CAPÍTULO 4: “TECNOLOGÍAS ALTERNATIVAS”

4.1 Tecnología inalámbrica WiFi

4.1.1 Historia

En 1999 Symbol Technologies en conjunto con Nokia crearon una asociación conocida como Wireless Ethernet Compatibility Alliance, WECA. Esta asociación pasó a denominarse Wi-Fi Alliance en 2003. El objetivo de la misma fue crear una marca que permitiese fomentar de una manera más sencilla la tecnología inalámbrica y asegurar la compatibilidad de equipos.

De esta manera, en abril de 2000 WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos. Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en Alliance - Certified Products.

En el año 2002 la asociación WECA estaba formada ya por casi 150 miembros en su totalidad.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

4.1.2 Definición

WiFi es un conjunto de redes que no requieren de cables y que funcionan con base en ciertos protocolos previamente establecidos. Si bien fue creado para acceder a redes locales inalámbricas, hoy es muy frecuente que sea utilizado para establecer conexiones a Internet.

WiFi es una marca de la compañía Wi-Fi Alliance que está a cargo de certificar que los equipos cumplan con la normativa vigente que en el caso de esta tecnología es la IEEE 802.11.

En concreto, esta tecnología permite a los usuarios establecer conexiones a Internet sin ningún tipo de cables y puede encontrarse en cualquier lugar que se haya establecido un "punto de acceso" WiFi.

Para contar con este tipo de tecnología es necesario disponer de un punto de acceso que se conecte al módem y un dispositivo WiFi conectado al equipo. Aunque el sistema de conexión es bastante sencillo, trae consigo riesgos ya que no es difícil interceptar la información que circula por medio del aire.

Actualmente, en muchas ciudades se han instalados nodos WiFi que permiten la conexión a los usuarios. Cada vez es más común ver personas que pueden conectarse a Internet desde cafés, estaciones de metro y bibliotecas, entre muchos otros lugares.

4.1.3 Funcionamiento

La tecnología Wi-fi está basada en el estándar IEEE 802.11, sin embargo, eso no quiere decir que todo producto que trabaje con estas especificaciones sea Wi-fi. Para que un determinado producto reciba un sello con esta marca, es necesario que sea evaluado y certificado por Wi-fi Alliance. Esta es una forma de garantizar al usuario que todos los productos con el sello Wi-fi Certified siguen las normas de funcionalidad que garantizan la compatibilidad entre sí. Sin embargo, eso no significa que los dispositivos que no tengan el sello no funcionen con dispositivos que lo tengan. La base del Wi-fi está en el estándar 802.11.

El estándar 802.11 establece normas para la creación y para el uso de redes inalámbricas. La transmisión de esta red es realizada por señales de radiofrecuencia, que se propagan por el aire y pueden cubrir áreas de centenares de metros cuadrados. Como existen incontables servicios que pueden utilizar señales de radio, es necesario que cada uno opere de acuerdo con las exigencias establecidas por el gobierno de cada país. Esta es una manera de evitar problemas, especialmente con las interferencias.

Es bueno saber que, para que una red de este tipo sea establecida, es necesario que los dispositivos, también llamados “estaciones” se conecten a dispositivos que suministran el acceso. Estos son genéricamente denominados Access Point (AP). Cuando una o más estaciones se conectan a un AP, se obtiene, por lo tanto, una red, que es denominada Basic Service Set (BSS). Por cuestiones de seguridad y por la posibilidad de existir más de un BBS en una determinada localidad, es importante que cada uno reciba una identificación denominada Service Set Identifier (SSID), un conjunto de caracteres que, después de definido, es insertado en cada paquete de datos de la red. En otras palabras, el SSID no es más que el nombre dado a cada red inalámbrica.

Para que una red WiFi pueda funcionar se necesitan cumplir las siguientes etapas:

- El dispositivo o estación sondea el área en busca de un Access Point enviando peticiones y esperando la respuesta de un AP cercano. Si existen varios AP se elige de acuerdo a la intensidad de la señal que otorga.
- La estación envía un paquete RTS que es una petición de envío.
- Si el AP al que se envió el RTS está libre, contestará con un CTS indicando que está disponible para recibir información.
- Una vez que la estación envía los datos al AP, éste responde con un ACKNOWLEDGEMENT (ACK o acuse de recibo), en caso de haber recibido los datos o con un NACK en caso de no haberlos recibido. Así la estación sabrá si tiene

que volver a enviar la información o tendrá una confirmación de que ya fue recibida la información transmitida. Ver figura 4.1.

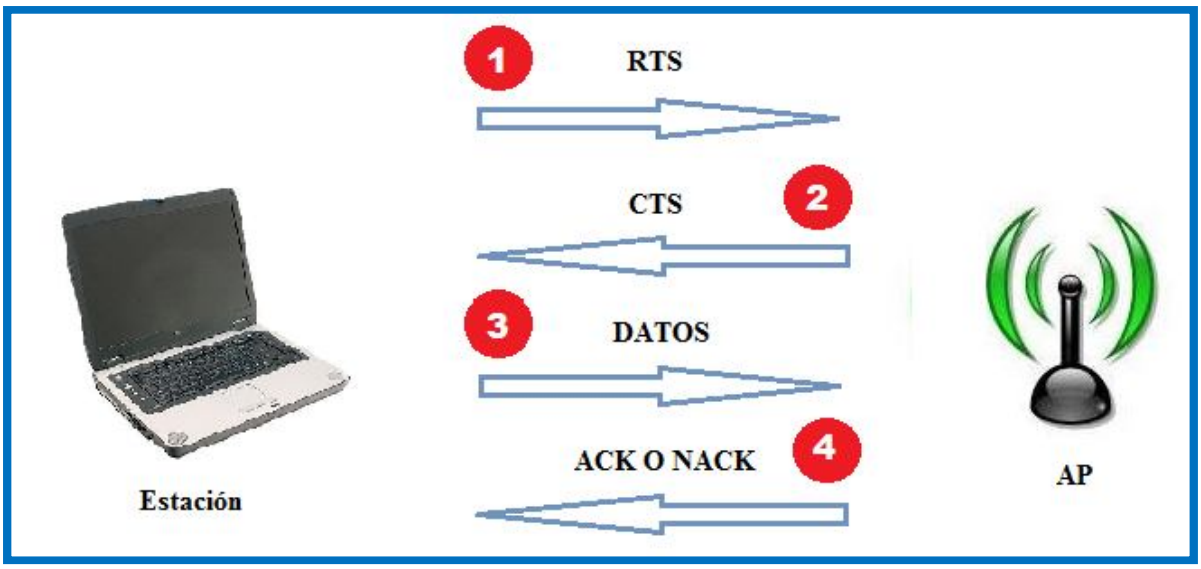

Figura 4.1 Funcionamiento WiFi

4.1.4 Papel de las capas Física y MAC en WiFi

Capa física

La capa física del modelo OSI en WiFi tiene la función de resolver todos los aspectos relacionados con la transmisión y recepción de las tramas. La capa Física ofrece tres tipos de codificación de información: FHSS, DSSS y OFDM

La banda 2.4 Ghz es una banda definida para uso ISM y usada libremente sin necesidad de licencias. La capa Física está dividida en dos partes:

- PLCP (Physical Layer Convergence Procedure – Procedimiento de Convergencia de Capa Física) **:** trata las tramas de MAC y las coloca en el formato adecuado para la PMD.

- PMD (Physical Medium Dependent Layer – Capa Física Dependiente del Medio): se encarga de manejar directamente las comunicaciones de radio sobre el medio inalámbrico.

Capa MAC

Esta capa se encuentra sobre el nivel físico, el capa MAC tiene a su cargo tareas como la fragmentación y el acceso al medio compartido. Los mecanismos de acceso al medio

indican cómo los dispositivos de la red comparten el canal de comunicación. Con eso se sabe cuándo un dispositivo transmite y cuándo recibe.

Uno de los aspectos más importantes en la capa MAC es el direccionamiento, ya que éste permite a los nodos reconocer si la trama va dirigida a ellos y quién es el remitente.La figura 4.2 muestra las capas físicas y de enlace WiFi.

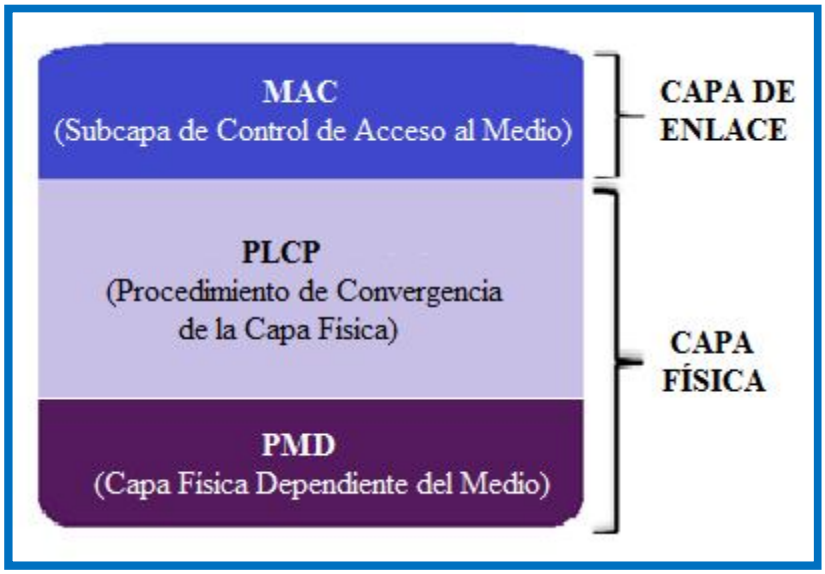

Figura 4.2 Capa Física y de Enlace en WiFi.

4.1.5 Estándares WiFi

El estándar IEEE 802.11 WiFi posee seis técnicas de transmisión por modulación:

i. PSK (Modulación por desplazamiento de fase).
ii. BPSK (Modulación por desplazamiento de fase binaria).
iii. QPSK (Modulación por desplazamiento de fase en cuadratura).
iv. CCK (Complementary Code Keying - Código Complementario de Llave).
v. QAM (Quadrature Amplitude modulation - Modulación en Amplitud por Cuadratura).
vi. FSK (Frequency Shift Keying - Modulación por Conmutación de Frecuencia).

Originalmente el estándar IEEE 802.11 manejaba velocidades de 1 hasta 2 Mbps y operaba a una frecuencia de 2.4 Ghz. Del mismo modo el estándar 802.11 define al protocolo CSMA/CA como su método de acceso. Uno de los principales obstáculos es que existió interoperabilidad entre los equipos de diferentes marcas. El problema anterior fue resuelto en el estándar 802.11b.

Los principales estándares 802.11 son:

802.11a

El estándar 802.11a utiliza el mismo grupo de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbits, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbits. La velocidad de datos se reduce a 1000, 48, 36, 24, 18, 12, 9 o 6 Mbits en caso necesario. 802.11a tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

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

802.11b

802.11b tiene una velocidad máxima de transmisión de 11 Mbits y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbits sobre TCP y 7.1 Mbits sobre UDP.

Es el estándar más conocido como WiFi, nació de la versión original. Ofrece velocidades de 11 Mbps, 5.5 Mbps, 2Mbps y 1 Mbps con un alcance de entre 100-300 metros, éste depende de la velocidad y de los obstáculos que existan

802.11c

Es menos usado que los primeros dos, pero por la implementación que este protocolo refleja. El protocolo ‘c’ es utilizado para la comunicación de dos redes distintas o de diferentes tipos, así como puede ser tanto conectar dos edificios distantes el uno con el otro, así como conectar dos redes de diferente tipo a través de una conexión inalámbrica. El protocolo ‘c’ es más utilizado diariamente, debido al costo que implica las largas distancias de instalación con fibra óptica, que aunque más fidedigna, resulta más costosa tanto en instrumentos monetarios como en tiempo de instalación.

802.11d

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

802.11e

La especificación IEEE 802.11e ofrece un estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales, con la capacidad añadida de resolver las necesidades de cada sector. A diferencia de otras iniciativas de conectividad sin cables, ésta puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales. La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que mantiene compatibilidad con ellos. Estas prestaciones resultan fundamentales para las redes domésticas y para que los operadores y proveedores de servicios conformen ofertas avanzadas.

El documento que establece las directrices de QoS, aprobado el pasado mes de noviembre, define los primeros indicios sobre cómo será la especificación que aparecerá a finales de 2001. Incluye, asimismo, corrección de errores (FEC) y cubre las interfaces de adaptación de audio y vídeo con la finalidad de mejorar el control e integración en capas de aquellos mecanismos que se encarguen de gestionar redes de menor rango. El sistema de gestión centralizado integrado en QoS evita la colisión y cuellos de botella, mejorando la capacidad de entrega en tiempo crítico de las cargas.

Estas directrices aún no han sido aprobadas. Con el estándar 802.11, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access, equivalente a DCF.
- (HCCA) HCF Controlled Access, equivalente a PCF.

En este nuevo estándar se definen cuatro categorías de acceso al medio (Ordenadas de menos a más prioritarias).

- Background (AC_BK)
- Best Effort (AC_BE)
- Video (AC_VI)
- Voice (AC_VO)

Para conseguir la diferenciación del tráfico se definen diferentes tiempos de acceso al medio y diferentes tamaños de la ventana de contención para cada una de las categorías.

802.11f

Es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

802.11g

Es la evolución del estándar 802.11b, Este utiliza la banda de 2.4 Ghz pero opera a una velocidad teórica máxima de 54 Mbits, que en promedio es de 22.0 Mbits de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas o equipos de radio apropiados. La tabla 4.1 muestra una comparativa entre los diferentes estándares 802.11.

Tabla comparativa de estándares 802.11			
	Banda de frecuencias	Velocidad máxima	Modulación
802.11a	5 Ghz	54 Mbps	OFDM
802.11b	2.4 Ghz	11 Mbps	DSSS
802.11g	2.4 Ghz	54 Mbps	DSSS Y OFDM

Tabla 4.1 Estándares 802.11.

4.1.6 Tarjetas WiFi

Una tarjeta de red es aquel dispositivo que nos permite conectarnos a Internet o cualquier tipo de red accediendo a sus recursos. Las tarjetas inalámbricas, son aquellas que vienen a sustituir a las tarjeta de red cableadas, para su funcionamiento utilizan ondas de radio, dentro de algunos de sus fabricantes destacan: Intel, Atheros, Linksys, etc.
Estas tarjetas se deben ajustar a una normativa para poder comunicarse entre sí, dentro de las más comunes destacan la 802.11b, 802.11g y la 802.11n.

Existen los siguientes tipos de tarjetas de red inalámbricas:

- PC cards: fueron muy utilizadas en un principio en equipos portátiles de cómputo. Existen dos tipos de dichas tarjetas, el primero de 16 bits conocido también como PC Card y el segundo de 32 bits llamado Card Bus. Las tarjetas PC Cards inicialmente se conocían como tarjetas PCMCIA (Personal Computer Memory Card International Association-Asociación Internacional de Tarjetas de Memoria para la Computadora Personal).

- Tarjetas PCI: son utilizadas en computadoras de escritorio. Están conformadas por una pequeña antena para recibir y enviar la señal, dicha antena es externa y existen algunas tarjetas PCI que contienen conectores para colocar antenas de mayor potencia. Las tarjetas PCI ofrecen velocidades de 54 hasta 108 Mbps, lo cual resulta idóneo para aplicaciones multimedia. La interfaz PCI soporta los algoritmos de cifrado WPA/WPA2, AES y WEP protegiendo así los datos en la transmisión de los mismos. Para proteger de accesos no autorizados a la red se hace uso de EAP y 802.1x.

- Tarjetas con interfaz USB: éstas son bastante prácticas en la mayoría de los casos Una diferencia puntual entre las tarjetas de red inalámbricas PCI y las inalámbricas USB, es que las segundas tienen menos potencia con respecto a las PCI con lo cual la intensidad de la conexión es menor.

- Tarjetas Compact Flash y Secure digital: este tipo de tarjetas inicialmente se utilizaban como medio de almacenamiento en PDAs (Personal Digital Assistant o Asistente personal digital). Posteriormente se creó una variante de tarjeta que permitía la conexión WiFi. Estas tarjetas son utilizadas en palms o pocket pc.

Las tarjetas inalámbricas poseen varios modos de funcionamiento:

a) Master o maestro.

En este modo la tarjeta inalámbrica opera como si fuera un punto de acceso, con lo cual va a emitir periódicamente el nombre de la red, además permite que otras tarjetas se asocien a la red gestionando el tráfico de todas las tarjetas que están asociadas a la misma.

b) Administrado

Este es el modo más común de funcionamiento y consiste en que la tarjeta se asocia a un punto de acceso y éste coordina a todas las tarjetas asociadas a él para minimizar los errores de transmisión. En ocasiones es necesario saber el nombre de la red WiFi que gestiona el punto de acceso, lo que se conoce como SSID (Service Set IDentifier), aunque prácticamente todos los puntos de acceso emiten el nombre de la red que gestionan periódicamente y los sistemas informan de que han detectado nuevas redes WiFi a las que se pueden asociar.

c) Modo Monitor

En este modo las tarjetas pueden analizar todos los canales de radio que se utilizan en redes WiFi, con la meta de buscar nuevas redes. Este modo es de utilidad si se desean descubrir redes inalámbricas en lugares nuevos o para saber cuáles son los puntos de mayor concentración de redes inalámbricas.

4.1.7 Validación de Usuarios

Un mecanismo de autenticación (validación) es aquel que tiene como función proporcionar una conexión segura en la transmisión. Existen tres mecanismos para la realizar la validación de usuarios en WiFi, los cuales se describen a continuación:

Open Athentication (Autenticación abierta).

Este es el protocolo por defecto que utilizan las redes inalámbricas. Los usuarios que inician el proceso de autenticación ante un punto de acceso son registrados en la red, es decir verifica a todo usuario que pide ser autenticado.

Este proceso se divide en dos partes:

- La tarjeta de red del equipo de cómputo envía una trama de solicitud de autenticación al punto de acceso.
- El punto de acceso responde con una trama de autenticación que indica si acepta o rechaza la autenticación en el campo de código de estado de la trama.

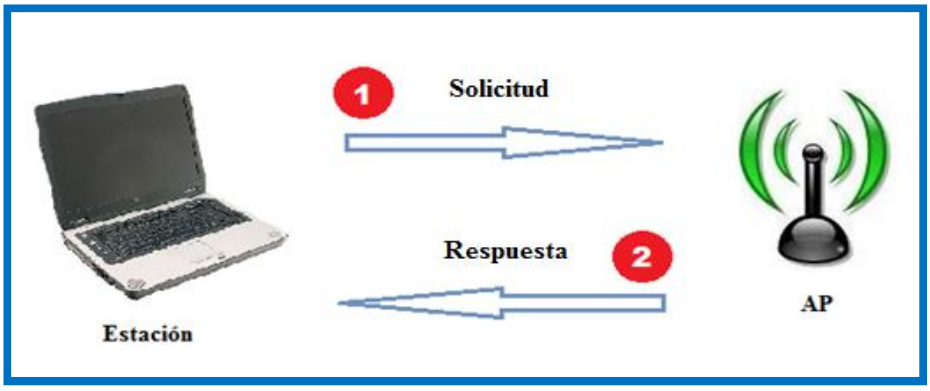

Figura 4.3 Autenticación abierta.

Una de las vulnerabilidades encontradas en este mecanismo es que todos los usuarios son autenticados y por lo tanto tienen acceso a la red.

Shared Key Authentication (Autenticación de clave compartida).

En este escenario es necesario que tanto los clientes como los puntos de acceso compartan una clave secreta para así iniciar el proceso de autenticación. Este proceso funciona de la siguiente manera:

- El cliente hace una solicitud de mensaje al punto de acceso (AP).
- El punto de acceso le envía al cliente un texto cualquiera para que sea cifrado con la clave WEP (Wireless Equivalent Privacy**)** del cliente. El texto es diferente cada vez que se solicita una validación.
- El cliente envía el texto cifrado al punto de acceso.
- El punto de acceso descifra con su clave WEP el texto cifrado y compara si éste último coincide con el texto original. Si los textos coinciden el punto de acceso da autorización de validación al cliente.
- El cliente puede conectarse a la red.

La figura 4.4 muestra cómo funciona la autenticación de clave compartida.

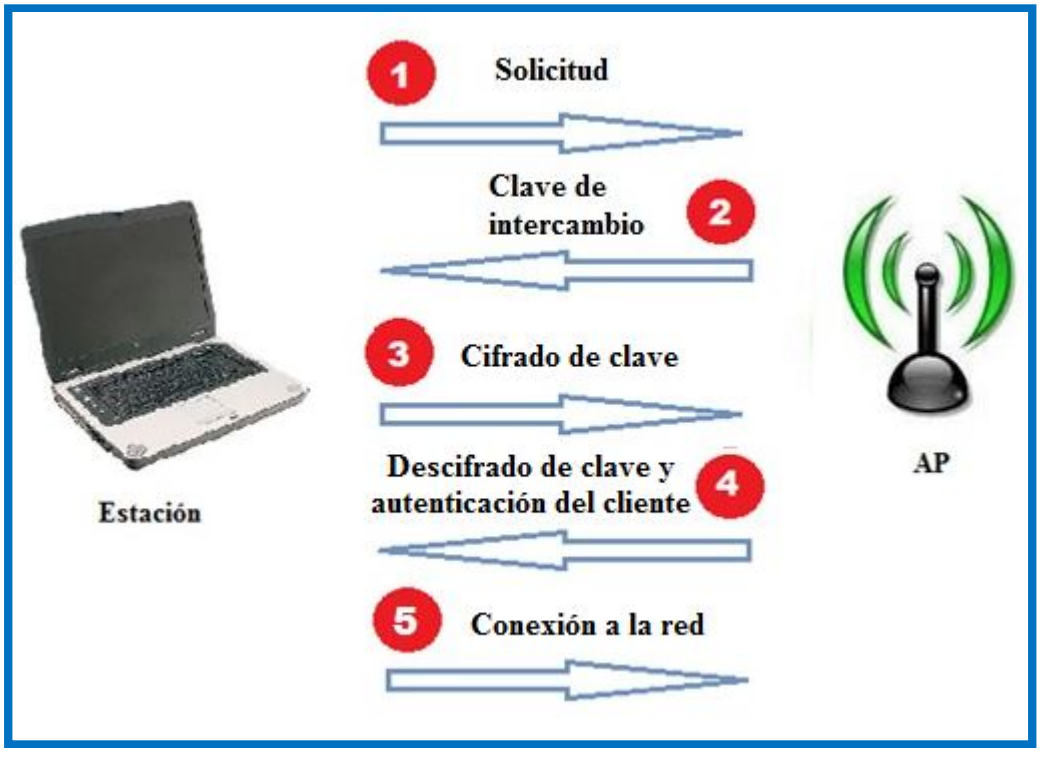

Figura 4.4 Autenticación de clave compartida.

Validación basada en dirección MAC

Una dirección MAC es un identificador hexadecimal que corresponde a una tarjeta o interfaz de red. Cada dispositivo posee su propia MAC determinada y configurada por el IEEE y por el fabricante.
Aquí el punto de acceso contiene una lista de todas las direcciones de los equipos de cómputo que pueden utilizar la red inalámbrica, limitando así los accesos no autorizados a la red.

4.1.8 Seguridad WiFi

Las vulnerabilidades que presenta esta especificación son uno de los problemas más importantes a los cuales se enfrenta la tecnología WiFi. Existen diferentes alternativas para proporcionar seguridad a las redes inalámbricas, las más usuales son la utilización de protocolos de seguridad. La seguridad en las redes inalámbricas es un aspecto fundamental y que se debe tener en cuenta en todo momento. Las redes WiFi pueden ser de dos tipos: abiertas y cerradas.

Red Abierta

En las redes abiertas cualquier equipo de cómputo o dispositivo que cuente con la tecnología WiFi que se encuentre cercano al punto de acceso puede conectarse a Internet a través de él.

Red Cerrada

En las redes cerradas, el equipo de cómputo detectará una red inalámbrica cercana disponible, pero si se desea acceder a ella se debe introducir una contraseña. En una red cerrada si se desea modificar la seguridad en la misma red, es indispensable tener conocimiento de los siguientes parámetros:

- El identificador SSID: es el nombre de la red WiFi que crea el punto de acceso. En general es el nombre del fabricante pero se puede modificar a conveniencia.

- La clave WEP: es indispensable indicar la contraseña que tendrán que introducir los equipos que se quieran conectar.

- La clave compartida WPA y WPA2: como en el caso anterior, se debe elegir una clave de acceso para poder conectarse a la red WiFi.

- En los sistemas WEP y WPA así como WPA2 las comunicaciones se transmiten cifradas para protegerlas, es decir, que los números y letras se cambian por otros mediante un factor. Sólo con la clave adecuada se puede recuperar la información. Entre más grande sea el factor de cifrado (más bits), más difícil resulta romper la clave.

Servicio de autenticación en redes WiFi

Existen tres servicios fundamentales que hacen la diferencia entre una red cableada y una inalámbrica: la autenticación, el control de acceso y la confidencialidad. La autenticación es la identificación de los usuarios de confianza en la red y que son autorizados para conectarse y navegar en la misma, teniendo acceso a los servicios y recursos que ésta ofrece.

Las formas comunes para autenticarse en las redes WiFi son:

a) Service Set Identifier (SSID)

Es una contraseña configurada por el administrador de la red, la contraseña es de máximo 32 caracteres alfanuméricos, este código sirve para identificarse con la red y de esa manera conectarse a la misma. Algunos vendedores de productos inalámbricos se refieren al SSID como el nombre de la red.

El SSID tiene dos variantes principales:

- Basic Service Set Identifier (BSSID): es utilizado en las redes Ad-Hoc.
- Extended Service Set Identifier (ESSID): es utilizado en las redes de infraestructura.

Una estrategia común para la seguridad de la red inalámbrica es desactivar el SSID, esta medida sólo sirve para el usuario promedio porque la red aparecerá como fuera de servicio.

b) Protocolo de Autenticación Extensible (EAP)

Es el modo de autenticación en el protocolo 802.1x, se utiliza entre la estación móvil y el punto de acceso. EAP es un protocolo de comunicación mutua entre los extremos de la comunicación. Una vez realizada la autenticación mutua el cliente y el servidor establecen una clave en particular para ese cliente durante su sesión activa. Las contraseñas que viajan por la transmisión son cifradas empleando el algoritmo de cifrado WEP. Es bueno aclarar que este protocolo no está limitado a las redes locales inalámbricas, ya que puede ser usado en redes cableadas, pero es más común su uso en redes inalámbricas.
Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas.

c) Protocolo 802.1x

Surgió como un método de autenticación de puertos en redes LAN para solucionar los problemas de seguridad que se tenían anteriormente con las redes inalámbricas WiFi. Este protocolo ofrece autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o evitando el acceso desde ese puerto en caso de que falle la autenticación.

Este protocolo consta de 3 elementos:

1. Solicitante (usuario).
2. Dispositivo autenticador (Access point o punto de acceso).
3. Servidor de autenticación.

Los elementos anteriores interactúan de la siguiente manera para ofrecer el siguiente funcionamiento:

- El usuario que quiere conectarse a la red manda un mensaje EAP, con lo que se inicia el proceso de autenticación.
- El punto de acceso responde con una solicitud de autenticación EAP para solicitar las credenciales del cliente.
- Posteriormente el usuario responde al punto de acceso con un mensaje EAP proporcionando los datos de autenticación que son remitidos al servidor de validación de la red local.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- El servidor puede aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso suministra un mensaje EAP de aceptación o rechazo y dependiendo del caso permitirá o no que el usuario se conecte a la red.
- Establecida la autenticación, el servidor acepta al usuario y después el punto de acceso establece el puerto autorizado para el usuario. En el protocolo 802.1x se debe distinguir entre puertos no controlados y puertos controlados. Los puertos no controlados son empleados por el punto de acceso para comunicarse con el servidor de autenticación, independientemente de que se haya autorizado a un usuario la conexión inalámbrica.

Los puertos controlados son aquellos que solamente se utilizan si el usuario cumplió con éxito el proceso de autenticación.

Cifrado en redes WiFi

Wireless Equivalent Privacy (WEP)

WEP es el algoritmo de cifrado para el estándar 802.11. La vulnerabilidad más clara de este algoritmo es utilizar la misma clave para el cifrado de todas las tramas. Con una clave estática facilita a cualquier atacante la tarea de capturar la información enviada y recibida del punto de acceso, para después descifrar la clave WEP.

La mayoría de los dispositivos WiFi son compatibles con WEP, pero el inconveniente es que el servicio está desconectado por defecto. Como los usuarios no se preocupan por activar el sistema, entonces la red queda abierta y es en esos casos cuando se accede a información confidencial de otros equipos.

Problemas de WEP:

- Se da el uso de claves estáticas lo que da como resultado la ausencia de un mecanismo de gestión de claves. De lo anterior si se deseaba actualizar las claves estáticas, el personal debe visitar cada máquina lo que es difícil de lograr en un ambiente universitario o en uno corporativo.
- Las claves se comparten entre los usuarios de la red por tiempo ilimitado.
- Hay mucho tráfico en la red.

En algunos sectores se utiliza las redes virtuales (VPN) como solución a las vulnerabilidades de seguridad que tiene el protocolo WEP.

b) WiFi Protected Access (WPA)

Es un estándar que fue diseñado para operar con todos los dispositivos para redes inalámbricas. Utiliza un cifrado mejorado por el uso de la Temporal Key Integrity Protocol (TKIP) solucionando las inconvenientes de WEP, aportando una clave de 128 bits.

Entre las principales mejoras de WPA encontramos:

- Se reforzó el mecanismo de gestión de claves.
- Se añadió un código de integridad de mensaje (MIC) para controlar la integridad de los mensajes.
- Se incrementó el vector de inicialización de 24 a 48 bits.

WPA proporciona a los usuarios de una red inalámbrica un alto nivel de seguridad, garantizando que sólo los usuarios autorizados podrán acceder a la red y a la información. WPA para el proceso de autenticación hace uso del 802.11x es un protocolo orientado a la autenticación de puertos y junto con TKIP ofrecen cifrado dinámico de claves y autenticación mutua entre clientes móviles, es decir, generan periódicamente claves para cada usuario, para cada sesión y para cada paquete enviado.

Asimismo WPA será compatible con el estándar 802.11i que incluirá como opción de seguridad el algoritmo de cifrado simétrico AES.
Otra ventaja de WPA es que permite implementar redes WLAN abiertas y seguras en áreas públicas y universidades.

c) Modos de funcionamiento de WPA

WPA fue pensado y diseñado para utilizarse en dos ambientes de trabajo diferentes: en el hogar (home mode) y en las empresas (enterprise mode).

- Home mode: está enfocado a usuarios domésticos y a pequeñas redes. Utiliza una clave compartida en las estaciones de trabajo y puntos de acceso. Dicha clave sólo se utiliza para iniciar el proceso de autenticación.

- Enterprise mode: este modo de funcionamiento es utilizado en las empresas. Se necesita un servidor configurado para desempeñar las tareas de autenticación, autorización y contabilidad.

d) WiFi Protected Access 2 (WPA2)

Este protocolo de seguridad está basado en el estándar 802.11i, es considerada la segunda versión del mismo. El protocolo WAP2 utiliza el algoritmo de AES.
Como el algoritmo de cifrado AES es más robusto, es necesario tener un hardware más robusto, por lo que los puntos de acceso antiguos no son compatibles con WPA2. Para poder ser utilizado en computadoras es necesario que éstas soporten el WPA2 al igual que los puntos de acceso involucrados, ya que existen puntos de acceso que no lo soportan.

El WPA2 puede funcionar en dos modos distintos: WPA2-enterprise y WPA2-personal.
El modo WPA2-enterprise incluye todo el conjunto de los requisitos WPA2 y es compatible con la autenticación basada en 802.1x/EAP, mientras que el modo WPA2-personal está pensado principalmente para las pymes y los hogares que requieren una administración de la red menos compleja.

En la tecnología WiFi se utilizan mecanismos de autenticación y algoritmos de cifrado para conservar la privacidad en la información que se envía. Pero se deben tomar medidas extras para mantener la seguridad de la red, esta tarea será realizada por el administrador de la red. De acuerdo con sus necesidades se toma la decisión de implementar una de las siguientes medidas adicionales de seguridad.

Virtual Private Network (VPN)

Es una herramienta que se utiliza para proteger las comunicaciones que consiste en un conjunto de dispositivos conectados a través de canales seguros permitiendo el acceso remoto y servicio de la red de forma transparente y segura. Como la comunicación entre sitios es vulnerable a ataques, es por eso que el uso de una red privada virtual garantiza que el tráfico que circula entre diferentes puntos y tengan como medio una red pública sea privado. Un túnel es un medio por el cual viajan los paquetes de Internet pero son paquetes cifrados.
Las redes virtuales son implementadas en los routers porque los dispositivos VPN operan a nivel de red, en conexiones seguras utilizando encapsulación, cifrado y autenticación. Cuando un usuario remoto solicita un acceso remoto a la red se crea una conexión al servidor VPN.

Utiliza redes de comunicación a través de las redes IP públicas o privadas, dichos túneles garantizan la seguridad por medio del protocolo IPSec que es un método de cifrado muy robusto difícil de romper, además facilita la autenticación de los equipos de la red.

Existen varios tipos de VPN´s:

- Acceso remoto: es conocida también por el nombre de Virtual Private Dial-up (VPDN). Este tipo de red consiste en usuarios que se conectan a la red de manera remota utilizando el Internet como vínculo de acceso.
- Sitio a sitio: se pueden conectar múltiples sitios con un lugar fijo por medio de una red pública o privada. Este tipo de red se utiliza para conectar por ejemplo sucursales remotas de una empresa con su sede principal.
- Interna: es parecida a la de acceso remoto con la diferencia de que el medio de conexión es la red local del lugar.

Como toda tecnología, las VPN´s tienes sus ventajas y desventajas:

Ventajas

- Mejoran la productividad de la empresa al proporcionar mayor seguridad.
- Se puede extender su alcance geográfico.

Desventajas

- Si se tienen muchos usuarios en una red inalámbrica, las redes VPN pueden ser una solución costosa.
- Hoy en día fueron reemplazadas por los protocolos de seguridad WAP y WAP2, pero en su inicio fueron de gran utilidad.
- Fueron diseñadas para proteger a partir de la capa 3 del modelo OSI y las redes inalámbricas WiFi funcionan en capa 2.
- El principal inconveniente de utilizar las VPN como una solución de seguridad en las redes inalámbricas, es que la información se cifra dos veces. Con este proceso se generan retardos en la transmisión.La figura 4.5 muestra una VPN.

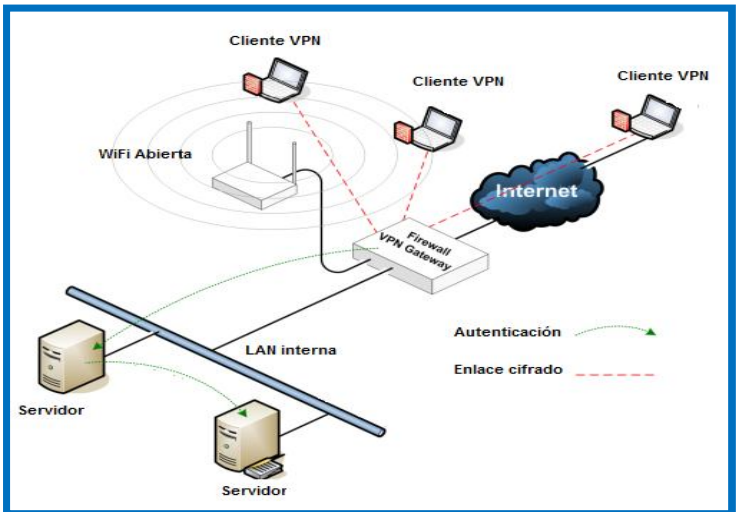

Figura 4.5 Red Privada Virtual (VPN).

Firewall

Un Firewall es un dispositivo que controla el tráfico existente entre una red interna y una red externa, de esta manera todo lo que entra y sale por medio de internet es analizado para decidir si es aceptado o es bloqueado. De esta manera el Firewall nos permite restringir los elementos no deseados de Internet.

4.1.9 Usos y Aplicaciones

En términos generales se puede decir que WiFi tiene tres usos principales:

1. Uso privado: es cuando se utiliza solamente en un ambiente privado, pudiendo ser una empresa, organización, oficina, casa, etcétera, en donde está limitado su uso a las personas de ese lugar.

2. Uso público: es cuando se utiliza para dar un servicio público de acceso a Internet. Algunos ejemplos de dicho uso son: hoteles, aeropuertos, centros de convenciones.

3. Uso comunitario: se utiliza para compartir información y dar acceso a recursos determinados a un grupo específico.

Es bueno destacar que las redes inalámbricas tienen muchas aplicaciones, dentro de algunas aplicaciones se destacan las siguientes:

- Redes marginales

Sus primeras aplicaciones fueron de carácter marginal, éstas se referían a la instalación de redes en lugares de difícil acceso o que era complicada la instalación de una red cableada.

- Redes corporativas en el escenario empresarial

Trata del caso más típico y para el cual fueron diseñadas este tipo de redes. Consiste en un conjunto de puntos de acceso esparcidos por toda la empresa formando así una red WLAN.

- Hot spot

Un hot spot inalámbrico permite que aquellos dispositivos que cuenten con WiFi se conecten a Internet a través de él. Los hot spots son redes WiFi abiertas al público de manera que cualquiera puede conectarse a ellas. Los hot spots tienen una cobertura de unos 30 metros aproximadamente, en ocasiones son gratuitas y en otras se debe pagar para conectarse a ellos. Los hot spot son utilizados en hoteles, aeropuertos, restaurantes o en espacios abiertos.

- Comunicaciones WiFi en hospitales

Esta aplicación es de gran utilidad para este tipo de escenarios porque facilita el acceso desde cualquier punto a recursos de diagnóstico y conocimiento especializado. La principal

ventaja es que el sistema sanitario se vuelve más eficiente y competitivo gracias al monitoreo de los pacientes.

- Conexión de banda ancha en hoteles

El contar con este servicio de tecnología inalámbrica representa un valor agregado que el hotel puede ofrecer sus clientes. Así tendría conexión inalámbrica a Internet desde las habitaciones y espacios comunes del mismo hotel.

- Conexión de banda ancha en campus universitarios

Con esta aplicación la red inalámbrica da cobertura a las zonas más comunes del área universitaria entre ellas destacan las bibliotecas, cafeterías, salones, laboratorios, etcétera, de esa manera todos los alumnos que dispongan de un dispositivo que cuente con la tecnología inalámbrica WiFi podrán conectarse a la red de la universidad.

- WiFi en las empresas

Si se cuenta con una red inalámbrica en una empresa es posible que todos sus empleados puedan conectarse disfrutando de la movilidad que ofrece el WiFi.

Asimismo las redes inalámbricas ofrecen a las empresas la opción de extender su red más allá de un solo edificio. En el caso de que una empresa cuente con dos edificios y entre ellos exista una clara línea de visualización, será posible el envío de datos a través de la red, usando la arquitectura punto a punto. El envío y recepción de datos se lleva a cabo por microondas y suele tener un alcance de aproximadamente 20 kilómetros. Con lo anterior la empresa puede ampliar su red sin la necesidad de pagar a una compañía externa el acceso a la red.

En el ambiente empresarial WiFi es de gran utilidad para realizar la supervisión de stocks, seguimiento de inventarios, la consulta a base de datos, la realización de pedidos y facturación desde cualquier parte del almacén haciendo uso de la red inalámbrica de lugar.

- WiFi en redes inalámbricas domésticas

Una red inalámbrica doméstica es mucho más sencilla y económica de instalar en todas los cuartos del hogar, en lugar de cablear todas las habitaciones con cable de red. Para montar una red inalámbrica se necesitan equipos de cómputo con tarjeta WiFi, un router inalámbrico y un proveedor de servicios a Internet.

El router inalámbrico tiene dos funciones principales:

- Conecta a todos los equipos entre sí, con lo que podrán compartir archivos y dispositivos.
- Conecta todos los equipos de cómputo a Internet.

Para lograr lo anterior, el router inalámbrico debe tener una IP, ésta permite que el dispositivo acceda a la red y es asignada por el proveedor de servicios de Internet.
Los equipos para que tengan conexión a la red necesitan una dirección IP que es asignada por el router inalámbrico.

- Comunicaciones internas en los transportes

Destacan en el sector ferroviario para gestionar las comunicaciones internas en dicho transporte. Asimismo ayuda a la transmisión de imágenes que muestra el estado de los andenes en las estaciones del metro.

4.2 Tecnología inalámbrica WiMax

4.2.1 Introducción

Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. El protocolo que caracteriza esta tecnología es el IEEE 802.16. Una de sus ventajas es dar servicios de banda ancha en zonas donde el despliegue de cable o fibra por la baja densidad de población presenta unos costos por usuario muy elevados tales como las zonas rurales.

El único organismo habilitado para certificar el cumplimiento del estándar y la interoperabilidad entre equipamiento de distintos fabricantes es el Wimax Forum: todo equipamiento que no cuente con esta certificación, no puede garantizar su interoperabilidad con otros productos.

Existen planes para desarrollar perfiles de certificación y de interoperabilidad para equipos que cumplan el estándar IEEE 802.16e lo cual hará imposible la movilidad, así como una solución completa para la estructura de red que integre tanto el acceso fijo como el móvil. Se prevé el desarrollo de perfiles para entorno móvil en las frecuencias con licencia en 2,3 y 2,5 Ghz.

4.2.2 Definición

WIMAX (W*orldwide Interoperability for Microwave Access / Interoperabilidad Mundial de Acceso por Microondas*) es un sistema que permite la transmisión inalámbrica de voz, datos y video en áreas de hasta 48 kilómetros de radio. Se proyectó como una alternativa inalámbrica al acceso de banda ancha ADSL y cable, y una forma de conectar nodos WiFi en una red de área metropolitana. Research and Markets ha hecho su estudio de futuro y prevé que para el año 2009 haya 15 millones de usuarios de esta tecnología móvil.

A diferencia de los sistemas WiFi que están limitados, en la mayoría de las ocasiones, a unos 100 metros (y hasta 350 metros en zonas abiertas), WIMAX tiene una velocidad de transmisión mayor que la de WiFi, y dependiendo del ancho de banda disponible, con tasas transferencia de 70 Mbps comparado con los 54 Mbps, como óptimo, que puede

proporcionar el sistema WiFi. En definitiva, WIMAX es un concepto similar a Wifi pero con mayor cobertura y ancho de banda.

El protocolo de comunicación digital es el denominado IEEE 802.16. El estándar 802.16d para terminales fijos, y el 802.16e para estaciones en movimiento. El estándar inicial 802.16 se encontraba en la banda de frecuencias de 10-66 Ghz. La nueva versión 802.16a, de marzo de 2003, usa una banda del espectro radioeléctrico más estrecha y baja, de 2-11 Ghz. En el estado español esta red inalámbrica funciona en las bandas de 5,4-5,8 Ghz.
Esta tecnología de acceso transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias. Está basada en **OFDM** (*Orthogonal Frequency Division Multiplexing / Multiplexación por División de Frecuencias Ortogonales*) con 256 subportadoras que puede cubrir un área de 48 Km, con una capacidad de transmisión de datos hasta 75 Mbps.La figura 4.6 ilustra una red básica WiMax.

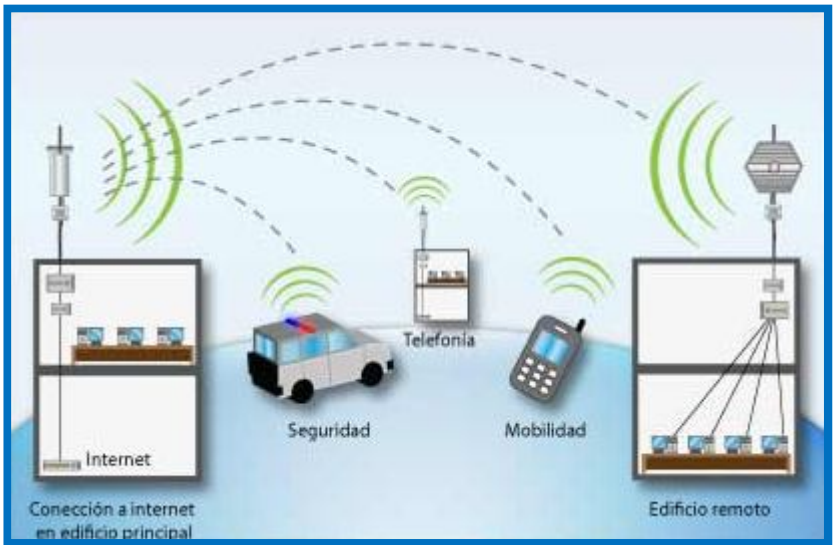

Figura 4.6 Red WiMax

4.2.2 Componentes de una red WiMax

WiMax es parecido a WiFi con la diferencia de que el primero emite en toda un área metropolitana, en lugar de una única ubicación. La arquitectura de la red WiMax es esquemáticamente similar a la arquitectura punto-multipunto de una red celular. El diseño de una red WiMax está basado en los siguientes principios:

- Espectro: la capacidad de utilizar ambos espectros, el licenciado y el no licenciado.
- Topología: soportar diferentes topologías de red (Punto-Multipunto y Malla).
- Adaptabilidad: independientemente de la topología de la red, debe ser capaz de integrarse con otras tecnologías o servicios como son el WiFi.
- Movilidad: la capacidad de extender la movilidad de la red de banda ancha ofreciendo sus servicios multimedia.

Dentro de los componentes que integran una red inalámbrica WiMax, se tienen:

a) Estación base WiMax (WiMax Base Station)

Una torre WiMax es también conocida como una estación base WiMax. La torre WiMax es parecida a una torre de telefonía con la diferencia de que presta servicios de Internet en lugar de servicio telefónico. Es importante destacar que una estación base no necesariamente debe residir en una torre, también puede estar localizada en terrazas de edificios y en otras estructuras elevadas. Usualmente una estación base da cobertura a un radio de aproximadamente 50 km, a esa área de cobertura de la estación base se le denomina célula, de esa forma cualquier nodo que se encuentre dentro de esa distancia tendrá acceso a Internet.

La antena de la estación base puede ser omnidireccional dando una forma circular a la célula, o antena direccional dando un rango de cobertura lineal, o antenas sectoriales dividiendo las células largas en áreas sectoriales más pequeñas. La estación base está conectada a la red pública usando los siguientes medios: fibra óptica, cable, microondas o cualquier otro medio de alta velocidad utilizando una conexión punto a punto.
WiMax idealmente usa línea de vista no directa y la arquitectura punto-multipunto para conectar residencias y empresas.

b) Receptor WiMax (WiMax Receiver)

Un receptor WiMax debe contener una antena por separado para recibir la señal o puede ser una tarjeta de red inalámbrica en una laptop o computadora de escritorio. Al receptor WiMax también se le denomina equipo local del cliente (CPE).

La primera generación de CPE fueron los denominados CPE outdoor, que eran estaciones suscriptoras al aire libre pequeñas con forma de disco.

La segunda generación de CPE fueron los CPE indoor que eran módems instalables por el usuario similares a los módems DSL.

La tercera generación de CPE son los que vendrán integrados en las laptops y en los dispositivos móviles.

c) Backhaul

Se refiere a la conexión que existe entre el punto de acceso y el proveedor de servicios de Internet y la conexión entre este último y la red. En la mayoría de los escenarios de desarrollo WiMax es posible conectar varias estaciones base a otro backhaul.

4.2.3 Estándares WiMax

WiMax es el nombre comercial de estándares inalámbricos IEEE. Es común pensar que WiMax es una tecnología homogénea cuando en realidad es el nombre comercial de un grupo de estándares IEEE de redes inalámbricas.

El estándar original 802.16 da cobertura a conexiones LOS en un rango de frecuencias 10-66 Ghz, soportando velocidades de hasta 280 Mbps y cubriendo áreas de 50 km. Es importante destacar que existen dos versiones prácticas de este estándar: IEEE 802.16-2004 y la IEEE 802.16e. La primera es utilizada para sistemas inalámbricos fijos y la segunda está definida para el acceso a móviles A continuación se describen todos los estándares 802.16:

802.16ª

Fue publicado el primero de abril del 2003, tenía la función de hacer uso del espectro licenciado y no licenciado, asimismo incorpora las características de sin línea de vista (NLOS) y calidad de servicio (QoS). En los enlaces NLOS en frecuencia de 2-11 Ghz, soporta velocidades de 75 Mbps, cubriendo distancias de 5 a 8 km, fue diseñado para soportar multimedia (voz, video, datos). Éste fue olvidado ya que posteriormente se centró la atención en el IEEE 802.16-2004.

802.16b

Incrementó el espectro de 5 a 6 Ghz. Asimismo incluyó una mejora al aportar una fuerte calidad de servicio, para la transmisión en tiempo real de voz y video con lo que permitía transmitir con baja distorsión en la señal.

802.16c

Opera en el rango de frecuencias de 66 Ghz. Dentro de sus mejoras destaca una mejor interoperabilidad entre los equipos de diferentes fabricantes.

802.16-2004

Se le conoce como la versión fija del estándar WiMax y fue aprobado en junio del 2004, además este estándar sustituyó a la versión 802.16a. Este estándar opera en frecuencias de 2 a 11 Ghz, su velocidad de transferencia es de 70 Mbps, siendo su rendimiento real de 40 Mbps. La cobertura de radio es de aproximadamente 4 a 7 millas. Es una nueva tecnología de acceso inalámbrico fijo, es de gran utilidad para el acceso básico y de voz en aquellos lugares donde se carece de cualquier otra tecnología que presta el servicio de Internet. Este estándar es una solución viable para el backhaul inalámbrico y para las redes celulares, en particular si se emplea el espectro con licencia. Asimismo esta tecnología ofrece una alternativa inalámbrica al módem por cable y a DSL, porque 802.16-2004 es exclusivamente para el acceso fijo, es decir, Internet en hogares de banda ancha de manera inalámbrica.

El estándar 802.16-2004 también puede soportar voz sobre IP, en el caso de utilizar el códec G.729 puede soportar hasta 96 llamadas de voz simultáneamente en un mismo canal de radio de 3. 5 MHz. Después de la aprobación del estándar 802.16-2004 se encontraron algunos errores que debieron corregirse, lo que dio paso a la creación de un nuevo estándar denominado 802.16e. Posee modulación OFDM que es menos compleja que la modulación OFDMA con lo que el despliegue es más rápido y es menos costoso. Se carece de mucha

flexibilidad al momento de controlar el ancho de banda. Soporta las técnicas de acceso al medio: TDD y FDD. Además este estándar está diseñado para soportar las denominadas smart antenas (antenas inteligentes).

802.16e

Este estándar estaba previsto para ser aprobado a mediados del año 2005, pero esto no sucedió hasta el último cuarto de ese año. Ofrece una velocidad de transferencia de 50 Mbps y su cobertura es de 1 a 3 millas. Es otra variación del 802.16 que le sigue al 802.16-2004, con la característica de que ambos estándares operan a la misma frecuencia (11 Ghz) y la diferencia que éstos no son compatibles, con lo cual se necesita una nueva solución de hardware y software, además es un impedimento si se desea escalar del estándar 802.16-2004 al 802.16e. Una característica nueva y clave que aporta este nuevo estándar es la portabilidad, cosa de la cual carecía el 802.16-2004, el objetivo del 802.16e es el mercado móvil ya que soporta sesiones de voz y datos. Una aplicación del mercado móvil es la telefonía móvil y utiliza la tecnología OFDMA, dicha técnica es más compleja que OFDM y se tiene una mejor asignación del ancho de banda para cada usuario.

En el estándar una extensión base puede transmitir a múltiples estaciones suscriptoras al mismo tiempo pero en canales separados, similarmente múltiples estaciones suscriptoras pueden transmitir al mismo tiempo a una extensión base. Cada canal tiene una anchura desde 1.25 hasta 20 Mhz.

En resumen, el nuevo estándar IEEE 802.16e ofrece mejoras a la tecnología respecto al estándar original WiMax. Estas mejoras pueden ser clasificadas de la siguiente manera:

- *Movilidad:* el soporte de la movilidad es la nueva y principal característica de este nuevo estándar, el cual introduce una nueva capa MAC que permite que una estación suscriptora mantenga su conexión activa mientras se mueve de una extensión base a otra. Y está diseñado para soportar aplicaciones móviles con velocidades arriba de 160 kph.

- *Alta disponibilidad:* la alta disponibilidad en los ambientes sin línea de vista directa pueden ser soportados con el móvil WiMax, utilizando una antena avanzada así como canales de codificación y técnica de modulación dinámica.

- *NLOS:* nuevas tecnologías han sido introducidas en el WiMax móvil, éstas incluyen soporte para la tecnología de antenas inteligentes, así como múltiples entradas múltiples salidas (MIMO), que son mecanismos que incrementan el funcionamiento de los enlaces NLOS.

- *Seguridad:* basándose en las características del estándar original WiMax, la especificación móvil WiMax introduce un número de mejoras. Por ejemplo, la introducción del algoritmo de cifrado estándar (AES).

Con esta versión se tiene soporte a los dispositivos móviles como son: los smartphones (teléfonos inteligentes), PDA's (Personal Digital Assistant-Asistente Personal Digital).

4.2.4 Modos de operación

Los modos de operación definidos en WiMax son:

- Punto-multipunto (PMP): en este modo de operación existe una estación base que controla toda la red en donde todos los usuarios de la misma se conectan a dicha estación base, con lo cual la topología punto multipunto es una topología centralizada porque la estación base es la controladora de la red.

  La transmisión de los datos se divide en tramas downlink y uplink usando las técnicas TDD y FDD. El estándar soporta este modo de operación en el rango de frecuencias de 10 a 66 Ghz, con lo cual la transmisión de datos se debe realizar utilizando líneas de vista directa (LOS). La figura 4.7 ilustra el modo PMP.

Figura 4.7 Modo PMP.

- Modo Malla (MESH): en este modo la comunicación se lleva a cabo entre los diferentes nodos de la red, así los usuarios se conectan unos con otros directamente. Y también la conexión puede llevarse a cabo entre el nodo y la estación base.

Figura 4.8 Modo MESH.

Este tipo de redes puede realizar las operaciones de maneras diferentes:

- Distribuida: todos los nodos de la red se deben coordinar entre sí al momento de transmitir para evitar colisiones con los datos.
- Centralizada: existe una estación base Mesh que recopila todas las peticiones de envío de datos de todas las estaciones base de un determinado sector y otorgar los respectivos recursos para cada enlace y así iniciar la transmisión.

Así como entre un nodo y la estación base de operación no se requieren de una estación coordinadora que controle toda la red, aquí los usuarios se conectan unos con otros. Dentro de este modo de operación existen tres términos importantes: vecino, vecindario y vecindario extendido. Se denomina vecinos a aquellas estaciones que tienen un vínculo directo con un nodo. Los vecinos de un nodo forman un vecindario. Y un vecino extendido contiene adicionalmente todos los vecinos de un vecindario. Este modo de operación opera en los espectros de licencia y sin licencia a frecuencias de 2 a 11 Ghz utilizando enlaces NLOS.

4.2.5 Antenas WiMax

Las antenas de WiMax, así como las antenas para la radio del coche, el teléfono, la radio de FM, o la TV, se diseñan para optimizar el funcionamiento para un determinado uso.

a) Antenas Omnidireccionales

Las antenas direccionales son como un foco y las antenas omnidireccionales son como una bombilla que emite luz en todas las direcciones en menor intensidad que la de un foco, generando así un menor alcance. Las antenas omnidireccionales se utilizan en configuraciones punto-multipunto. La desventaja principal de una antena omnidireccional es que su energía se debe difundir 360 ° provocando la disminución de la fuerza de la señal. Las antenas omnidireccionales son buenas en situaciones donde existen muchos suscriptores cerca de la estación base. La figura 4.9 muestra una antena omnidireccional.

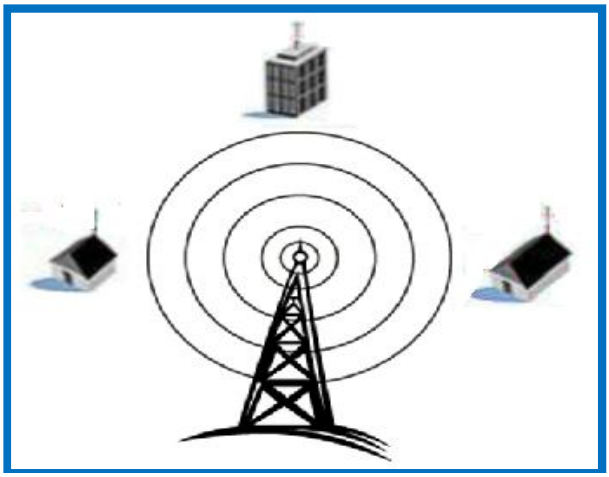

Figura 4.9 Antena omnidireccional

b) Antenas de sector

Las antenas de sector son la mezcla de las antenas direccionales con las antenas omnidireccionales. Una antena de sector sería como un foco que posee un haz de luz más ancho de lo normal. Con las antenas de sector también se puede tener una cobertura de 360º igual que una antena omnidireccional, para eso se deben instalar tres antenas sectoriales de 120º o cuatro antenas sectoriales de 90º, lo anterior es debido a que las antenas de sector brindan sólo cobertura a sectores estrechos. La figura 4.10 muestra una antena de sector.

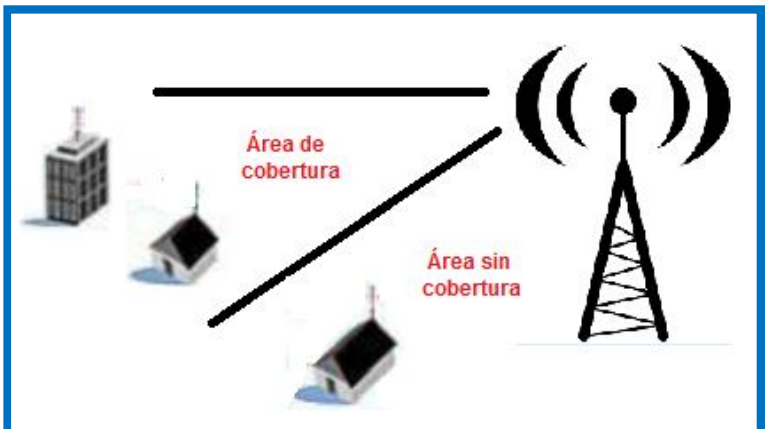

Figura 4.10 Antena de sector

c) Antenas de panel

Son antenas diseñadas para recibir y transmitir señales en una cierta orientación, de esa manera incrementa su efectividad en dicha dirección. Las antenas panel, son más útiles cuando se desea tener un área operacional en una dirección particular, de modo opuesto a un área operacional omnidireccional.
Este tipo de antenas son usadas por aplicaciones punto a punto.

4.2.6 Seguridad WiMax

Como ya hemos visto la seguridad es una prioridad en la implementación de redes inalámbricas. La privacidad, integridad y disponibilidad de la información son servicios fundamentales que se tienen que tomar en cuanta al diseñar, implementar y administrar una red inalámbrica. La seguridad de una red WiMax la podemos dividir en dos partes principales: la autenticación y el cifrado.

a) Autenticación

La autenticación es uno de los aspectos que ha recibido mayor atención dentro de la tecnología WiMax. La autenticación es el proceso con el cual la red se asegura que los usuarios finales y los suscriptores son clientes legítimos de los servicios de red. Así como en las redes privadas virtuales, en WiMax se utilizan claves de intercambio de cifrado para hacer válidas y seguras las sesiones en la red.

La estación suscriptora se comunica con la estación base utilizando los enlaces inalámbricos. Antes de la conexión, la estación suscriptora escanea su lista de frecuencias para encontrar una estación base.

La estación envía un mensaje de información de autenticación hacia la estación base, el mensaje enviado contiene el certificado de la estación. La estación envía entonces un mensaje de petición de autenticación, este mensaje puede contener los algoritmos soportados de cifrado. La autenticación finaliza cuando la estación suscriptora y la estación base poseen la AK (Authorization Key-Clave de Autorización).

Dentro de la autenticación existe un protocolo importante denominado PKM (Privacy Key Management- Administración de la privacidad de la clave) es un protocolo que define la metodología para una distribución segura de las claves que circulan entre la estación base y la estación suscriptora así como la sincronización de las mismas en este proceso. Existen dos versiones del protocolo PKM, PKM v1 y PKM v2, definidos en el estándar 802.16.

El protocolo PKM soporta tanto la autenticación unilateral y bilateral. En el modelo de la autenticación unilateral, la estación base puede autenticar la estación suscriptora, pero no en viceversa. En el caso de la autenticación bilateral o mutua, la estación base y la estación suscriptora son autenticadas ambas uno por la otra.

PKM v1

Soporta la autenticación basada en RSA, usando el certificado digital X.590. Una estación suscriptora utiliza el protocolo PKM para el intercambio de mensajes entre la estación base. El protocolo PKM sigue el modelo de una configuración cliente servidor, en donde la estación suscriptora es el cliente que se autentica con la estación base. El PKM establece una clave secreta de intercambio entre la estación suscriptora y la estación base denominada AK, durante el proceso de autorización la estación suscriptora presenta su único certificado X.509 que contiene la clave pública de la estación suscriptora y la dirección MAC de la misma.
El proceso detallado de la autorización y el intercambio de AK es descrito a continuación:

1: información de autenticación.

La estación suscriptora comienza la autorización al enviar un mensaje de información de autenticación a la estación base. Este mensaje de información de autenticación contiene el certificado X.509 de la estación suscriptora establecido por su fabricante.

Este certificado es usado por la estación base para identificar al fabricante de la estación suscriptora.

2: petición de autorización

Después del mensaje de información de autenticación la estación suscriptora manda a la estación base un mensaje de petición de autorización. El mensaje contiene los siguientes parámetros:

- Cert: es el certificado de la estación base el cual manda el mensaje de petición de autorización.
- Capacidades: consiste en el segundo parámetro del mensaje de petición de autorización, éste incluye los algoritmos de cifrado soportados por la estación suscriptora y los paquetes de criptografía.

- Paquete de criptografía: se definen como el conjunto de métodos o algoritmos para el cifrado de los datos, la autenticación de los datos y el cifrado de la clave denominada TEK a continuación se muestra la lista de los paquetes de criptografía soportados por el estándar 802.16 (ver tabla).
- CID: El tercer parámetro en el mensaje de petición de autorización se le denomina CID, en el estándar 802.16 todas las conexiones son identificadas por un CID.

Después del paso anterior y en respuesta al mensaje de petición de autorización, la estación base determina los algoritmos de cifrado y el protocolo que va a compartir con la estación suscriptora. La estación base rechaza la autorización al mensaje de petición si ninguno de los paquetes de criptografía ofrecidos por la estación suscriptora son satisfactorios.

3: respuesta a la autorización del mensaje

La respuesta a la autorización del mensaje es enviada de la estación suscriptora a la estación base en respuesta al mensaje de petición de autorización. El proceso de la reautorización es similar al de la autorización con la excepción de que el mensaje de información de autenticación no será publicado por la estación suscriptora. Además para evitar que existan interferencias entre la comunicación de la estación suscriptora y la estación base, la AK de la estación suscriptora debe tener tiempos de vida traslapados.

a) PKM v2

El PKM v2 se introduce como una parte innovadora que contiene el estándar 802.16e, añadiendo el protocolo de autenticación extensible (EAP), así como el soporte de la autenticación mutua RSA.
La autenticación mutua puede ser utilizada en dos modos de operación. El primero consiste en utilizar solamente la autenticación mutua. El segundo hace uso de la autenticación mutua y además se utiliza la autenticación EAP.

El proceso de la autenticación mutua consiste en:

- La estación base autentica la identidad de la estación suscriptora (cliente).
- La estación suscriptora autentica la identidad de la estación base.
- La estación base le provee a la estación suscriptora autenticada una AK
- La estación base le provee a la estación suscriptora autenticada las identidades y propiedades SA primarias y estáticas.

La tabla 4.1 ilustra una comparación de los protocolos PKM.

Tabla comparativa de protocolos PKM			
Característica	Autenticación	Calve de cifrado	Adicionales
PKM v1	Autenticación unilateral con el método RSA(se basa en el certificado x.509)	Triple DES, RSA y AES	-
PKM v2	Autenticación mutua: soporta los métodos EAP o RSA	Incluye el algoritmo AES con la clave wrap	Mejora el control de tráfico en la red

Tabla 4.1 Protocolos PKM.

b) Cifrado

Al mensaje que se va a enviar y por lo tanto a cifrar se le denomina texto plano y el resultado de cifrar el mensaje se le llama texto cifrado o criptograma. Varios algoritmos de cifrado son incluidos en la subcapa de seguridad del estándar 802.16. ¨Podemos destacar algunos:

- *DES (Data Encryption Standard):* los algoritmos DES y triple DES son algoritmos de cifrado de clave compartida o cifrado simétrico. El algoritmo DES se utiliza para cifrar el tráfico de datos. El algoritmo triple DES es utilizado para cifrar el tráfico.

- *AES (Advanced Encryption Standard):* es un algoritmo de cifrado de clave compartida o cifrado simétrico. El algoritmo AES utilizado para cifrar el tráfico de información en la red.

- *RSA (Rivest Shamir Adleman):* es un algoritmo de cifrado asimétrico de clave pública, es utilizado para cifrar el mensaje de respuesta de autorización usando la clave pública de la estación base.

En el tráfico de datos entre la estación suscriptora y la estación base en una red WiMax debe ser cifrado con los algoritmos antes mencionados. El cifrado se da en la capa MAC, en el caso del algoritmo triple DES el cifrado se lleva a cabo con una clave de 56 bits. En el algoritmo AES la encriptación se da con una clave de 128 bits.

El cifrado de los datos requiere de una clave denominada Transport Encryption Key (TEK) la cual usa AK del proceso de autenticación para crear la clave denominada Key Encryption Key (KEK). La clave TEK es generada de manera aleatoria por la estación base. La TEK es cifrada con triple DES, RSA y AES.

4.2.7 WiMax vs WiFi

WiFi fue diseñado para Redes de Área Local, como una alternativa a las redes cableadas. La principal diferencia de WiMax respecto a Bluetooth y WiFi, es que Bluetooth es utilizado para conectar dispositivos en un radio de 10 m aproximadamente, WiFi se utiliza para armar una red inalámbrica local dando cobertura a un radio de aproximadamente 100 m.WiMax permite la comunicación de dispositivos a mayores distancias con lo que es posible implementar una red WAN.

WiMax no ha sido diseñado para ser competidor de WiFi sino más bien para complementar a WiFi en aquellas carencias que la segunda presenta.

WiFi ha llegado a ser una de las tecnologías más populares inalámbricas para las redes de área local y esto ha sido gracias a su velocidad de transferencia, sin embargo, su popularidad tiene una limitación principal, su cobertura, en comparación con la nueva tecnología WiMax. No se debe olvidar que WiFi fue desarrollada para dar cobertura sobre áreas relativamente pequeñas, como son oficinas, edificios, mientras que WiMax da cobertura a varios kilómetros de distancia desde una sola estación.
WiFi trabaja utilizando el espectro sin licencia en el rango de frecuencias de 2.4 a 5 Ghz.
Es una solución barata y un camino fácil para proporcionar conectividad de alta velocidad en áreas locales. Mientras la tecnología WiMax utiliza tanto el espectro con licencia y el espectro sin licencia además de que posee fuertes mecanismos de autenticación dentro del mismo. La tabla 4.2 muestra una comparativa entre las principales características de WiFi y WiMax y nos da una mejor visión acerca de estas tecnologías y las diferencias que existen entre éstas.

Característica	WiFi	WiMax
Escala	Ancho de Banda 20 Mhz.	Ancho de Banda de 1.5 a 20 Mhz.
Acceso	TDD asimétrico.	TDD y FDD
Rango	100 m.	50 Km
Velocidad	54 Mbps.	75 Mbps

Tabla 4.2 Comparativa entre WiFi y WiMax.

Una de las diferencias más importantes entre WiFi y WiMax consiste en que WiFi no soporta la característica de “Calidad de Servicio”, además de que no fue desarrollada para

soportar la transmisión de voz. La tecnología WiMax contempla esas carencias de WiFi y ofrece esas habilidades desde su creación. WiMax puede soportar las aplicaciones en las empresas como voz sobre IP y videoconferencias.

Todavía los operadores utilizan la tecnología WiFi en entornos cerrados de uso común como son las cafeterías y los aeropuertos. Y utilizan la tecnología WiMax para entornos abiertos debidos a la distancia de cobertura. Los defensores de esta tecnología (Foro WiMax) indican que ésta posee varias ventajas sobre la tecnología WiFi, por ejemplo en los siguientes aspectos:

- Sólo son necesarias decenas de estaciones base (antenas WiMax) para ofrecer la misma cobertura de decenas o incluso cientos de puntos de acceso WiFi.
- No existe interferencia si se utiliza el licenciado de WiMax.
- No son necesarios los amplificadores de radio porque simplemente la señal WiMax es más fuerte que la señal WiFi.

4.2.8 Aplicaciones WiMax

WiMax proporciona múltiples soluciones para redes inalámbricas. Dentro de algunas conexiones soportadas por WiMax se encuentran: banda ancha en redes metropolitanas, backhaul en redes celulares, así como voz sobre IP. La figura 4.11 muestra el alcance de las aplicaciones WiMax.

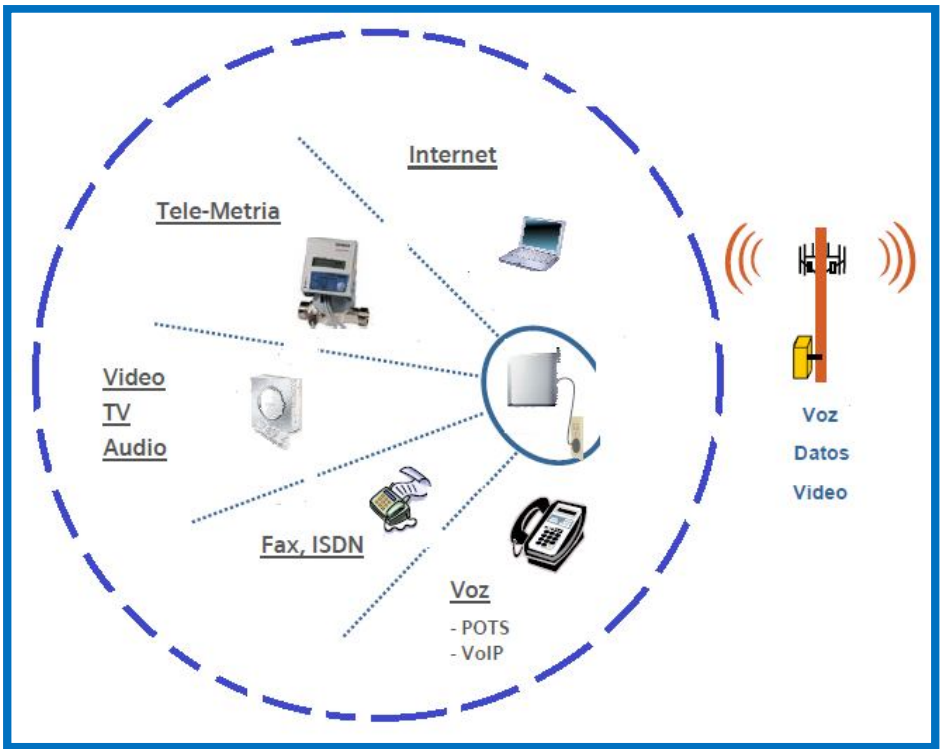

Figura 4.11 Aplicaciones WiMax.

a) Aplicación Celular backhaul

Algunos proveedores de servicio de telefonía celular se han dado a la tarea de implementar el backhaul inalámbrico como una mejor alternativa para este servicio. Debido al ancho de banda del IEEE 802.16 lo hace una excelente opción para el backhaul de empresas comerciales. Además con WiMax los operadores celulares tienen la oportunidad de disminuir su independencia de sus competidores.

Los puntos sobresalientes al utilizar WiMax como backhaul celular son:

- Dar servicio a múltiples antenas.
- Existe la capacidad de expandir el servicio móvil en un futuro.
- Es una solución más económica que el servicio tradicional.

b) Pymes

Para aquellas empresas que se encuentran fuera del alcance del DSL o que no son parte residencial del cableado estructurado, la tecnología WiMax representa un camino fácil y alcanzable para la conexión a banda ancha. También WiMax es una alternativa para dar cobertura a las áreas rurales.

c) Smartphones

La tecnología WiMax se está implementando en teléfonos celulares inteligentes, de esta manera, dichos teléfonos móviles están preparados para cambiar de una red WiMax a otra GSM o CDMA e incluyen voz sobre IP, videotelefonía, mensajería y conferencia multimedia, servicios telemáticos y de localización, y servicios multimedia tanto en difusión como bajo demanda.

d) Aplicaciones Médicas

En una situación de emergencia donde los pacientes requieren de atención médica inmediata, WiMax puede servir como la fundación de un hospital móvil. En donde el doctor puede diagnosticar a su paciente en otro lugar haciendo uso del enlace inalámbrico. El paciente que se encuentra en otra localidad puede enviar un reporte por ejemplo, presión arterial alta hacia la computadora del doctor, así posteriormente el doctor puede diagnosticar la enfermedad o padecimiento y dar un tratamiento adecuado.
La conexión entre el paciente y el doctor es haciendo uso de una conexión inalámbrica de enlace WiMax.

e) Aplicaciones Militares

WiMax es utilizado para el soporte de las simulaciones de entrenamiento y juegos de guerra en los campos militares. Los campamentos militares que se encuentran en diferentes locaciones pueden ser conectados a través de WiMax, éstos pueden intercambiar información de múltiples recursos de manera rápida y segura.

f) Aplicaciones en desastres naturales

WiMax puede ser utilizada como medio de comunicación en caso de desastres, como terremotos e inundaciones, en ese caso las redes cableadas fallen.
WiMax ayuda a conectar la localidad en desastre con los servicios telefónicos, hospitales, entre otros.

g) Instituciones Bancarias

Los sistemas de los bancos donde la seguridad es una prioridad puede ser conectada usando una red WiMax. WiMax no sólo presta una seguridad robusta, sino también un alto grado de escalabilidad. Por medio de WiMax las transacciones financieras, el correo electrónico, Internet y CCTV pueden comunicarse fácilmente.

4.2.9 WiMax en México

A pesar que desde años anteriores se ha tratado de difundir está tecnología en México el conocimiento de la misma es muy poco y su implementación en al país es aún menor. Hoy en día ya existen algunas compañías que ofrecen este servicio en el país pero aun no se ha regularizado el uso de este estándar para que este al alcance de los mexicanos. De esta manera surgen algunas preguntas cuya respuesta puede dar una mejor visión de ésta tecnología en México:

¿Es caro WiMax?

Implementar WiMax en una ciudad no lo es, requieres de un CPE Base Multipunto que permite radiar la señal de WiMax en toda la ciudad, dependiendo de la potencia del radio será la cobertura de la señal en algunos casos puede sobrepasar los 50 Km, requieres también PC Cards (para notebooks) WiMax para poder recibir la señal desde cualquier punto dónde andes, como si fuera un WiFi solo que en grande, obviamente los CPE Base y CPE Clientes aún no están a precios de risa como los router Linksys o 2Wire, pero para proyectos empresariales el precio ya es asequible y la inversión vale mucho la pena en comparación de rentar una red 3G.

¿Qué aplicaciones se le podrían dar a WiMax?

WiMax puede hacer que desde tú notebook o PDA puedas ver las cámaras que tienes en tú casa en tiempo real y con alta definición sin pagar ninguna renta o uso de ancho de banda, imagina tener conversaciones de voz con tus amigos, tener una videoconferencia ó transmitir a todos tus contactos un video stream de lo que estás viendo, imagina que desde tú PDA pudieras controlas las luces de tu casa, apagar ó prender dispositivos eléctricos mediante una tecnología de domótica como X10, si eres dueño de una empresa, imagina que en cualquier parte de la calle estés haciendo ventas, tomando pedidos, consultando información de tu base de datos, realizando un inventario, estés llevando tú extensión

telefónica vía voz sobre IP con el nuevo dispositivo de VoIP-WiMax y tener lo que es realmente una oficina virtual móvil.

¿Por qué ayudaría WiMax a México?

Porqué podría ser una forma económica y rápida de poder llevar las telecomunicaciones a los pueblos marginados de nuestro país y acercar la tecnología a los niños de los pueblos de México. Porqué a las empresas les permitiría llevar sus negocios hasta la puerta del cliente y así generar más movimientos y tener lo que realmente sería "movilidad empresarial", porqué aumentaría la innovación de los jóvenes al tener el conocimiento más cerca.

Definitivamente las aplicaciones de WiMax pueden ser muchas.

¿Por qué WiMax aún no sé usa en México?

Por desconocimiento de la tecnología también porqué la COFETEL aún no termina de revisar el protocolo, de definir que dispositivos pudieran ser permitidos para usarse en la frecuencia libre, entre otras cosas, pero definitivamente el costo no es un factor, pues un CPE Base está alrededor de los 1,500 dlls, y una PC Card alrededor de los 200 dlls, en un inicio quizá sea algo caro pero se abaratarían sin duda estos costos cuándo el uso sea masivo, hace algunos años el costo de un Access Point era de $ 1,000.00 dlls el más barato ahora se puede conseguir hasta en $ 20.00 dólares.

¿Ya hay productos WiMax disponibles en México?

Si hay varios distribuidores de dispositivos WiMax como Canopy Wireless, MotoWi4, RedLine, entre otros.