cual un radio cliente sea capaz de operar en múltiples dominios reguladores y al mismo tiempo mantener la compatibilidad con las regulaciones. Estos esfuerzos dieron frutos en junio del 2001 con la ratificación del estándar 802.11d para la operación en múltiples dominios.

El estándar está basado en la suposición de que el punto de acceso de una red Wi-Fi está dentro del cumplimiento con las regulaciones. Especifica la forma mediante la cual el punto de acceso descubre en el manejo de los paquetes[3] el dominio regulador con el cual es compatible. Hasta la fecha, sólo un fabricante, Symbol Technologies, ha adoptado este útil estándar.

Estándar IEEE 802.11h Es una evolución del IEEE 802.11a que permite asignación dinámica de canales y control automática de potencia para minimizar los efectos interferentes.

2.1.1.1 Comparativa de la familia de estándares IEEE 802.11

Entre todos los estándares el IEEE 802.11a es el más rápido, con un alto rendimiento de procesamiento por lo que apoya una carga pesada en redes y contenido de multimedia. En la banda en la cual trabaja representa una ventaja ya que en esta banda, trabaja poca gente y esto implica menor interferencia. Sus productos son los más costosos.

En el estándar IEEE802.11b, las soluciones son extensamente disponibles; cuenta con un amplio grupo de compañías y una variedad de formas. Los costos para la tecnología y para los productos van bajando su precio. Es susceptible a la interferencia en la banda de 2.4GHz, en hornos de microondas. En la mayoría de los casos son de poca velocidad.

[3] Agrupamiento lógico de información que incluye un encabezado que contiene la información de control y (normalmente) los datos del usuario. Los paquetes se usan con mayor frecuencia para referirse a las unidades de datos de la capa de red.

El estándar IEEE802.11g es compatible con redes 802.11b tiene una tarifa de datos más alta contra el estándar 802.11b y permite transmisiones más concurrentes. En la tabla 2.4 se puede apreciar un comparativo más detallado de los estándares 802.11.

	802.11a	**802.11b**	**802.11g**
FRECUENCIA	5 GHz.	2.400 - 2.4835 GHz.	2.412 - 2.4835 GHz.
MODULACIÓN	OFDM	DSSS	OFDM
VELOCIDAD MÁXIMA	54 Mbps	11 Mbps	54 Mbps
RANGO DE VELOCIDADES (Mbps)	54, 48, 36, 24, 18, 12, 9 y 6	11, 5.5, 2 y 1	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2 y 1
NÚMERO DE CANALES SIN SOBREPOSICIÓN	8	3	3
ANCHO DE BANDA	54 Mbps transmisión/~30 Mbps efectivos.	11Mbps transmisión/5.5 Mbps efectivos.	54 Mbps transmisión/~30 Mbps efectivos.
ANCHO DE BANDA EN UN ÁREA	432 Mbps (8X54)	33 Mbps (3X11)	162 Mbps (3X54)
MEDIA ACCESS PROTOCOL	CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).	CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).	CSMA/CA (Carrier Sense Multiple Access withCollision Avoidance).
USUARIOS EN UN ÁREA	512	192	192
EFICIENCIA POR CANAL (throughput)	18 Mbps	6 Mbps	12 Mbps
DISTANCIA	Hasta 100 m.	Hasta 100 m.	Hasta 125 m.
PRECIO	Alto.	Económico.	Accesible.
POPULARIDAD	Nuevo.	Amplia.	Nuevo.
COMPATIBILIDAD	Wi-Fi5[4].	Wi-Fi.	Wi-Fi , 802.11b.
A DESTACAR	Alta velocidad y número de usuarios.	Buen alcance y consumo de potencia.	Compatible con 802.11b y más alcance que 802.11a.

Tabla 2.4 Comparativo de la familia de estándares IEEE 802.11.

2.1.1.2 Acceso al medio

Diferentes tecnologías de capa física se definen para transmitir por el medio inalámbrico. La capa física consiste en dos protocolos los cuales son:

- *Protocolos con arbitraje:* FDMA (Frecuency Division Multiple Access) y TDMA (Time Division Multiple Access).
- *Protocolos de contienda:* CSMA/CA (Carrier-Sense, Multiple Access, Collision Avoidance), CSMA (Code División, Múltiple Access) y el CSMA/CD (Carrier Sense, Múltiple Access, Collision Detection).

[4] Equipos de diferente fabricantes de la marca Wi-Fi que son compatibles entre sí y utilizan la tecnología inalámbrica definida por el estándar IEEE 802.11a de la banda de 5GHz.

2.1.1.2.1 Protocolos con arbitraje

La *multiplexación en frecuencia (FDM)* divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo.

Una alternativa a este problema es asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, se llama *multiplexación en el tiempo (TDM)* y requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Esta técnica ha sido utilizada con cierto éxito sobre todo en las redes inalámbricas, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

2.1.1.2.2 Protocolos de acceso por contienda

CSMA, se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia PN. Este protocolo trabaja de la siguiente manera, se asigna una secuencia PN distinta a cada nodo, y todos los nodos pueden conocer el conjunto completo de secuencias PN pertenecientes a los demás nodos. Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia PN del destinatario. De esta forma se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

CSMA/CD, como en estos medios de difusión (radio, infrarrojos), no es posible transmitir y recibir al mismo tiempo, la detección de errores no funciona en la forma básica que fue expuesta para las redes cableadas. Se diseño una variación denominada detección de colisiones para redes inalámbricas. Este protocolo funciona de la siguiente forma, cuando un nodo tiene una trama que transmitir, lo primero que hace es generar una secuencia binaria pseudoaleatoria corta, llamada peine la cual se añade al preámbulo de la trama. A continuación, el nodo realiza la detección de la portadora si el canal está libre transmite la secuencia del peine. Por cada 1 del peine el nodo transmite una señal durante un intervalo de tiempo corto. Para cada 0 del peine el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y espera hasta que los otros nodos hayan transmitido su trama.

La eficiencia del funcionamiento del protocolo CSMA/DC depende del número de bits de la secuencia del peine ya que si dos nodos generan la misma secuencia, se producirá una colisión.

CSMA/CA, este protocolo es el más utilizado ya que evita colisiones en lugar de descubrir una colisión. En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir

su información, disminuyendo así la posibilidad de colisiones. La figura 2.1 muestra el funcionamiento del protocolo de contienda CSMA/CA.

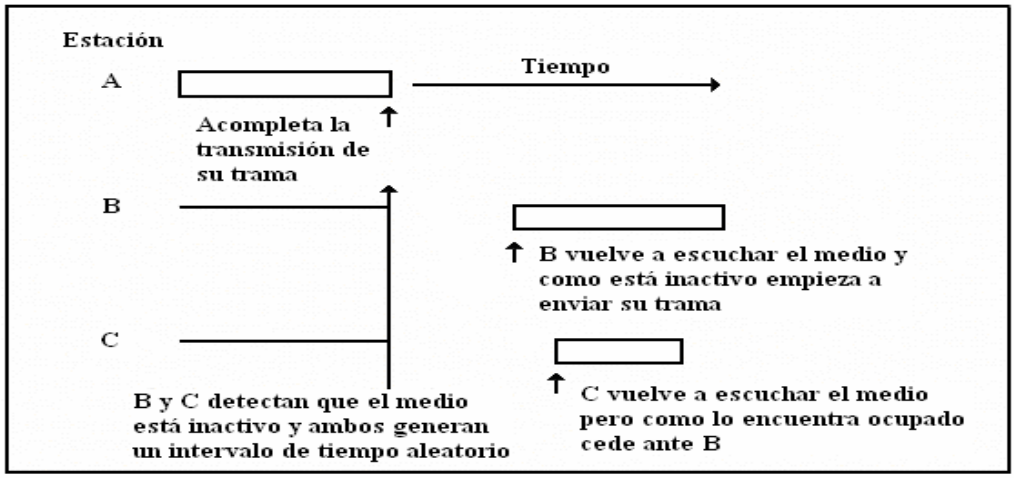


Figura 2.1 Funcionamiento del protocolo de contienda CSMA/CA.

2.1.1.2.3 Funcionamiento del protocolo de comunicaciones inalámbricas (CSMA/CA y MACA).

Este algoritmo funciona tal y como se describe a continuación y se muestra la figura 2.2 donde se puede ver un ejemplo del funcionamiento de acceso CSMA/CA:

1. Antes de transmitir información una estación debe testear el medio, o canal inalámbrico, para determinar su estado (libre/ocupado).
2. Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada *espaciado entre tramas* (IFS).
3. Si durante este intervalo de tiempo o bien ya desde el principio el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.
4. Una vez finalizada esta espera debida a la ocupación del medio la estación ejecuta el llamado algoritmo de Backoff[5], según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado *ventana de contienda* (CW)[6].
5. Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si

[5] El algoritmo de Backoff da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir. Por otra parte, el valor del slot time es 20µseg.

[6] Cada retransmisión provocará que el valor de CW, que se encontrará entre CWmin y CWmax se duplique hasta llegar al valor máximo.

el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición.

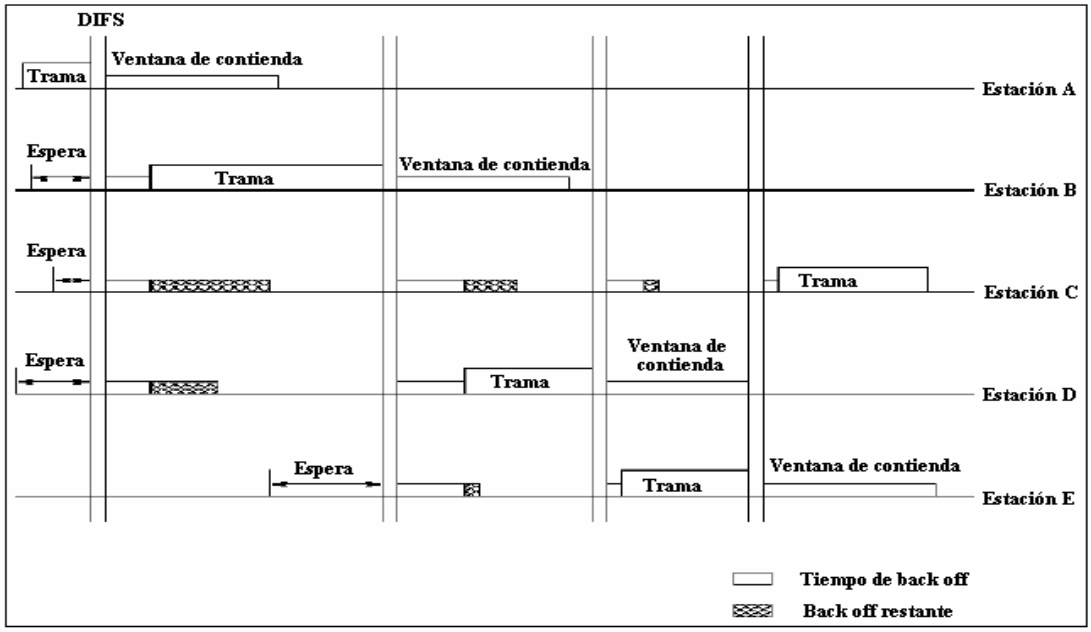


Figura 2.2 funcionamiento de acceso CSMA/CA.

Sin embargo, CSMA/CA en un entorno inalámbrico presenta una serie de problemas. Los dos principales problemas que son:

- Nodos ocultos: Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye.
- Nodos expuestos. Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

MACA (MultiAccess Collision Avoidance), según este protocolo, antes de transmitir el emisor envía una trama RTS (Request To Send), indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (Clear To Send), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos. Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS.
- Al escuchar un CTS, hay que esperar según la longitud.

2.1.1.2.4 Nivel de acceso al medio MAC

La capa física proporciona una serie de servicios a la capa MAC o capa de acceso al medio. Los diferentes métodos de acceso están diseñados según el modelo OSI y se

encuentran ubicados en el nivel físico y en la parte inferior del nivel de enlace o subnivel MAC.

Además, la capa de gestión MAC controla aspectos como sincronización y los algoritmos del sistema de distribución, que se define como el conjunto de servicios que precisa o propone el modo infraestructura. Se describen los aspectos y tipos de tramas MAC.

Descripción funcional MAC La arquitectura MAC se compone de dos funcionalidades básicas: la función de coordinación puntual (PFC) y la función de coordinación distribuida (DFC), como lo muestra la figura 2.3.

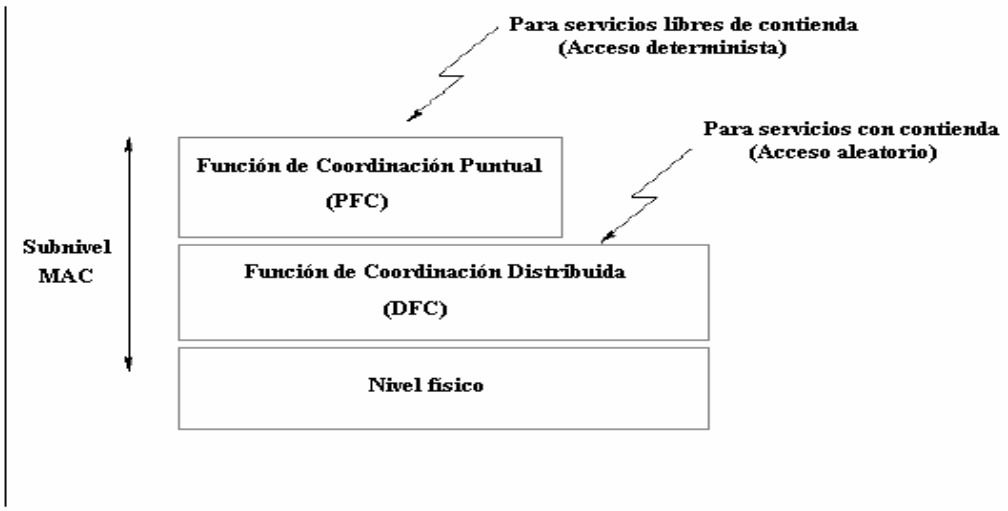


Figura 2.3 Descripción funcional MAC.

Función de coordinación puntual (PFC) Por encima de la funcionalidad DFC se sitúa la función de coordinación puntual, PFC, asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas. Es una técnica de interrogación circular desde el punto de acceso para este nivel. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio.

Estos dos métodos de acceso pueden operar conjuntamente dentro de una misma celda o conjunto básico de servicios dentro de una estructura llamada *supertrama*. Un parte de esta supertrama se asigna al periodo de contienda permitiendo al subconjunto de estaciones que lo requieran transmitir bajo mecanismos aleatorios. Una vez finaliza este periodo el punto de acceso toma el medio y se inicia un periodo libre de contienda en el que pueden transmitir el resto de estaciones de la celda que utilizan técnicas deterministas. El funcionamiento de PFC es totalmente compatible con el modo DFC, observándose que el funcionamiento es transparente para las estaciones.

Función de coordinación distribuida (DFC) Se define función de coordinación como la funcionalidad que determina, dentro de un conjunto básico de servicios (BSS),

cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio.

El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles no tolerados por los servicios síncronos.

Las características de DFC se pueden resumir en estos puntos:

- Utiliza MACA (CSMA/CA con RTS/CTS) como protocolo de acceso al medio.
- Necesario reconocimientos ACK's, provocando retransmisiones si no se recibe.
- Usa campo Duration/ID que contiene el tiempo de reserva para transmisión y ACK. Esto quiere decir que todos los nodos conocerán al escuchar cuando el canal volverá a quedar libre.
- Implementa fragmentación de datos.
- Concede prioridad a tramas mediante el espaciado entre tramas (IFS).
- Soporta Broadcast y Multicast sin ACK's.

Espaciado entre tramas (IFS) El tiempo de intervalo entre tramas se llama IFS. Durante este periodo mínimo, una estación estará escuchando el medio antes de transmitir. Se definen cuatro espaciados para dar prioridad de acceso al medio inalámbrico. La figura 2.4 muestra el espaciado entre tramas (IFS).

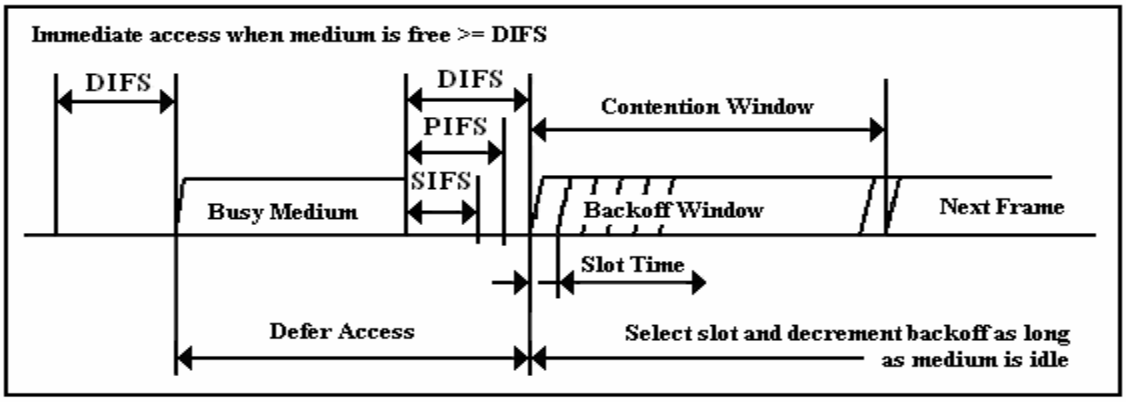


Figura 2.4 Espaciado entre tramas IFS.

- SIFS (Short IFS): Este es el periodo más corto. Se utiliza fundamentalmente para transmitir los reconocimientos. También es utilizado para transmitir cada uno de los fragmentos de una trama. Por último, es usado por el Point Control (PC) para enviar testigo a estaciones que quieran transmitir datos síncronos.

- PIFS (PCF): Es utilizado por estaciones para ganar prioridad de acceso en los periodos libres de contienda. Lo utiliza el PC para ganar la contienda normal, que se produce al esperar DIFS.
- DIFS (DCF): Es el tiempo de espera habitual en las contiendas con mecanismo MACA. Se utiliza pues para el envío de tramas MAC MPDU's y tramas de gestión MMPDU's.
- EIFS (Extended IFS): Controla la espera en los casos en los que se detecta la llegada de una trama errónea. Espera un tiempo suficiente para que le vuelvan a enviar la trama u otra solución.

2.1.2 Estándar de redes inalámbricas de área metropolitana (802.16)

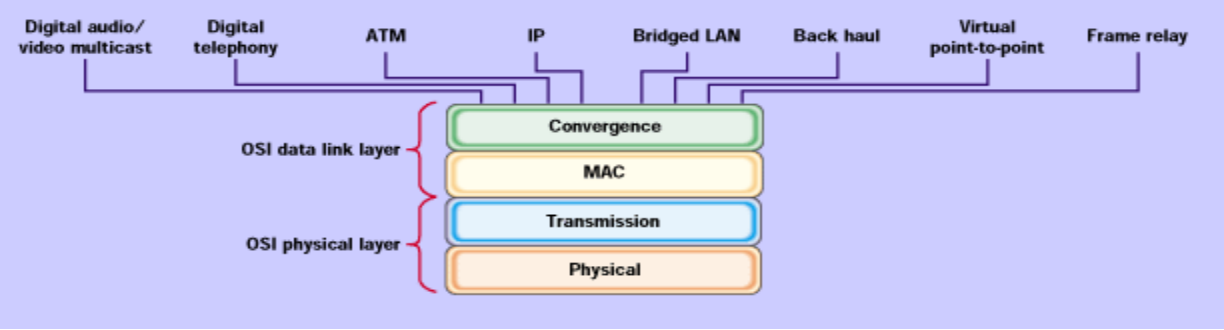
El estándar 802.16, es una tecnología de red de área metropolitana inalámbrica (Wireless MAN, WMAN) que puede conectar hotspots basados en 802.11 y proveer extensión inalámbrica para acceso de última milla de banda ancha en instalaciones de cable y DSL. El estándar IEEE 802.16 hace referencia a un sistema BWA (Broadband Wireless Access) de alta tasa de transmisión de datos y largo alcance (hasta 50 km), escalable, y que permite trabajar en bandas del espectro tanto "licenciado" como "no licenciado". El servicio, tanto móvil como fijo, se proporciona empleando antenas sectoriales tradicionales o bien antenas adaptativas con modulaciones flexibles que permiten intercambiar ancho de banda por alcance. La velocidad de transmisión de datos puede llegar a 70 Mbps, lo que significa un ancho de banda considerable para transportar datos de unas 60 empresas que tengan accesos tipo T1 y centenares de hogares con conexiones tipo DSL, usando sólo un sector de una estación base. Algunas especificaciones del Estándar 802.16 se muestran en la tabla 2.5.

	802.16	**802.16a**	**802.16e**
Espectro	10 - 66 GHz	< 11 GHz	< 6 GHz
Funcionamiento	Solo con visión directa	Sin visión directa (NLOS)	Sin visión directa (NLOS)
Tasa de bit	32 - 134 Mbit/s con canales de 28 MHz	Hasta 75 Mbit/s con canales de 20 MHz	Hasta 15 Mbit/s con canales de 5 MHz
Modulación	QPSK, 16QAM y 64 QAM	OFDM con 256 subportadoras QPSK, 16QAM, 64QAM	Igual que 802.16a
Movilidad	Sistema fijo	Sistema fijo	Movilidad pedestre
Anchos de banda	20, 25 y 28 MHz	Seleccionables entre 1,25 y 20 MHz	Igual que 802.16a con los canales de subida para ahorrar potencia
Radio de celda típico	2 - 5 km aprox.	5 - 10 km aprox. (alcance máximo de unos 50 km)	2 - 5 km aprox.

Tabla 2.5 Especificaciones Estandar 802.16

Una estación de base típica puede albergar hasta seis sectores. La calidad de servicio está integrada dentro del MAC, permitiendo la diferenciación de los niveles de servicio. Los proveedores de servicio de Internet inalámbrico están desplegando acceso inalámbrico de banda ancha en más de 2500 mercados sin servicio de los Estados Unidos usando soluciones de tecnología propietaria. Al emplear soluciones basadas en 802.16, estos proveedores de servicios incrementarán el performance del sistema y la confiabilidad, al tiempo que bajarán los costos del equipamiento y los riesgos de inversión.

El estándar IEEE 802.16 Wireless MAN (Air Interface for Fixed Broadband Wireless Access Systems) define los niveles físico y de acceso al medio, MAC para un acceso inalámbrico de banda ancha. 802.16 admite dos métodos de duplexión: en el dominio de la frecuencia y en el dominio del tiempo, como lo muestra la figura 2.5. En el primer caso se utilizan dos portadoras diferentes, una para el enlace ascendente y otra para el descendente, ambas de 28 MHz, mientras que en el segundo caso, ambos enlaces comparten una única portadora, con una anchura de canal de 28 MHz.



Fígura 2.5 Estructura del protocolo IEEE 802.16: Broadband Wireless MAN Standard (Wi-MAX).

Para el caso de duplexión en el dominio de la frecuencia, y para facilitar el abaratamiento de los equipos terminales, se contempla el caso de terminales semidúplex (que no pueden transmitir y recibir simultáneamente), no así para la estación base, que necesariamente debe presentar un comportamiento dúplex. El sistema contempla un esquema flexible de transmisión, con modulación y codificación adaptativas en función de las condiciones de enlace que cada terminal ve de forma independiente. Esto significa que una terminal próxima a la estación base, con unas buenas condiciones de transmisión, no se vera afectada por una terminal mucho más alejada, aunque las condiciones de transmisión no sean tan óptimas, como se muestra en la figura 2.6.

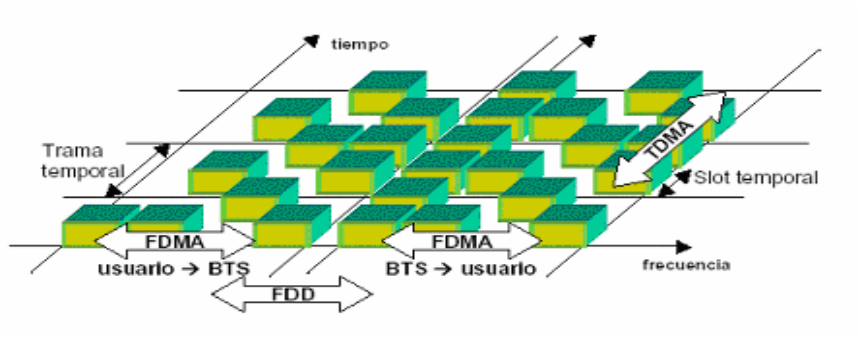


Figura 2.6 Sistema flexible de transmisión.

Puesto que el sistema es punto a multipunto, el sistema incorpora un mecanismo de acceso múltiple al enlace ascendente (el compartido por todas las estaciones terminales). La forma utilizada es TDMA (Time División Múltiple Access). La organización de dicho enlace ascendente viene determinado por la estación base, que lo propaga a todas las estaciones terminales mediante el enlace descendente. Por el contrario, al enlace descendente sólo accede la estación base, por lo que no es necesario ningún mecanismo de acceso múltiple. El enlace descendente se organiza mediante múltiplexación por división en el tiempo, agrupando los mensajes dirigidos a terminales con el mismo esquema de transmisión. La organización de dicho enlace descendente se propaga en la misma trama, utilizando el esquema de transmisión más robusto (el apto para las peores condiciones de transmisión), de forma que todos los terminales puedan acceder a dicha estructura.

La capa de control de acceso al medio incorpora los mecanismos necesarios para el acceso compartido al enlace ascendente, incluyendo mecanismos de resolución de contiendas en aquellas situaciones previstas en la norma: el registro de los equipos terminales y la respuesta a un sondeo de difusión. El MAC es orientado a conexión, de forma que cada comunicación establecida entre la estación base y un equipo terminal lo hace por una conexión determinada. Además, en el momento en que un equipo terminal se registra en la estación base, está establece una serie de conexiones predefinidas, que permiten tanto la gestión del equipo terminal, como la solicitud de anchura de banda por parte de éste. Incorpora también mecanismos de control de la calidad de servicio, permitiendo asignar anchura de banda a los equipos terminales en función de las necesidades de los abonados que conectan. El estándar tiene definidos cuatro métodos de solicitud de reserva de ancho de banda, para cuatro tipos de servicios diferentes:

- *Servicio garantizado no solicitado:* La estación base asigna periódicamente espacio disponible en el enlace ascendente para cada conexión de este tipo que se haya establecido.
- *Servicio con sondeo en tiempo real:* Diseñado para el soporte de conexiones en tiempo real que generan paquetes de tamaño variable según intervalos de tiempo constantes.
- *Servicio con sondeo en tiempo diferido:* Diseñado para el soporte de conexiones que no presenta requisitos de tiempo real.

- *Servicio mejor esfuerzo:* Pensado para el tráfico de este tipo, como podría ser el acceso a Internet.

Como complemento a la 802.16 WMAN, IEEE ha publicado otro estándar, el 802.16.2, que contempla prácticas recomendadas para la coexistencia de sistemas fijos de acceso inalámbrico de banda ancha. El grupo de trabajo 802.16 sigue desarrollando trabajos en el entorno de las redes de acceso inalámbrico.

Actualmente tiene abiertas varias líneas de trabajo:

- La 802.16a, que pretende extender el ámbito de aplicación del estándar 802.16 para que también incorpore las bandas (con y sin licencia) de 2 a 11 GHz.
- La 802.16c, para facilitar las especificaciones de interoperabilidad. La 802.16.2a, que incorpora las bandas de 2 a 11 GHz, así como los sistemas punto a punto. En marzo de 2002 se creó un grupo de estudio para el acceso móvil inalámbrico de banda ancha (MBWA).

HiperAccess (High Performance Radio Access) Es la denominación del proyecto que la ETSI está desarrollando, bajo el auspicio del Broadband Radio Access Networks ETSI Project (EP-BRAN), en el campo del acceso fijo inalámbrico. Actualmente están publicados los estándares correspondientes al nivel físico [ETSITR 101 999] y al nivel de control de enlace [ETSITR 102 000].

El estándar se centra en sistemas punto a multipunto bajo licencia, en frecuencias por encima de los 11 GHz, haciendo especial hincapié en las bandas de frecuencia candidatas para la prestación del servicio de acceso fijo inalámbrico (26/28 GHz, 32 GHz y 40 GHz).

2.1.2.1 Introducción a la Modulación por Espectro Discreto

Se tienen distintas tecnologías aplicables a las comunicaciones digitales inalámbricas para su transmisión y recepción, el *espectro discreto*, es el usado por la mayor parte de los sistemas sin cables, desarrollado por los militares para comunicaciones seguras y confiables en el cual se consume más ancho de banda pero la señal es más fácil de detectar (rechaza la interferencia) y más difícil de descifrar.

El análisis de protocolo de comunicación nos indica que dentro de la capa física de una red se define la modulación y señalización característica de la transmisión de datos, RF (Radio Frecuencia) es el método común usado para las redes inalámbricas.

La definición de la modulación por espectro disperso puede enunciarse en dos partes:

1. El espectro disperso es un modelo de transmisión en el cual la secuencia de datos ocupa un ancho de banda en exceso del ancho mínimo necesario para enviar.
2. La dispersión del espectro se consigue antes de la transmisión mediante el uso de un código que es independiente de la secuencia de datos. El mismo código se utiliza en el receptor (operando en sincronía con el transmisor) para desdispersar la señal recibida de manera que sea posible recuperar la secuencia original de datos.

Así entonces hay dos tipos de tecnología de transmisión RF en espectro disperso estos son las tecnologías de: Direct Sequence (Secuencia Directa) y Frecuency Hopping (Frecuencia de Saltos). Ambas técnicas se definen para operar en ISM Band[7], comercialmente la banda de frecuencias es de 2.4 GHz, ocupando típicamente 83 MHz de banda desde los 2.400 GHz hasta 2.483 GHz.

En su secuencia de operación ambas técnicas se fundamentan en la disponibilidad de un código de dispersión semejante al ruido conocido como secuencia pseudoaleatoria o de pseudoruido. Una secuencia de pseudoruido es una secuencia binaria periódica con una forma de onda similar al ruido, este pseudoruido es usualmente generado usando circuitos lógicos los cuales consisten básicamente en compuertas consecutivas de dos estados de memoria (1 ó 0), un reloj que ayuda a cambiar los estados de cada compuerta y un dispositivo de retroalimentación lógico esto se representa en el figura 2.7.

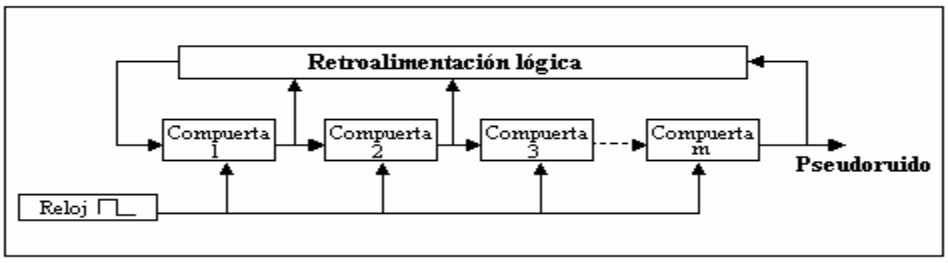


Figura 2.7 Diagrama de bloques de un circuito de retroalimentación con registro de m compuertas.

2.1.2.2 Tecnología Direct Sequence (DSSS)

Se trata de un método de modulación de espectro distribuido que genera un esquema de bits redundantes por cada bit transmitido. El esquema de bits, denominado chip o código de chips, permite a los receptores eliminar por filtrado las señales que no utilizan el mismo esquema de bits, entre las que se cuentan el ruido y la interferencia. El código de chips cumple dos funciones primarias:

[7] ISM Band (Industrial Scientific and Medical) es un conjunto de anchos de bandas para uso no regulado. El espectro de operación se encuentra en la frecuencia de los 2.4 GHz.

1. Identifica los datos de modo que el receptor pueda reconocerlos como pertenecientes a un transmisor determinado. El transmisor genera el código de chips y sólo los receptores que lo conocen pueden descifrar los datos.
2. El código de chips distribuye los datos en todo el ancho de banda disponible.

Este método opera en un canal determinado, luego la señal va separándose por mezcla con un código de pseudoruido. Trabaja tomando un paquete de datos (de 0 y 1) y lo modula con un segundo modelo que es la secuencia de chipping. En 802.11 esta secuencia se conoce como el Código de Barker, está formada por 11 bits que tiene propiedades matemáticas que lo hacen ideal para modular radiofrecuencias. El código Barker genera series de objetos de datos llamados chips. Cada bit se codifica por el Código Barker de 11 bits y cada grupo de 11 chips codifica 1 bit de datos.

Los chips más largos requieren mayor ancho de banda, pero ofrecen una mayor probabilidad de recuperar los datos originales. Aun si uno o más bits del chip son alterados durante la transmisión, la tecnología incorporada al sistema de radio puede recuperar los datos originales empleando técnicas estadísticas, sin necesidad de que sean retransmitidos.

Los receptores de banda angosta no designados ignoran las señales DSSS como ruido de banda ancha y baja potencia. Las redes WLAN 802.11b emplean el método DSSS y ofrecen un mayor caudal de datos que sus contrapartes FHSS debido al mayor aprovechamiento inherente al protocolo DSSS, que tienen costos mayores para su fabricación que FHSS, y utiliza más poder. El FHSS será descrito más adelante.

Modelo de Modulación en Secuencia Directa La técnica de modulación por secuencia directa se suele implementar con un modulador, en el que la fase de la señal portadora varía en concordancia con la señal de datos a transmitir, y un generador de pseudoruido utilizado para ensanchar el espectro de la señal de datos.

Hay dos formas posibles de enfocar la implementación de la secuencia directa, ya que los procesos llevados a cabo por el modulador y el generador de pseudoruido se pueden cambiar de orden. En esta sección asumiremos que en una primera etapa el transmisor ensancha la señal de datos, y en una segunda etapa, la señal se modula. De esta forma se podrá explicar cada etapa por separado. En el receptor basta con seguir el orden inverso: primero demodular la señal recibida y después proceder a su desensanchamiento para recuperar la información original. El procedimiento que acabamos de explicar puede verse con más claridad en la figura 2.8.

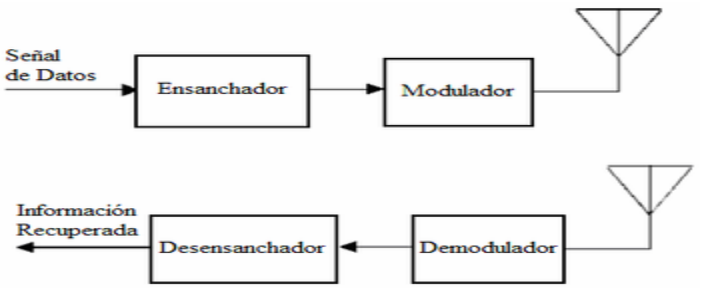


Figura 2.8 Diagrama de bloques de un sistema de transmisión sencillo (parte superior) y receptor de espectro ensanchado en secuencia directa (parte inferior).

El transmisor En la figura 2.9 volvemos a representar el diagrama de bloques de un transmisor en secuencia directa, pero esta vez se han detallado los componentes que lo constituyen:

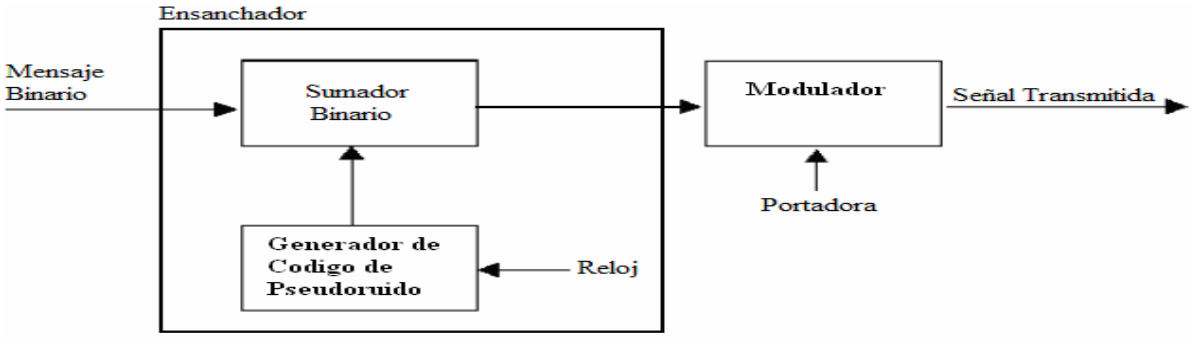


Figura 2.9 Transmisor de secuencia directa.

El ensanchador Vemos que el ensanchador de la figura 2.8 esta compuesto por un generador de código de pseudoruido y un sumador binario. La salida binaria del generador de pseudoruido se suma en módulo 2 con el mensaje binario que contiene la información que queremos transmitir, como se muestra en la figura 2.10.

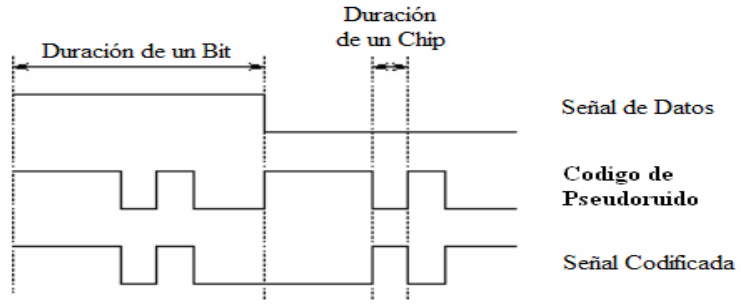


Figura 2.10 Ensanchado mediante código de pseudoruido.

Los sistemas DSSS, debido a una técnica de modulación mas eficiente, pueden operar con un SNR (Signal to Noise Ratio) tan bajo como 12 dB.

Para cierto nivel de interferencia de todas las bandas (interferencia que se relaciona a todo el espectro utilizado por el radio), los sistemas DSSS pueden ser operados con menores niveles de señal, y por lo tanto, para el mismo nivel de energía transmitida, los sistemas DSSS pueden operar a distancias mas largas. Recordemos también, que al hablar de "todo el espectro utilizado por el radio" nos referimos a 83.5 MHz en FHSS (toda la banda ICM) mientras que en DSSS es de solo 22 MHz (una de las sub-bandas). Las posibilidades de tener una interferencia cubriendo un rango de 22 MHz son evidentemente mas grandes que las posibilidades de una interferencia cubriendo un rango de 83.5 MHz. Una interferencia de 22 MHz de ancho, puede bloquear completamente un sistema DSSS, mientras que bloquearía solo el 33% de los saltos de otro sistema como FHSS.

El estándar IEEE 802.11 en lo referente a los sistemas DSSS utiliza una secuencia de dispersión perfectamente conocida de 11 chips, y puede modular uno de los 14 canales definidos en el estándar. Como la secuencia utilizada es conocida de antemano, la frecuencia de la portadora es fija para el sistema, y el número de posibles frecuencias es limitado, sería relativamente fácil para cualquiera "escuchar", "sintonizar" la señal de cualquier sistema DSSS. La protección del mensaje debe ser lograda por medio de la encriptación de datos. Esta opción incrementa el costo total de una implementación de este tipo, al mismo tiempo que reduce el desempeño, debido a que grandes recursos de procesamiento serán requeridos para el proceso de encriptación.

2.1.2.3 Tecnología Frecuency Hopping

La técnica Frequency Hopping Spread Spectrum (Salto de Frecuencia en Espectro Disperso), implica un cambio periódico en la frecuencia a transmitir, esto es, la señal debe de ser considerada como una secuencia de modulación ráfaga de los datos variante en el tiempo con respecto a la frecuencia portadora pseudoaleatoria, el conjunto de las posibles frecuencias portadoras es llamado *hopset*. Cada cambio de frecuencia (salto) ocurre dentro de la banda de frecuencias que incluye un número de canal, cada canal es definido como una región espectral con una frecuencia central del hopset en el largo del ancho de banda suficiente para incluir una ráfaga de modulaciones en banda angosta (usualmente FSK[8]) para cada correspondiente frecuencia portadora. El ancho de banda de un canal usado en el conjunto de saltos es llamado banda ancha instantánea. Los datos son enviados por saltos de la portadora que se transmite y que aparenta ser aleatoria en los canales los cuales son conocidos solo por el receptor deseado. Si solo hay una frecuencia portadora (canal sencillo) esta es usada sobre cada salto, la modulación de datos digitales es llamada entonces modulación por canal sencillo, en el figura 2.11, se ilustra este proceso por medio de bloques para canal sencillo para el caso

[8] FSK, Frequency Shift Keying, es la modulación digital por cambio de frecuencia, esta modulación es muy parecida a la modulación por frecuencia, excepto que la señal modulante es una secuencia de pulsos binarios que varía, entre dos niveles de voltaje discreto, en lugar de una forma de onda analógica que cambia de manera continua.

del transmisor, en tanto que en el Figura 2.12, se ilustra el proceso por bloques del receptor.

Es de notar que el receptor sincroniza el patrón de frecuencia de la señal recibida, así el sintetizador indica la decodificación del salto que se trata en ese momento, de esta forma las colisiones en Frequency Hopping son desechadas ya sea por el ruido u otras frecuencias no deseadas.

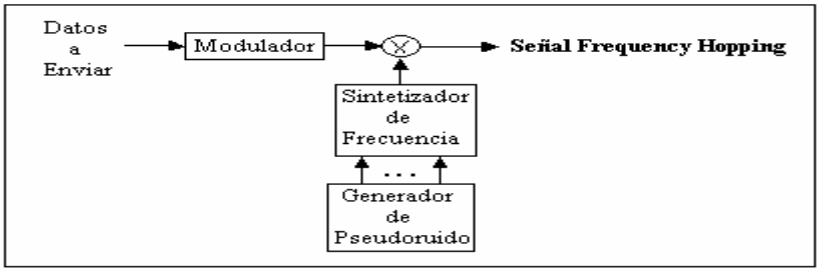


Figura 2.11 Proceso de bloques para el transmisor en Frecuencias de saltos para canal.

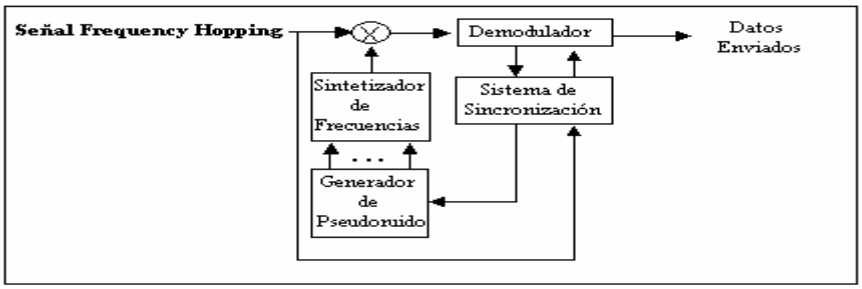


Figura 2.12 Proceso de bloques para el receptor en Frecuencias de saltos para canal.

Frequency Hopping se clasifica principalmente en rápida (Fast) o lenta (Slow), Fast Frequency Hopping ocurre si existe más de una frecuencia de salto durante cada símbolo transmitido, esto implica que el promedio de saltos es igual o excedente al promedio de los símbolos enviados, Slow Frequency Hopping ocurre si uno o más símbolos son transmitidos en el intervalo entre el salto de frecuencias, se describen las ventajas y desventajas de Frecuency Hopping:

Ventajas de Frequency Hopping.

- Alta tolerancia a interferencias.
- Alta seguridad contra intercepción de la señal.

Desventajas de Frequency Hopping.

- Baja/Media velocidad.
- Difícil de sincronizar a larga distancia.

2.1.3 Velocidades de transmisión y cobertura

La velocidad de transmisión es el número de bits transmitidos por segundo cuando se envía un flujo continuo de datos. Un comparativo dentro de las WLAN entre RF, BlueTooth y en 802.11b, es el que se indica en la tabla 2.6, así como su cobertura.

	RF	BlueTooth	802.11b
Cobertura.	45.72 m.	9.15 m.	121.92 – 304.8 m.
Velocidad de transmisión.	1 o 2 Mbps.	1 Mbps.	11 Mbps.

Tabla 2.6 Comparativa de cobertura y velocidad de transmisión.

En el estándar 802.11 se define una técnica de cambio de velocidad que permite a las redes reducir las velocidades de datos a medida que ocurren cambios en la distancia, calidad y fuerza de la señal.

Los productos de redes inalámbricas basados en los estándares 802.11 se les llama Wi-Fi, en particular solo se refieren a los productos compatibles con el estándar 802.11b con velocidades máximas de 11 Mbps inicialmente hasta 54 Mbps basados en las especificaciones de los estándares 802.11g y 802.11a.

El estándar 802.11b en realidad soporta un total de cuatro velocidades de datos: 1, 2, 5.5 y 11 Mbps, donde todas estas velocidades están disponibles en el mismo medio físico, específicamente una porción de casi 80 MHz de amplitud del espectro de frecuencia del radio, iniciando en 2.400 GHz, que luego se divide entre 11 y 14 canales, dependiendo de la cantidad exacta del espectro asignado por las distancias agencias internacionales. Las bases para las cuatro velocidades de datos que proporciona el estándar 802.11b son tres tipos de modulación:

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

Los estándares 802.11a y 802.11g son estándares complementarios que proporcionan una velocidad de datos máxima de 54 Mbps, no tan alta como la Ethernet, pero sustancialmente mayor que la 802.11b. Las velocidades básicas definidas en el estándar 802.11a son 6.12 y 24 Mbps.

La multiplexión por división ortogonal de frecuencias (OFDM) es un medio de transmisión y es un punto principal de comunicación entre lo estándares 802.11a y 802.11g.

OFDM, es un medio de transmisión que se adapta particularmente para la transmisión a través de frecuencias de radio. El OFDM es una técnica de transmisión, al igual que el acceso múltiple por división de código (CDMA), el cual se usa en ciertos tipos de teléfonos portátiles o en el espectro extendido de secuencias directas (DSSS), los cuales representan los medios de transmisión del espectro extendido especificado por 802.11b y que se usan en los Wi-Fi de 11 Mbps.

Con OFDM, un rango determinado de frecuencias, se divide en canales separados o subportadores. Durante la transmisión, estos canales subportadores u ortogonales se juntan o multiplexan. Tanto par el estándar 802.11a como para el estándar 802.11g se emplean distintos tipos de modulación y cada uno de ellos codifica y aumenta el número de bits por transmisión para alcanzar velocidades de datos más altas. Mientras sean más grande el número de bits codificados, tendrá que ser mas clara la señal para que la transmisión sea recibida y remodulada de forma exitosa.

Capítulo III

Seguridad de la Comunicación

Elección de topología
DHCP
NAT
Seguridad en las redes inalámbricas

La seguridad en redes inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión, las características de seguridad en la WLAN, se basa especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan en el ingreso a la red y protegen al sistema de administración de acceso no autorizado.

Desde sus comienzos, 802.11 ha proporcionado algunos mecanismos de seguridad básicos para impedir que esta libertad mejorada sea una posible amenaza. Por ejemplo, los puntos de acceso (o conjuntos de puntos de acceso) 802.11 se pueden configurar con un identificador del conjunto de servicios (SSID). La tarjeta NIC también debe conocer este SSID para asociarlo al AP y así proceder a la transmisión y recepción de datos en la red. Esta seguridad, si se llegase a considerar como tal, es muy débil debido a estas razones:

- Todas las tarjetas NIC y todos los AP conocen perfectamente el SSID.
- El SSID se envía por ondas de manera transparente (incluso es señalizado por el AP).
- La tarjeta NIC o el controlador pueden controlar localmente si se permite la asociación en caso de que el SSID no se conozca.
- No se proporciona ningún tipo de cifrado a través de este esquema.

Aunque este esquema puede plantear otros problemas, esto es suficiente para detener al intruso más despreocupado.

Las especificaciones 802.11 proporcionan seguridad adicional mediante el algoritmo WEP (Wired Equivalent Privacy). WEP proporciona a 802.11 servicios de autenticación y cifrado. El algoritmo WEP define el uso de una clave secreta de 40 bits para la autenticación y el cifrado, y muchas implementaciones de IEEE 802.11 también permiten claves secretas de 104 bits. Este algoritmo proporciona la mayor parte de la protección contra la escucha y atributos de seguridad física que son comparables a una red con cable.

Una limitación importante de este mecanismo de seguridad es que el estándar no define un protocolo de administración de claves para la distribución de las mismas. Esto supone que las claves secretas compartidas se entregan a la estación inalámbrica IEEE 802.11 a través de un canal seguro independiente del IEEE 802.11. El reto aumenta cuando están implicadas un gran número de estaciones, como es el caso de un campus corporativo.

Para proporcionar un mecanismo mejor para el control de acceso y la seguridad, es necesario incluir un protocolo de administración de claves en la especificación. Para hacer frente a este problema se creó específicamente el estándar 802.1x.

Seguridad - 802.1x Para ofrecer una mayor seguridad de la que proporciona WEP, el equipo de conexiones de red de Windows XP trabajó con IEEE, distribuidores de red y otros colaboradores para definir IEEE 802.1x. 802.1x es un borrador de

estándar para el control de acceso a redes basado en puerto que se utiliza para proporcionar acceso a red autenticado para las redes Ethernet. Este control de acceso a red basado en puerto utiliza las características físicas de la infraestructura LAN conmutada para autenticar los dispositivos conectados a un puerto LAN. Si el proceso de autenticación no se realiza correctamente, se puede impedir el acceso al puerto. Aunque este estándar se ha diseñado para redes Ethernet con cable, se puede aplicar a las redes LAN inalámbricas 802.11.

Concretamente, en el caso de las conexiones inalámbricas, el punto de acceso actúa como autenticador para el acceso a la red y utiliza un servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) para autenticar las credenciales del cliente. La comunicación es posible a través de un "puerto no controlado" lógico o canal en el punto de acceso con el fin de validar las credenciales y obtener claves para obtener acceso a la red a través de un "puerto controlado" lógico. Las claves de que dispone el punto de acceso y el cliente como resultado de este intercambio permiten cifrar los datos del cliente y que el punto de acceso lo identifique. De este modo, se ha agregado un protocolo de administración de claves a la seguridad de 802.11.

Los pasos siguientes describen el planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red.

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando una estación inalámbrica entra en el alcance del punto de acceso, éste envía un desafío a la estación.
- Cuando la estación recibe el desafío, responde con su identidad. El punto de acceso reenvía la identidad de la estación a un servidor RADIUS que realiza los servicios de autenticación.
- Posteriormente, el servidor RADIUS solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad. La estación envía sus credenciales al servidor RADIUS (a través del "puerto no controlado" del punto de acceso).
- El servidor RADIUS valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.
- El punto de acceso utiliza la clave de autenticación para transmitir de manera segura las claves correctas a la estación, incluida una clave de sesión de unidifusión para esa sesión y una clave de sesión global para las multidifusiones.
- Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.

3.1 ELECCIÓN DE TOPOLOGÍA

La topología representa la manera en la cual los diseñadores van a proporcionar los diferentes servicios de la red a cada cliente (terminal de usuarios), no existe una topología mejor que otra, su funcionamiento es diferente y es precisamente esta diferencia las que las hace mejores que otras solo bajo circunstancias muy especificas.

Las redes inalámbricas se pueden dividir en dos topologías distintas, la topología Ad-Hoc (punto a punto) y la topología por infraestructura en donde cada cliente envía su comunicación a una central o punto de acceso, para este caso podemos hablar en la práctica de dos tipos de topologías por configuración que es: estrella y malla.

3.1.1 Enlace troncal entre edificios punto-punto

En una red con esta topología, cada computadora puede actuar como cliente y como servidor, conectando dos edificios directamente. En un enlace PTP (Peer to Peer), dos dispositivos monopolizan un medio de comunicación. Debido a que no se comparte el medio, no se necesita un mecanismo para identificar las computadoras, y por lo tanto, no hay necesidad de direccionamiento, como se muestra en la figura 3.1.

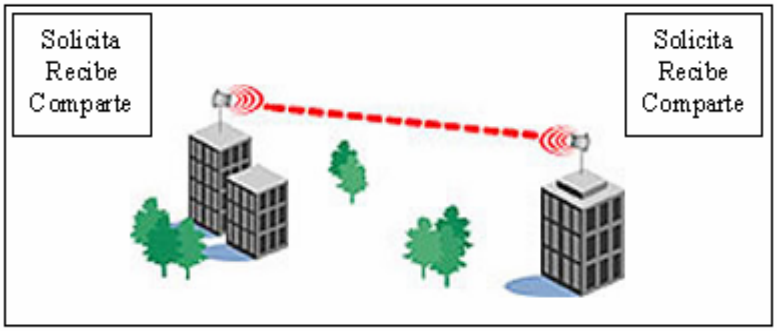


Figura 3.1 Topología punto a punto.

3.1.2 Topología Estrella

Aquí cada estación está directamente conectada a un nodo central común, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción, enlazando de esta manera diferentes edificios como se muestra en la figura 3.2. El nodo central llamado hub o base en el caso inalámbrico, gestiona la distribución de la información a los demás nodos. Mantiene la ventaja de que cualquier nodo puede fallar sin afectar al resto y la desventaja de si el hub falla la red quedara incomunicada. Además debe de cumplir el requisito necesario de línea de vista, lo cual quiere decir que cada nodo debe de estar libre de obstáculos en el radio (medio de comunicación) del nodo a la base.

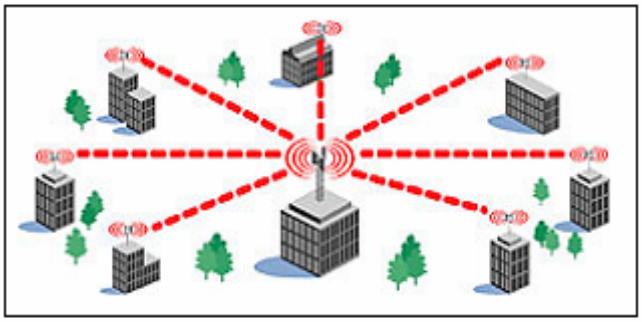


Figura 3.2 Topología Estrella.

3.1.3 Topología Malla

Esta clase de topología permite sin tener que definir un nodo central o analizar los requisitos de la línea de vista a la estación base tener comunicación, esto es debido a que cada nodo se comunicara con cada otro nodo dentro de la malla en un determinado rango (típicamente 800 m), esparciendo con esto la comunicación a través de múltiples salto (paso por nodos) hasta llegar al destino deseado. El camino seleccionado para llegar de un nodo a otro dependerá de la configuración establecida ya que puede tratarse por demanda (ocupando los nodos no ocupados) o por difusión encargándose el nodo receptor de discriminar la información ya recibida o alguna otra definida por el fabricante o diseñador, como se muestra en la figura 3.3.

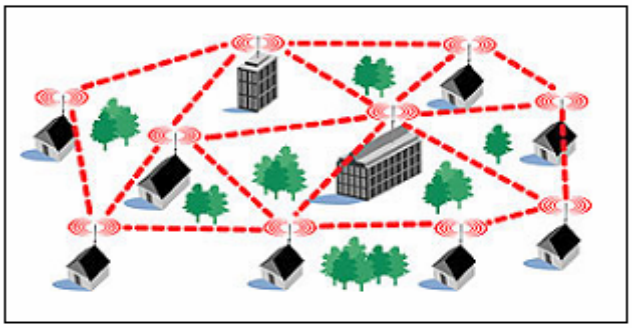


Figura 3.3 Topología Malla.

3.2 DHCP

DHCP son las siglas en inglés del protocolo de configuración dinámica de servidores (Dynamic Host Configuration Protocol). Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadoras conectadas a la red.

DHCP se basa en el conocido modelo Cliente-Servidor. Utiliza un protocolo de comunicaciones muy sencillo, basado en UDP[1] sobre IP. Los clientes de una red que utilicen este protocolo utilizan direcciones IP que les "alquila" un servidor (no tiene porqué ser local).

El cliente recibe, junto con la dirección, algunos parámetros adicionales: gateway por defecto, servidor WINS, servidor DNS, etc. Lo que DHCP consigue es que la asignación y liberación de las direcciones IP en una red sea dinámica y automática; se evita las duplicidades y se optimiza el consumo de direcciones.

La intervención del administrador de redes, aún en grandes configuraciones es mínima. Cada vez que un cliente se inicia, pide una dirección IP o una renovación de la que tiene alquilada actualmente.

El protocolo DHCP permite manejar rangos de direcciones IP de forma dinámica y automatizada.

El protocolo dinámico de configuración de HOST (DHCP) proporciona un mecanismo a través del cual las computadoras que usan el TCP/IP puedan obtener una dirección IP automáticamente cuando ingresan a una red. DHCP es un estándar abierto, desarrollado por el grupo de DHC del Internet Engineering Task Force (IETF).

El parámetro más importante de la configuración asignado por DHCP es la dirección IP. A una computadora se le debe asignar inicialmente una dirección IP específica que es apropiada a la red a la que pertenece esa computadora, y la cual no se asigna a ninguna otra computadora en esa red. Si una computadora se mueve a una nueva red, se le debe asignar una nueva dirección IP. DHCP se puede utilizar para manejar estas asignaciones automáticamente.

DHCP especifica otros parámetros importantes de la configuración, tales como la sub-máscaras y el servidor de nombres de dominio (DNS). Usando DHCP, un administrador de la red puede evitar la configuración "manual" de computadoras individuales con aplicaciones complejas y confusas, porque esas computadoras pueden obtener todos los parámetros requeridos de la configuración automáticamente mediante un servidor DHCP.

3.2.1 Asignación de direcciones IP

Sin DHCP, cada dirección IP debe configurarse manualmente en cada computadora y, si la computadora se mueve a otro lugar en otra parte de la red, se debe de configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar

[1] Unidad de datos del protocolo (PDU, Protocol Data Unit). Conjunto de datos especificado en un protocolo de una capa dada y que consta de información de control del protocolo de esa capa y, posiblemente, de datos del usuario de esa capa.

y enviar una nueva IP si la computadora es conectada en un lugar diferente de la red. El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- *Asignación manual:* Donde la asignación se basa en una tabla con direcciones MAC (pares de direcciones IP ingresados manualmente por el administrador). Sólo las computadoras con una dirección MAC que figure en dicha tabla recibirá el IP que le asigna dicha tabla.
- *Asignación automática:* Donde una dirección IP libre obtenida de un rango determinado por el administrador se le asigna permanentemente a la computadora que la requiere.
- *Asignación dinámica:* El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido.

El DHCP es una alternativa a otros protocolos de gestión de direcciones IP de red, como el BOOTP (Bootstrap Protocol). DHCP es un protocolo más avanzado, pero ambos son los usados normalmente.

3.2.2 Parámetros configurables

Un servidor DHCP puede proveer de una configuración opcional a la computadora cliente. Lista de opciones configurables:

- Dirección del servidor DNS.
- Nombre DNS.
- Puerta de enlace de la dirección IP.
- Dirección de Publicación Masiva.
- Máscara de subred.
- Tiempo máximo de espera del ARP (Protocolo de Resolución de Direcciones).
- MTU (Unidad de Transferencia Máxima) para la interfaz.
- Servidores NIS (Servicio de Información de Red).
- Dominios NIS.
- Servidores NTP (Protocolo de Tiempo de Red).
- Servidor SMTP.
- Servidor TFTP.
- Nombre del servidor WINS.

DHCP Discover La computadora cliente publica masivamente en la subred local para encontrar un servidor disponible. El router puede ser configurado para redireccionar los paquetes DHCP a un servidor DHCP en una subred diferente. La implementación cliente crea un paquete UDP (Protocolo de Datagramas de Usuario) con destino 255.255.255.255 y requiere también su última dirección IP conocida, aunque esto no es necesario y puede llegar a ser ignorado por el servidor.

DHCP Offer El servidor determina la configuración basándose en la dirección del soporte físico de la computadora cliente especificada en el registro CHADDR (Dirección de hardware del cliente). El servidor especifica la dirección IP en el registro YIADDR (Su Dirección IP).

DHCP Request El cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor.

DHCP Acknowledge El servidor confirma el pedido y lo publica masivamente en la subred. Se espera que el cliente configure su interfase de red con las opciones que le fueron asignadas.

La figura 3.4 muestra la configuración del DHCP con lo mencionado anteriormente.



Figura 3.4 Configuración del DHCP.

3.3 NAT

La traducción de direcciones de red, o NAT (Network Address Translation), es un método mediante el que las direcciones IP son mapeadas desde un dominio de direcciones a otro, proporcionando encaminamiento[2] transparente a las maquinas finales. Existen muchas variantes de traducción de direcciones que se presentan a distintas aplicaciones. Sin embargo todas las variantes de dispositivos NAT debería compartir las siguientes características:

- Asignación transparente de direcciones.
- Encaminamiento transparente mediante la traducción de direcciones.
- Traducción de la carga útil de los paquetes de error ICMP.

NAT permite aprovechar los bloques de direcciones reservadas generalmente, una red interna se suele configurar para que se use uno o más de estos bloques de red. Estos bloques son:

10.0.0.0 / 8 (10.0.0.0 – 10.255.255.255)
172.16.0.0 / 12 (172.16.0.0 – 172.31.255.255)
192.168.0.0 / 16 (192.168.0.0 – 192.168.255.255)

NAT puede operar de cuatro maneras distintas, las cuales son:

1. *Estático:* Se asigna una dirección IP pública a cada dirección IP privada, por ello se recomienda para equipos y/o aplicaciones que necesitan de direcciones IP públicas.
2. *Dinámico:* Muy similar al anterior, sólo que la asignación de las direcciones internas hacia las externas depende del momento en el que los equipos de la red local se dan de alta en el sistema NAT, tomando la primera disponible. Por ende la única diferencia es que la dirección pública no siempre es la misma.
3. *Por registro de dominios:* Se emplea para garantizar la comunicación entre una red local e Internet cuando las direcciones IP de la red local son iguales a direcciones públicas. Para evitar conflictos, el equipo NAT guarda un registro de qué dirección privada asignar a una comunicación entrante y de igual manera, qué dirección pública asignar a una comunicación saliente. Como es claro, se necesita un rango de direcciones públicas para hacer esta doble asignación.
4. *Por asignación de puertos:* En este esquema, sólo se dispone de una dirección IP pública, misma que conserva el equipo NAT. Cuando un equipo de la red local desea comunicarse con el exterior, para los equipos remotos se estará recibiendo una solicitud de la dirección del NAT con un número de puerto específico.

[2] Se refiere al reenvío de paquetes, no al intercambio de información de encaminamiento.

El cuarto método usa una característica especial del protocolo TCP/IP llamada multiplexado, donde un equipo puede mantener conexiones con uno o más sistemas de forma simultánea a través de los puertos TCP o UDP. Mientras la dirección IP permite el enlace entre los sistemas, los puertos facilitan que cada enlace tenga una identificación exclusiva.

3.3.1 Operación básica

Para que una red privada tenga acceso a Internet, el acceso debe ser por medio de un dispositivo ubicado en la frontera de las dos redes que tenga configurado NAT para la traducción de direcciones, en estos casos lo más conveniente es poner a un router para que los paquetes sean enviados hacia él. Existen dos tipos de asignación de direcciones:

- *Asignación estática de direcciones:* Existe un mapeo uno a uno de direcciones para las máquinas entre una dirección privada de red y una dirección externa de red durante el tiempo en funcionamiento del NAT. La asignación estática de direcciones asegura que NAT no tiene que administrar la gestión de direcciones con los flujos de sesión.

  Ejemplo: Cuando el host A con dirección IP X1 envía un paquete al servidor B con dirección IP Y1, al pasar estos paquetes por el NAT, los datos llegan al servidor B. Las relaciones de direcciones de la tabla del router son puestas estáticamente como lo muestra la figura 3.5 en la parte de la tabla NAT estático.

- *Asignación dinámica de direcciones:* Las direcciones externas son asignadas a las máquinas de la red privada, o viceversa, de manera dinámica, basándose en los requisitos de uso y el flujo de sesión que el NAT determine heurísticamente. Cuando la última de las sesiones que use una dirección asociada termine, NAT liberará la asociación para que la dirección global pueda ser reciclada para su posterior uso. La naturaleza exacta de la asignación de direcciones es específica de cada implementación de NAT.

  Ejemplo: En este caso sucede lo mismo que en el anterior los paquetes que salen del host A, en este caso la tabla muestra una lista con las direcciones válidas disponibles para ser usadas, estas direcciones son asignadas dinámicamente a los host’s como lo muestra la figura 3.5, en la parte de la tabla NAT dinámico.

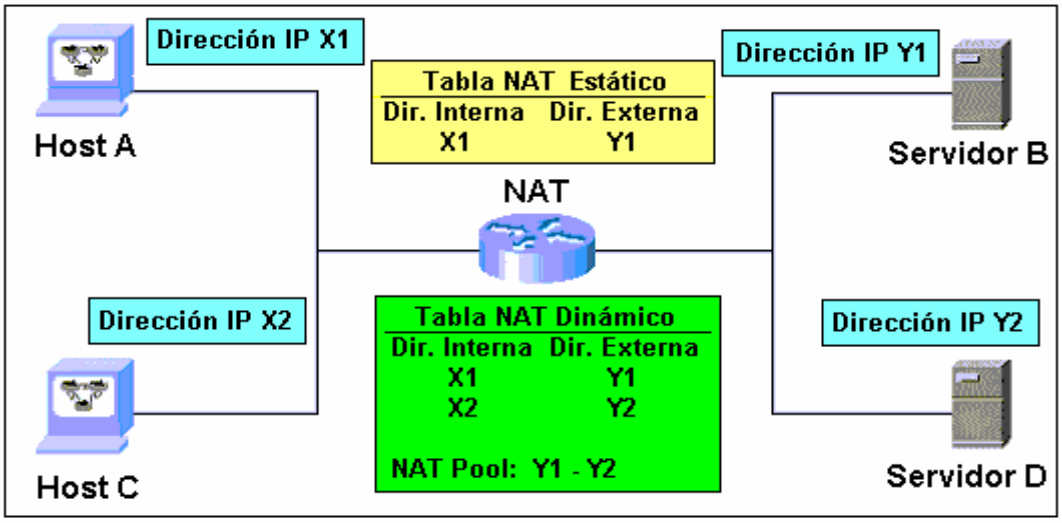


Figura 3.5 Asignación de direcciones NAT.

Existen dos variantes del NAT Tradicional: NAT Básico y NAPT (Network Address Port Translation ó traducción de dirección de red y puerto).

NAT Básico La operación de NAT Básico es como se describe a continuación: una zona con un conjunto de direcciones de red privadas puede ser habilitada para comunicarse con una red externa mapeando dinámicamente el conjunto de direcciones privadas a un conjunto de direcciones de red válidas globalmente, cada dirección tiene garantizada una dirección global para ser mapeada a ella. De lo contrario, los nodos habilitados para tener acceso simultáneo a la red externa son limitados por el número de direcciones en el conjunto global.

NAPT Este modelo es adecuado para muchos grupos de redes pequeñas para acceder a redes externas usando una sola dirección IP asignada del proveedor de servicio. Este modelo debe ser extendido para permitir acceso entrante mapeando estáticamente un nodo local por cada puerto de servicio de la dirección IP registrada.

3.4 SEGURIDAD EN LAS REDES INALÁMBRICAS

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), de si es una red ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores, las cuales se describen más adelante.

3.4.1 El problema de la seguridad de una red inalámbrica

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Cualquier equipo que se encuentre a unos metros de un punto de acceso, podría tener acceso a la red inalámbrica. Por ejemplo, si varias empresas tienen sede en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse 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 posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa, lo antes mencionado se muestra en la figura 3.6.

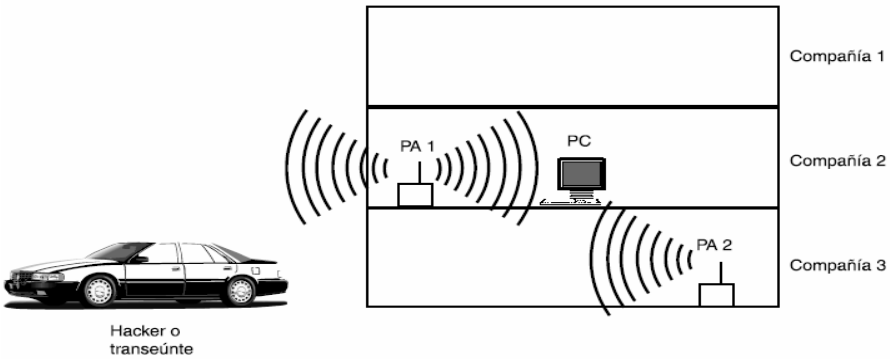


Figura 3.6 Acceso no autorizado a la red inalámbrica.

Lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbrico en la red de una empresa. Es muy común encontrar redes en las que el acceso a Internet se protege adecuadamente con un firewall bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio. Cualquier persona que desde el exterior capte la señal del punto de acceso, tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en la Internet, emplear la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, entre muchas otras cosas. Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía.

La mala configuración de un acceso inalámbrico es, desgraciadamente, una cosa muy común. Un estudio publicado en el 2003 por RSA Security Inc. encontró que de 328 puntos de acceso inalámbricos que se detectaron en el centro de Londres, casi las dos terceras partes no tenían habilitado el cifrado mediante WEP (Wired Equivalent Protocol). Además, 100 de estos puntos de acceso estaban divulgando información que permitía identificar la empresa a la que pertenecían, y 208 tenían la configuración con la que vienen de fábrica.

Existen dos prácticas bien conocidas para localizar redes inalámbricas:

- *El warchalking:* Que consiste en caminar por la calle con una computadora portátil dotada de una tarjeta inalámbrica, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red, esto se muestra en la figura 3.7.

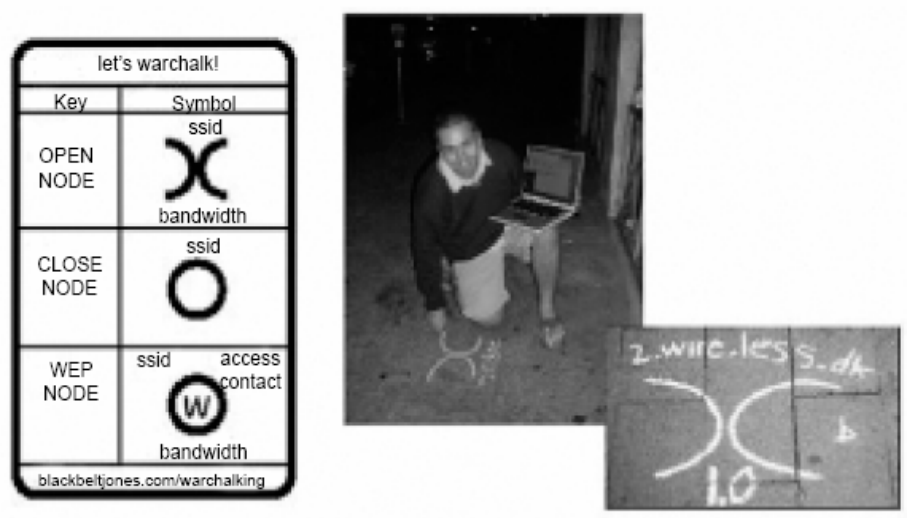


Figura 3.7 Warchalking y su simbología.

- *El wardriving:* Propio para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de una computadora portátil con una tarjeta inalámbrica, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas o de papas fritas) un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en la Internet, esto se muestra en la figura 3.8.



Figura 3.8 Wardriving, a la izquierda se puede observar el equipo necesario (computadora, GPS y antena), a la derecha los triángulos indican sobre el mapa la posición de redes inalámbricas.

Una vez localizada una red inalámbrica, una persona podría llevar a cabo dos tipos de ataques:

- Ingresar a la red y hacer uso ilegítimo de sus recursos.
- Configurar un punto de acceso propio, orientando la antena de tal modo que las computadoras que son clientes legítimos de la red atacada se conecten a la red del atacante. Una vez hecho esto, el atacante podría robar la información de dichas computadoras, instalarles software maligno o dañar la información.

3.4.2 Garantizando la seguridad de una red inalámbrica

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas. A continuación se da una descripción de cada uno de ellos.

Método 1, Filtrado de direcciones MAC Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

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 impráctico para uso en redes medianas o grandes:

- No escala bien, porque 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. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.
- 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 las listas.

- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computadora, empleando programas tales como AirJack o WellenReiter, entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.
- 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 es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

Método 2, Wired Equivalent Privacy (WEP): El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas. El algoritmo WEP cifra de la siguiente manera:

- A la trama en claro se le ingresa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.
- Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.
- 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.
- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 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.
- 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).
- Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.
- El IV y la trama se transmiten juntos.

Lo mencionado anteriormente se muestra en la figura 3.9.

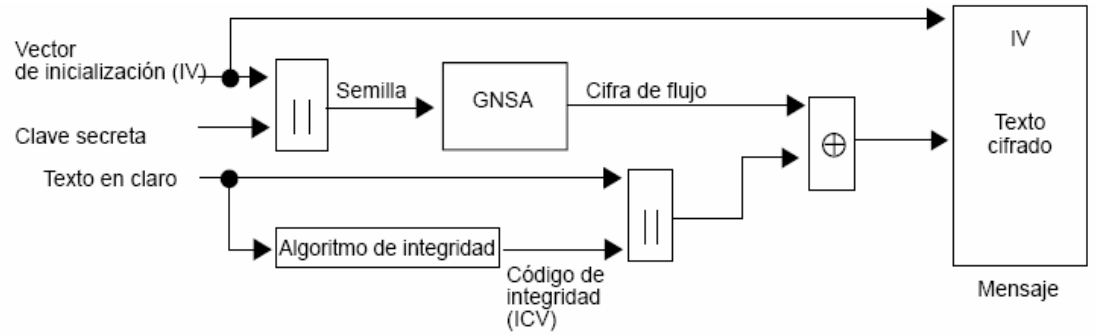


Figura 3.9 Funcionamiento del algoritmo WEP en modalidad de cifrado.

En el receptor se lleva a cabo el proceso de descifrado:

- Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
- 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.
- 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.
- A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.
- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

En la figura 3.10 se muestra lo antes mencionado.

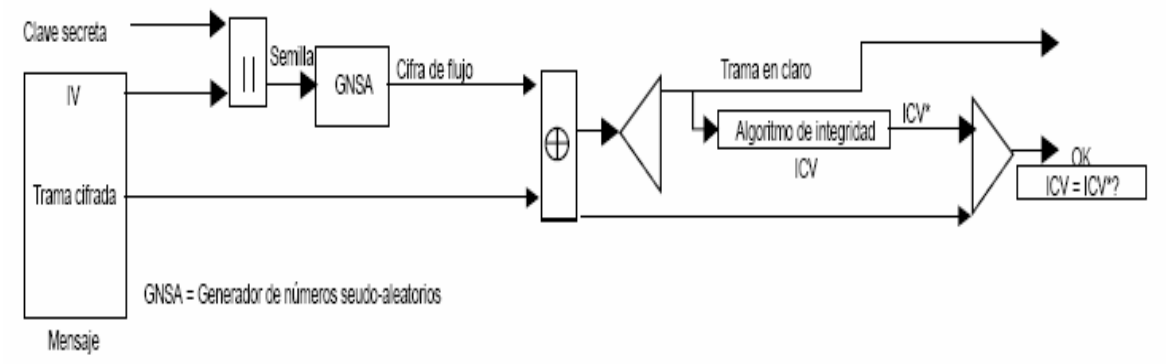


Figura 3.10 Funcionamiento del algoritmo WEP en modalidad de descifrado.

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

- La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca,

o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

- El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 224 IV distintos. Esto no es problemático 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 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. 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.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack, que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

Método 3, Las VPN: Una red privada virtual (Virtual Private Network, VPN) 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.

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 router, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. 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, sólo cuando éste ha sido debidamente autorizado y autenticado, como se muestra en la figura 3.11.

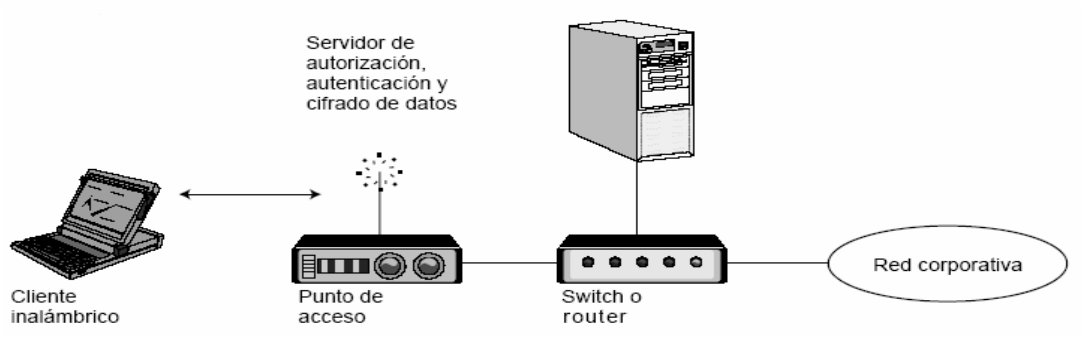


Figura 3.11 Estructura de una VPN para acceso inalámbrico seguro.

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.

Método 4, 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 uso en redes de área local por cable, 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:

- El suplicante, o equipo del cliente, que desea conectarse con la red.
- 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 (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.
- El autenticador, que es el equipo de red (switch, router, 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 autoriza.

La figura 3.12 muestra la autenticación del sistema 802.1x.

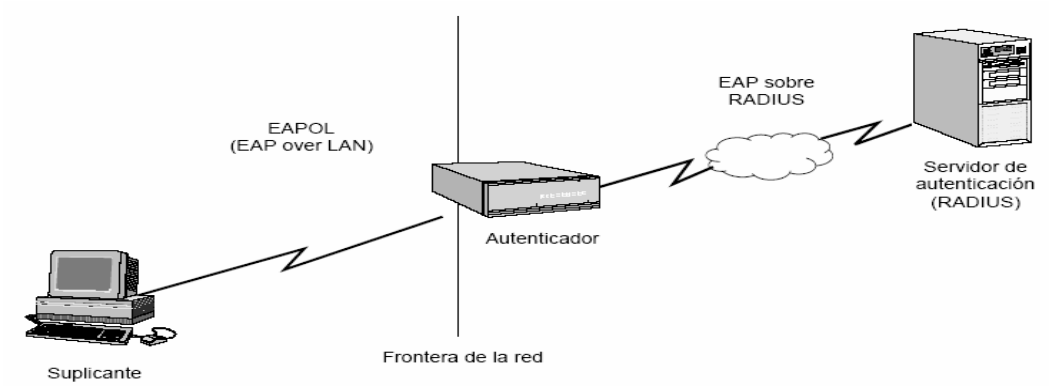


Figura 3.12 Arquitectura de un sistema de autenticación 802.1x.

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

- El proceso inicia cuando la computadora de trabajo se enciende y activa su interfaz de red (en el caso por cable) 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 computadora de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso 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. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.
- El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) 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.
- El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

La figura 3.13 muestra el dialogo EAPOL-RADIUS.

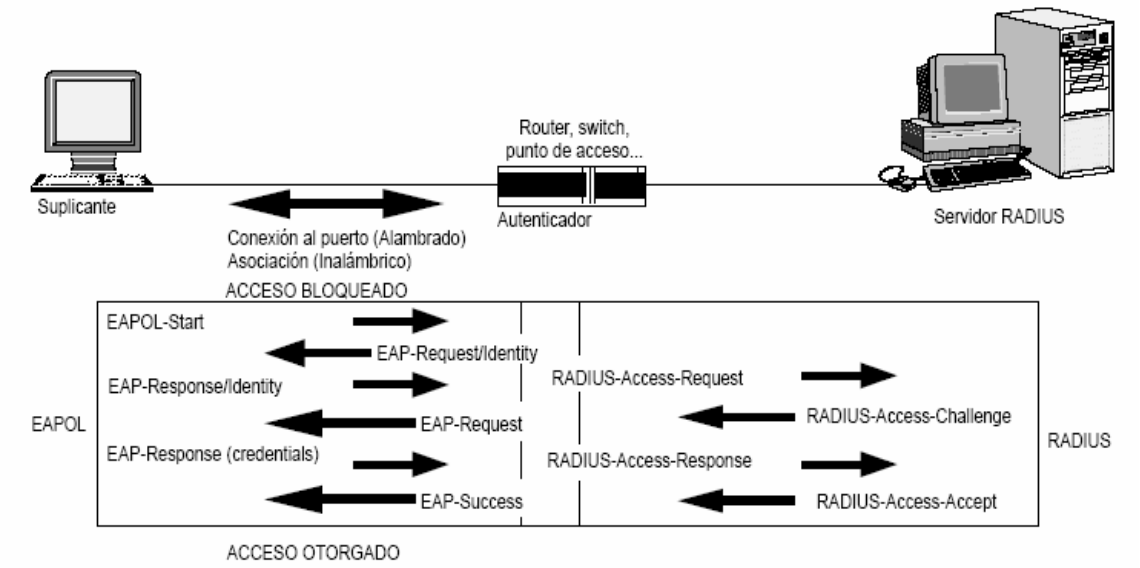


Figura 3.13 Dialogo EAPOL-RADIUS.

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 cinco minutos), para evitar el ataque de rompimiento de la clave descrito en la sección referente a WEP.

Existen varias 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 (es decir, el servidor autentica al cliente y viceversa) y 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 servicios 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, CHAP, MS-CHAP ó MS-CHAP v2.

- *PEAP:* Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAPTTLS, 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.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

- 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, 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.

Las variantes de EAP que utilizan contraseñas son las siguientes:

- EAP-MD5: Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. 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 está 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.
- LEAP: Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.
- 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.

Método 5, WPA (WI-FI Protected Access): Es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para redes inalámbricas) 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.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). 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 mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.

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

1. *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 usarán para cifrar los datos.
2. *Modalidad de red casera, o 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. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

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

Capítulo IV

Configuración y Conectividad de Puntos de acceso

Tipo de hardware a utilizar
Características

4.1 TIPO DE HARDWARE A UTILIZAR

4.1.1 Puntos de acceso

Punto de Acceso (Access Point o AP) Es el dispositivo que sirve como punto de conexión común para acceso de múltiples usuarios de la red inalámbrica. Un punto de acceso es un dispositivo de ancho de banda compartido conectado a la red local, permitiendo acceso a los servicios de esta red, la figura 4.1 muestra algunos tipos de puntos de acceso.



Figura 4.1 Distintos tipos de puntos de acceso.

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 y el 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.

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

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

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

Un punto de acceso es un hardware que por un lado tiene una antena y por otro un conector RJ45, que permite que el trafico de una red inalámbrica pase a una Ethernet y viceversa, como se muestra en la figura 4.2.

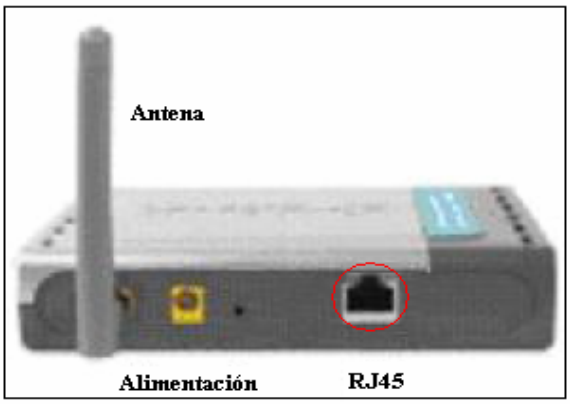


Figura 4.2 Punto de acceso con conector RJ45.

Para efectuar la comunicación se emplean ondas electromagnéticas de baja potencia a una frecuencia de 2.4 GHz. Las configuraciones que se pueden adoptar son:

- *Ad-Hoc (punto a punto):* Sirve para comunicar dos equipos. Es como utilizar un cable cruzado en una red Ethernet, son necesarias dos tarjetas de red.
- *Residencial Gateway:* Es la solución idónea para integrar la red de cable con una red inalámbrica en entornos domésticos. En ella hay un solo punto de acceso al que pueden conectarse varios dispositivos.
- *Access Point:* Igual que el anterior pero con varios puntos de acceso. Soporta roaming entre los puntos de acceso.

Dependiendo de la potencia del punto de acceso, cada equipo puede separarse a una distancia máxima del punto de acceso, la velocidad de transmisión máxima es de 11 Mbps (la velocidad de una red Ethernet típica es de 10 Mbps, aunque cada vez son más populares de 100 Mbps).

4.1.2 Antenas

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

Todos los equipos inalámbricos ya incorporan sus propias antenas. No obstante, cuando se desea disponer de una red de mayor alcance o cobertura, a veces, resulta conveniente sustituir la antena incorporada en el dispositivo por otra antena exterior con mayor ganancia. La mayoría de las antenas que incorporan los equipos inalámbricos son

antenas internas. Esto quiere decir que son antenas que vienen incluidas dentro de la unidad del punto de acceso o del adaptador de red (tarjeta PCI, PCMCIA o dispositivo USB), en la figura 4.3 se muestran algunos tipos de accesorios inalámbricos con antenas internas.



Figura 4.3 Accesorios inalámbricos.

Las antenas internas ofrecen la gran ventaja de la comodidad al formar parte del propio dispositivo, pero tienen el inconveniente del alcance. Si se necesita aumentar el alcance sin instalar nuevos puntos de acceso, la mejor solución es colocar una antena externa. Con una buena antena externa la señal de un punto de acceso puede llegar a superar los 15 Km de alcance siempre y cuando no haya obstáculos, como edificios o árboles y que la antena este bien colocada, a continuación se muestran unos ejemplos de antenas externas en la figura 4.4.



Figura 4.4 Ejemplos de antenas externas.

Su potencia se mide en dB[1](decibelios) y se toma como referencia a la antena isotrópica, el valor de potencia se representa en dBi (decibelios en relación a la antena isotrópica), la cual tendría una potencia de 1 dBi. Las hay de dos tipos los cuales son:

1. *Direccionales:* Concentran la energía radiada en una sola dirección, por lo que consiguen que la energía radioeléctrica llegue bastante más lejos (mayor alcance, aunque en una sola dirección). Deben estar orientadas hacia el emisor porque su rango de operación es de 8º a 30º.
2. *Omnidireccionales:* Son aquellas que radian en todas direcciones y también pueden captar la señal procedente de todas las direcciones. Estas antenas tienen una potencia mayor que las antenas internas que vienen incluidas en los adaptadores de red, pero menor que una antena externa direccional. No es necesario orientarlas porque su rango es de 360º.

En el mercado existen tantos tipos de antenas como ha permitido la imaginación: yagui, de panel, parabólica de disco, parabólica de rejilla, de techo, patch, dipolo, planas, compactas, móviles, sectoriales, espiral, guía-onda, anular, etc. No obstante, todos estos tipos de antenas pueden agruparse en dos tipos: omnidireccional y direccional, en la figura 4.5 se muestra el lóbulo principal de propagación de la señal en distintas antenas.

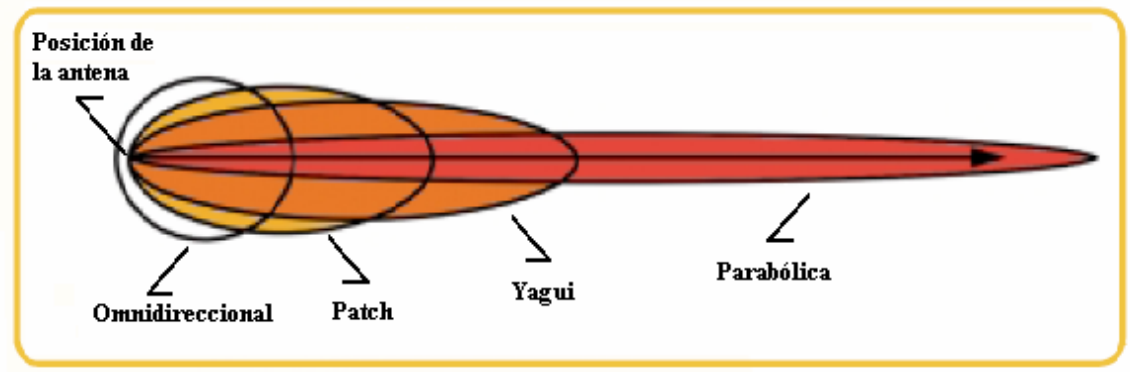


Figura 4.5 Lóbulo de propagación de diferentes antenas.

4.1.2.1 Conectores de antena, cables de antena y adaptadores de red

Las antenas externas se conectan a los equipos inalámbricos mediante un cable. Lo normal es que el cable que une el dispositivo inalámbrico con la antena sea un cable de tipo coaxial. Para conectar el cable a la antena y a los dispositivos inalámbricos, se utilizan los conectores. Tanto la antena como los equipos inalámbricos disponen de un conector donde se deben enchufar sus correspondientes conectores de los extremos del cable.

[1] El decibelio es una unidad que se calcula como el logaritmo de una relación de valores.

Tanto el cable, como cada conector, añaden pérdidas a la señal de radio. Para evitar estas pérdidas, aparte de utilizar cables y conectores de calidad, hay que procurar utilizar un cable lo más corto posible y el número de conectores imprescindibles. Esto último quiere decir que hay que evitar conectores para extender la longitud del cable o para adaptar tipos de cables o conectores.

La utilización de conectores parece muy sencilla, pero todo se complica por el hecho de que no existe una regulación que especifique cómo deben ser los conectores. Esto trae consigo que existan muchos modelos distintos de conectores, algunos muy extendidos y otros específicos de un fabricante (conectores propietarios), la figura 4.6 muestra los diferentes tipos de conectores.

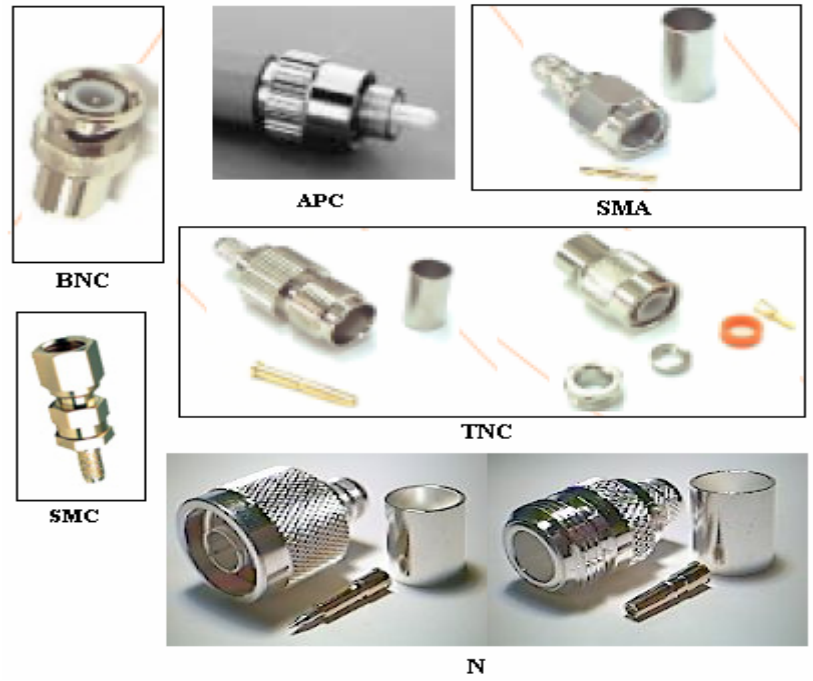


Figura 4.6 Tipos de conectores.

Los tipos de conectores más comunes son los siguientes:

- **N**. Navy (marina): Es el conector más habitual en las antenas de 2.4 GHz. Trabaja bien con frecuencias de hasta 10 GHz. Es un conector de tipo rosca.
- **BNC**. Bayonet Navy Connector (conector de tipo bayoneta de la marina): Es un conector barato utilizado en las redes Ethernet del tipo 10Base2. Es un tipo de conector muy común, pero poco apto para trabajar en la frecuencia de 2.4 GHz.
- **TNC**. Threaded BNC (conector BNC roscado): Es una versión roscada del conector BNC. Este tipo de conector es apto para frecuencias de hasta 12 GHz.
- **SMA**. Sub-Miniature Connector (conector subminiatura): Son unos conectores muy pequeños, van roscados y trabajan adecuadamente con frecuencias de hasta 18 GHz.
- **SMC:** Se trata de una versión todavía más pequeña de los conectores tipo SMA. Son aptos para frecuencias de hasta 10 GHz.

- **APC-7**. Amphenol Precisión Conector (conector Amphenol de precisión): Se trata de un conector con muy poca pérdida, y muy cara, fabricado por la empresa Amphenol.

El cable introduce pérdidas en la señal que van desde los 0.05 a 1 dB por metro (dependiendo de la calidad del cable). Por tanto, a menor longitud del cable, menores pérdidas. El cable tiene soldado un conector en cada extremo, como se muestra en la figura 4.7.



Figura 4.7 Cable con conectores.

Los cables más utilizados son los de tipo LMR. Éstos son cables fabricados por Times Microwave System. Una alternativa son los cables Heliax fabricados por Andrew Corporation. Éstos son unos cables que introducen muy poca pérdida a la señal pero a cambio de un alto coste. Por dar una última referencia también se aconsejan los cables fabricados por Belden, la figura 4.8 muestra algunos ejemplos de cables.

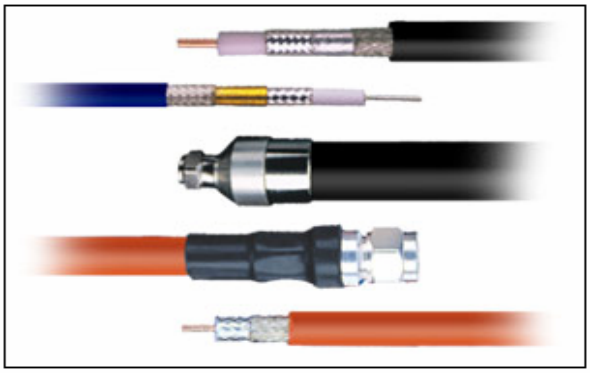


Figura 4.8 Ejemplos de cables.

A diferencia de las antenas, los adaptadores de red inalámbrico no suelen disponer de un conector tipo N. Esto quiere decir que no se puede conectar directamente el cable de la antena (con conector N) al equipo inalámbrico (con conector distinto, posiblemente propietario). Por tanto, para permitir la conexión, se utilizan adaptadores del conector tipo N al del tipo del equipo inalámbrico. A estos adaptadores se les conoce mejor como: *pigtail (literalmente, trenza)*, como lo muestra la figura 4.9.

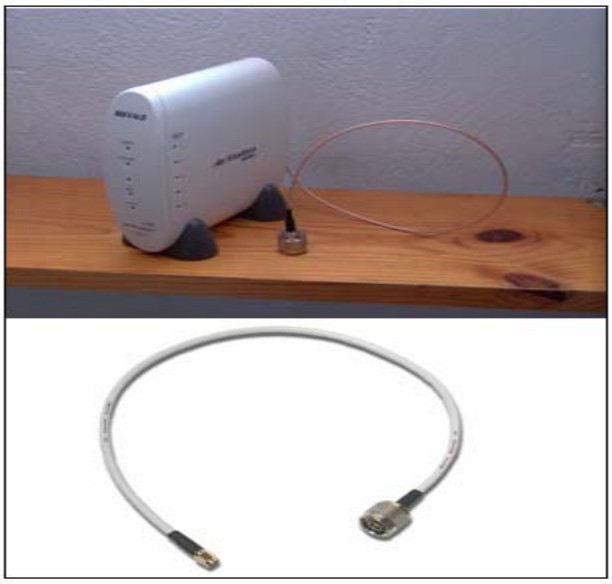


Figura 4.9 Ejemplo de un adaptador Pigtail.

4.1.3 Configuración y conexión de dispositivos

Existen dos formas diferentes de configurar dispositivos wireless 802.11, las cuales son:

1. *Modo BSS:* Es el que se utiliza normalmente. Este modo también se denomina modo infraestructura. En esta configuración se conectan un determinado número de puntos de acceso a una red cableada. Cada red wireless posee su propio nombre. Este nombre es el *SSID* de la red. Los clientes wireless se conectan a estos puntos de acceso. El estándar IEEE 802.11 define el protocolo que se utiliza para realizar esta conexión. Un cliente wireless puede asociarse con una determinada red wireless especificando el SSID. Un cliente wireless también puede asociarse a cualquier red que se encuentre disponible; basta con no especificar ningún SSID.

2. *Modo IBSS:* Conocido como modo Ad-Hoc, se ha diseñado para facilitar las conexiones punto a punto. En realidad existen dos tipos de modos Ad-Hoc. El primer tipo se denomina modo Ad-Hoc del IEEE; este modo se encuentra especificado en el estándar IEEE 802.11. El segundo tipo se denomina modo Ad-Hoc de demostración o de Lucent (y algunas veces, también se le llama simplemente modo Ad-Hoc, lo cual es bastante confuso); este es el modo de funcionamiento antiguo, anterior al estándar 802.11, del modo Ad-Hoc debería utilizarse sólo en instalaciones propietarias.

Los AP son dispositivos de red wireless que funcionan de forma equivalente a los hub’s o concentradores, permitiendo que varios clientes wireless se comuniquen entre sí.

A menudo se utilizan varios AP para cubrir un área determinada como una casa, una oficina u otro tipo de localización delimitada.

Los AP poseen típicamente varias conexiones de red: la tarjeta wireless y una o más tarjetas Ethernet que se utilizan para comunicarse con el resto de la red. Los AP se pueden comprar como tales pero también se puede configurar un sistema FreeBSD para crear nuestro propio AP wireless utilizando un determinado tipo de tarjetas wireless que poseen tales capacidades de configuración.

No basta con tener los dispositivos, estos deben ser configurados, y si la configuración se realiza efectivamente, se pueden aprovechar al máximo las capacidades de los mismos. Utilizando como hardware; dos computadoras, dos AP, una antena omnidireccional y una unidireccional, unos ejemplos de configuración son los siguientes:

- *Primera configuración:* Utilizando dos AP separados a unos 10 m de distancia para que emplearan las antenas internas con las que vienen estos dispositivos, que en condiciones normales son capaces de comunicarse hasta 120 m de distancia.

  En la configuración inicial de los AP se emplean las IP's con las que vienen predeterminadas de fábrica, se emplean dos hub's, dos computadoras y dos AP, cada computadora y cada AP se conectan a un hub. Una vez vista la funcionalidad se puede disponer del montaje de las antenas, una omnidireccional y una unidireccional, conectadas cada una a un AP.

  Inicialmente se pueden colocar los AP con una máscara de red que permita la comunicación de una sede a otra, esta configuración es realmente sencilla y no requiere ninguna modificación a ninguno de los elementos de la red con la que se cuenta, a parte de la configuración de los AP, esto se muestra en la figura 4.10.

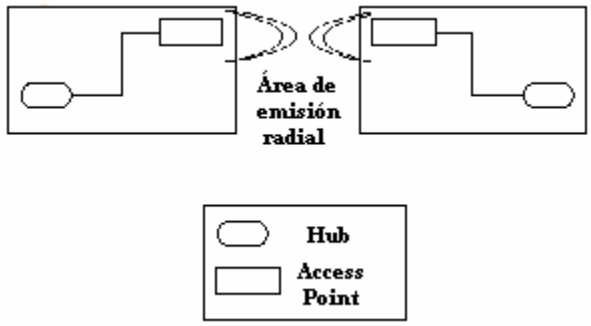


Figura 4.10 Primera configuración.

- *Segunda configuración:* Otra posible configuración que puede implementarse, es la ubicación de una computadora que hiciera las veces de un router entre una sede y otra, para colocar un segmento adicional que mantuviera a los dos AP por fuera de las dos redes, es decir, se requerirán dos computadoras, con

sus tarjetas de red respectivamente, es decir uno en cada sede para lograr este efecto, como se muestra en la figura 4.11.

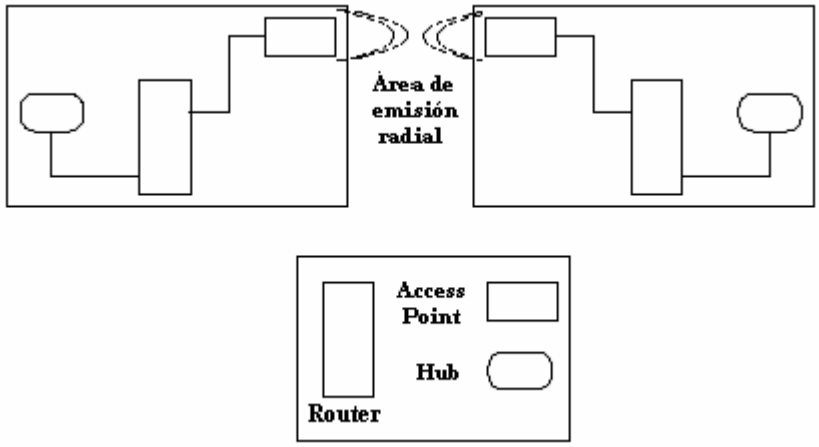


Figura 4.11 Segunda configuración.

- *Tercera configuración:* Finalmente se puede escoger la configuración de colocar una computadora para que hiciera las veces de un router en una de las sedes que contenga a un AP y en la otra sede una AP colocado directamente al hub, como se muestra en la figura 4.12.

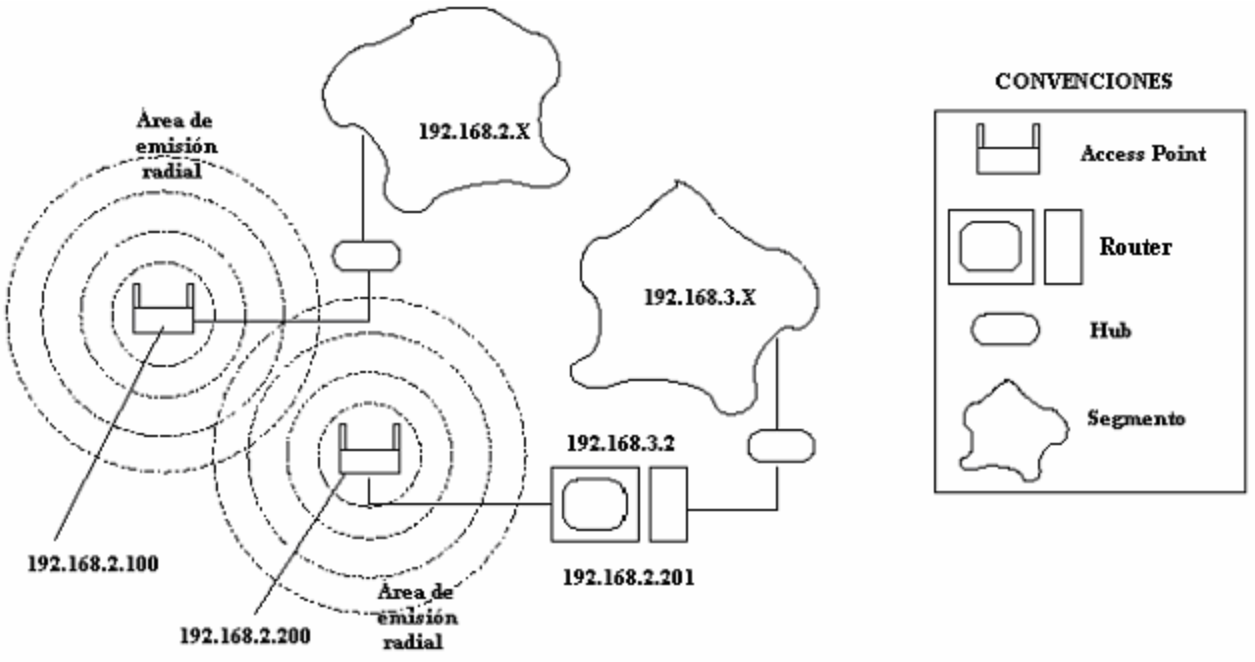


Figura 4.12 Tercera configuración.

En la figura 4.13 se muestra cómo estarían colocadas las antenas para que los ejemplos de las configuraciones antes mencionados tengan un buen funcionamiento.

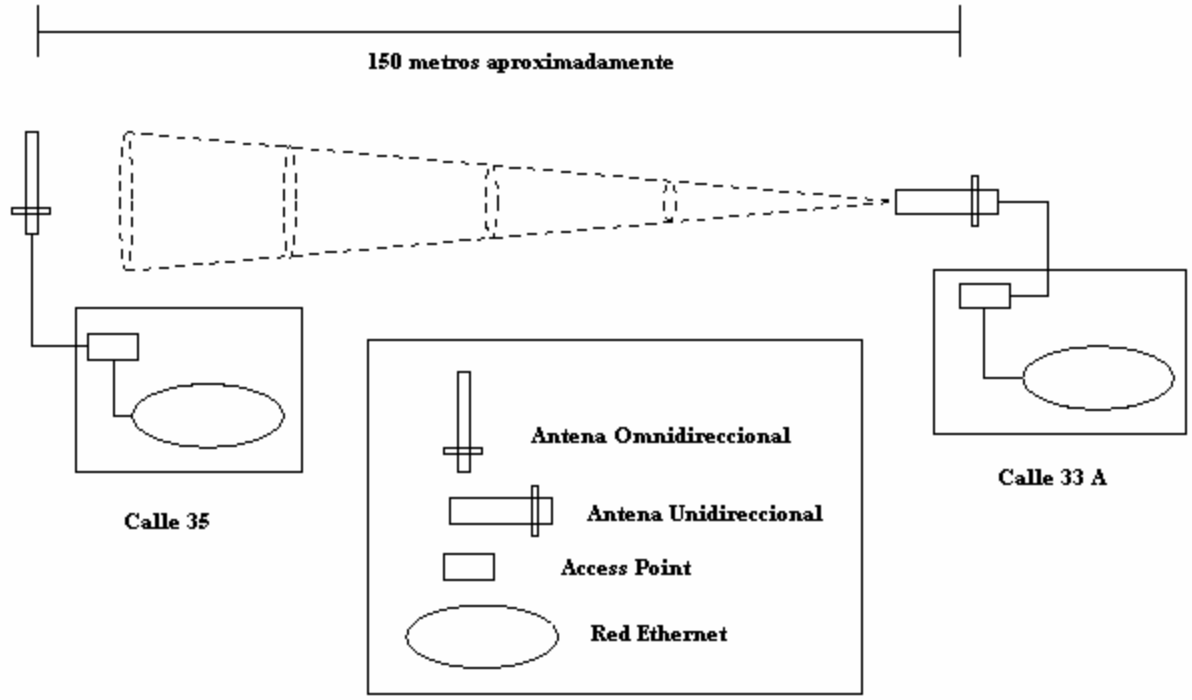


Figura 4.13 Ubicación de antenas.

4.1.3.1 Arquitectura de configuración de puntos de acceso

Existen diversos diseños de AP en el mercado, tanto en la forma física como en la arquitectura. La selección de la forma principal puede ser crítica en sus implementaciones, para el soporte, mantenimiento, costo general, seguridad y confiabilidad. Hay dos implementaciones arquitectónicas principales:

1. En la primera arquitectura, el AP tiene mucha capacidad de procesamiento y usa su inteligencia en el extremo de la red. Se conecta directamente a la red al mismo tiempo que un AP es independiente, que no depende de ningún servidor o controlador de red para mantener la conexión con los clientes inalámbricos. Cuando un AP falla solo ese AP queda afectado quedando operando todos los demás dispositivos, como se muestra en la figura 4.14.

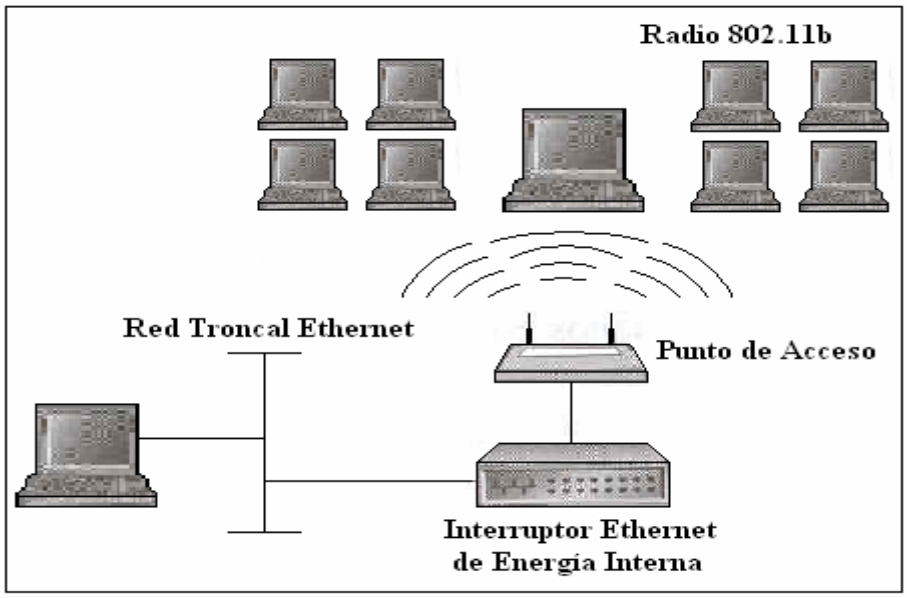


Figura 4.14 Primer arquitectura del AP.

En instalaciones grandes se requiere de un servidor de administración para que proporcione el soporte, configuración y administración. Los puntos de acceso inteligentes son muy sencillos de instalar.

2. La segunda arquitectura, se usan algunos AP con inteligencia pequeña y un controlador central, como lo muestra la figura 4.15.

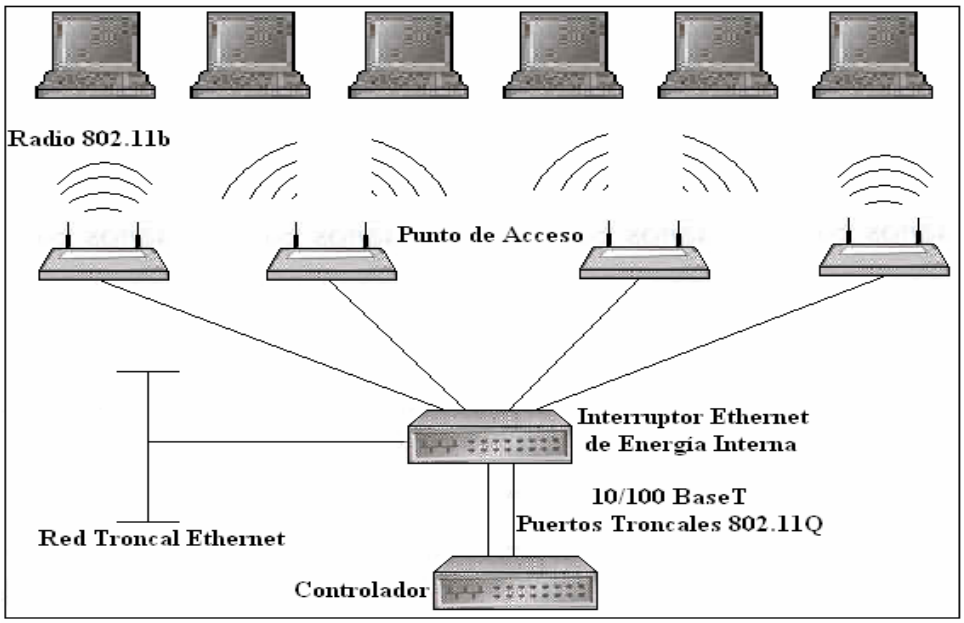


Figura 4.15 Segunda arquitectura de los AP.

En este sistema WLAN, la inteligencia no se emplea en el AP sino en un controlador central de red. En este tipo de sistema todo el tráfico fluye hacia el controlador, el cual administra la autentificación, seguridad, archivos de configuración,

etc. El problema que representa es que si existe un punto de falla en el controlador, cualquier AP que este enlazado con este controlador también falla.

La mayoría de los AP fueron diseñados para proporcionar soporte a una sola plataforma y radio, un radio por AP. Algunos están fabricados con ranuras PCMCIA duales de manera que también se pudiera operar un segundo radio, los cuales proporcionaban una ruta de migración de 900 MHz a 2.4 GHz, algunos fabricantes duplicaron el ancho de banda mediante el uso de radios iguales en el AP, lo cual provocaba un problema de insensibilización del receptor. La sensibilidad del receptor o umbral del receptor es la capacidad del receptor de “escuchar y entender” alguna fuerza de señal mínima. Este valor representa la señal mas baja que un receptor puede recibir y recobrar la información o datos de la señal.

Han aparecido en el mercado una variedad de AP de banda dual, diseñados para proporcionar soporte para 802.11b como para 802.11a de manera simultanea, esta arquitectura se puede usar para migrar de una tecnología a otra o para agregar ancho de banda. Los radios AP se ofrecen en distintas variedades, algunos son internos y no pueden acceder desde el exterior, esto significa que la antena también es interna lo cual implica una configuración mínima de antenas, en otros casos los radios se pueden conectar al AP lo que ofrece capacidad de actualización, sin embargo el estilo de la interfase del radio puede presentar dos problemas, uno debe tener la capacidad de estar asegurado al AP, segundo para la banda de 5 GHz, la selección de la antena es muy limitada (usos en interiores). Para 2.4 GHz, la tarjeta común es una PCMCIA, esto significa que las antenas externas tendrán que usar un cable o conector muy pequeño, provocando fallas probablemente. Si se desea usar antenas externas, se debe considerar un AP que utilice conectores de antenas TNC, SMA o N. Otro problema es la capacidad de actualización, si se desea un sistema que proporcione soporte para 802.11a y 802.11b, se debe considerar un AP que proporcione soporte para ambos dispositivos, esto mantiene bajos costos de instalación, además de costos de infraestructura cableada. Si se desea iniciar con 802.11b y después cambiar a 802.11g se debe verificar que el AP use una interfase Cardbus o mini-PCI en el radio, en lugar de una interfase PCMCIA y soporte actualizaciones hacia la tecnología que se desee.

Otra característica importante es la energía en línea que soportan muchos fabricantes, la cual puede ahorrar una cantidad enorme de los costos de instalación.

Algunos AP, pueden conectarse inalámbricamente con otro AP y funcionar como bridges entre dos redes diferentes, también puede amplificarse la señal de alguno o ambos AP empleando antenas externas.

4.1.3.2 Aspectos básicos de cobertura en los puntos de acceso

Para contar con una cobertura y seguridad en las redes inalámbricas, se toman en cuenta cinco aspectos importantes, los cuales son:

1. *Controlar el área de transmisión y cierres de todos los puntos de acceso:* Muchos puntos de acceso permiten ajustar el poder de su señal. Por esto se colocan los puntos de acceso lo más lejos posible de las paredes y ventanas exteriores, y probar el poder de la señal para que un usuario únicamente pueda conectarse en estos sitios. Luego asegurarse de cambiar la contraseña predeterminada en los puntos de acceso, utilizando una contraseña más segura para proteger a estos.
2. *Para tener compatibilidad (comprar hardware del mismo fabricante):* Mientras la norma IEEE tiene compatibilidad entre los dispositivos inalámbricos de diferentes fabricantes, las interpretaciones de las normas y las extensiones de propiedad exclusiva pueden impedir la integración total de estos dispositivos.
3. *Usar el SSID (Identificador de Aparatos de Servicio Inteligente):* Adquirir puntos de acceso que permitan deshabilitar la transmisión de los SSID para evitar que los puntos de acceso transmitan el nombre de la red y se asocie con clientes que no están configurados con su SSID. También cambiar un SSID predeterminado para el punto de acceso (y al mismo tiempo, cambiar la contraseña del administrador y el usuario predeterminado).
4. *Explorar con regularidad los puntos de acceso invasores:* Las tarjetas para las redes inalámbricas se pueden configurar como puntos de acceso y se requiere muy poco esfuerzo para convertir un equipo cliente en un punto de acceso invasor. Explorar con regularidad los puntos de acceso invasores en la red mediante el uso de herramientas de exploración inalámbrica.
5. *Usar autentificación de direcciones MAC:* Si se tiene un número administrable de usuarios y pocos puntos de acceso, la dirección MAC permite restringir los conexiones a sus puntos de acceso al especificar la única dirección de da cada dispositivo autorizado en una lista de control de acceso y al permitir únicamente aquellos dispositivos específicos que se conectan a la red inalámbrica.

4.2 CARACTERÍSTICAS

4.2.1 Características de puntos de acceso

Usando los puntos de acceso inalámbricos, los usuarios pueden comunicarse con las redes cableadas existentes. Existe una gran cantidad de fabricantes de hardware que distribuyen puntos de acceso y tarjetas de red wireless, aunque las capacidades de unos y otras varían, por ejemplo, se tiene el *Punto de acceso a red local inalámbrica Intel PRO/Wireless 2011B:*

Independientemente de que necesite ampliar el alcance de una red cableada o desplegar rápidamente una red local completamente inalámbrica, los puntos de acceso a la red proporcionan infraestructura de red fiable y fácil de instalar. La solución basada en los estándares de Intel es idónea para edificios antiguos, espacios de oficina alquilados, proyectos temporales y cualquier lugar donde la conectividad cableada resulte poco práctica o costosa. Este punto de acceso, que funciona como un hub inalámbrico, sirve

de conexión entre la red cableada de la que ya se disponga y los dispositivos inalámbricos. Los administradores pueden gestionar y controlar el rendimiento de la red de forma remota a través de un navegador Web. El punto de acceso a red local inalámbrica también ofrece una solución innovadora y rentable para conectar redes y funciona como repetidor para crear una estructura principal (backbone) inalámbrica que llegue a zonas de difícil acceso. Los puntos de acceso son fáciles de instalar y se suministran con una herramienta de inspección del emplazamiento que facilita su correcta colocación para obtener la cobertura y el rendimiento deseados.

- *Configuración local:* Puerto de consola directo.
- *Configuración remota:* HTTP, Telnet, SNMP, PPP, TFTP.
- *Número máximo de sistemas clientes:* 256 (se recomiendan otras).
- *Alcance a 1 Mbps (Típico):* 460 m en entorno abierto, 90 m en oficina.
- *Alcance a 11 Mbps (Típico):* 120 m en entorno abierto, 30 m en oficina.
- *Dimensiones:* longitud: 24,69 cm.; anchura: 18,34 cm.; altura: 4,85 cm.
- *Peso:* 0.454 Kg. (con fuente de alimentación).
- *Alimentación:* Entrada: 85 a 279 Vca; salida: 12 Vcc.

A continuación se muestra la tabla 4.1 con diferentes ejemplos de los puntos de acceso, donde se analizan sus características principales de alcance ó cobertura, protocolo, frecuencia y velocidad de transmisión, etc.

Fabricante y Dimensiones	Alcance de Transmisión y Recepción	Protocolo IEEE	Frecuencia de Transmisión GHz	Velocidad de Transmisión Mbps	Sistema operativo
3Com 320 x 200 x 70 mm	100 m 115 m	802.11a 802.11b		6 - 54 1 – 11	Windows ME, 2000, 98, 95 y NT 4.0.
ADAPTEC 151 x 151 x 25 mm	50 – 80 m 150 – 300 m	802.11b	2.4	11	Windows 98, 2000, ME y XP.
AVAYA 261 x 185 x 50 mm	15 m 40 m		2.4 5	11 54	Windows 98, 2000, ME y XP.
BENQ 172 x 130 x 26 mm	91.4 m 366 m	802.11a	5	54	Windows 98 SE, ME, 2000, XP (soporta NDIS5), Linux.
CISCO 183.7 x 166.7 x 42.2 mm		802.11a	5.15 – 5.35 5.15 – 5.25	54	
CNET 175 x 110 x 36 mm	30 m 100 m	802.11b	2.4 2.4835	10 100	Windows 95, 98, ME, NT, 2000, XP y Linux.

Tabla 4.1 Algunos ejemplos de puntos de acceso y sus características.

4.2.2 Características de antenas externas

Adicionalmente las antenas externas dependiendo de su especificación pueden tener distintas potencias, que eventualmente pueden emplear unos amplificadores de señal para maximizar su alcance. En la tabla 4.2 se muestran algunos modelos y características de antenas externas como ejemplos.

Direccionales		
Modelo	Potencia (Ganancia)	Distancia máxima teórica
COR-2400 EX	12 dBi	2 Km.
HG2419G	19 dBi	18 Km.
HG2424GC	24 dBi	26 Km.

Omnidireccionales		
Modelo	Potencia (Ganancia)	Distancia máxima teórica
AEO11	11 dBi	2 Km.
AEO13	13 dBi	3 Km.
HG2415U	15 dBi	5 Km.

Tabla 4.2 Ejemplos de modelos de antenas y su potencia.

Cabe mencionar que para el caso de los AP y las antenas externas existen muchas más marcas y modelos en el mercado, en este caso se tomaron las antes mencionadas ya que son las más conocidas.

Capítulo V

Configuración y Conectividad de Clientes

Tipo de hardware a utilizar
Características

Cada usuario individual de la red inalámbrica MAN tiene consigo un dispositivo para conectarse a la red este dispositivo puede ser por ejemplo una computadora portátil (LapTop), un asistente personal (Hand Help) o incluso se puede tratar de una computadora personal de escritorio, a cada usuario le corresponde una conexión especifica con respecto al equipo con el cual se desea conectar, y es aquí, en cada dispositivo, donde se deben de configurar las opciones (protocolos, direcciones, velocidad, login, password, etc.) necesarias, que dependen tanto del software (sistemas operativo) como hardware que se trate, para poder acceder a la red y sus recursos, dicho proceso lo llamaremos configuración en el caso del software y conectividad en el caso del adaptador de red (tarjeta de red) para nuestro dispositivo.

Llamaremos “cliente” al dispositivo con el cual nuestro usuario desea conectarse a la red de la empresa o institución, aunque éste puede variar en su forma en esencia conserva la misma funcionalidad del proceso de comunicación, enviar y recibir información. Depende del cliente el poder elegir un adecuado adaptador de red (conectividad), los adaptadores de red son las tarjetas que actúan como interfaz del cliente para que puedan comunicarse a una red inalámbrica. Los adaptadores de red son también conocidos como tarjetas de red, interfaz de red o NIC (Network Interface Cards).

Los adaptadores de red son esencialmente una estación de comunicación por radio que se encargan de la comunicación con otros adaptadores (modo Ad-Hoc) o con un punto de acceso (modo infraestructura). Para la selección de la tarjeta de red se debe de cumplir la compatibilidad con el cliente tanto física (Hardware) como de sistema operativo (Software). Posterior a esto comienza la configuración.

Hablamos del software cuando tenemos una determinada plataforma de sistema operativo a usar, si bien esta pude ser la más común en el mercado también puede ser la menos conocida, casos como Windows en sus diferentes versiones para sistemas operativos (dentro de los más conocidos) o UNIX en sus diferente versiones y/o distribuciones incluyendo a Linux. Por lo tanto el elegir la forma de conectividad del cliente se encuentra con la compatibilidad que guarda con la tarjeta de red y al mismo tiempo con nuestro sistema operativo que deberá soportar dicha tarjeta, criterio importante a tomar en cuenta al decidirse por un producto ya que la configuración correcta de nuestra tarjeta de red con respecto a nuestro cliente dependerá de la existencia e instalación de “Drivers” adecuados para el funcionamiento correcto y por lo tanto de la comunicación.

Si tomamos en cuenta que hoy en día el cliente más usado en los dispositivos móviles para intercambio de información empresarial son las LapTops, la figura 5.1 muestra la tendencia del uso de las LapTops en el mercado con respecto a la tecnología móvil, podemos pronosticar entonces que las tarjetas de red más comunes a usar son del tipo PCMCIA (las cuales se detallan más adelante) para la cuestión del hardware.

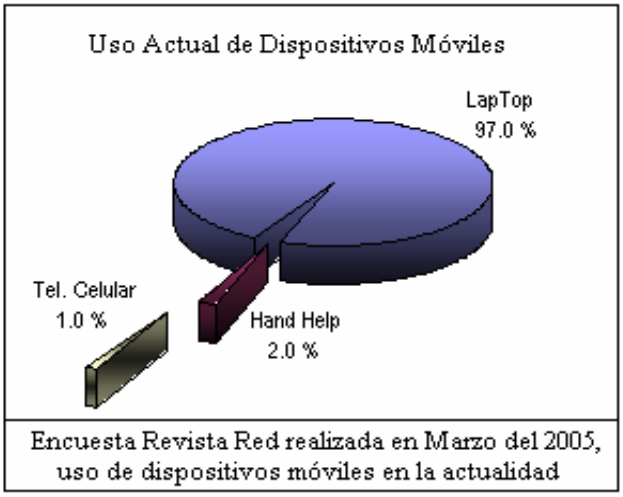


Figura 5.1 Uso actual de los dispositivos móviles.

Y por el lado del software podemos afirmar que el 98% de las LapTop's nuevas en el primer trimestre de este año tienen de fabrica precargado como sistema operativo Windows en su versión XP Home Edition, la figura 5.2 muestra lo antes mencionado.

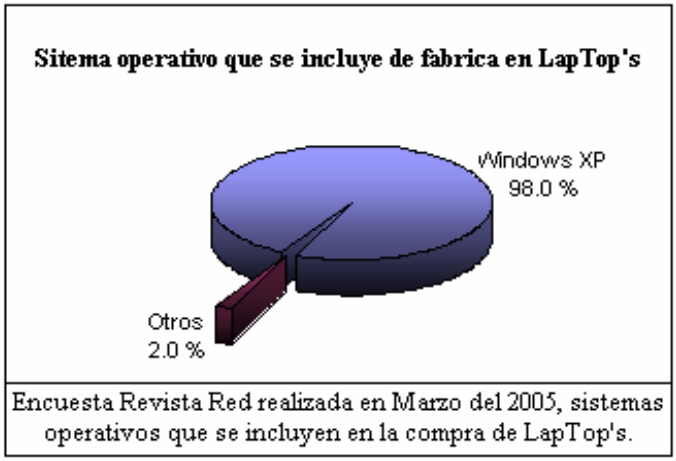


Figura 5.2 Sistemas Operativos incluidos en LapTop's.

Por lo tanto teniendo en cuenta que en lo general nos encontraremos con estos tipos de hardware y software en los clientes podemos hablar de un ejemplo de cómo se configura nuestra tarjeta de red, lo cual se describe a continuación.

Al insertar la tarjeta de comunicaciones, el sistema operativo Windows XP reconocerá un nuevo dispositivo wireless "LAN PC Card". El primer paso es actualizar el drive de este dispositivo de la siguiente forma:

1.- Desde "Mi PC", con el botón derecho del ratón, acceder a la ventana donde aparece la figura 5.3 y pulsar "Propiedades".



Figura 5.3 Propiedades de Mi PC.

2.- Aparecerá la pantalla propiedades del sistema, como se muestra en la figura 5.4.



Figura 5.4 Propiedades del sistema.

3.- En ella seleccionar la pantalla “Hardware” y aparecerá la pantalla que muestra la figura 5.5.



Figura 5.5 Pantalla de Hardware.

4.- Elegimos la opción “Administrador de dispositivos” aparecerá como en la figura 5.6.

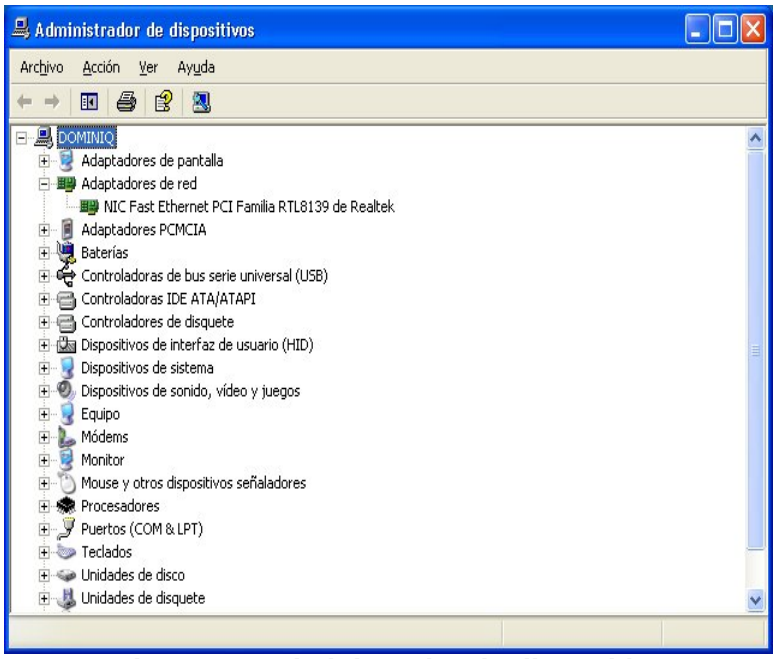


Figura 5.6 Administrador de dispositivos.

5.- Seleccionamos el adaptador de red inalámbrico “Tarjeta PC LAN” y sobre ella oprimimos botón derecho del Mouse, y seleccionamos “Actualizar dispositivo”, aparecerá como en la figura 5.7.

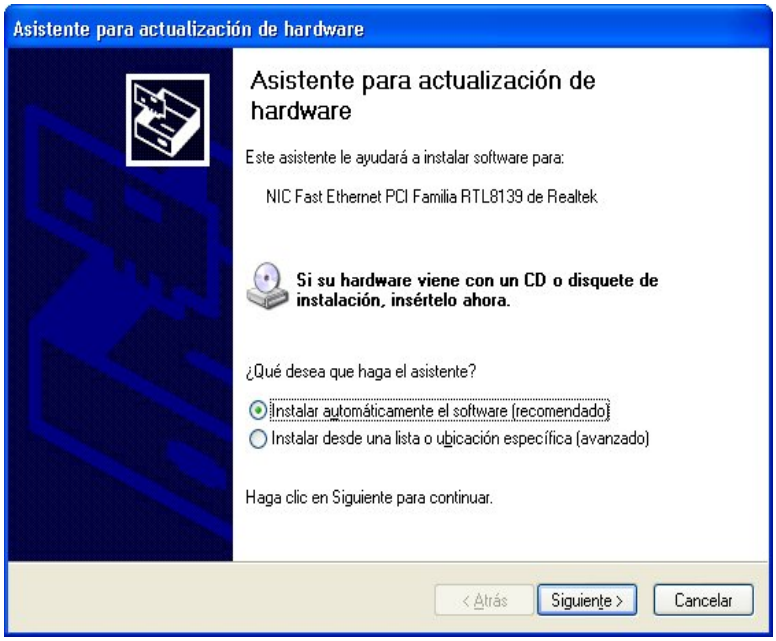


Figura 5.7 Actualizar dispositivos.

6.- Seleccionamos “Instalar desde una lista o ubicación específica (Avanzado)” pasaremos a una ventana como la mostrada en la figura 5.8.

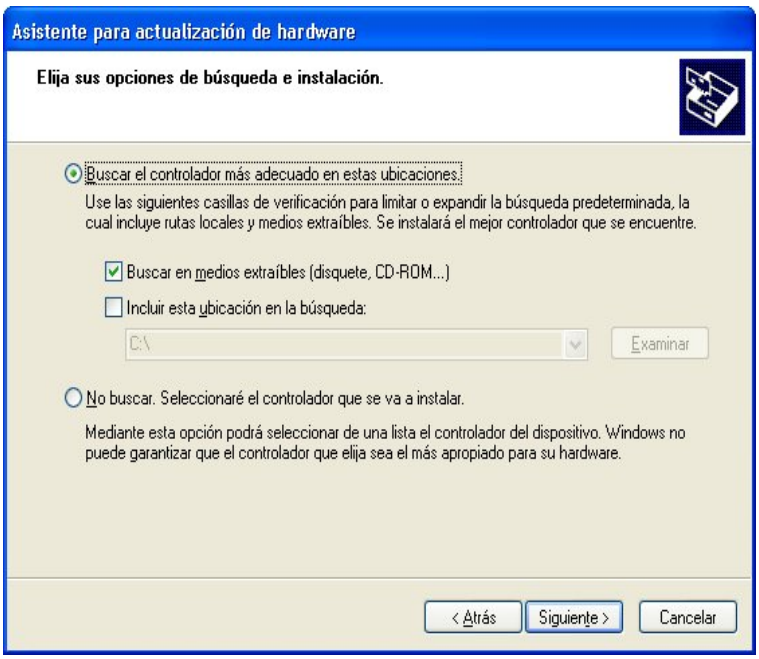


Figura 5.8 Asistente para actualización de hardware.

7.- Después de lo anterior pasaremos a una ventana como se muestra en la figura 5.9, donde se selecciona el adaptador de red.

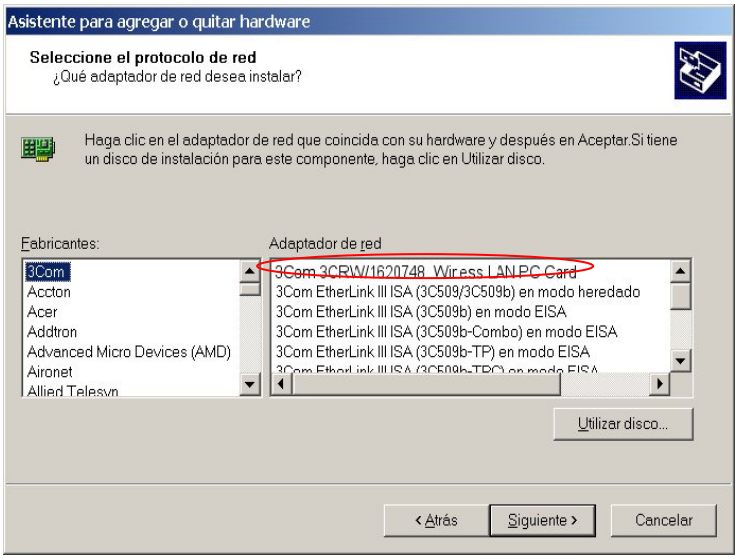


Figura 5.9 Selección del adaptador de red.

8.- En ella se especificará que nuestro adaptador de red es el señalado en la ventana y seleccionaremos “Utilizar disco”, como lo muestra la figura 5.10.



Figura 5.10 Instalación desde disco.

9.- En la ventana anterior seleccionaremos “Examinar” para ver el contenido del disco y poder elegir el controlador para la tarjeta y seleccionaremos abrir el archivo correspondiente, ver figura 5.11.

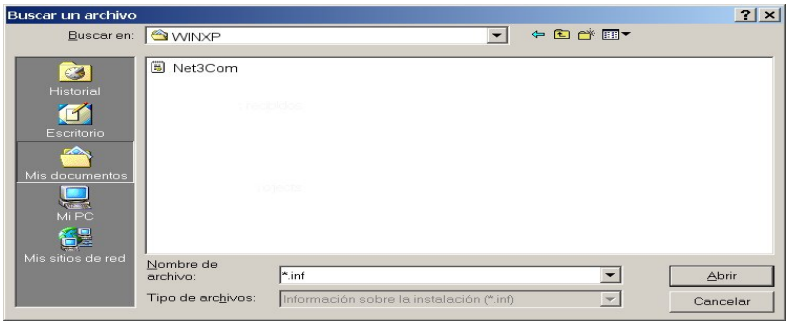


Figura 5.11 Elección del controlador requerido.

10.- Con esto queda instalado el controlador para nuestra tarjeta de red, aparecerá la siguiente ventana donde seleccionaremos “Finalizar”, como se muestra en la figura 5.12.

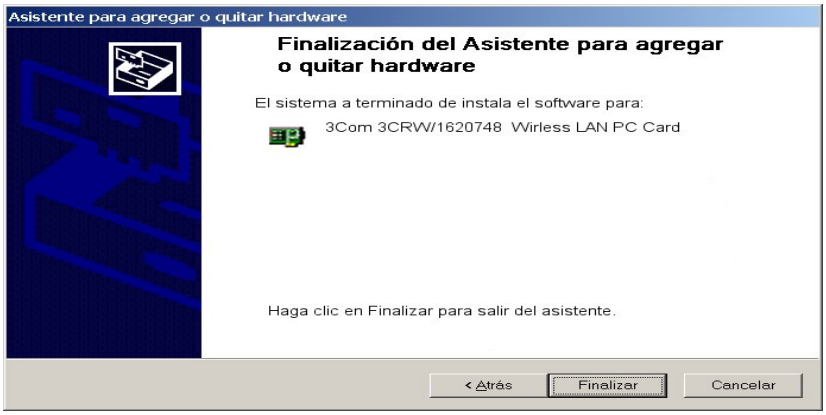


Figura 5.12 Finalización de instalación del hardware.

5.1 TIPO DE HARDWARE A UTILIZAR

Como se mencionó al comienzo de este capítulo el adaptador de red debe de ser de acuerdo al cliente que se trate, ya que se puede tratar de una Laptop, una computadora de escritorio e incluso un PDA (Personal Digital Assistant), de tal forma que encontramos aquí tarjetas inalámbricas de diferentes tipos, ya sea PCMCIA para el caso de Laptops, tarjetas USB o PCI para computadoras de escritorio y tarjetas Compact Flash para el caso de PDA, si bien la gama de tarjetas es mayor a las mencionadas podemos generalizar que las tarjetas PCMCIA son las más comunes por tratarse para uso de Laptops (computadoras portátiles) que ofrecen la movilidad para los usuarios y pueden aprovechar las flexibilidades que ofrece la red inalámbrica.

Tarjeta PCMCIA Estas tarjetas reciben su nombre del estándar PCMCIA (Personal Computer Memory Card International Association, asociación de la industria de fabricantes de hardware para computadoras portátiles encargada de la elaboración de estándares). Las tarjetas PCMCIA de 16 bits pueden recibir el nombre de PC Card y las de 32 bits el de CARD BUS, con el tamaño similar a las tarjetas de crédito y grosor de 3.3 mm para el tipo I utilizadas comúnmente para ampliaciones de memoria de 5 mm para el tipo II habitualmente para adaptadores de red inalámbricos y de 10.5 mm para el tipo III usadas por ejemplo para discos duros.

Tarjeta PCI Las tarjetas tipo PCI (Peripherial Components Interconnect, Interconexión de Componentes Periféricos) tienen la ventaja de ser más baratas que las PCMCIA y ser por lo regular del tipo Plug & Play de 32 bits pero con el mayor inconveniente que requieren ser instalados en el interior de la computadora de escritorio que por lo regular es un equipo que no tiene movilidad.

Tarjetas Compact Flash Se les conoce como clientes PDA a los asistentes personales reconocidos por que caben en la palma de la mano, debido a su pequeño tamaño

los PDA pueden llevarse en todo momento y a todo lugar, dentro de los adaptadores para este tipo de clientes se encuentra las tarjetas de red inalámbricas Compact Flash, parecidas a las tarjetas PCMCIA II que se adaptan a la ranura compact flash dentro del cliente con 3.3 mm de grosor.

5.2 CARACTERÍSTICAS

Tarjeta PCMCIA Las tarjetas PCMCIA suelen ser del tipo II con bus de 32 bits tipo Card Bus, como ejemplo se muestra la figura 5.13.



Figura 5.13 Tarjeta PCMCIA.

Características principales de una tarjeta PCMCIA marca D-Link DWL-AG650 Wireless.

- *Para tipo de dispositivo (cliente):* LapTop.
- *Compatibilidad S.O:* Windows 98, ME, 2000, XP.
- *Tipo de tarjeta:* PCMCIA.
- *Tipo de red inalámbrica:* 802.11a, 802.11b y 802.11g.
- *Velocidad de comunicación:* 54 Mbps.
- *Bandas de comunicación:* 2.4 Ghz y 45 Ghz.
- *Tecnología:* DSSS (Direct Sequence Spread Spectrum).

Tarjeta PCI Las tarjetas PCI tienen la ventaja de ser más baratas que las PCMCIA y ser por lo regular del tipo Plug & Play de 32 bits, como ejemplo se muestra las figura 5.14.



Figura 5.14 Tarjeta PCI.

Características principales de una tarjeta PCI marca D-Link DWL-AG510 Wireless.

- *Para tipo de dispositivo (cliente):* Escritorio.
- *Compatibilidad S.O:* Windows 95 OSR2, 98 SE, ME, NT, 2000, XP.
- *Tipo de tarjeta:* PCI.
- *Tipo de red inalámbrica:* 802.11a, 802.1x.
- *Velocidad de comunicación:* 11 Mbps.
- *Bandas de comunicación:* 2.4 Ghz.
- *Tecnología:* DSSS (Direct Sequence Spread Spectrum).

Otro tipo de tarjeta PCI son conocidas como adaptadores de red PCI tienen ventajas similares a las tarjetas PCI, como ejemplo se muestra la figura 5.15.



Figura 5.15 Adaptador de red PCI.

Características principales de un adaptador PCI.

- *Para tipo de cliente:* Escritorio (Desktop).
- *Compatibilidad S.O:* Windows 98SE, ME, 2000, XP.
- *Tipo de tarjeta:* PCI.
- *Tipo de red inalámbrica:* 802.11a, 802.11b, 802.11g.
- *Velocidad de comunicación:* 54 Mbps.
- *Bandas de comunicación:* 2.4 Ghz y 5 Ghz.

Tarjetas Compact Flash Las tarjetas Compact Flash, son muy parecidas a las tarjetas PCMCIA II, como ejemplo se muestra la figura 5.16.



Figura 5.16 Tarjeta Compact Flash.

Características principales de la tarjeta Compact Flash Tipo I inalámbrica marca D-Link compatible con Windows CE 3.0 para Pocket PC.

- *Para tipo de cliente:* PDA.
- *Compatibilidad S.O:* Windows CE ver 3.0.
- *Tipo de tarjeta:* Compact Flash.
- *Tipo de red inalámbrica:* 802.11b y 802.11g.
- *Velocidad de comunicación:* 11, 5.5, 2 o 1 Mbps.
- *Bandas de comunicación:* 2.4 Ghz.
- *Tecnología:* DSSS (Direct Sequence Spread Spectrum).

A medida en que la tecnología avanza seguramente encontraremos diferentes tipos de dispositivos móviles con diferentes características, y con su debida tarjeta de red correspondiente e incluso con su propio sistema operativo, he aquí el motivo de no poder globalizar en una sola configuración, o en una sola tarjeta de red de manera universal la selección, configuración y conectividad de los clientes, sin embargo podemos mencionar que el proceso de selección del hardware adecuado, compatibilidad del software y configuración en general son y serán pasos que se seguirán llevando a cabo como lo es hoy en día o hasta que un solo proveedor integre todo lo anterior.

Capítulo VI

Configuración y Conectividad de Servicios

Tipo de hardware
Características
Tipos de servicios

La configuración y conectividad de los servicios que se ofrecen en una red inalámbrica depende del hardware a utilizar, los AP (Puntos de Acceso), las tarjetas al cliente, antenas.

6.1 TIPO DE HARDWARE

Las redes inalámbricas están formadas por dos componentes esencialmente: puntos de acceso (AP) y Adaptadores de cliente tarjetas PCMCIA, PC, Puentes. Otro tipo de hardware a ocupar dependiendo la implementación a realizar es equipos de computo como servidores de punto de acceso para la administración. El tipo de hardware que se ocupa para una conexión punto a punto seria: una tarjeta PC para el cliente, una placa adaptador, un cable adaptador, una antena direccional, conectores. Sin embargo para una conexión punto a multipunto el hardware a ocupar es un access point, un cable adaptador, una antena omnidireccional, cables coaxiales y conectores esto es para el punto central para el remoto tarjeta PCCard, placa adaptador, cable adaptador, antena direccional, cables coaxiales y conectores. Los AP Access Point ofrecen servicios de autentificación a bajo nivel (MAC, DHCP, NAT).

6.2 CARACTERÍSTICAS

Arquitectura de IEEE 802.11 El componente elemental de una red inalámbrica es un conjunto básico de servicios (BSS, Basic Service Set), consiste en un número de estaciones ejecutando el mismo protocolo MAC y compitiendo por el acceso al mismo medio inalámbrico compartido. En la tabla 6.1 se muestra la terminología IEEE 802.11.

Punto de Acceso(AP)	Cualquier entidad que tenga la funcionalidad de una estación y proporcione acceso al sistema de distribución a través del medio inalámbrico a las estaciones asociadas.
Conjunto básico de servicios(BSS)	Conjunto de estaciones controladas por una sola función de coordinación.
Función de Coordinación	Función lógica que determina cuando una estación funciona dentro de un BSS tiene permiso para transmitir y puede recibir PDU.
Sistema de Distribución(DS)	Sistema utilizado para interconectar un conjunto de BSS y LAN integradas para crear un ESS.
Conjunto Extendido de servicios(ESS)	Conjunto de uno o mas BSS interconectados y LAN integradas que aparece como un único BSS en la capa LLC de cualquier estación asociada con uno de los BSS.
Unidad de datos del protocolo MAC(MPDU)	Unidad de datos intercambiada entre entidades MAC usando los servicios de la capa física.
Unidad de datos del servicio MAC (MSDU)	Información entregada como una unidad entre usuarios MAC.
Estación	Cualquier dispositivo que contenga capas físicas y MAC compatibles con IEEE 802.11.

Tabla 6.1 Terminología IEEE 802.11

Un BSS puede funcionar aisladamente o bien estar conectado a un sistema trocal de distribución (DS, Distribution System) a través de un punto de acceso (AP, Access Point) que efectúa las funciones de puente. El protocolo MAC puede ser completamente distribuido o bien estar controlado por una función central de coordinación ubicada en el punto de acceso. Un DS puede ser un conmutador, una red cableada u otra red inalámbrica.

La configuración más simple se muestra en la figura 6.1, en donde cada estación pertenece aun BSS aislado: cada estación se encuentra dentro del rango de otras estaciones que pertenecen al mismo BSS. La asociación entre una estación y un BSS es dinámica, puesto que una estación puede apagarse, salirse de la distancia máxima permitida o incorporarse de nuevo.

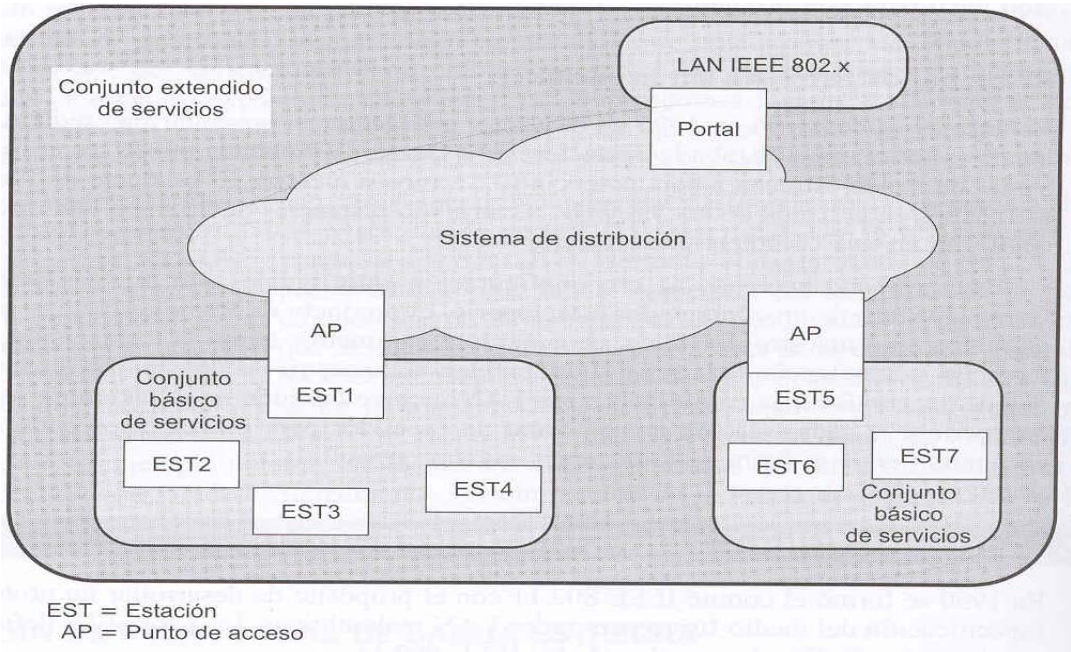


Figura 6.1 Arquitectura 802.11

Un conjunto extendido de servicios (ESS, Extended Service Set) consiste en dos o más conjuntos básicos de servicios interconectados mediante un sistema de distribución. Un sistema de distribución por lo general es una red cableada troncal o también puede ser cualquier red de comunicaciones. El conjunto extendido de servicios aparece a nivel de control de enlace lógico (LLC) como una única red lógica.

En la figura 6.1, se indica que un AP se implementa como parte de una estación. El AP constituye la lógica dentro de una estación que proporciona el acceso al DS a través de los servicios de distribución, además de servir como estación.

Arquitectura de IEEE 802.16 El estándar IEEE 802.16 WirelessMAN (Air Interface for Fixed Broadband Wireless Access Systems) define los niveles físico y de acceso al

medio, MAC para un acceso inalámbrico de banda ancha. 802.16 admite dos métodos de duplexión: en el dominio de la frecuencia y en el dominio del tiempo. En el primer caso se utilizan dos portadoras diferentes, una para el enlace ascendente y otra para el descendente, ambas de 28 MHz, mientras que en el segundo caso, ambos enlaces comparten una única portadora, con una anchura de canal de 28 MHz. En el capítulo II en la parte de estándar de redes inalámbricas de área metropolitana (802.16) se detalla más específicamente este tipo de arquitectura.

6.3 TIPOS DE SERVICIOS

Servicios IEEE 802.16 El estándar tiene definidos cuatro métodos de solicitud de reserva de ancho de banda, para cuatro tipos de servicio diferentes:

- *Servicio garantizado no solicitado:* La estación base asigna periódicamente espacio disponible en el enlace ascendente para cada conexión de este tipo que se haya establecido.
- *Servicio con sondeo en tiempo real:* Diseñado para el soporte de conexiones en tiempo real que generan paquetes de tamaño variable según intervalos de tiempo constantes.
- *Servicio con sondeo en tiempo diferido:* Diseñado para el soporte de conexiones que no presenta requisitos de tiempo real.
- *Servicio mejor esfuerzo:* Pensado para el tráfico de este tipo, como podría ser el acceso a Internet.

Servicios de IEEE 802.11 La normativa IEEE 802.11 define nueve servicios que debe ser proporcionado por una red inalámbrica para ofrecer una funcionalidad equivalente a la inherente a una red cableada tradicional. En la tabla 6.2 se muestran los servicios y se indican dos formas de categorizarlos.

Servicio	Proveedor	Usado para dar soporte a
Asociación	Sistema de Distribución	Entrega de MSDU
Autentificación	Estación	Acceso a la LAN y seguridad
Fin de la autentificación	Estación	Acceso a la LAN y seguridad
Disociación	Sistema de distribución	Entrega de MSDU
Distribución	Sistema de distribución	Entrega de MSDU
Integración	Sistema de distribución	Entrega de MSDU
Entrega de MSDU	Estación	Entrega de MSDU
Privacidad	Estación	Acceso a la LAN y seguridad
Reasociación	Sistema de distribución	Entrega de MSDU

Tabla 6.2 Servicios IEEE 802.11

1. El proveedor de servicios puede ser tanto la estación como el DS. Los servicios de la estación son implementados en cada estación IEEE 802.11, incluyendo la estación que constituye el AP. Los servicios de distribución son proporcionados

entre BSS diferentes y deben ser implementados en un AP o en cualquier otro dispositivo de propósito específico conectado al sistema de distribución.

2. Tres de los servicios enumerados se emplean para controlar el acceso a una red IEEE 802.11 y para proporcionar confidencialidad. Los seis servicios restantes dan soporte a la entrega de unidades de datos de servicio MAC (MSDU, MAC Service Data Units) entre estaciones. Un MSDU es un bloque de datos que el usuario MAC le pasa a la capa MAC, generalmente en la forma de una PDU LLC.

Distribución de mensajes dentro de un DS Hay dos servicios implicados en la distribución de mensajes dentro de un DS, estos son las distribución y la integración. La distribución es el servicio primario utilizado por las estaciones para intercambiar tramas MAC cuando la trama debe atravesar el DS para pasar de una estación en un BSS a otra estación en un BSS diferente. El servicio de integración permite la transferencia de datos entre una estación situada en una LAN IEEE 802.11 y otra estación en una LAN IEEE 802.1x que ese encuentre integrada con la primera, este servicio realiza la traducción de direcciones y cualquier otra conversión lógica requerida para el intercambio de datos.

Servicios relacionados con la asociación El principal objetivo de la capa MAC es la transferencia de MSDU entre entidades MAC. Este servicio puede llevar a cabo sus funciones, necesita disponer de información acerca de las estaciones que se encuentran dentro del ESS. Esta información es la proporcionada por los servicios relacionados con la asociación. Antes de que el servicio de distribución pueda entregar o aceptar datos de una estación, esta debe estar asociada. El estándar define tres tipos de transiciones basadas en la movilidad:

1. *Sin transición:* Una estación de este tipo es estacionaria o se desplaza únicamente dentro del rango de comunicación directa de las estaciones conectadas a un solo BSS.
2. *Transición BSS:* Se define como el desplazamiento de una estación desde un BSS hasta otro BSS de destino ubicado en el mismo ESS. La entrega de datos a la estación necesita que la función de direccionamiento sea capaz de reconocer la nueva localización de la estación.
3. *Transición ESS:* Se define como el desplazamiento de una estación desde un BSS ubicado en un determinado ESS hasta otro BSS perteneciente a un ESS diferente del primero.

Para entregar un mensaje dentro de un DS, el servicio de distribución necesita conocer donde se encuentra ubicada la estación de destino. El DS necesita conocer la identidad del AP al que el mensaje deberá ser entregado con objeto de que tal mensaje alcance la estación de destino. Una estación debe mantener una asociación con el AP dentro de su BSS actual, existen tres servicios vinculados con este requisito:

1. *Asociación:* Establece una asociación inicial entre una estación y un AP. La identidad y dirección de una estación deben conocerse antes de que la misma pueda transmitir o recibir tramas en una red inalámbrica.
2. *Reasociación:* Permite que una asociación previamente establecida sea transferida desde un AP hasta otro, haciendo así posible que una estación móvil pueda desplazarse desde un BSS hasta otro.
3. *Disociación:* Constituye una notificación, bien de una estación o bien por parte de un AP, de que una asociación existente deja de tener validez.

Servicios de acceso y privacidad Existen dos características de una red cableada que no son inherentes a una red inalámbrica:

1. Para poder transmitir sobre una red cableada, una estación debe estar físicamente conectada a la misma. Sin embargo, en el caso de una red inalámbrica, cualquier estación situada dentro de un rango similar al de otros dispositivos de la red puede transmitir.
2. Con objeto de recibir una transmisión desde una estación que forma parte de una red cableada, la estación receptora debe igualmente estar conectada al medio. En el caso de una red inalámbrica cualquier estación dentro del rango apropiado puede recibir. De esta forma, una red cableada proporciona cierto grado de privacidad, limitando la recepción de datos a aquellas estaciones conectadas a la red.

El estándar IEEE 802.11 define tres servicios que proporcionan estas dos características una red inalámbrica.

Autenticación: Es utilizada para que una estación pueda comunicar su identidad a otras estaciones. El servicio de autenticación es utilizado por las estaciones para establecer su identidad con otras con las que se desee comunicar. El estándar IEEE 802.11 da soporte a varios esquemas de autenticación y permite que la funcionalidad de los mismos pueda extenderse. El estándar no impone ningún esquema de autenticación concreto, que podría ir desde algún procedimiento inseguro hasta esquemas de cifrado de llave publica. El estándar IEEE 802.11 precisa de una autenticación correcta y aceptada mutuamente antes de que una estación pueda establecer una asociación con un AP.

Fin de la autenticación: Este servicio es invocado siempre que se vaya a dar por finalizada una autenticación existente.

Privacidad: Se utiliza para asegurar que los contenidos de los mensajes no sean leídos por alguien diferente al receptor legítimo. El estándar incluye el uso opcional de mecanismos de cifrado apara asegurar la privacidad.

Capítulo VII

Resultados

Comparación entre tecnologías de comunicación
Ventajas y desventajas de implementación
Guía de implementación para redes MAN

7.1 COMPARACIÓN ENTRE TECNOLOGÍAS DE COMUNICACIÓN

Existen varias tecnologías utilizadas en redes inalámbricas. El empleo de cada una de ellas depende de la aplicación.

El estándar 802.11 define varios métodos y tecnologías de transmisión para implantaciones de redes inalámbricas. Este estándar incluye varias técnicas de transmisión como:

- Espectro extendido con salto en frecuencia (FHSS).
- Espectro extendido en secuencia directa (DSSS).
- Multiplexión por división ortogonal de frecuencias (OFDM).
- Banda Ancha (BroadBand).

Espectro extendido con salto en frecuencia (FHSS) Utiliza una portadora de banda angosta que cambia la frecuencia en un patrón conocido tanto por el transmisor como por el receptor. Tanto transmisor como receptor están debidamente sincronizados comunicándose por un canal que está cambiado a cada momento en frecuencia de un modo rápido y continuo.

FHSS es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto, donde se tienen una cantidad de receptores diseminados en un área relativamente cercana al punto de acceso.

Espectro extendido en secuencia directa (DSSS) Genera un patrón de bits redundante para cada bit que sea transmitido. Este patrón de bit es llamado código chip. Entre más grande sea este chip, es más grande la probabilidad de que los datos originales puedan ser recuperados (pero, por supuesto se requerirá más ancho de banda). Más sin embargo si uno o mas bits son dañados durante la transmisión, técnicas estadísticas embebidas dentro del radio transmisor podrán recuperar la señal original sin necesidad de retransmisión. DSSS se utilizará comúnmente en aplicaciones punto a punto.

El inconveniente del DSSS en relación con el FHSS es que es más vulnerable a las interferencias de la banda estrecha. El intervalo de frecuencias se divide en 13 canales solapados, de 22 MHz de "anchura" cada uno.

Las ventajas del DSSS son:

- Permite mayores velocidades de datos (5.5 Mbps y 11 Mbps).
- La iteración es menos complicada en comparación con los sistemas FHSS, ya que éstos siempre transmiten en un único canal.

Inconvenientes del DSSS:

- En un área sólo pueden funcionar 3 sistemas de forma simultánea.

- Necesita componentes más rápidos y caros que los sistemas FHSS equivalentes.
- Más consumo y requisitos que los sistemas FHSS.

Multiplexión por división ortogonal de frecuencias (OFDM) Esta organización está basada básicamente en una tecnología patentada conocida como W-OFDM (Wide-Band Orthogonal Frecuency División Multiplexing).

En la OFDM, se usan múltiples frecuencias portadoras de la onda (o tonos) para dividir los datos a lo largo del espectro disponible, considerando que cada tono es ortogonal (independiente o sin relaciones) a los tonos adyacentes.

Dentro de las principales características de OFDM se encuentra la posibilidad de operar NLOS (Non Line Of Sight) es decir sin garantía de línea de vista real.

En segunda instancia, enlaces de mayores velocidades que las provistas por la red WipLL FHSS que operan en nuestros nodos.

Una diferencia importante entre OFDM, DSSS y FHSS es que cada uno de los canales envía energía en forma secuencial en FHSS y DSSS, dentro de OFDM, toda la energía se envía a lo largo de todos los canales al mismo tiempo. OFDM solo requiere de bandas de protección en torno a un conjunto de tonos, tiene una eficiencia espectral más alta.

Banda Ancha Un sistema de radio de banda angosta transmite y recibe información en un radio de frecuencia específica. La banda amplia mantiene la frecuencia de la señal de radio lo más angosta posible para pasar la información. El cruzamiento no deseado entre canales es evitado al coordinar cuidadosamente diferentes usuarios en diferentes canales de frecuencia. En un sistema de radio la privacidad y la no interferencia se incrementan por el uso de frecuencias separadas de radio. El radio receptor filtra todas aquellas frecuencias que no son de su competencia. La desventaja de esta tecnología es el uso amplio de frecuencias, uno para cada usuario, lo cual es impráctico si se tienen muchos usuarios.

Estándar 802.16 Introduce el equipamiento de acceso a banda ancha, cubre el rango de frecuencias de 2 a 11 GHz, donde la tecnología de red de área metropolitana (Wi-MAX) conecta hotspots basados en el estándar 802.11. Cubre 50 Km lineales y brinda conectividad de banda ancha, la velocidad de transmisión de datos llega hasta 70 Mbps.

El estándar 802.16 admite dos métodos de duplexión, en frecuencia y tiempo, en el dominio de frecuencia utiliza dos portadoras diferentes una para el enlace ascendente y otra para el descendente, ambas a 28 MHz, sin embargo para el tiempo ambos enlaces comparte una misma portadora con un canal de 28 MHz. En la tabla 7.1 se menciona la comparativa entre las tecnologías antes mencionadas.

TECNOLOGÍA	CARACTERÍSTICAS	VENTAJAS	DESVENTAJAS
Banda Ancha	• Frecuencia de 2 a 11 GHz. • Distancia que cubre 50 Km. • Transferencia de Datos 70 Mbps. • Número de usuarios son miles.	• Mayor cobertura. • Mayor velocidad de transmisión. • Seguridad en la transmisión de datos. • Punto a Punto o Punto a Multipunto.	• Costo. • Aun es un estándar nuevo lo cual todavía puede tener muchas variantes.
FHSS	• Frecuencia es de 2.4 GHz. • Transmite datos en portadoras que cambian en función del tiempo. • Distancia 100 m. • Transferencia de datos es de 11 Mbps a 55 Mbps. • Conexión de usuarios docenas.	• Alta tolerancia a interferencia. • Alta seguridad en la transmisión de la señal.	• Baja/Media velocidad. • Difícil sincronizar a larga distancia. • Difícil en arquitectura Punto a Multipunto.
DSSS	• Banda angosta dispersa sobre un amplio espectro. • Baja amplitud. • Frecuencia de 2.4 GHz. • Distancia 100 m. • Transferencia de Datos es de 11 Mbps a 55 Mbps. • Conexión de usuarios docenas.	• Alta velocidad. • Más resistencia contra la interferencia.	• Afectaciones por ruido y multitrayectorias. • Limite de velocidad.
OFDM	• Transmite señales simultáneas de alta velocidad. • Divide el espectro en varios sub-portadores. • Frecuencia de 2.4 GHz. • Distancia 100 m. • Transferencia de Datos es de 11 Mbps a 55 Mbps. • Conexión de usuarios docenas.	• Alta eficiencia espectral. • Alta velocidad de transmisión. • No requiere retransmisión de datos.	• Costo. • Requiere mayor capacidad de procesamiento.

Tabla 7.1 Comparativa entre tecnologías.

Podemos concluir que cada una de estas tecnologías en general tienen ventajas que para otra pueden ser desventajas, el elegir un tipo de tecnología va a depender de la implementación que se desee realizar para una red WMAN, así como de todos los factores que influyen en dicha implementación, como son: la conectividad, la escalabilidad, la confiabilidad, la seguridad, la compatibilidad, el costo, la cobertura, la velocidad, la instalación, etc. Un aspecto muy importante que se debe considerar es el requerimiento que tenga una empresa donde se desee implementar la red, así como las

razones por las cuales se va a implementar, donde se tendrán que evaluar todos los factores anteriormente mencionados. Por ejemplo, veamos la figura 7.1.

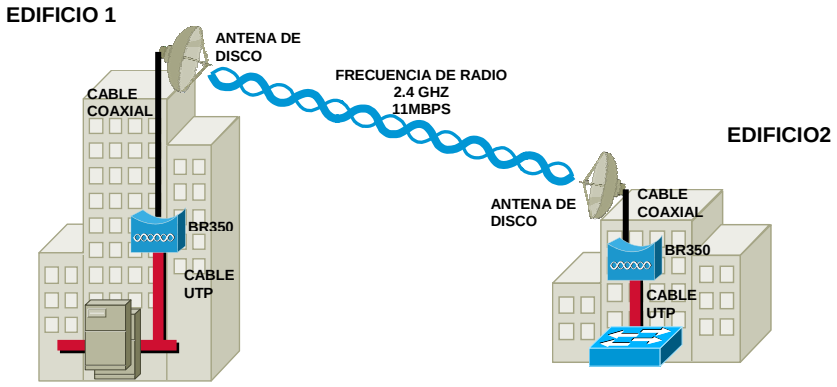


Figura 7.1 Ejemplo de una red WMAN.

Si se desea implementar la conexión entre dos edificios donde la distancia entre ellos es de 14 Km, si analizamos la tecnología a ocupar de acuerdo a la tabla anterior se ocuparía Banda Ancha, con una conexión Punto a Punto, la cual nos proporcionaría una mayor cobertura, alta velocidad de transmisión, seguridad en la transmisión. Sin embargo si la distancia es menor a 100 m, se puede ocupar otro tipo de tecnología ya sea la OFDM, DSSS o FHSS, las cuales tiene menor cobertura.

7.2 VENTAJAS Y DESVENTAJAS DE IMPLEMENTACIÓN

Actualmente las empresas tiene necesidad de instalar una red inalámbrica con el fin de poder interconectar computadoras o dispositivos móviles para así consultar y/o transferir la información de un dispositivo a otros situados en lugares diferentes en cada momento, es decir que tienen movilidad dentro de un área metropolitana. Para cada empresa existen algunas ventajas o desventajas en la instalación de una red de tipo WMAN lo cual se puede traducir que lo que para unos es ventaja para otros representa una desventaja, todo depende de las razones, requisitos, políticas y seguridad que requiera cada empresa.

7.2.1 Razones de implementación

Las siguientes razones que se deben de tener en cuenta en la planeación de una implementación, son las propuestas en este trabajo como las que generalmente debemos de considerar y resolver para cada caso individual que pueda presentarse si esta representa una ventaja o desventaja en la toma de nuestra decisión.

Tiempo de instalación Hablamos de tiempo de instalación a aquellas acciones y/o procesos en los cuales se requiere seguir o esperar de su cumplimiento para obtener una parte o la totalidad de la red instalada, este tiempo de instalación se

puede dividir en: la instalación de los servicios, la instalación de cada antena de comunicación o en la conectividad y configuración de los clientes.

Debemos de tener en cuenta que el principal tiempo de instalación en una red cableada es el tendido de cables y modificaciones de la estructura de las edificaciones por donde esta pasará en tanto que para una red inalámbrica bastará con un estudio previo de cobertura y la puesta de antenas sobre los edificios teniendo mínimos cambios con la infraestructura actual.

Movilidad La movilidad la podemos encontrar en aquella demanda que pide la operación de la empresa a través del desplazamiento de nuestros clientes y/o en aquellas aplicaciones que requieren ser en un tiempo real ya sea consultadas o actualizadas. El identificar la ubicación y lejanía de los clientes frecuentes o clientes importantes así como la información necesaria para operar la empresa con los clientes son motivos los cuales impulsan la valuación de esta razón.

Costo El costo se basa en la comparación de llevar a cabo dos o mas acciones, teniendo en mente el beneficio que una u otra pueden tener, por ejemplo: si para conectar dos edificios lejanos mediante una red cableada del tipo MAN representaría un alto costo, tiempo y molestias, ya que se tendría que pasar por varios edificios, zonas transitadas o con diversos obstáculos. Es por tal motivo que a una empresa le conviene una red WMAN porque su instalación es más factible o cuando se quieren hacer cambios en la infraestructura de la red, las redes inalámbricas tienen una marcada ventaja porque solo necesitan instalar otra celda inalámbrica o añadir un cliente inalámbrico. En una red cableada no es posible hacerlo de una manera fácil porque se debe tomar en cuenta varios parámetros como, puertos libres en el *patch panel*, puertos libres en los *hub's* y distancia del *patch panel* hasta el punto de red que se desea instalar. Este tipo de elecciones dependerán de la relación costo y beneficio que se tenga en ese momento.

También influyen factores como: el tiempo, costo del equipo, cambios en la infraestructura, seguridad, cobertura y crecimiento a futuro, etc.

Instalación en lugares de difícil acceso Cada lugar a comunicar tiene características geográficas y demográficas individuales que en ocasiones no permiten una instalación cómoda o práctica, para cada caso, si bien en una red inalámbrica puede solo necesitarse de una línea de vista se debe además asegurar que exista la infraestructura y seguridad para la instalación de la antena que dará la comunicación. Conocer el terreno y tener un estudio de cobertura de nuestra red a implementar nos indicará con que prioridad debe ser considerado este punto.

Escalabilidad La escalabilidad es la facilidad con la cual nuestra red puede crecer si bien en cobertura también en el soporte del número de clientes, cada equipo que incluiremos en la implementación tiene especificaciones de compatibilidad con algún otro equipo y de crecimiento de clientes que pueden conectarse simultáneamente, por lo tanto el saber el crecimiento tanto en número de clientes

como en distancias necesarias a cubrir en planes futuros dan el peso necesario para que esta razón sea evaluada y considerada.

Flexibilidad En todo momento la empresa puede tender a cambiar las políticas o reglas de conexión con la misma infraestructura o tal vez realizar conexiones con clientes con los cuales se este trabajando conjuntamente o por cambios en el personal que laboran en la actualidad, estos cambios implican tener la facilidad de llevarse a cabo o adaptarse a ellos sin necesidad de una re-implementación de nuestra red, así por ejemplo en una topología tipo maya de cuatro nodos podemos tener la posibilidad de implementar dos redes punto a punto que permitan a aplicaciones con alta demanda disponer de los recursos sin tener más información que la necesaria para la comunicación.

Saturación del medio (Interferencia) La interferencia de una señal la conocemos como aquellas señales que se encuentran en el medio y que no son parte de nuestra comunicación, en zonas donde ya existan comunicaciones inalámbricas es de vital importancia el tener este punto en cuenta para saber si se tiene como ventaja o desventaja, no olvidemos que las frecuencias de 2.5 y 3.5 GHz no requieren licencia para transmitir lo cual es aprovechado por particulares o empresas dando como resultado una saturación del medio bajando con esto el rendimiento de nuestra comunicación.

Seguridad Es de suma importancia tener presente que tipo de seguridad podemos tener en todo tipo de intercambio de información, si bien no existe seguridad absoluta que dure de por vida si existen las mínimas medidas que deben de llevarse a cabo para que no cualquiera pueda tener la posibilidad de obtener nuestra información. La codificación de datos o complejidad de algoritmos de transmisión nos dan la seguridad de que la información se encontrará protegida y solo será usada por el receptor que deseamos, cada producto para una red de este tipo menciona que tipo de seguridad es incluida y su debida especificación, comparación que se debe de hacer entre más de dos productos similares para poder seleccionar aquel que se adecue a nuestro proyecto.

A pesar de ser nombradas en el orden anterior estas razones de implementación no se debe de considerar con el mismo grado de importancia o como un orden absoluto para cualquier implementación ya que cada caso de implementación determinará que prioridad y peso se le da a cada una obteniendo cual se convertirá en una ventaja o desventaja de gran peso.

7.2.2 Requisitos de implementación

El usuario debe contar con el equipo necesario para conectarse a la red, ya sea a través de una computadora, PDA, NoteBook, Pocket PC u otro dispositivo similar los cuales deben contar con la tecnología necesaria para realizar una conexión inalámbrica.

En la actualidad la gran mayoría de los equipos nuevos llevan integradas esta tecnología, pero para el caso de la mayoría de los potenciales usuarios del sistema que no cuenten con equipos de última tecnología, existe la disponibilidad de tarjetas externas de fácil instalación que funcionan a través de las ranuras PCMCIA.

Por otro lado el sistema debe contar con Access Point de tecnología inalámbrica que permita conectar a los usuarios en cualquier punto. El número de estos equipos necesarios en cada zona dependerá mucho de la infraestructura y la dificultad de propagación de las señales necesarias para la conexión inalámbrica.

Un requerimiento importante para que esta tecnología sea un real aporte a la conectividad es que la conexión sea rápida, es decir, que en horarios pico puedan alcanzarse velocidades razonables; cómoda, con señal suficiente en los puntos importantes para no sufrir problemas de conexión; y seguridad, donde los usuarios estén relativamente libres de ataques indeseados u otro tipo de problema de seguridad.

Una red de computadoras está conectada tanto por hardware como por software. El hardware incluye tanto las antenas, tarjetas de red, los puntos de acceso, los clientes móviles, etc. y el software incluye los programas que se utilizan para administrar los dispositivos, el sistema operativo. Los tipos de conexiones son muchos y se pueden combinar entre ellos haciéndolos muy flexibles, las más importantes o las más comunes son las conexiones punto a punto y punto a multipunto. En la figura 7.2 se muestra una red inalámbrica con los elementos que intervienen en esta, en donde se pueden identificar los requisitos necesarios de la implementación.

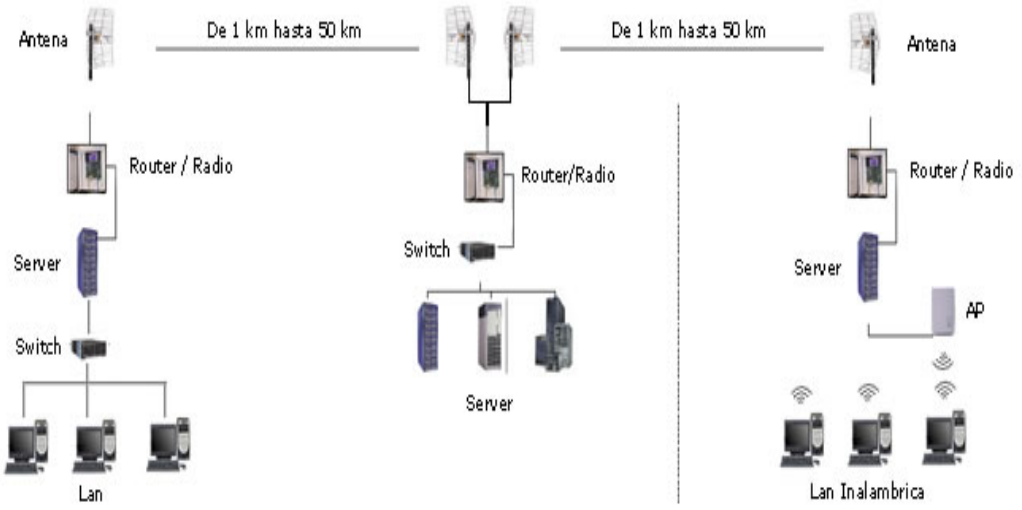


Figura 7.2 Red inalámbrica.

Para implementar una red inalámbrica se requiere de los siguientes requisitos:

- *Antenas:* El uso de antenas es imprescindible si se quiere ofrecer un servicio de calidad en un radio aceptable. Además, la interconexión entre nodos distantes requerirá el uso de las mismas. De la teoría de antenas sabemos que

dependiendo de la zona de cobertura que queramos establecer, se necesita un tipo de antena diferente: omnidireccional o direccional.

La distancia depende de la antena utilizada (y eventualmente de un amplificador):

- De 2 a 300 metros con una antena omnidireccional.
- De 1 Km con una direccional.
- De 2 a 3 Km con una omnidireccional amplificada (200mW).
- Algunos Km con una antena parabólica.
- De 50 a 60 Km con una antena parabólica o direccional amplificada (algunos watios).

Hay que tener en cuenta que la amplificación puede violar las especificaciones FCC y otras leyes locales, por lo que hay que procurar tener información concisa sobre la legislación vigente. En la tabla 7.2 tenemos las características de antenas con sus diferentes tipos.

ANTENAS			
TIPO	**MODELO**	**GANANCIA**	**DISTANCIA MÁXIMA TEORICA**
Omnidireccional	HG2415U	15 dBi	5 Km.
Omnidireccional	AEO13	13 dBi	3 Km.
Omnidireccional	AEO11	11 dBi	2 Km.
Omnidireccional	HG2415U-PRO	15 dBi	2 Km.
Omnidireccional	HG2412U	12 dBi	1.5 Km.
Direccionales	HG2424GC	24 dBi	26 Km.
Direccionales	HG2419G	19 dBi	18 Km
Direccionales	HG2430D	30 dBi	16 Km.
Direccionales	HG5829D	29 dBi	15 Km.
Direccionales	HG2424G	24 dBi	12 Km.
Direccionales	COR-2400 EX	12 dBi	2 Km.

Tabla 7.2 Características de antenas.

Algunos ejemplos de este tipo de antenas se muestran en los anexos en la parte de catálogo de antenas.

- *Access Point:* El Access Point (AP), es el elemento más importante de la red, sus características deben ser:

  - ✓ Centralizar todas las conexiones de la red.
  - ✓ Encargarse de administrar todos los accesos de las diferentes computadoras que se encuentran en la red.
  - ✓ Asignar direcciones IP (Internet Protocol) a cada una de las computadoras de la red.
  - ✓ De preferencia contener Software de seguridad (Firewall) para evitar que intrusos puedan penetrar en la red.

- ✓ Tener la misma función de un Switch, excepto que no utiliza cables.
- ✓ Incluir de preferencia puertos RJ45 10/100 para conectar aquellas computadoras que no requieran un acceso sin cables.
- ✓ Contar con velocidad de transmisión y recepción desde 11 hasta 54 Mbps.
- ✓ Tener un alcance de varios Kms (por medio de repetidores).
- ✓ Tener beneficios adicionales como:

    - o Capacidades de router entre distintas redes.
    - o Seguridad en el trasporte de información.
    - o Permitir que una conexión de Internet sea compartida con todas las computadoras de la red.

- ✓ Ser compatibles con la tecnología Wi-Fi.

En la tabla 4.2 del Capítulo IV se observan algunas características de AP y algunos ejemplos de este tipo de AP se muestran en los anexos en la parte de catálogo de AP.

- *Tarjetas de red:* Las tarjetas de red se utilizan en PC's de escritorio como en las LapTops. Sus características deben ser:

    - ✓ Establecer la comunicación con el Access Point.
    - ✓ Funcionar a velocidades de 11 a 54 Mbps.
    - ✓ Ser compatible con redes cableadas, para ser posible la comunicación entre ellas.
    - ✓ Poder acceder a más de un AP con la misma tarjeta.
    - ✓ Ser compatibles en su mayoría con Wi-Fi.

En la tabla 7.3 se muestran algunos ejemplos de tarjetas de red.

TARJETAS DE RED				
Modelo	**Protocolo IEEE**	**Frecuencia de Transmisión GHz**	**Velocidad de Transmisión Mbps**	**Sistema operativo**
Tarjeta PCI WMP55AG	802.11a 802.11b	5 2.4	54	Windows ME, 2000, 98 y XP
Tarjeta PCI WMP54GS	802.11g	2.4	54	Windows 98, 2000, ME y XP
Tarjeta PCI WMP54G	802.11g	2.4	54	Windows 98, 2000, ME y XP
Tarjeta PCMCIA WPC55AG	802.11a 802.11g	5 2.4	54 54	Windows 98, 2000, ME y XP
Tarjeta PCMCIA WPC54GS	802.11g	2.4	54	Windows 98, 2000, ME y XP
Tarjeta PCMCIA WPC11	802.11b	2.4	11	Windows 98, 2000, ME y XP

Adaptador USB WUSB544AG	802.11a 802.11b	5 2.4	54 54	Windows 98, ME, 2000 y XP
Adaptador USB WUSB54G	802.11g	2.4	54	Windows 98, ME, 2000 y XP
Adaptador USB WUSB12	802.11b	2.4	11	Windows 98, 2000, ME y XP
Adaptador USB USBBT100	802.11b	2.4	11	Windows 98, 2000, ME y XP

Tabla 7.3 Características de tarjeta de red.

Algunos ejemplos de este tipo de tarjetas de red inalámbricas se muestran en los anexos en la parte de catálogo de tarjetas de red inalámbricas.

7.2.3 Seguridad en redes inalámbricas

Durante el estudio y evaluación de la implementación de una red inalámbrica la seguridad en estas redes es una necesidad, dadas las características de la información que por ellas se transmiten. Existen diversos métodos para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red. Los diversos métodos son los siguientes:

- *Método 1, MAC:* Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso.
- *Método 2, WEP:* El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado.
- *Método 3, VPN:* Este método resulta especialmente atractivo para proteger redes inalámbricas, debido a que funciona sobre cualquier tipo de hardware inalámbrico y supera las limitaciones del método WEP.
- *Método 4, 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.
- *Método 5, WPA:* Este estándar busca subsanar los problemas del método WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

En conclusión, la restricción de acceso mediante direcciones MAC es insuficiente para cualquier red, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta inalámbrica cualquiera.

El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso del WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

El uso del método VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

La alternativa del método 802.1x y EAP es la adecuada si los equipos de la red inalámbrica se pueden actualizar, o si se va a montar una red nueva. Puede usarse la solución de WEP con clave dinámica, o la de WPA; ambas ofrecen un excelente grado de protección.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de las empresas.

7.3 GUÍA DE IMPLEMENTACIÓN PARA REDES WMAN

El contar en cualquier proyecto con las referencias necesarias, ya sea manuales de procesos, técnicos, manuales técnicos, de administración o algunos otros son referencias básicas y necesarias para conducirnos en las diferentes etapas que nos lleve al objetivo final, ya sea durante el inicio, desarrollo, finalización y mantenimiento del proyecto.

Sin embargo al contar también con un documento conciso, sencillo en interpretación y sencillo en manejo, nos ayuda no a sustituir los documentos bases, sino a ser prácticos y objetivos y más aún cuando nuestro proyecto requiere de un tiempo de respuesta rápido y efectivo, por lo tanto si se tienen concentrados aquellos pasos o procesos a llevar a cabo durante la ejecución de un proyecto bastará con seguirlos o comprobar su realización de lo descrito en cada uno (de forma explicita o de forma implícita). Si bien un documento de este tipo no funge como un manual de implementación o de procedimientos en donde se puedan encontrar todas las respuestas si puede plantear en que punto se detiene o en que punto se encuentra el desarrollo de nuestro proyecto así como cual será la secuencia a seguir. Podemos plantear como ejemplo la realización de un programa de facturación, algo como lo siguiente sería la lista de pasos:

1. Levantamiento de requerimientos.
2. Selección del lenguaje.
3. Selección de la Base de Datos (BD).
4. Diagrama ER (Entidad-Relación) de la BD.
5. Diagrama de programación.
6. Construcción de BD y programación.
7. Pruebas betas.
8. Implantación.

9. Pruebas finales de campo.

En este ejemplo podemos ver una serie de nueve puntos que describen una serie de pasos necesarios que involucra el proyecto, no menciona como deben de tomarse los requerimientos o que hacer con estos, ni para que tipo de plataforma se toma el lenguaje y la Base de Datos, es más ni como serán las pruebas ni cuando y esto es debido a que el conjunto de procesos para cada paso se encuentra implícito en cada punto mencionado o asentado y se dirige a aquellos proyectos que guardan la relación y enfoque del objetivo con que se hizo la lista, en este caso para la realización de algún otro software puede ser aplicada la lista.

Estos pasos son generales y pueden ser aplicados a más de un caso relacionado con el tema, este ejemplo pertenece al tipo de documentos que se conoce como *Lista de Revisión o "Check List"*, donde el cumplimiento de cada paso queda en manos del responsable el cual palomea o indica por medio de una marca cada punto o paso realizado y continua hasta el final para cumplir con el resto del proyecto.

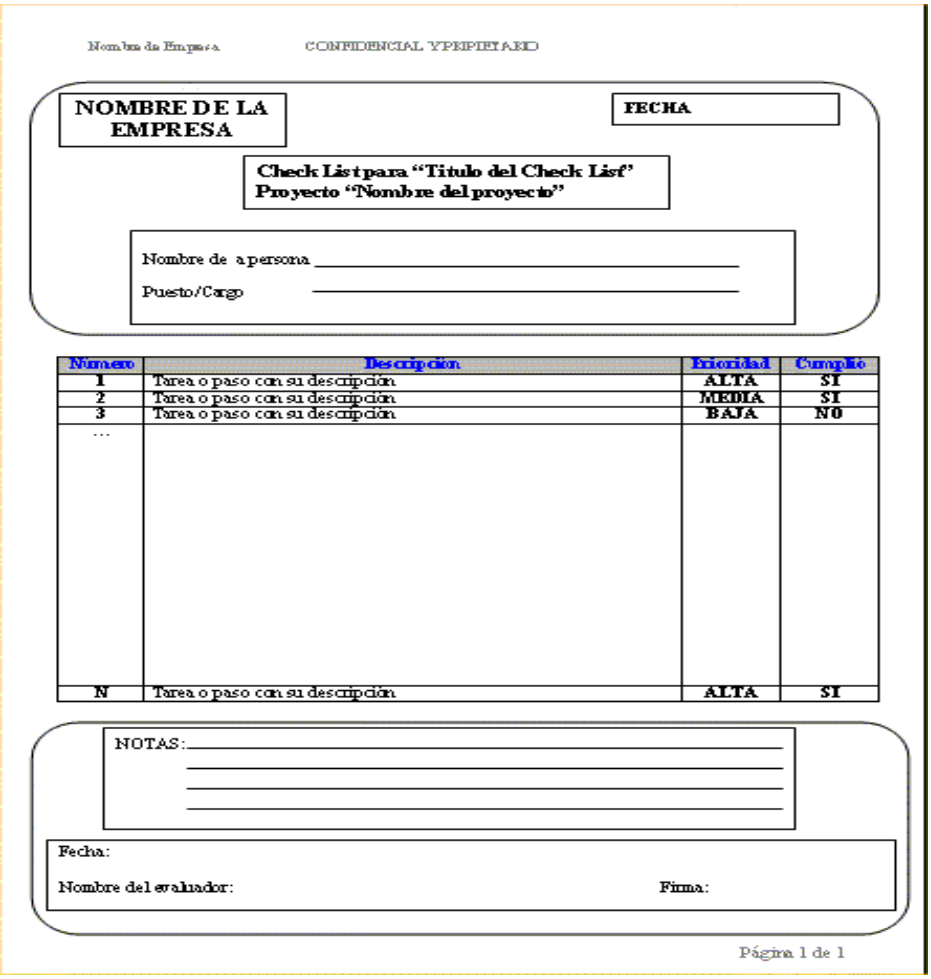
El check list es usado principalmente en el campo técnico, debido a que cada paso puede ser separado y definido individualmente con sus componentes (cada punto puede tener su propio check list), en nuestro caso usaremos el check list como una guía de implementación ya que si bien mencionará los pasos necesarios en cada proceso de la implementación de una red WMAN no hará referencia al uso especifico de dispositivos o herramientas de software o de telecomunicaciones a emplear, ya sean marcas o características, estás se dejarán abiertas al diseñador o al conjunto de personas responsables de implementar la red así como también la tecnología con la que se cuente en ese momento.

7.3.1 ¿Qué es un Check List?

Es el documento que nos ayuda a través de una serie de sentencias tipo pregunta o de sentencia simplemente para seguir el camino necesario de un proyecto haciendo que cada paso o tarea sea cumplido (palomeado) cuando se tengan los elementos suficientes (componentes de cada paso) que indiquen que se a cumplido con el paso o tarea de ese instante, y se esta en condiciones de revisar el siguiente.

Un check list es formado por 3 partes principalmente, la cabecera o identificación del check list que indica, Nombre de check list, Nombre del Proyecto, Fecha, Nombre del la persona que revisa, Cargo o Puesto, Nombre de la empresa donde se lleva a cabo y la hora que puede ser opcional. El detalle de tareas que componen el check list las cuales se encuentran con un número consecutivo, descripción del paso o tarea, peso de la tarea (depende de cada caso y convención puede ser opcional, sugerida, obligatoria requerida, etc.) y finalmente resultado del check list al pie de la página donde se indica a partir del cumplimiento o no de los pasos, las acciones, en forma de nota, a tomar para la realización del proyecto, Fecha y Firma del evaluador.

Definiremos el siguiente formato de check list como la forma propuesta a usar durante este trabajo, a continuación se muestra en la figura 7.3.


Nombre de Empresa CONFIDENCIAL Y PROPIETARIO

NOMBRE DE LA EMPRESA

FECHA

Check List para "Titulo del Check List"
Proyecto "Nombre del proyecto"

Nombre de a persona _____
Puesto/Cargo _____

Número	Descripción	Prioridad	Cumplio
1	Tarea o paso con su descripción	ALTA	SI
2	Tarea o paso con su descripción	MEDIA	SI
3	Tarea o paso con su descripción	BAJA	NO
...			
N	Tarea o paso con su descripción	ALTA	SI

NOTAS: _____

Fecha:

Nombre del evaluador: Firma:

Página 1 de 1

Figura 7.3 Formato del Check List a utilizar.

El como definir los pasos necesarios para un check list queda a cargo del diseñador o del comité (preferentemente) al cual se le encargue esta labor, se debe de tener en cuenta, para esto las siguientes recomendaciones:

1. Tener siempre claro el objetivo hacia el cual se encaminará el check list.
2. Hacer una lista en desorden de las tareas que intervengan en el proyecto.
3. Identificar las acciones previas y herramientas que llevan hacia un fin específico del proyecto, por ejemplo: los levantamientos de requerimientos implican programar una serie de entrevistas, ejecutarlas, realizar diagramas, etc.
4. Reunir las acciones y herramientas necesarias bajo un nombre que pueda describir la tarea o paso.
5. Asignar el orden mediante el cual deban de ser ejecutadas.
6. Asignar a cada tarea o paso enlistadas una prioridad, esta puede ser ALTO, MEDIO o BAJO, definiendo el peso de cada prioridad, puede ser ALTO tarea indispensable para el proyecto, MEDIO, tarea necesaria más no indispensable

y BAJO tarea que completa otras tareas pero por si sola puede ser omitida para el proyecto.

7. Realizar la comprobación contemplando todo lo necesario para que el proyecto se ejecute, en caso de ser necesario agregar o resumir las tareas o pasos que se consideren.

La evaluación del check list nos indica si se ha cumplido lo necesario para la finalización del proyecto en el caso de una implementación nos indicará si esta se llevo a cabo satisfactoriamente además de indicarnos durante el desarrollo de la implementación en que paso nos encontramos cual fue el paso anterior y cual será el paso siguiente formando así la guía de implementación que se pretende entregar, adicionalmente podemos encontrar al final del check list lo que nos hace falta para cumplir toda la implementación o el por que no se pudo cumplir la implementación satisfactoriamente, por ejemplo un criterio para esta evaluación es de que si existe alguna tarea o paso con prioridad ALTA sin cumplir la implementación no podrá realizarse.

Durante la evaluación del contenido del check list se debe de considerar que existen tareas implícitas no detalladas pero que por si mismas contemplan otro check list o un manual por su posible complejidad pero que no tiene más relación con el proyecto. Definir estas tareas implícitas de cada paso de nuestro check list a realizar es parte de la documentación que soporta al documento.

7.3.2 Tecnología a ocupar

Con la llegada al mercado de las tecnologías de comunicación de datos inalámbricas presentan una gran oportunidad de mejorar para las Empresas y Administraciones Públicas, tanto para su gestión como para su negocio. Entre las características más atractivas de estas tecnologías se encuentran:

- Alternativa o extensión de una solución de cableado (costo accesible y sencillez).
- Aumento en la productividad.
- Reutilización de infraestructura y rapidez de instalación.
- Acceso a la información en tiempo real y movilidad.
- Servicios de valor añadido.

Sin embargo, la incorporación de las tecnologías inalámbricas con todas las garantías y máximo aprovechamiento plantea toda una serie de nuevos retos para el usuario, y requiere dar respuesta a nuevas cuestiones que afectan a diferentes aspectos, como seguridad, planificación, interferencias, costo y movilidad, etc.

Cada usuario de red inalámbrica sufre una problemática propia que debe solventar en un entorno también propio y diferenciado, por lo que no existen soluciones universales. De esta manera se pueden establecer diferentes segmentos en función de

las necesidades para cada tipo de problema: Hogar, Educación, Pequeñas y Medianas Empresas (Pymes), Corporaciones y "Hot Spot" o "Wireless ISP".

Dependiendo del segmento en el que nos encontramos, hay que sopesar aspectos tales como capacidad de cobertura radio, capacidad de actualización, mecanismos de seguridad incorporados y soportados, herramientas de gestión incluida y el precio que deben ser evaluados en conjunto para definir la opción adecuada. En los anexos en la parte de check list se encuentra el check list para esta sección.

7.3.3 Distribución de antenas

Sabemos que la comunicación de una red inalámbrica se basa en una serie de antenas de diversos tamaños, tecnologías y características especiales para cada caso, dependiendo las distancias a las cuales se desea enviar la señal de nuestra red y/o el área en la cual nuestros clientes requerirán el conectarse nos indicará la cobertura que es necesaria cubrir para tal efecto y para esto es necesario el establecer las ubicaciones donde se pondrán las antenas que cumplan dicha cobertura.

Para este punto comencemos nombrando aquellas tareas previas que se requieren en la distribución de las antenas:

- *Estudio de oficinas a conectar:* Indica que oficinas serán conectadas por medio de las antenas de alcance metropolitano, se debe de tener en cuenta la distancia entre cada oficina.
- *Tipo de antena:* Puede ser omnidireccional o direccional el tipo de antena que vamos a utilizar, para una topología punto a punto se usa las antenas direccionales en tanto que para una topología en malla se usan las antenas omnidireccionales.
- *Alcance y cobertura:* Se debe de tomar en cuenta la potencia de transmisión entre nuestras antenas la cual debe de ser lo suficiente para garantizar el servicio.
- *Topología:* Indicará el tipo y número de antenas que utilizaremos en nuestra red.
- *Seguridad:* La seguridad puede estar incluida en la antena, es decir dentro del dispositivo de emisión y recepción de la señal se pueden incluir los métodos de seguridad de la comunicación, como puede ser la verificación redundante, o métodos para cifrar la información como lo puede ser el WEP.
- *Geografía:* En la distribución de las antenas se debe de tener en cuenta los tipos de lugares físicos adecuados y accesibles para la instalación, fijando siempre lugares altos que garanticen la línea de vista si es el caso o lugares en donde se pueda tener una emisión y recepción libre dependiendo la tecnología que se haya seleccionado.
- *Saturación del medio:* Al seleccionar los lugares convenientes se debe de medir aquellas señales producidas por antenas vecinas e indicar si es viable la instalación de nuestra antena en ese sitio.

- *Compatibilidad de Antenas:* Asegurar que cada antena que se selecciona cumpla con la tecnología de comunicación, versión de sistema, características eléctricas, etc. que aseguran su funcionalidad entre cada una de ellas.
- *Estación base:* Elegir y establecer la estación que fungirá como principal en nuestra red.
- *Línea de vista:* Realizar las mediciones adecuadas para garantizar que entre las antenas se tiene la posibilidad, así como el estudio de obstáculos que se presentan para obtener el espacio despejado.
- *Energía:* garantizar que en la ubicación a elegir se cuente con la alimentación para el equipo de la antena y para la antena misma y su correcto funcionamiento.

En los anexos en la parte de check list se encuentra el check list para esta sección. Las prioridades manejadas en el check list las podemos nombrar como:

- *Alta:* Se considera indispensable y necesaria para cubrir el proyecto, cada punto del check list marcado con una prioridad de este tipo debe de ser cubierta por ser la base para la implementación y sin estos puntos no podrá ser posible llegar al objetivo de la distribución de las antenas.
- *Media:* Indispensable pero no con un carácter obligatorio, por ejemplo es necesario conocer el tipo de antena que se colocará en la distribución sin embargo no será necesario que se realice la instalación de la misma para saber su ubicación que es en teórica la más idónea.
- *Baja:* Deseable pero no requerida para el cumplimiento del proyecto, esta prioridad es manejada cuando una acción o un requerimiento puede ser omitido pero no desechado y puede ser cumplido durante la operación del proyecto, por ejemplo durante la distribución puede ser deseable contar con una zona despejada para su fácil identificación del punto donde será colocada la antena, sin embargo quitará tiempo al estudio de la distribución, si la zona se puede indicar con facilidad limpiando fácilmente se realizará en caso contrarío se puede llevara acabo esta tarea al momento de instalar la antena.

El llenar este check list y evaluar las notas nos puede garantizar el tener los recursos necesarios e identificación de los puntos adecuados para la implementación de cada antena, es de suma importancia el mencionar que para casos particulares el check list puede crecer o disminuir, dependerá del diseñador o el comité técnico de la implementación.

7.3.4 Distribución de AP

Durante la implementación encontraremos casos en los cuales varios clientes de la empresa se concentren bajo un mismo sitio esto puede ser en las oficinas centrales localizadas dentro de un edificio y separadas entre pisos u oficinas separadas entre edificios contiguos y además que a su vez estos clientes demanden comunicación hacia otros clientes más lejanos miembros de la misma empresa.

Se ha visto que la solución para clientes lejanos que se encuentran conectados por medio de antenas de largo alcance (adaptadas para cada caso, puede ser un estación base o un cliente) sin embargo para el caso en donde se tiene una cobertura limitada por el área de trabajo optaremos por los llamados Access Point (AP) los cuales permiten la libertad de movimiento, además de los beneficios de instalación, costo y tiempo como se han planteado en este trabajo los cuales al estar conectados a una estación base o una antena de largo alcance (nodo) nos garantiza el acceder a toda la WMAN.

Si bien los AP pueden ser sustituidos por tarjetas individuales para que cada cliente pueda conectar directamente a la estación base o a los diferentes nodos de la red WMAN, hoy en día el uso de AP es la solución ideal para la comunicación de un grupo concentrado en un mismo sitio con una cobertura limitada esto en tanto la otra tecnología de tarjetas individuales amortice su costo quedando y quede hoy en día restringida solo para ciertos clientes. Puntos a considerar para la distribución de AP:

- *Tipo de AP:* Este punto se refiere a la tecnología que maneja nuestro AP, la forma que debe de tener el AP, si será colocado en la pared en un pedestal o en lo alto de un poste, así como también las características que deben guardar si se ubicará en el interior o fuera de la oficina.
- *Compatibilidad con los clientes:* Este punto se refiere a que cada adaptador de red que manejen los clientes sea de acuerdo al AP que se vaya a colocar, cumpliendo las características de velocidad, especificación y cobertura, entre otras características apropiadas.
- *Compatibilidad con la estación base o el nodo:* Para poder acceder a nuestra red WLAN requerimos que cada punto de acceso pueda conectarse a la antena de la estación base o las antenas que sirven como nodo, es necesario por lo tanto el contar con la interfaz, las conexiones o la especificación necesaria para que esto se pueda cumplir.
- *Configuración del AP:* Indicar al AP las propiedades de conexión a nuestros servidores, así como que clientes accederán a el, son parte de las reglas básicas que todo dispositivo de la red debe cumplir
- *Estudio de la ubicación de las diferentes áreas de trabajo:* Aquí nos referimos a que debe de realizarse un levantamiento de las diferentes áreas de trabajo que se desea cubrir y posterior a esto conocer en dónde y cuántos AP serán requeridos.
- *Estudio de la Saturación del medio:* Al igual que con las antenas podemos tener diferentes frecuencias en el medio que pueden hacer que este se encuentre saturado, dando como resultado un mal funcionamiento en nuestra comunicación, esto puede modificar nuestra propuesta original para convertirse en la más adecuada.
- *Seguridad de la comunicación:* Clientes no deseados o ajenos a la empresa pueden pretender el acceder a nuestra red, es importante tener en cuenta que tipo de seguridad tiene nuestro AP, ya sea por autentificación o alguna otra que incluya el mismo AP.
- *Conexión del AP a los servicios:* El AP puede antes de enviar o recibir señales de la red WMAN, pasar por una serie de servidores los cuales se encarguen de

la seguridad, codificación y/o aseguren el envío de los mensajes a y desde la Red, si es así debemos asegurar que se cuenta con lo medios para realizar dicha conexión.

En los anexos en la parte de check list se encuentra el check list para esta sección. Las prioridades en este caso se encuentran como:

- *Alta:* Indispensable y necesaria para cubrir el proyecto.
- *Media:* Indispensable pero no con un carácter obligatorio.
- *Baja:* Deseable pero no requerida para el cumplimiento del proyecto.

El llenar este check list y evaluar las notas que nos puede garantizar el tener los recursos necesarios e identificar los puntos adecuados para la implementación de cada AP, es de suma importancia el mencionar que para casos particulares el check list puede crecer o disminuir, dependerá del diseñador o el comité técnico de la implementación.

7.3.5 Servicios a implementar

Cada vez con mayor frecuencia el acceso a portales, se realiza desde distintas vías de acceso, desde un navegador de PC cuando el usuario se encuentra en la oficina, un navegador, PDA o WAP de teléfono móvil cuando se encuentra fuera de la misma. Es importante ofrecer las distintas formas de conectividad que existen en una red inalámbrica desde el tipo de hardware que se va a utilizar, su configuración y formas de conectividad para que hagan más eficiente la conectividad, hasta los estándares que mejor se adaptan y sobretodo la que mejor le convenga en este caso a cada cliente a utilizar. Debe conocer los equipos que se están utilizando AP, tarjetas inalámbricas, antena omnidireccional, etc. Y sobre este punto ofrecer la mejor arquitectura de estándares a utilizar ya sea 802.11 o 802.16 basándonos en una serie de preguntas en la cual a través de estas nosotros podemos recopilar la información necesaria para adaptarnos a las necesidades que el cliente esta requiriendo y de esta forma poder ofrecer un servicio de mayor calidad en la instalación de una red inalámbrica. De acuerdo a esto establecimos una serie de preguntas en la cual las clasificamos según nuestro punto de vista como las adecuadas para la instalación de su red inalámbrica.

En los anexos en la parte de check list se encuentra el check list para esta sección. De acuerdo a la clasificación tenemos:

- *Alta:* Indispensable y necesaria para cubrir el proyecto.
- *Media:* Indispensable pero no con un carácter obligatorio.
- *Baja:* Deseable pero no requerida para el cumplimiento del proyecto.

El llenar este check list y evaluar las notas que nos puede garantizar el tener los recursos necesarios e identificar los puntos adecuados para la implementación de cada AP, es de suma importancia el mencionar que para casos particulares el check list puede crecer o disminuir, dependerá del diseñador o el comité técnico de la implementación.

7.3.6 Funcionalidad de la red inalámbrica

Dentro de las funciones que debe ofrecer una red inalámbrica se encuentran las siguientes:

- Estar basada en estándares y contar con certificación.
- Instalación simple.
- Robusta y confiable.
- Escalabilidad.
- Facilidad de uso.
- Servidor para una administración más fácil.
- Seguridad.
- Una aplicación que detecte localidades.

En este punto se toman en cuenta los resultados obtenidos en las evaluaciones hechas previamente las cuales son:

Tecnología a ocupar: Se tienen distintas tecnologías aplicables a las comunicaciones inalámbricas para su transmisión y recepción las cuales son: Direct Sequens Spread Spectrum (DSSS, Espectro Extendido por Secuencia Directa), Frecuency Hopping Spreed Spectrum (FHSS, Espectro Extendido por Frecuencia de Saltos), Orthogonal Frecuency Division Multiplexing (OFDM, Multiplexión por División Ortogonal de Frecuencias) y Banda Ancha.

Dependiendo de la tecnología a ocupar se pueden tener ventajas o desventajas en la funcionalidad de la red inalámbrica.

Distribución de antenas: Las clasificaciones de las antenas pueden atender a numerosos criterios, siendo los principales por su ubicación y por la forma del lóbulo de emisión de la radiación. Atendiendo a la ubicación, las antenas pueden ser de interiores o de exteriores.

Antenas para interiores su volumen es pequeño y no suelen ser de gran potencia. Antenas para exteriores son robustas y suelen tener gran potencia. Por la forma de su patrón de emisión, hay omnidireccionales (cobertura circular), direccionales o sectoriales (cubren un determinado ángulo) y muy directivas (ángulos por debajo de los 12 grados). Además de todo lo anterior, hay que tener en cuenta la ganancia que presenta cada modelo de antena para realizar correctamente un diseño, encontrando modelos comerciales desde 2 a 24 decibelios (dB).

Pese a ser un elemento al cual se le presta escasa atención a la hora de realizar una instalación, es sin embargo uno de los pilares fundamentales de todo diseño. Una inadecuada selección de antenas puede suponer una deficiente cobertura en la zona de operación, con áreas de sombra con imposibilidad de

recepción y otras con escasa señal que fuerzan a trabajar a un ratio de bits muy bajo, degradando las prestaciones de todo el conjunto.

Distribución de AP: El punto de acceso es el encargado de gestionar las comunicaciones inalámbricas de su área de cobertura. Entre las funciones que realiza es la de identificar nuevos usuarios, manejo de comunicaciones de usuarios en movimiento, control de frecuencias asignadas, etc.

Este dispositivo también tiene funciones de control de acceso y seguridad, de forma que garantiza que los usuarios que accedan a la red sean únicamente los estipulados y además que las comunicaciones que realiza sean seguras.

Dependiendo del modelo que se utilice, este dispositivo implementa diferentes funciones, pero su misión elemental es adaptar la información transmitida en un medio inalámbrico a otro cableado, garantizando la calidad y seguridad de la transmisión.

Servicios a implementar: Se tienen dos estándares los cuales cuentan con diferentes servicios dependiendo del estándar ocupado se obtienen los siguientes servicios:

El estándar IEEE 802.16 tiene definidos cuatro métodos de solicitud de reserva de ancho de banda, para cuatro tipos de servicio diferentes:

- Servicio garantizado no solicitado.
- Servicio con sondeo en tiempo real.
- Servicio con sondeo en tiempo diferido.
- Servicio mejor esfuerzo.

El estándar IEEE 802.11 define nueve servicios que deben ser proporcionados por una red inalámbrica para ofrecer una funcionalidad equivalente a la inherente a una red cableada tradicional.

- Asociación.
- Autentificación.
- Fin de la autentificación.
- Disociación.
- Distribución.
- Integración.
- Entrega de MSDU.
- Privacidad.
- Reasociación.

Cabe mencionar que estos tipos de servicios están detallados en el capitulo VI.

Seguridad: La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro,

se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad. El canal de las redes inalámbricas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Opcionalidades de seguridad:

- *WEP:* El sistema WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, tiene distintas debilidades que lo hacen no seguro, por lo que deben buscarse otras alternativas. Los objetivos de WEP, son proporcionar confidencialidad, autentificación y control de acceso en redes.
- *WPA:* La tecnología WPA como IEEE 802.11i solucionan todos los fallos conocidos de WEP y, en estos momentos, se consideran soluciones fiables. WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos. Mientras no se descubran problemas de seguridad en WPA, esta implementación puede ser suficiente en los dispositivos.
- *VPN's:* Protege los datos de usuarios remotos conectados desde Internet a la red, se ocupa para asegurar los extremos de la comunicación. La tecnología VPN es un poco costosa en recursos para su implementación en redes Wireless.

En los anexos en la parte de check list se encuentra el check list para esta sección. De acuerdo a la clasificación tenemos:

- *Alta:* Indispensable y necesaria para cubrir el proyecto.
- *Media:* Indispensable pero no con un carácter obligatorio.
- *Baja:* Deseable pero no requerida para el cumplimiento del proyecto.

El llenar este check list y evaluar las notas que nos puede garantizar el tener los recursos necesarios e identificar los puntos adecuados para la implementación de cada AP, es de suma importancia el mencionar que para casos particulares el check list puede crecer o disminuir, dependerá del diseñador o el comité técnico de la implementación.

CONCLUSIÓN

En la actualidad la excitante tecnología para redes inalámbricas esta naciendo como solución para implementaciones empresariales, publicas y domesticas, optimizando recursos y proponiendo mayor flexibilidad en la comunicación de las redes.

La forma o formas en que se lleva a cabo la comunicación inalámbrica se describen en los protocolos 802.11 y 802.16 de la IEEE, en los cuales se especifican las normas y estándares de comunicación inalámbrica en las capas de enlace y física del modelo OSI como referencia.

En esta evaluación consideramos que el tipo de modulación a ocupar para el estándar 802.11 están basados en el espectro discreto las cuales son: FHSS y DSSS, debido a que la mayoría de los productos inalámbricos actuales manejan este tipo de modulación y para el estándar 802.16 admiten dos métodos de duplexión los cuales son: en frecuencia y tiempo, conocido como banda ancha, cabe mencionar que la banda ancha no es totalmente conocida y difundida en la actualidad.

Un dispositivo importante para la implementación de la red inalámbrica de tipo MAN son los puntos de acceso (AP), los cuales controlan la asignación del tiempo de transmisión para todas las computadoras o dispositivos inalámbricos y permiten que las computadoras o dispositivos móviles estén conectados o en comunicación con la red.

Podemos encontrar que para la seguridad de las redes inalámbricas existen técnicas que fortalecen los inconvenientes de los mecanismos de estas redes y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes, el estándar 802.11 cuenta con el WEP (Encriptación y Autentificación) y el estándar 802.16 cuenta con el WPA (Acceso de Protección Wi-Fi).

Finalmente el uso de documentos sencillos y fáciles de interpretar permitirá que el proceso de implementación sea ordenado, claro y de fácil seguimiento, el uso de Check List es idóneo para este tipo de trabajo ya que son usados en proyectos como: instalaciones, configuraciones, validaciones de procesos, carga de programas, mantenimiento y en general en el campo de las Tecnologías de Informática (IT, Informatic Tecnology), sin sustituir la documentación necesaria para este tipo de proyectos como puede ser la memoria técnica o manuales especializados.

Anexos

Catalogó de antenas
Catalogó de AP
Catalogó de tarjetas y adaptadores de red inalámbricos
Check list

A1 – 1 CATALOGÓ DE ANTENAS

ANTENAS DIRECCIONALES

HG2417P-120 : Sectorial HyperG 120º 17 dBi



Tipo	Direccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	17 dBi
Cobertura vertical	7 grados
Cobertura horizontal	120 grados
Alcance	4000 metros
Dimensiones : Alto, Ancho, Profundo	9 x 1 x 0 cm
Conectores y cables incluidos	La antena tiene directamente un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

ANT24-1800, 18dBi, Exterior



Tipo	Direccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	18 dBi
Cobertura vertical	15 grados
Cobertura horizontal	15 grados
Alcance	5000 metros
Dimensiones : Alto, Ancho, Profundo	36 x 36 x 1 cm
Conectores y cables incluidos	La antena tiene un cable de 0.45 metros terminado en un conector del tipo N-Hembra. El kit incorpora también un cable pigtail para conectarla directamente a un punto de acceso o adaptador de red inalámbrica.

DWL-M60AT, 6dBi, (para DWL-660)



Tipo	Direccional
Apta para interiores	Si
Apta para exteriores	No
Herrajes incluidos	No
Ganancia	6 dBi
Cobertura vertical	80 grados
Cobertura horizontal	80 grados
Alcance	500 metros
Dimensiones : Alto, Ancho, Profundo	8 x 7 x 1 cm
Conectores y cables incluidos	La antena lleva directamente un cable de 1.50 metros terminado en un conector especial.

HG5824D Parabólica 24dBi 5.8Ghz



Tipo	Direccional
Apta para interiores	No
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	24 dBi
Cobertura vertical	9 grados
Cobertura horizontal	9 grados
Alcance	11000 metros
Dimensiones : Alto, Ancho, Profundo	43 x 43 x 12 cm
Conectores y cables incluidos	La antena tiene directamente un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

HG2424G Parabólica, 24dBi, Exterior



Tipo	Direccional
Apta para interiores	No
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	24 dBi
Cobertura vertical	8 grados
Cobertura horizontal	8 grados
Alcance	12000 metros
Dimensiones : Alto, Ancho, Profundo	100 x 60 x 12cm
Conectores y cables incluidos	La antena tiene un cable de 0.50 metros terminado en un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

HG2415P-180 : Sectorial HyperG 180º 15 dBi



Tipo	Direccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	15 dBi
Cobertura vertical	10 grados
Cobertura horizontal	179 grados
Alcance	3500 metros
Dimensiones : Alto, Ancho, Profundo	10 x 2 x 1 cm
Conectores y cables incluidos	La antena tiene directamente un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

ANT24-1200, 12dBi, Exterior



Tipo	Direccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	12 dBi
Cobertura vertical	23 grados
Cobertura horizontal	80 grados
Alcance	1500 metros
Dimensiones : Alto, Ancho, Profundo	28 x 4 x 8 cm
Conectores y cables incluidos	De la antena sale un cable de 3.00 metros que se conecta directamente al conector en el punto de acceso o adaptador de red inalámbrica.

HG2412Y : Direc HyperG Yagi 12dBi Exterior



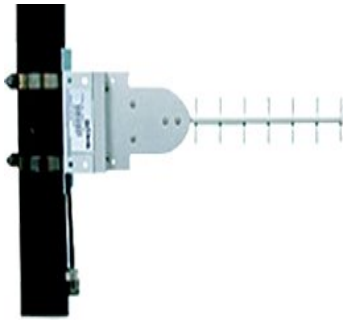
Tipo	Direccional
Apta para interiores	No
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	12 dBi
Cobertura vertical	45 grados
Cobertura horizontal	45 grados
Alcance	2000 metros
Dimensiones : Alto, Ancho, Profundo	40 x 9 x 0 cm.
Conectores y cables incluidos	La antena tiene un cable de 0.15 metros terminado en un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

ANT24-1400, 14dBi, Exterior



Tipo	Direccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	14 dBi
Cobertura vertical	30 grados
Cobertura horizontal	30 grados
Alcance	3000 metros
Dimensiones : Alto, Ancho, Profundo	24 x 24 x 6 cm
Conectores y cables incluidos	La antena tiene un cable de 0.50 metros terminado en un conector del tipo N-Hembra. El kit incorpora también un cable pigtail para conectarla directamente a un punto de acceso o adaptador de red inalámbrica.

ANT24-1201, 12dBi, Interior



Tipo	Direccional
Apta para interiores	No
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	12 dBi
Cobertura vertical	50 grados
Cobertura horizontal	50 grados
Alcance	1000 metros
Dimensiones : Alto, Ancho, Profundo	28 x 8 x 4 cm.
Conectores y cables incluidos	La antena tiene un cable de 0.50 metros terminado en un conector del tipo N-Hembra. El kit incorpora también un cable pigtail para conectarla directamente a un punto de acceso o adaptador de red inalámbrica.

ANT24-1801, 18dBi, Exterior



Tipo	Direccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	18 dBi
Cobertura vertical	15 grados
Cobertura horizontal	15 grados
Alcance	5000 metros
Dimensiones : Alto, Ancho, Profundo	100 x 8 x 8 cm
Conectores y cables incluidos	La antena tiene un cable de 0.45 metros terminado en un conector del tipo N-Hembra. El kit incorpora también un cable pigtail para conectarla directamente a un punto de acceso o adaptador de red inalámbrica.

HG2409PCR-NF : Direc HypeG PCircular Der. 8dBi



Tipo	Direccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	No
Ganancia	8 dBl
Cobertura vertical	65 grados
Cobertura horizontal	65 grados
Alcance	1200 metros
Dimensiones : Alto, Ancho, Profundo	11 x 11 x 2 cm
Conectores y cables incluidos	La antena tiene un cable de 0.50 metros terminado en un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

ANTENAS OMNIDIRECCIONALES

ANT24-0400, 4dBi (para DWL-660)



Tipo	OmniDireccional
Apta para interiores	Si
Apta para exteriores	No
Herrajes incluidos	No
Ganancia	4 dBi
Cobertura vertical	40 grados
Cobertura horizontal	360 grados
Alcance	200 metros
Dimensiones : Alto, Ancho, Profundo	19 x 6 x 4 cm
Conectores y cables incluidos	La antena lleva directamente un cable de 1.00 metros terminado en un conector especial.

ANT24-0401, 4dBi



Tipo	OmniDireccional
Apta para interiores	Si
Apta para exteriores	No
Herrajes incluidos	No
Ganancia	4 dBi
Cobertura vertical	63 grados
Cobertura horizontal	360 grados
Alcance	400 metros
Dimensiones : Alto, Ancho, Profundo	13 x 13 x 4 cm
Conectores y cables incluidos	De la antena sale un cable de 3.00 metros que se conecta directamente al conector en el punto de acceso o adaptador de red inalámbrica.

ANT24-0500, 5dBi



Tipo	OmniDireccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	No
Ganancia	5 dBi
Cobertura vertical	32 grados
Cobertura horizontal	360 grados
Alcance	400 metros
Dimensiones : Alto, Ancho, Profundo	33 x 1 x 1 cm
Conectores y cables incluidos	La antena tiene directamente un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

RE05U-RSP : HyperG RangeXtender 5dBi



Tipo	OmniDireccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	No
Ganancia	5 dBi
Cobertura vertical	40 grados
Cobertura horizontal	360 grados
Alcance	500 metros
Dimensiones : Alto, Ancho, Profundo	15 x 0 x 0 cm
Conectores y cables incluidos	De la antena sale un cable de 1.82 metros que se conecta directamente al conector en el punto de acceso o adaptador de red inalámbrica.

DWL-50AT, 5dBi



Tipo	OmniDireccional
Apta para interiores	Si
Apta para exteriores	No
Herrajes incluidos	No
Ganancia	5 dBi
Cobertura vertical	85 grados
Cobertura horizontal	360 grados
Alcance	300 metros
Dimensiones : Alto, Ancho, Profundo	0 x 0 x 0 cm
Conectores y cables incluidos	Se conecta directamente al conector en el punto de acceso o adaptador de red inalámbrica.

RE09U-RSP : HyperG RangeDoubler, 8 dBi



Tipo	OmniDireccional
Apta para interiores	Si
Apta para exteriores	No
Herrajes incluidos	No
Ganancia	8 dBi
Cobertura vertical	20 grados
Cobertura horizontal	360 grados
Alcance	900 metros
Dimensiones : Alto, Ancho, Profundo	40 x 3 x 3 cm
Conectores y cables incluidos	De la antena sale un cable de 1.82 metros que se conecta directamente al conector en el punto de acceso o adaptador de red inalámbrica.

ANT24-0800, 8dBi, Exterior



Tipo	OmniDireccional
Apta para interiores	No
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	8 dBi
Cobertura vertical	15 grados
Cobertura horizontal	360 grados
Alcance	800 metros
Dimensiones : Alto, Ancho, Profundo	63 x 1 x 1 cm
Conectores y cables incluidos	La antena tiene un cable de 0.50 metros terminado en un conector del tipo N-Hembra. El kit incorpora también un cable pigtail para conectarla directamente a un punto de acceso o adaptador de red inalámbrica.

HGV2410U : HyperG 10dBi Exterior



Tipo	OmniDireccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	No
Ganancia	10 dBi
Cobertura vertical	8 grados
Cobertura horizontal	360 grados
Alcance	1200 metros
Dimensiones : Alto, Ancho, Profundo	102 x 3 x 3 cm
Conectores y cables incluidos	La antena tiene directamente un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

HG2415U-PRO : HyperG RangeXtreme Pro 15dBi



Tipo	OmniDireccional
Apta para interiores	Si
Apta para exteriores	Si
Herrajes incluidos	Si
Ganancia	15 dBi
Cobertura vertical	8 grados
Cobertura horizontal	360 grados
Alcance	2000 metros
Dimensiones : Alto, Ancho, Profundo	103 x 10 x 10 cm
Conectores y cables incluidos	La antena tiene directamente un conector del tipo N-Hembra. Si se desea conectar a un punto de acceso o a un adaptador de red inalámbrica precisará de un cable Pigtail.

A2 – 1 CATALOGÓ DE AP

Punto de acceso 802.11b Hot Spot



Aplicaciones	• Solución ideal para configuraciones del tipo Hot Spot. Ofrece hasta 11 Mbps de velocidad y dispone de varios modos operativos que le confiere innumerables posibilidades: Punto de acceso, Bridge, Punto de acceso cliente y como Gateway doméstico. • BOSSWAPH está específicamente diseñado para usuarios Hot Spot debido a su capacidad multifunción. Permite configurarse para trabajar como Punto de acceso, Punto de acceso cliente o como punto de acceso Gateway doméstico. Para uso doméstico, el BOSSWAPH permite enlazarse con la conexión Internet, proveniente de un módem o de un router ADSL, permite dar múltiples sesiones a ordenadores portátiles de acceso BOSSWAPH. • Un usuario puede conectarse a un punto de acceso en un determinado momento, desplazarse a otra zona en la que existe otro BOSSWAPH y estar conectado sin necesidad de enlazar los puntos de acceso entre ellos pos cable. El número máximo de conexiones WDS es de ocho enlaces por punto de acceso BOSSWAPH. • Este punto de acceso es el componente ideal para estructuras Hot Spot ya que ofrece una implementación rápida, fácil y segura.
Características Técnicas	• Compatible IEEE 802.11b estándar y Wi-Fi compliant. • Soporta cliente para AAA y EAP RADIUS. • Soporta protocolo Spanning Tree. • Soporta 802.1x, seguridad con RADIUS port-based. • Soporta port Dynamic WEP key, re-keying. • RC4 compatible con WEP 64/128 bits para encriptación de seguridad. • Soporta filtro de direcciones MAC. • Dispone de IP sharing que permite a múltiples estaciones acceder a Internet utilizando una única conexión. • Firewall incluido para prevenir trafico e intrusos no deseados. • Dispone de DHCP server para configuración sencilla IP. • Soporta función VPN pass through. • IP Routing con NAT, PPPoE cliente. • Soporta Power Over Ethernet (PoE). • Antena extraíble para cambio por otras de distintas características.

Punto de acceso integrado multifunción



Aplicaciones	• Punto de acceso integrado multifunción, AP, Bridge, AP cliente, 802.11b. • BOSSWAPK está preparado para instalarse en exteriores. • Ofrece funciones firewall, encriptación y de seguridad. Dispone de módulo integrado de alta potencia para enlaces de larga distancia así como POE (Power Over Ethernet) para facilitar la instalación y puesta en marcha. Es un punto de acceso doblemente práctico ya que en una único dispositivo se concentra la electrónica wireless y la antena plana totalmente aislada y protegida de las inclemencias del tiempo. • Elevadas prestaciones nos ofrece este AP Router compacto (AP+antena+POE) para cada configuración wireless exterior. • Puede programarse la potencia de transmisión de trabajo (+19dBm) ofreciendo alta ganancia de enlace ya que va montado sobre una antena plana de 10dBi para comunicaciones de larga distancia y entornos WISP. Facilita enormemente la instalación de puntos clientes WISP ya que dispone de alimentación POE y antena plana integrada. • Puede utilizarse para enlaces inter-edificio, para soluciones WISP o para hoteles para citar algunos ejemplos. • La facilidad de instalación y mantenimiento de estructuras punto a multipunto le confieren unas características únicas para este tipo de entornos en el que la instalación para múltiples usuarios no sea una tarea

	tediosa y complicada. • Simplemente, se instala el BOSSWAPK en la fachada o en un mástil de forma fácil. En pocos minutos el punto de acceso wireless ya está en funcionamiento. • Si las distancias son superiores al alcance de la antena integrada y al disponer de una etapa de potencia amplificada y conector para antena exterior, en cualquier momento puede instalarse una antena de otras características o tipo para cubrir el enlace y la zona deseada.
Características Técnicas:	• IEEE 802.11b y compatible Wi-Fi. • Montado con antena de alta ganancia de 10 dBi. • IEEE 802.3a, f Power over Ethernet. • Potencia de salida TX programable. • Alta velocidad de salida hasta 11 Mbps. • Protegido para uso exterior, estanqueidad. • Posibilidad de utilizar la antena integrada o antena exterior. • Ofrece encriptación WEP 64/128-bit y 2 capas aisladas (Layer x 2). • Multi función: Punto de acceso, Router, Bridge y Bridge Cliente (configurable). • Administración remota y actualización por firmware.

Punto de acceso multifunción, AP, Bridge, AP cliente, 802.11b



Aplicaciones	• El punto de acceso BOSSWAP ofrece varias funciones para conectividad wireless en un único dispositivo. Compatible con los estándar 802.11b, ofrece conectividad Direct Sequence Spread Spectrum (DSSS) para enlaces bridge de modo transparente y propiedades roaming. • El BOSSWAP ofrece también bridge punto a punto, permitiendo estructuras basadas en punto a punto o punto a multipunto utilizadas en los enlaces inter-edificio.
Características Técnicas	• Chip INTERSIL. • Conectores RJ-45 10 Mbps. • Estándares IEEE 802.11b. • Compatibilidad S.O. Windows 98/ME/2000/XPWIN CE (Plataforma ARM). • Temperatura 10º C a 50º Operacional. • Humedad 10% a 95% (Sin condensación). • Frecuencia 2.4 - 2.4835 GHz. • Encriptación 64/128 bits encriptación WEP. • Utilidades de software Utilidad de control software. • Canales Europa 13 (1-13). USA 11 (1-11). Francia 4 (10-13). Japón 14 (1-14). • Velocidad de datos 11, 5.5, 2, 1 Mbps. • Potencia 14 dBm. • Antena Extraíble, puede utilizarse otros tipos y modelos con mayor ganancia o mejor cobertura. • Alcances Interiores 35-100 m Exteriores 100-300 m. • LED's Encendido, Link y Actividad. • Arquitectura de red Infraestructura, Acces Point, AP Client, Bridge. • Otras especificaciones Dispone de SNMP manager para configuración y mantenimiento. Filtros de seguridad IP y MAC.

Punto de acceso router, bridge 802.11b+g de 54 Mbps

Aplicaciones:	• BOSSWAPR54 trabaja bajo el protocolo IEEE 802.11g estándar, y modulación OFDM (Orthogonal Frequency Division Multiplexing). • Gracias a la tecnología de modulación ODFM, 802.11g amplía el rendimiento de 802.11b utilizando (CCK) Complementary Code Keying desde los 5.5 Mbps y 11 Mbps a los 54 Mbps. • BOSSWAPR54 dispone también de optimización en lo que concierne al transporte de datos multimedia, por ejemplo, transmisiones de datos DVD,



	vídeo o broadcast son optimizadas al máximo. • BOSSWAPR54, punto de acceso wireless, permite la conexión de usuarios 802.11g o 802.11b a la red. Incluye 4 puertos switch full duplex 10/100 para conectar usuarios o dispositivos que utilizan cable Ethernet. • BOSSWAP54 permite compartir datos en red y la conexión a Internet.
Características Técnicas:	• Compatible con IEEE 802.11b y 802.11g estándar sobre 2.4 GHz. • Fácil de instalar, velocidad wireless hasta 54 Mbps. • Encriptación WEP de 128 bits, filtros MAC o dirección IP. • Control avanzado de Seguridad Internet, incluyendo Bloqueo Web, filtros IP y MAC, tecnología NAT. • Puede ser asignado como Servidor DHCP para la red existente. • Ofrece compartición Cable/DSL Internet con Switch de 4 puertos 10/100. • Dispone de protección NAT para red privada con VPN pass-through y soporte para múltiples y simultáneas sesiones IPsec, L2TP y PPTP. • Configuración y mantenimiento basado en WEB. • Encriptación WPA (WPA, es un nuevo certificado de seguridad establecido por la Wi-Fi Alliance que ofrece una mayor seguridad en la protección de datos respecto al tradicional WEP. La función dinámica WPA sustituye a la WEP estática para todos los casos). • Selección de modo y velocidad manual o automática. • Incluye conmutador (switch) 10/100 Mbps de 4 puertos. • Incluye router y puerto WAN para la conexión de Módem ADSL con puerto Ethernet. • Puertos Ethernet LAN: Cuatro puertos 10/100 Mbps (RJ45) WAN: Un puerto 10 Mbps (RJ45). Ethernet: IEEE 802.3 / IEEE 802.3u. • 802.11b: 11 y 5.5 Mbps – CCK. • 2 Mbps – DQPSK, 1 Mbps – DBPSK. • 802.11g OFDM. • Velocidad de Operación 802.11b 11, 5.5, 2 y 1 Mbps, 802.11g 54, 48, 36, 24, 18, 12, 9, 6 Mbps. • Potencia de Transmisión 15 dBm 1 NTR máximo. • Sensibilidad de Recepción 11 Mbps 10-5 BER a –80 dBm típico. • 54 Mbps 10-5 BER a –65 dBm típico. • Canales 802.11b Estados Unidos:11 ; Europa:13 802.11g Estados Unidos, Europa y Japón: 13. • Protocolos Soportados TCP/IP, IPX, NetBEUI, DHCP, NAT, Cliente PPPoE. • Gestión Configuración WEB. • Actualización de firmware mediante navegador. • Soporte Cliente DHCP, Servidor http, Roaming en la misma subred. • Restauración de parámetros por defecto, Backup/Restore. • Soporte Firmware Selección de velocidad, Selección de dominio de regulación, DMZ, Servidor virtual, Filtrado IP, VPN pass-through (soporta PPTP, L2TP e IPsec). • Seguridad ESSID, soporta rehabilitación de distribución ESSID, Filtrado de direcciones MAC (ACL), Encriptación WPA.

Access Point Marca Trendware Modelo TEW-311BRP

Aplicaciones:	• El TEW-311BRP de TRENDnet es un punto de acceso inalámbrico de IEEE 802.11b, Router Broadband y Switch Fast Ethernet de 4 puertos 10/100Mbps. • Comparte su conexión de Internet de banda ancha (Broadband) con estaciones alámbricas e inalámbricas. • La instalación y configuración del TEW-311BRP es fácil y rápida por medio del navegador de Internet y la conexión inalámbrica proporciona una velocidad de hasta 22 Mbps para transmisión de datos. • El TEW-311BRP también funciona como firewall (NAT) protegiendo la red



	de los hackers.
Características Técnicas:	• Equipado con cuatro puertos Switch con Auto-negociación / Auto MDI-X/MDI-II dando mayor flexibilidad a la conectividad de redes. • Dos Antenas de 2 dBi fijas. • Control de acceso con dirección MAC para clientes inalámbricos Reconocidas o Negadas (Granted or Denied). • Configuración vía Navegador o Telnet (configuración remota disponible). • El servidor DHCP asigna hasta 253 direcciones IP y 4 direcciones IP reservadas. • Como cliente DHCP soporta una dirección IP global del ISP. • Network Address Translation (NAT) para mantener al los hackers fuera de la red. • Servidor Virtual (1 DMZ host y 10 entradas de Servidor Virtual) y ofrece características “Packet Filter”. • Soporta las aplicaciones de Internet como E-mail, FTP, ICQ, NetMeeting, PING, Telnet, etc. • Capacidades de Router dinámico y estático (Dynamic and Static Routing Capabilities). • Memoria flash para actualizar el firmware. • IEEE 802.11b (Red inalámbrica) Wireless LAN, IEEE 802.3, y IEEE 802.3u. • Configuración por Navegador o Telnet (posibilidad de administración remota). • Tecnología de Modulación: DSSS, PBCC (Packet Binary Convolutional Coding), 11-chip Barker Séquense. • Canales: 11 Canales (US y Canadá). • DHCP (Cliente y Servidor), IP, NAT, PPPoE, TCP, UDP. • Modo inalámbrico: Access Point (Infrastructure). • Rango de Transmisión: 22, 11, 5.5, 2, y 1 Mbps (ajuste automático). • Rango de Frecuencia: 2.4 ~ 2.4835 GHz. • Seguridad: 64/128/256-bit WEP Encryption. • Antena: 2 x 2 dBi. Antenas Externas Fijas (longitud = 115 mm). • Poder de Salida: 15 dBm (máx.). • Sensibilidad de Recepción: - 82 dBm (Típica). • Sensibilidad de Recepción: 1, 2, 5.5 y 11Mbps. • Puerto Local: 4 puertos de Switch UTP/STP 10/100 Mbps Auto MDI-X/MDI-II. • Puerto WAN: UTP/STP RJ-45 10 Mbps MDI-X. • Integración Sencilla: Router de Internet, Punto de Acceso y Switch de 4 puertos 10/100Mbps todo en uno. Comparte la conexión Internet de banda ancha con Clientes alámbricos e inalámbricos. • Control de Tráfico: Controla el tráfico de redes con el DMZ, Protocol Filter, y Virtual Server. • Funcionamiento: Comparte el acceso a la Internet de alta velocidad con una conexión inalámbrica de hasta 22 Mbps.

A3 – 1 CATALGÓ DE TARJETAS Y ADAPTADORES DE RED INALÁMBRICOS

TARJETA WIRELESS-G PCI CARD



Características

- Conectividad Wireless-G (802.11g) para el PC de escritorio.
- Increíbles velocidades de transferencia de datos de hasta 54 Mbps en la banda de radio de 2.4 GHz.
- Funcionamiento con redes Wireless-B (802.11b) a 11 Mbps.
- Protección de la comunicación inalámbrica mediante encriptación de datos de hasta 128 bits y WPA.

ADAPTADOR PCI WIRELESS-B



Características

- Conectividad Wireless-B (802.11b) para el PC de escritorio.
- Velocidades de transferencia de datos de hasta 11 Mbps en el radio de 2.4 GHz.
- El asistente de configuración que se incluye guía paso a paso durante la configuración.

ADAPTADOR PCI WIRELESS-G CON SPEEDBOOSTER



Características

- Conectividad Wireless-G de alta velocidad para el PC de escritorio, ahora con la mejora del rendimiento que aporta SpeedBooster.
- La nueva tecnología SpeedBooster aumenta el rendimiento de la red inalámbrica hasta en un 35%.
- También es compatible con redes Wireless-G estándar y Wireless-B.
- Comunicaciones inalámbricas protegidas gracias a la encriptación de hasta 128 bits y WPA.
- Conectividad Wireless-G 802.11g.
- Velocidades de transferencia de datos de hasta 54 Mbps en el radio de 2.4 GHz.

ADAPTADOR DE RED USB WIRELESS-B



Características

- Permite conectar el ordenador de escritorio o portátil a una red Wireless-B (802.11b) a velocidades de hasta 11 Mbps.
- Sencillez: la compatibilidad con USB evita la necesidad de instalar ninguna herramienta en el ordenador de escritorio o portátil.
- Protección de la comunicación inalámbrica mediante encriptación de datos de hasta 128 bits.
- El asistente de configuración incluido le guía paso a paso durante la misma.
- Velocidades de transferencia de datos de hasta 11 Mbps en el radio de 2.4 GHz.

INEXQ_PCCARD54



Características

- Tarjeta de red para laptop inalámbrica 54 Mbps.
- Compatible con IEEE 802.11g.
- Adaptador inalámbrico PC Card Drive (PCMCIA).
- Tecnología 2.4 Ghz.
- Antena interconstruida.
- 300 m de alcance.
- Compatible Wi-Fi/WPA.

ADAPTADOR PARA ORDENADOR PORTÁTIL WIRELESS-G CON SPEEDBOOSTER



Características

- Red Wireless-G de alta velocidad para ordenador portátil, ahora con la mejora del rendimiento que aporta ApeedBooster.
- La nueva tecnología SpeedBooster aumenta el rendimiento de Wireless-G hasta en un 35%.
- También es compatible con redes Wireless-G estándar y Wireless-B.
- Comunicaciones inalámbricas protegidas gracias a la encriptación de hasta 128 bits y WPA.
- Conectividad Wireless-G 802.11g.
- Velocidades de transferencia de datos de hasta 54 Mbps en el radio de 2.4 GHz.

TARJETA WIRELESS-B COMPACTFLASH



Características

- Conectividad Wireless-B para prácticamente todos los Pocket PC.
- Encaja en ranuras CompactFlash (CF) de tipo I o II.
- Administración de alimentación incorporada para ahorro de batería.
- Utilidad de administración en pantalla para una fácil configuración.
- Velocidades de transferencia de datos de hasta 11 Mbps en el radio de 2.4 GHz.
- Conectividad Wireless-B 802.11b.

ADAPTADOR PARA ORDENADOR PORTÁTIL WIRELESS-G



Características

- Red Wireless-G (802.11g) de alta velocidad para ordenador portátil.
- Velocidades de transferencia de datos de hasta 54 Mbps: 5 veces más rápido que Wireless-B (802.11b).
- Funciona con redes Wireless-B (a 11 Mbps).
- Seguridad inalámbrica: encriptación WEP de hasta 128 bits y WPA.
- Banda de radio de 2.4 GHz.

ADAPTADOR PARA ORDENADOR PORTÁTIL WIRELESS-B



Características

- Conectividad Wireless-B (802.11b) para ordenadores portátiles.
- Velocidades de transferencia de datos de hasta 11 Mbps en el radio de 2.4 GHz.
- Encriptación de 128 bits para protección de datos.
- El asistente de configuración que se incluye guía paso a paso durante la configuración.

INEXQ USB54



Características

- Tarjeta Inalámbrica USB. 54 Mbps.
- Se conecta a una LAPTOP o PC.
- Compatible con cualquier Access Point de 11, 54 Mbps y Estándar 802.11x.
- Compatible con INFINITUM.
- Adecuada para comunicar dos máquinas si no se tiene Access Point.

TARJETA USB INALÁMBRICA



Características

- Tarjeta Inalámbrica USB 11Mbps.
- Se conecta a una LAPTOP o PC.
- Compatible con cualquier Access Point de 11, 54 Mbps y con el estándar 802.11x.
- Compatible con INFINITUM.
- Adecuada para comunicar dos máquinas si no se tiene Access Point.

TARJETA USB INALÁMBRICA TWINMOS



Características

- Tarjeta Inalámbrica USB 11Mbps.
- Se conecta a una LAPTOP o PC.
- Compatible con cualquier Access Point de 11, 54 Mbps y con el estándar 802.11x.
- Compatible con INFINITUM.

A4 – 1 CHECK LIST

Para la parte de tecnología a ocupar se tiene el chekc list siguiente:

NOMBRE DE LA EMPRESA

CONFIDENCIAL Y PROPIETARIO

FECHA

Check List "Tecnología a ocupar"
Proyecto "Red W-MAN"

Nombre de la persona _____

Puesto/Cargo _____

Número	Descripción	Prioridad	Cumplió
1	La red a instalar es para el hogar o para empresa	**ALTA**	
2	Que áreas se necesitan cubrir	**ALTA**	
3	El medio ambiente es el correcto	**ALTA**	
4	Equipo a utilizar	**ALTA**	
5	Seguridad	**ALTA**	
6	Velocidad de transmisión requerida	**ALTA**	
7	Usuarios enlazados	**ALTA**	
8	Instalación de equipos	**ALTA**	
9	Configuración de hardware	**ALTA**	
10	Configuración de software	**ALTA**	
11	Pruebas de transmisión	**ALTA**	
12	Pruebas de configuración	**ALTA**	
13	Pruebas de enlace en equipos	**ALTA**	

NOTAS: _____

_____

_____

_____

Fecha: _____

Nombre del evaluador: _____ Firma: _____

Para la parte de distribución de antenas se tiene el chekc list siguiente:

NOMBRE DE LA EMPRESA

CONFIDENCIAL Y PROPIETARIO

FECHA

Check List "Distribución de antenas"
Proyecto "Red W-MAN"

Nombre de la persona _____

Puesto/Cargo _____

Número	Descripción	Prioridad	Cumplió
1	Se tienen ubicadas las oficinas a cubrir	**ALTA**	
2	Estudio Geográfico	**ALTA**	
3	Se ha elegido la topología a usar	**ALTA**	
4	Tipo de antena	**ALTA**	
5	Estudio de cobertura	**ALTA**	
6	Elección de la estación base	**MEDIA**	
7	Alimentación de energía de las antenas	**BAJA**	
8	Línea de vista	**MEDIA**	
9	Compatibilidad entre antenas	**ALTA**	
10	Estudio de saturación del medio	**ALTA**	
11	Seguridad	**MEDIA**	

NOTAS: _____

_____

_____

_____

Fecha: _____

Nombre del evaluador: _____ Firma: _____

Para la parte de distribución de AP se tiene el chekc list siguiente:

NOMBRE DE LA EMPRESA

CONFIDENCIAL Y PROPIETARIO

FECHA

Check List "Distribución de AP"
Proyecto "Red W-MAN"

Nombre de la persona _____

Puesto/Cargo _____

Número	Descripción	Prioridad	Cumplió
1	Estudio de la ubicación de las diferentes áreas de trabajo	**ALTA**	
2	Compatibilidad con los clientes	**ALTA**	
3	Compatibilidad con la estación base o el nodo	**ALTA**	
4	Estudio de la saturación del medio	**MEDIA**	
5	Selección del AP	**ALTA**	
6	Configuración del AP	**MEDIA**	
7	Conexión del AP a los servicios	**MEDIA**	
8	Seguridad de la comunicación	**MEDIA**	

NOTAS: _____

_____

_____

_____

Fecha: _____

Nombre del evaluador: _____ Firma: _____

Para la parte de servicios a implementar se tiene el chekc list siguiente:

NOMBRE DE LA EMPRESA

CONFIDENCIAL Y PROPIETARIO

FECHA

Check List "Servicios a implementar"
Proyecto "Red W-MAN"

Nombre de la persona _____

Puesto/Cargo _____

Número	Descripción	Prioridad	Cumplió
1	AP a utilizar	**ALTA**	
2	Estándar a utilizar	**MEDIA**	
3	Configuración y distribución de hardware (AP, antenas, tarjetas inalámbricas, PC's, PDA, etc)	**ALTA**	
4	Software a utilizar	**MEDIA**	
5	Compatibilidad	**ALTA**	
6	Interferencia con el medio	**MEDIA**	
7	Conectividad entre los servicios	**ALTA**	
8	Pruebas de seguridad	**ALTA**	
9	Pruebas de conexión	**ALTA**	

NOTAS: _____

_____

_____

_____

Fecha: _____

Nombre del evaluador: _____ Firma: _____

Para la parte de funcionalidad de la red inalámbrica se tiene el chekc list siguiente:

NOMBRE DE LA EMPRESA

CONFIDENCIAL Y PROPIETARIO

FECHA

Check List "Funcionalidad de la red inalámbrica"
Proyecto "Red W-MAN"

Nombre de la persona _____

Puesto/Cargo _____

Número	Descripción	Prioridad	Cumplió
1	Tecnología a ocupar	**ALTA**	
2	Distribución de antenas	**ALTA**	
3	Distribución de AP	**MEDIA**	
4	Servicios a implementar	**ALTA**	
5	Seguridad	**MEDIA**	

NOTAS: _____

Fecha: _____

Nombre del evaluador: _____ Firma: _____

Bibliografía

Libros consultados

Titulo	Autor	Editorial
Todo acerca de redes de computación.	Kevin Staltz.	
Introducción a la informática.	Alberto Prieto, Antonio Lloris y Juan Carlos Torres.	
Administración de Sistemas de Información.	LOUDON.	Prentice Hall.
Organización y Arquitectura de computadoras.	Stallings, William (2001).	Pearson Educación.
Fundamentos de redes.	Bruce A. Hallberg.	Mc Graw Hill.
Transmisión de datos y redes de comunicaciones.	Behrouz A. Forouzan.	Mc Graw Hill.
Redes de computadores, protocolos, normas e interfaces.	Black, Uyless.	Alfaomega.
Redes para proceso distribuido, 2da. edición actualizada.	García Tomás, Jesús, Santiago Fernando y Patín Mario.	Alfaomega.
Comunicaciones y redes de procesamiento de datos.	González Sainz, Nestor.	Mc-Graw Hill.
Comunicaciones y redes de computadoras.	Stallings, William.	Prentice Hall.
Redes de computadoras.	Tanenbaum, Adrew.	Pearson Educación.
802.11 (Wi-Fi) Manual de Redes inalámbricas.	Neil Reid y Ron Seide.	Mc Graw Hill
Wireless LANs.	Geier, J.	Mac Millan.
WLAN Security Risks.	Dennis Fisher.	Prentice Hall.
Seguridad en Redes Wireless.	Eduardo Tabacman.	Mc Graw Hill.
Redes de computadoras.	Tanenbaum, Adrew.	Pearson Educación.
Manual de Tecnologías de Conectividad Inalámbrica.	Jorg Altenheimer.	
Wireless LAN: El estándar IEEE 802.11.	Francisco López Ortiz.	
Redes inalámbricas: IEEE 802.11.	Enrique de Miguel Ponce, Enrique Molina Tortosa, Vicente Mompó Maicas.	
Computer Networks.	Andrew Tannenbaum.	
Wi-Fi. Cómo construir una red inalámbrica.	José A. Carballar.	Alfaomega.

Direcciones consultadas de Internet

http://www.warchalking.org
http://www.smc.com
www.e-advento.com/tecnologia/wlan_intro
http://www.cybercursos.net
www.symantec.pl/region/mx/enterprisesecurity/content/framework/LAM_3245
www.idc.com
www.airespace.com
www.nortelnetworks.com
www.morelosnet.com/wwan.html
http://www.cisco.com/en/US/about/ac123/ac114/ac173/Q1-05/tech_wireless
http://secont.dyndns.org
www.ieee802.org
http://www.wi-fiplanet.com/news/article.php
http://www.optize.es/servlet
http://wireless.org.au