Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

UTILIZACIÓN DE LA TECNOLOGÍA WIMAX PARA MEJORAR LA EFICIENCIA DE LAS REDES INALÁMBRICAS

JOSÉ ALBERTO CÓRDOVA PAZ
Asesorado por Ing. Herbert Solórzano

Guatemala, Octubre de 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

UTILIZACIÓN DE LA TECNOLOGÍA WIMAX PARA MEJORAR LA EFICIENCIA DE LAS REDES INALÁMBRICAS

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JOSÉ ALBERTO CÓRDOVA PAZ

ASESORADO POR ING. HERBERT SOLÓRZANO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRÁCTICO EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Inga. Ligia Maria Pimentel
EXAMINADOR	Inga. Elizabeth Domínguez
EXAMINADOR	Ing. Luis Alberto Vettorazzi España
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

UTILIZACIÓN DE LA TECNOLOGÍA WIMAX PARA MEJORAR LA EFICIENCIA DE LAS REDES INALÁMBRICAS,

tema que me fuera asignado por la Escuela de Ciencias y Sistemas de la Facultad de Ingeniería con fecha 21 de enero de 2004.

José Alberto Córdova Paz

AGRADECIMIENTOS

Agradezco a:

Dios, porque para Él es toda la gloria y el me proveyó de todo lo necesario para llegar a este momento.

Mis padres, Jorge Leonardo y Dora Estela, porque ustedes han sido el ejemplo de esfuerzo, sacrificio, pero sobretodo, de amor. Gracias por apoyarme.

Mis hermanos, porque de alguna forma siempre me motivaron a continuar y contribuyeron a que llegara al final del camino.

Mis amigos, Allan Fong, Cesar Benítez, Cesar de León, Delmi, Edwin, Elías, Ervin, Javier, Jimmy, Jorge Espinoza, Jorge Tobar, José, Juan René, Julio, Kenneth, Magno, Mónica, Pablo, Oscar, Otto, Ronald, Vicky, William; a Álvaro, Chamalé, Edmar, Efraín, Gabi, Juan Miguel, Maco, Neto, Pablo Cerezo, Pablo, Vetto; Darvin, José Luis, Víctor, por ser mis compañeros en la búsqueda de mis metas, pero también lo son al llegar a ellas.

Laura, por haber sido mi segundo aliento cuando más lo necesité. Por compartir alegrías y tristezas. Por apoyarme en todo momento. Te amo.

Mi asesor, Ing. Herbert Solórzano, por colaborar en el desarrollo de este trabajo de graduación, por brindarme consejos y compartir su conocimiento.

Todos aquellos que no mencioné, pero cuya influencia en mi vida no pasó desapercibida.

Todos ustedes me han ayudado a hacer realidad mi sueño.

DEDICATORIA

Dedico el presente trabajo de graduación a:

Dios, por poner un sueño en mi corazón y darme fuerzas para lograrlo.

Mis padres, por el apoyo incondicional en todos los momentos vividos a lo largo de mi carrera.

Mi familia, por haberme ayudado a llevar esta carga hasta el final.

Mis amigos y compañeros, porque siempre me ayudaron a levantarme en los momentos difíciles.

Todas las personas que creyeron en mí y estuvieron conmigo en este largo camino.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES VII
GLOSARIO IX
RESUMEN XVII
OBJETIVOS XIX
INTRODUCCIÓN XXI

1. ESTÁNDAR 802.11

1.1 Especificación del estándar 802.11 1
1.1.1 Historia 1
1.1.2 Componentes de una red inalámbrica 2
1.1.2.1 Puntos de acceso 2
1.1.2.2 Estaciones 3
1.1.3 Topologías de red 4
1.1.3.1 Ad hoc 4
1.1.3.2 Infraestructura 5
1.1.4 *Roaming* 7
1.1.5 Capas del 802.11 8
1.1.5.1 Capa física 8
1.1.5.1.1 DSSS 9
1.1.5.1.2 FHSS 10
1.1.5.1.3 IR 11
1.1.5.2 Capa MAC 12
1.1.5.2.1 DCF 13
1.1.5.2.2 PCF 13

1.2 Estándares más utilizados 14
1.2.1 802.11a 14
1.2.2 802.11b 14
1.2.3 802.11g 15
1.3 Otros estándares definidos 16
1.3.1 802.11c 16
1.3.2 802.11d 17
1.3.3 802.11e 17
1.3.4 802.11f 17
1.3.5 802.11h 18
1.3.6 802.11i 18
1.3.7 802.11 IR 19
1.3.8 802.11j 19
1.3.9 802.11k 19
1.3.10 802.11m 19
1.3.11 802.11n 20
1.3.12 802.11r 20
1.3.13 802.11s 20

2. ESTÁNDAR 802.16

2.1 BWA 21
2.2 Especificación del estándar 802.16 23
2.2.1 Historia 23
2.2.2 Componentes de una red 802.16 25
2.2.2.1 Estación base 25
2.2.2.2 Estación suscriptora 26
2.2.3 Topologías de red 26
2.2.3.1 Redes en malla 26
2.2.3.2 Redes punto a multipunto 27

2.2.4 Capas 29
2.2.4.1 Capa MAC 29
2.2.4.1.1 Subcapa de convergencia de servicio específico 30
2.2.4.1.2 Subcapa parte común MAC 30
2.2.4.1.3 Subcapa de privacidad 31
2.2.4.2 Capa física 31
2.2.4.2.1 WirelessMAN-SC 32
2.2.4.2.2 WirelessMAN-SCa 32
2.2.4.2.3 WirelessMAN-OFDM 33
2.2.4.2.4 WirelessMAN-OFDMA 33
2.2.4.2.5 WirelessHUMAN 33
2.3 Estándares definidos 34
2.3.1 802.16a 34
2.3.2 802.16b 35
2.3.3 802.16c 35
2.3.4 802.16d 35
2.3.5 802.16e 36
2.3.6 802.16f 36
2.3.7 802.16.2 37
2.3.8 802.16.3 37

3. ANÁLISIS COMPARATIVO ENTRE WI-FI Y WIMAX

3.1 Características 39
3.1.1 802.11 39
3.1.1.1 Escalabilidad 39
3.1.1.2 Cobertura 40
3.1.1.3 Rendimiento 40
3.1.1.4 Calidad de servicio (QoS) 40

3.1.1.5 Seguridad 40
3.1.1.6 Movilidad 41
3.1.2 802.16 41
3.1.2.1 Escalabilidad 41
3.1.2.2 Cobertura 42
3.1.2.3 Rendimiento 42
3.1.2.4 Calidad de servicio 42
3.1.2.5 Seguridad 43
3.1.2.6 Movilidad 43
3.1.3 Resumen de las características 43
3.2 Aplicaciones 44
3.2.1 Aplicaciones del 802.11 44
3.2.2 Aplicaciones del 802.16 45
3.3 Ventajas y desventajas 46
3.3.1 Ventajas del 802.11 46
3.3.2 Desventajas del 802.11 47
3.3.3 Ventajas del 802.16 47
3.3.4 Desventajas del 802.16 48
3.4 Medición de los beneficios 48
3.4.1 Retorno de Inversión (ROI) 48
3.4.1.1 Caso de estudio: ROI en Intel 49
3.4.1.2 Pasos para realizar un estudio de ROI 51
3.4.2 Economías de escala 53
3.5 Tendencias 53
3.5.1 Crecimiento 54
3.5.2 Futuro 56
3.5.2.1 802.11 57
3.5.2.2 802.16 57

4. METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UNA RED WIMAX

4.1 Factores a considerar para la implementación 59
4.1.1 Leyes 59
4.1.2 Frecuencias 60
4.1.3 Disponibilidad de dispositivos 61
4.1.4 Integración con la tecnología actual 61
4.2 Análisis de factibilidad 62
4.2.1 Factibilidad técnica 62
4.2.2 Factibilidad económica 63
4.2.3 Factibilidad humana 64
4.2.4 Factibilidad de mercado 65
4.2.5 Estudio de impactos 65
4.2.5.1 Impacto ambiental 65
4.2.5.2 Impacto social 66
4.2.5.3 Impacto cultural 67
4.2.6 Resultado del análisis 68
4.3 Implementación 68
4.3.1 Aspectos a considerar 68
4.3.1.1 Servicios 69
4.3.1.2 Selección del esquema de red 69
4.3.1.3 Selección del estándar a utilizar 70
4.3.2 Requerimientos de hardware 70
4.3.3 Plan de implantación 71

CONCLUSIONES 75
RECOMENDACIONES 77
BIBLIOGRAFÍA 79
APÉNDICE A SEGURIDAD EN REDES INALÁMBRICAS 81

APÉNDICE B ECOSISTEMA TECNOLÓGICO 101

ÍNDICE DE ILUSTRACIONES

FIGURAS

1	Topología de red ad hoc	5
2	Topología de red de infraestructura	6
3	Esquema de una red en malla	27
4	Esquema de una red punto a multipunto	28
5	Diagrama de las capas del 802.16	29
6	Retorno de Inversión en Intel utilizando WLAN's	50
7	Beneficios y costos por usuario en una WLAN	51
8	Volumen generado por las soluciones inalámbricas	55
9	Tasa de penetración de WiMAX	56
10	Esquema general del ecosistema tecnológico	104
11	Ecosistema tecnológico de Wi-Fi	105
12	Esquema general del ecosistema tecnológico de WiMAX	109
13	Ecosistema tecnológico de WiMAX	110

TABLAS

I	División de frecuencias para DSSS	10
II	Espectros para redes inalámbricas de banda ancha	22
III	Resumen de características	44
IV	Tecnologías identificadas para el ecosistema tecnológico	107

GLOSARIO

3G Tercera generación de dispositivos y servicios móviles. Se realiza una transferencia de información en tiempo real, sin importar el lugar y el momento. Puede incluirse el manejo de imágenes, acceso a Internet y hasta videoconferencias.

ARP Protocolo utilizado para obtener la dirección MAC de un dispositivo solicitándola por medio de un *broadcast* que contiene la dirección IP del dispositivo.

Autenticación Método utilizado para confirmar la identidad de un usuario que intenta acceder a la red. Se realiza utilizando credenciales.

Banda Es una frecuencia o un rango de frecuencias. Existe una división de bandas y cada país tiene asignadas cada una de ellas.

Banda ancha Describe un medio de comunicación capaz de transmitir una gran cantidad de información a través de múltiples canales, sobre un sólo medio de comunicación.

BWA *Broadband Wireless Access* (Acceso Inalámbrico de Banda ancha). Tecnología que intenta proveer acceso inalámbrico a redes, con altas tasas de transferencia. Se refiere a contar con ancho de banda mayor a 1MHZ soportando tasas de transferencia mayores de 1.5 Mbps.

Cable coaxial Medio de transmisión muy utilizado para implementación de redes, consistente de un cable conductor central rodeado de un aislante dieléctrico.

Canal Un camino eléctrico, electromagnético u óptico para realizar la comunicación entre dos nodos.

DCF *Definition Coordination Function* (Función de Coordinación Distribuida). Técnica utilizada en Wi-Fi para administrar la transmisión a través del medio permitiéndole a cada nodo escuchar nodos cercanos para determinar si están transmitiendo, antes de iniciar una transmisión.

Docsis Especificación de la Interfaz de Servicios de Datos sobre Cable. Es una interfaz estándar que especifica la forma en que se intercambia información a través de cable.

DSL Línea Suscriptora Digital. Es una tecnología que es utilizada para brindar acceso de banda ancha sobre líneas de cableado telefónico. Puede transmitir datos y video.

DSSS *Direct Sequence Spread Spectrum* (Espectro Ensanchado de Secuencia Directa). Proceso de codificación binaria que dispersa los datos combinándolos con un patrón multibit o código seudo-ruido.

EAP Protocolo de Autenticación Extensible. Es un protocolo que soporta múltiples mecanismos de autenticación. Se encuentra definido en el RFC 2284. Es utilizado por el método 802.1X.

Encriptación Es el proceso de alterar la información para que sólo las personas que tienen derecho a recibir esta información puedan entenderla.

Ethernet Es una red de área local diseñada por Xerox Corp. Transmite a través de cable y utiliza como técnica de control de acceso al medio CSMA/CD. Fue estandarizado por el IEEE como el 802.3. Recientemente ha surgido una nueva versión más rápida que la original, llamada *GigabitEthernet*.

ETSI Instituto Europeo de Estándares de Telecomunicaciones. Es una organización encargada de manejar los estándares utilizados para telecomunicaciones en Europa.

FHSS *Frequency Hopping Spread Spectrum* (Espectro Ensanchado con Saltos de Frecuencia). Técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aleatorias, entre las que se realizan saltos de manera síncrona con el transmisor.

Fibra óptica Es un cable hecho de capas de fibra de vidrio muy pequeñas, a través de las cuales viaja la información transformada en señales ópticas, generadas por un láser o LED.

Hacker Persona que pretende utilizar los recursos de una red para los que no tiene autorización.

HyperLAN Red de Área Local de Alto Desempeño. Es un conjunto de estándares de comunicaciones para WLAN utilizado en Europa y adoptado por el ETSI.

IEEE *Institute of Electrical and Electronic Engineers* (Instituto de Ingenieros Eléctricos y Electrónicos). Es la organización encargada de manejar los estándares para telecomunicaciones. Estos estándares son aplicables en su mayoría para América, ya que en otras regiones existen institutos que se encargan de estas funciones.

IR *Infra Red* (Infrarrojo). Ondas electromagnéticas cuya frecuencia se encuentra arriba de las microondas, pero por debajo del espectro visible.

Interferencia Es cuando se produce una señal no deseada que impide el paso libre de la señal de radio.

LAN Es un grupo de dispositivos conectados a través de una red de tamaño pequeño. En estas redes los dispositivos se encuentran conectados a distancias cercanas.

MAC *Media Access Control* (Control de Acceso al Medio). Es una de las subcapas dentro de la capa de enlace de datos del modelo OSI. En ella se especifica la forma en que se controla el paso de la información entre las capas superiores y el medio físico de transmisión.

MAN Es un conjunto de dispositivos interconectados a través de una red. El tamaño de estas redes es mayor al de las LAN's. Pueden llegar a ser hasta de 50 Km. de distancia.

Modular Es un método para codificar la información que se transmite. Consiste en reemplazar los datos originales por secuencias generadas para cada valor. Reduce el riesgo de pérdida de información.

Multiplexar Permitir el envió de múltiples señales simultáneamente a través del mismo canal de transmisión.

NIC Es una tarjeta que permite la comunicación entre una PC y una red. Esta tarjeta controla el flujo de la información, desde y hacia la PC.

Nodo Un usuario con una NIC inalámbrica. Puede ser cualquier dispositivo que forme parte de la red.

PCF *Point Coordination Function* (Función de Coordinación de Punto). Técnica utilizada en el estándar IEEE 802.11 que permite la transferencia de marcos libres de contención basándose en un mecanismo de prioridad.

OSI Modelo de referencia desarrollado por la Organización Internacional para Estandarización en 1984. Define los estándares para la comunicación entre redes utilizando dispositivos de diferentes fabricantes y a través de diferentes aplicaciones. Es el modelo principal de la arquitectura de redes. Está basado en capas.

PCMCIA Tarjeta que sirve como dispositivo de entrada y salida, y en su mayoría es utilizada en PC's portátiles. Tiene un conector de 68 pines. Provee conexión hacia redes inalámbricas.

Paquete Es la unidad de transmisión de datos sobre una red, desde su origen hasta su destino.

Puente Dispositivo que conecta dos segmentos de red y transmite los paquetes entre ellos, utilizando el mismo protocolo de comunicación.

Protocolo Es un conjunto de reglas que definen el formato de los paquetes, además de el control de las comunicaciones entre varios dispositivos. Pueden ser de bajo o de alto nivel.

Radio frecuencia Ondas electromagnéticas a través de las que viaja información. Es un método alternativo para las redes cableadas. Es el medio más utilizado para las comunicaciones inalámbricas.

RADIUS Servicio de Autenticación de Usuarios Remota. Es un protocolo de seguridad descrito en el RFC 2865. Sirve para autenticar y autorizar usuarios. Utiliza un servidor RADIUS que es el encargado de autenticar a los usuarios.

RC4 Es un método de encriptación llamado Rivest Chipre 4. Fue creado por RSA *Data Security Inc*. Es utilizado por los métodos de seguridad WEP y TKIP.

Router Es un dispositivo que reenvía paquetes entre diferentes redes. Puede determinar hacia qué red está dirigido un paquete.

Sniffer Es un programa capaz de monitorear el tráfico dentro de una red. Es una herramienta muy utilizada por los *hackers* para obtener información de las redes.

Topología Es la forma en que se encuentra estructurada una red. Las topologías pueden ser físicas o lógicas.

X.509 Es el estándar más utilizado para certificados digitales. Puede utilizarse para certificar productos, seguridad o usuarios. Existen varias implementaciones propietarias que no son compatibles entre ellas.

RESUMEN

Actualmente el estándar más comercializado en el uso de redes inalámbricas es el 802.11b, que se deriva del estándar original 802.11. Este estándar está definido para redes de área local. De la misma forma en que las redes cableadas tienen diferentes clasificaciones, así han surgido en las redes inalámbricas, contando no sólo con redes de área local, sino también con redes de área metropolitana. Surgió la necesidad de crear un estándar para las redes de área metropolitana, que definiera las características para su funcionamiento, de la misma forma en que lo hace el 802.11 en las WLAN. Este nuevo estándar es el 802.16.

El IEEE es el encargado de la creación de los estándares, y en sus distintos grupos de trabajo se han ido desarrollando diferentes versiones, tanto del 802.11 como del 802.16. Cada una de estas versiones tiene sus propias características, y en algunos casos buscan definir aspectos que no se habían tomado en cuenta en versiones anteriores.

El 802.16 además de estar definido para ser utilizado en redes de mayor tamaño que el 802.11, también cuenta con características superiores a éste que lo hacen un fuerte competidor para la tecnología inalámbrica utilizada actualmente. Al utilizar una red inalámbrica se obtienen grandes beneficios, mayores que los obtenidos con las redes cableadas. Al mejorar las características del 802.11, el 802.16 permite también que los beneficios sean mayores.

Se han realizado estudios sobre ambos estándares, para determinar el crecimiento del mercado y cuáles son las tendencias futuras de cada uno de ellos. Los resultados de los estudios han revelado que al 802.16 comenzara su dominio en el mercado de redes inalámbricas para el año 2007, año en el que se espera que el 802.11 inicie su etapa de declinación.

Los productos 802.16 son compatibles con el estándar 802.11, aunque aún se encuentran en desarrollo. También se encuentra en desarrollo la elaboración del estándar 802.16e que permitirá brindar la capacidad de movilidad a las redes 802.16.

Existen diversos factores a considerar para realizar el despliegue de una red 802.16. Estos factores pueden variar para cada país, pero es importante tomarlos en cuenta. También es importante realizar un plan para realizar el despliegue, habiendo considerado anteriormente los factores mencionados.

Un aspecto que no puede pasarse por alto es el de la seguridad. Este tema es importante para cualquier tipo de redes, incluyendo las inalámbricas. Los dos estándares, el 802.11 y el 802.16, tienen diferentes métodos y características de seguridad, aunque los métodos utilizados por el 802.11 no brindan mucha confiabilidad para su utilización, actualmente se están desarrollando nuevos métodos para cubrir los problemas actuales. En la definición del 802.16 se incorporan mejores métodos de seguridad que el 802.16, y éste es uno de los factores que contribuyen a las tendencias de crecimiento y aceptación de este nuevo estándar.

OBJETIVOS

- **General**

  Establecer las bases para comercializar el uso de la tecnología WIMAX para telecomunicaciones en nuestro país.

- **Específicos**

1. Analizar y evaluar el estándar utilizado actualmente para redes inalámbricas
2. Analizar y evaluar el estándar propuesto para redes MAN inalámbricas
3. Evaluar comparativamente ambos estándares
4. Desarrollar una metodología de implementación de redes WIMAX
5. Identificar el grado de comercialización que puede tener la tecnología WIMAX

INTRODUCCIÓN

Hoy en día el uso de las telecomunicaciones se ha vuelto indispensable, ya que con el incremento en el uso de Internet, así como otros tipos de redes, en nuestras vidas, también se ha requerido que constantemente mejore la forma de acceder a ellas y el desempeño que nos brindan para comunicarnos.

Una tecnología que revolucionó el mundo de las telecomunicaciones fue la de redes inalámbricas, ya que con ellas se provee de la capacidad de comunicación móvil. Este fue un gran avance, debido a que ya no era necesario tener estaciones de trabajo estáticas, sino que podían realizarse las comunicaciones a través de redes desde cualquier lugar, y con nuevos dispositivos cada vez más pequeños y transportables.

Desde su surgimiento, las redes inalámbricas han tenido un gran crecimiento, ya que ofrecen ciertos beneficios en comparación con las redes fijas. Pero como todas las tecnologías, es necesario que se dé el siguiente paso en el desarrollo de las redes inalámbricas, para mejorar sus características e ir desplazando a las redes fijas como medio principal de telecomunicación.

Es por esto que se ha creado la certificación 802.16, también conocida como WIMAX, que pretende mejorar las capacidades actuales de comunicación con redes inalámbricas. Aunque su comercialización aún no es fuerte, se estima que tendrá una gran penetración al mercado y que será la tecnología de telecomunicaciones que se utilizará en un futuro próximo.

En el capítulo uno se presentará la definición de la tecnología que es utilizada actualmente en redes inalámbricas, el estándar 802.11, mostrando sus aspectos técnicos y algunas características que presentan las implementaciones de este tipo de redes. En el capitulo dos se muestra un planteamiento técnico del estándar 802.16, mostrando algunas características que se espera sean alcanzadas cuando penetre en el mercado. En el capitulo tres se realizará un análisis entre ambas tecnologías (802.11 y 802.16) conociendo ya sus aspectos técnicos y basándose en lo que cada una tiene para ofrecer, además de las implicaciones de utilizar cada una de ellas. En el capitulo cuatro se pretende desarrollar una metodología de implementación de la tecnología WIMAX, mostrando las limitaciones que pueden presentarse y qué logros pueden alcanzarse con ella. Finalmente, en el apéndice A se presentan los aspectos de seguridad para los dos estándares, mostrando además qué problemas presentan cada uno de ellos.

1. ESTÁNDAR 802.11

El estándar 802.11 fue creado para definir la forma en que se realizan las comunicaciones a través de redes inalámbricas de área local. Para conocer su funcionamiento es necesario conocer el proceso por el que ha pasado esta tecnología, desde sus inicios, durante su evolución, hasta llegar a la madurez y aceptación que ha alcanzado actualmente.

1.1 Especificación del estándar 802.11

La especificación del estándar 802.11 contiene la estructura del funcionamiento de las rede inalámbricas. Es importante conocer el funcionamiento interno de estas redes, pero también es importante tener como referencia un marco histórico sobre la evolución de dicho estándar.

1.1.1 Historia

Una red inalámbrica es aquella que utiliza ondas electromagnéticas para realizar la conexión de distintos dispositivos en una red, en lugar de utilizar cualquier tipo de cable (UTP, coaxial, fibra óptica) para este propósito. Estas redes brindan una mayor movilidad y autonomía de los usuarios con respecto a las redes cableadas.

En el año 1990 se creó el Grupo de Trabajo 802.11, perteneciente al Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, *Institute of Electrical and Electronical Engineers*).

El grupo de trabajo que se creó tenía como propósito desarrollar un estándar que definiera la forma en que se realiza la comunicación utilizando redes inalámbricas, así como lo hace el 802.3 para redes cableadas (*Ethernet*).

Después se creó el primer estándar para redes inalámbricas en el año 1997, y desde entonces ha sido adoptado por la mayoría de fabricantes de dispositivos inalámbricos. Este estándar define un conjunto de requerimientos que deben de cumplir los fabricantes de productos inalámbricos para que pueda existir una intercomunicación y compatibilidad entre ellos.

Dicho estándar fue creado para operar sobre redes LAN, llamadas WLAN, que son redes de pequeño tamaño. Opera sobre la frecuencia de los 2.4 GHz. y puede alcanzar velocidades de transmisión entre 1 y 2 Mbps. Adoptó el nombre de Wi-Fi que significa Fidelidad Inalámbrica, y es la marca que deben de tener todos los productos certificados para trabajar sobre el estándar 802.11.

Además, en 1999 se creó la Alianza Wi-Fi, que inicialmente se llamó Alianza de Compatibilidad Inalámbrica-Ethernet (WECA, *Wireless Ethernet Compatibility Alliance*). Esta alianza tiene como función certificar la interoperabilidad de los productos que están basados en el estándar 802.11, ya que deben cumplir con todos los requerimientos que se encuentran definidos en el estándar.

1.1.2 Componentes de una red inalámbrica

Al igual que las redes cableadas, las redes inalámbricas se forman a través de diversos elementos que las componen. Estos elementos son dispositivos de comunicación que son capaces de enviar y recibir información en forma de ondas.

1.1.2.1 Puntos de acceso

Son nodos de la red que tienen la funcionalidad de un transmisor y receptor de las señales que transitan por la red. Además puede ser utilizado como un puente, ya que puede unir varias redes. Debido a que cada punto de acceso (PA) solo tiene un rango de distancia hacia el cual puede llegar, en ocasiones es necesario colocar varios de ellos para cubrir toda el área deseada. De aquí surge el concepto de *roamming*, que consiste en pasar de un PA a otro sin perder la comunicación. Los PA's se conectan a redes cableadas, pero también pueden funcionar independientemente, solo para ampliar el rango de transmisión de la red.

1.1.2.2 Estaciones

Las estaciones son los dispositivos que utilizan las personas que se conectan a las WLAN a través de los PA. Estos dispositivos deben de tener tarjetas *wireless*, que pueden ser de varios tipos: PCMCIA, PCI o USB. Las tarjetas tienen que cumplir con los estándares de Wi-Fi, y dependiendo del estándar sobre el que están desarrolladas, así será su funcionamiento al conectarse a la red.

En el estándar 802.11 se definen cuatro servicios que debe tener una estación para que pueda conectarse exitosamente a la red:

- Autenticación. Sirve para controlar el acceso a la red y así mejorar la seguridad.
- Des-autenticación. Sirve para eliminar a un usuario de la red y así evitar que pueda utilizar los recursos de la red.
- Privacidad. Sirve para brindar una protección de la información que fluye a través de la red.

- Envío de Datos. Sirve para asegurar la transmisión y recepción de información de una manera confiable.

1.1.3 Topologías de red

Existen dos topologías que pueden ser utilizadas cuando se implementan redes con el estándar 802.11. Cada una de ellas indica la forma en que se realiza la conexión y los elementos que están involucrados en la estructura.

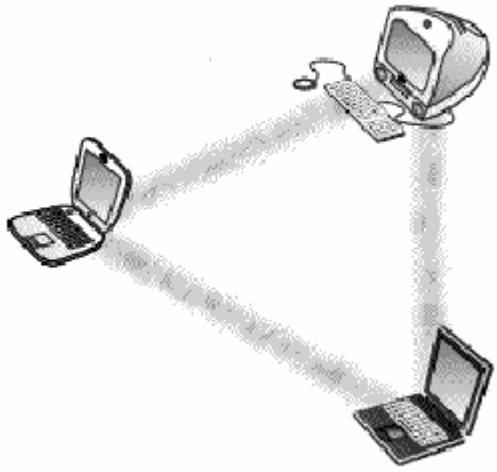
1.1.3.1 Ad-hoc

A esta topología de red se le llama Conjunto Independiente de Servicios Básicos (IBSS, *Independent Basic Service Set*). Es la topología mas básica para WLAN's. Es un grupo de estaciones de trabajo inalámbricas que se comunican entre ellas directamente, es decir, sin tener PA's para realizar la conexión. Es por ésta razón que se llaman ad-hoc, ya que fácilmente puede adaptarse a los requerimientos de implementación de una red inalámbrica, teniendo sus respectivas limitaciones, como puede ser un limitado rango de comunicación.

En esta topología no existen funciones de retransmisión, por lo que las estaciones que forman parte de la red deben encontrarse dentro del rango de transmisión. Todos los nodos de la red funcionan como *routers*, realizando las tareas de encontrar rutas para el encaminamiento de los paquetes, para que así, cualquier paquete llegue a su destino, aunque éste no sea directamente accesible desde el origen. Esta topología es utilizada cuando no es necesario contar con una infraestructura para brindar servicios, ni debe de conectarse una LAN cableada a la WLAN.

Un ejemplo de una red con topología ad-hoc es el mostrado en la figura 1, que muestra la forma en que tres computadoras con tarjetas inalámbricas pueden conectarse sin la necesidad de tener otro dispositivo inalámbrico entre las conexiones.

Figura 1. Topología de red ad-hoc



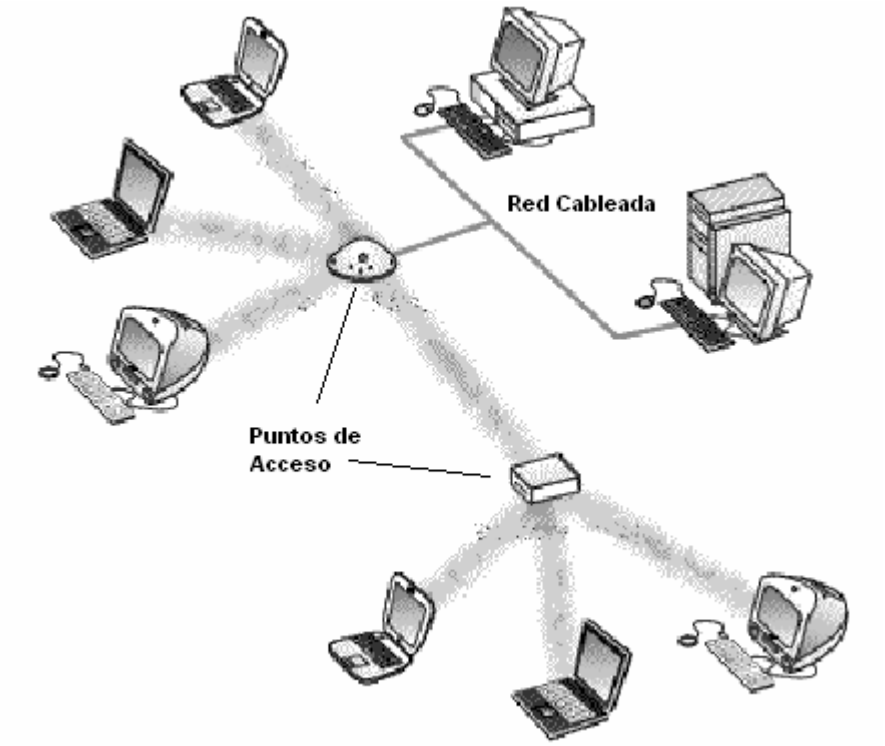
Fuente: Antonio Ruiz Moya. **Redes inalámbricas universitarias**. Pág. 9.

1.1.3.2 Infraestructura

Esta topología esta compuesta por uno o varios puntos de acceso, además de tener un grupo de estaciones inalámbricas. Cada estación se comunica con las demás a través de los PA (no directamente como en la topología ad-hoc), logrando con esto una ampliación en el área de comunicación.

Además, al utilizar la topología de infraestructura se pueden implementar servicios que no pueden ser implementados con la topología ad-hoc, y esto hace que sea mas utilizada por empresas que utilizan o que brindan estos servicios. La figura 2 muestra un ejemplo de una red que utiliza una topología de infraestructura, ya que utiliza algunos dispositivos inalámbricos para interconectar a las estaciones.

Figura 2. Topología de red de infraestructura



Fuente: Antonio Ruiz Moya. **Redes inalámbricas universitarias**. Pág. 9.

Cuando se utiliza una sola red se le llama Grupo de Servicios Básico (BSS, *Basic Service Set*) y pueden formarse grupos de varios BSS, llamados Grupo de Servicios Extendidos (ESS, *Extended Service Set*) y que sirven para realizar acciones como el *roamming*.

Dentro de la topología de infraestructura, los PA pueden utilizarse de tres maneras diferentes:

- *Gateway*. Para comunicar redes internas con externas.
- *Bridge*. Para unir varios puntos de acceso y así extender los servicios y rangos de transmisión.
- *Router*. Para unir diferentes WLAN, dentro del área de cobertura del punto de acceso.

Cada punto de acceso tiene un limite de 64 estaciones que pueden estar conectadas hacia él, aunque éste limite puede ampliarse colocando múltiples puntos de acceso, como en el ESS.

1.1.4 *Roamming*

Es el proceso de desplazarse de un BSS hacia otro sin perder la comunicación. Esto significa que un dispositivo sale de la cobertura de un punto de acceso y entra en la cobertura de otro.

También puede darse el cambio de vinculación de una estación a un PA debido a una saturación en el canal, realizando funciones de balanceo de carga.

La capa MAC es la encargada de vincular una estación móvil con un PA. La vinculación se realiza en función de la potencia de la señal que recibe la estación desde el PA.

Cuando una estación pierde la señal a medida que se aleja del punto de acceso, éste realiza un proceso llamado barrido (*sweeping*), que consiste en buscar alternativas de canales a los cuales puede conectarse la estación.

Después realiza el proceso de escaneo (*scanning*), que consiste en evaluar la calidad de la señal de cada PA encontrado en el proceso anterior, para así poder realizar la asociación de la estación con el nuevo PA. Para que pueda darse el *roamming* es necesario que la red tenga una topología de ESS.

1.1.5 Capas del 802.11

Partiendo del modelo OSI, que define las capas necesarias para la comunicación a través de redes, se definen en el estándar 802.11 las 2 capas inferiores: la capa física y la de enlace de datos (o capa MAC).

1.1.5.1 Capa física

En esta capa se definen las características físicas que debe tener el medio por el que se realizará la transmisión de datos. Existen tres formas para realizar la transmisión a través del medio físico: DSSS y FHSS, que son métodos por radio frecuencia y el método infrarrojo.

La radiofrecuencia puede utilizar frecuencias de banda ancha y banda estrecha. El 802.11 se encuentra definido dentro de la frecuencia de banda ancha. También se definió en el estándar que se usaría la banda de frecuencia de los 2.4 GHz, en el rango de 2400 – 2483 MHz.

Los métodos DSSS y FHSS utilizan el Espectro Disperso (SS, *Spread Spectrum*), que consiste en utilizar un ancho de banda más grande del que necesita el sistema para transmitir, y con ello se logra tener una mayor calidad en las señales, ya que no son afectadas significativamente por la interferencia.

1.1.5.1.1 DSSS

Espectro Ensanchado por Secuencia Directa (*Direct Sequence Spread Spectrum*). Puede soportar tasas de transmisión en el rango de 1 a 2 Mbps. Divide los 2.4 GHz en 14 canales, cada uno de 5 MHz, y necesita de 25 MHz para que los canales múltiples puedan funcionar correctamente. La información se envía a través de estos canales sin tener que realizar saltos entre ellos.

Cada *bit* de la señal se convierte en una secuencia de bits, llamada código de trozos (*chipping code*), y sirve para minimizar el impacto de las interferencias y el ruido en la señal, además de ser usado como un método de detección y corrección de errores. Aún cuando parte de la señal se pierde, tiene una gran capacidad de recuperación, ya que puede reconstruir la información en base a la secuencia de *bits* utilizada, y evitando así el reenvío de paquetes.

Comúnmente se utiliza la secuencia de Barker, que consiste en dividir cada bit en un código de 11 bits. Existen dos métodos para modular la señal: DBPSK (Fase de Conversión de Clave con Diferenciación Binaria) y DQPSK (Fase de Conversión de Clave con Diferenciación Cuadrática).

Cuando el receptor recibe los datos, recibe las secuencias de 11 bits por cada bit de la señal original, y para recuperar la información tiene que realizar un proceso de desmodularización con el mismo código utilizado por el emisor.

Además de la división de las frecuencias en canales, se realizó una asignación de varios canales a cada país, como se muestra en la tabla I. En la tabla aparecen las instituciones que regulan la asignación de frecuencias en distintas regiones, los canales, y las frecuencias de cada canal asignadas a cada institución, mostradas en MHz.

Tabla I. División de frecuencias para DSSS

Canal	FCC (Norte América)	ETSI (Europa)	Japón
1	2412	N/D	N/D
2	2417	N/D	N/D
3	2422	2422	N/D
4	2427	2427	N/D
5	2432	2432	N/D
6	2437	2437	N/D
7	2442	2442	N/D
8	2447	2447	N/D
9	2452	2452	N/D
10	2457	2457	N/D
11	2462	2462	N/D
12	N/A	N/D	2484

Fuente: Jan Boer. ***Direct sequence spread spectrum, physical layer specification*, IEEE 802.11**. Pág. 17.

1.1.5.1.2 FHSS

Espectro Ensanchado por Saltos de Frecuencia (*Frecuency Hopping Spread Spectrum*). Solo soporta tasas de transmisión de 1 Mbps. En esta técnica se divide la banda de 2.4 GHz en 75 canales, cada uno de 1 MHz.

Se realiza una modulación de la señal, que será enviada a través de un patrón de saltos, que determina por que frecuencias se transmitirá la información y los intervalos de tiempo para realizar los saltos. Tanto el emisor como el receptor deben de conocer este patrón. Los saltos de frecuencias hacen que se reduzca la posibilidad de interferencia entre estaciones, ya que la interferencia se da solo si transmiten por la misma frecuencia en el mismo instante de tiempo.

Existe un intervalo de tiempo, que tiene que ser menor de 400 ms, en el que se transmite una parte de la información. Al cumplirse cada intervalo de tiempo la transmisión se realiza en una frecuencia diferente, siguiendo el patrón de saltos.

1.1.5.1.3 IR

Infra-Rojo. Se utiliza luz infrarroja para transmitir los datos, teniendo dos tasas de transmisión: 1 Mbps (Tasa Básica de Acceso) y 2 Mbps (Tasa Mejorada de Acceso).

Existe un concepto llamado Modulación por Posición por Pulsos (PPM) que consiste en variar la posición de los pulsos para representar diferentes valores binarios. Cuando se transmite a 1 Mbps se utiliza un PPM de 16 y cuando se hace a 2 Mbps se utiliza un PPM de 4.

Debido a que trabajan de forma similar a la luz, se ven afectados de la misma forma que ella, ya que no pueden transmitir a través de objetos opacos que bloqueen el paso de la luz.

Este medio de transmisión tiene tanto ventajas como desventajas respecto a la Radio Frecuencia (RF). Algunas ventajas son:

- Ancho de banda amplio.
- Seguridad de transmisión.
- Resistencia a las interferencias.
- No tiene una gran limitación a su uso por entidades reguladoras.
- Bajo consumo de potencia.

Entre las desventajas tenemos:

- Puede existir interferencia debido a objetos.
- Tiene restricciones en el rango de transmisión.
- Velocidad de transmisión baja.

Existen dos clasificaciones para las redes infrarrojas. Estas son de corta apertura y de gran apertura. En los sistemas de corta apertura solo se cuenta con un haz infrarrojo que tiene que estar dirigido directamente entre el emisor y el receptor para que pueda existir comunicación. Esto hace que los sistemas no sean demasiado móviles, aunque si son inalámbricos. En los sistemas de gran apertura puede existir un rebote de la señal, permitiendo así que no exista un posicionamiento fijo entre el emisor y el receptor.

1.1.5.2 Capa MAC

Esta capa es similar a la utilizada para redes *Ethernet*, definida en el 802.3, y tiene tres funciones:

- Proveer entrega de datos confiable.
- Proveer un método de control de acceso al medio (CSMA/CA).
- Proveer un método de protección para la información brindando seguridad y privacidad.

Además, en el 802.11 la capa MAC realiza algunas funciones que normalmente son hechas en protocolos de capas superiores, como la fragmentación, retransmisión y acuses de recibo de paquetes, manejo de diferentes tasas de transmisión y gestión de la potencia de transmisión.

Existen dos métodos de acceso definidos en el estándar 802.11, y estos son: Función de Coordinación Distribuida y Función de Coordinación Puntual.

1.1.5.2.1 DCF

Función de Coordinación Distribuida (*Distributed Coordination Function*). Define un método básico para el acceso al medio. Este método es el CSMA/CA. Es un método de control de acceso que sirve para compartir el medio de transmisión, y es similar al CSMA/CD del 802.3, con la diferencia de que en CSMA/CD se detectan las colisiones, en cambio en CSMA/CA éstas se evitan, ya que es muy difícil detectar una colisión a través del medio inalámbrico.

CSMA/CA trabaja de la siguiente manera: una estación que quiere transmitir primero detecta el estado del medio. Si existe alguna otra estación transmitiendo, el medio esta ocupado, entonces esperará un tiempo aleatorio para realizar la transmisión. Si el medio esta libre, entonces la estación puede transmitir ocupando el medio.

1.1.5.2.2 PCF

Función de Coordinación Puntual (*Point Coordination Function*). Utiliza un coordinador que se encuentra en los puntos de acceso e identifica qué estación tiene el derecho de transmitir. Se utiliza un proceso llamado RTS/CTS.

La estación que desea transmitir realiza una petición de envío (RTS, *Request To Send*). El punto de acceso determina si la estación puede transmitir (CTS, *Clear To Send*). La estación que reciba el CTS es la que tiene permiso de transmitir.

1.2 Estándares más utilizados

Dentro del IEEE se crearon diversos grupos de trabajo enfocados a diferentes áreas de la especificación del estándar 802.11. En estos grupos de trabajo se desarrollaron 3 especificaciones que actualmente son las más utilizadas y comercializadas.

1.2.1 802.11a

Trabaja sobre la banda de los 5 GHz y puede llegar a alcanzar tasas de transmisión de 54 Mbps. En la más baja velocidad llega a alcanzar un rango de 50 metros, que pueden decaer a la mitad si se aumenta la velocidad al máximo. Utiliza Multiplexación Ortogonal por División de Frecuencia (OFDM, *Orthogonal Frecuency Division Multiplexing*). Para la capa física utiliza el método DSSS.

Sus principales ventajas son la velocidad que provee y la poca interferencia que existe, ya que no trabaja en la banda de 2.4 GHz como los otros estándares. Entre sus desventajas se encuentran la incompatibilidad con los estándares 802.11b y g, además de que no puede ser utilizado en Europa por la banda que utiliza, ya que se encuentra asignada para ser utilizada por HyperLAN. Tampoco incorpora características de QoS, que se refieren a transmisión de voz y video.

1.2.2 802.11b

Trabaja sobre la banda de los 2.4 GHz, alcanzando una velocidad máxima de transmisión de 11 Mbps. Para multiplexar la información utiliza la técnica de Código de Modulación Complementario (CCK, *Complementary Code Keying*).

Ese método de multiplexado permite utilizar altas tasas de transmisión utilizando eficientemente el radio del espectro. Utiliza el método DSSS para la transmisión en la capa física.

Tiene las siguientes ventajas: ha sido adoptado fácilmente por la mayoría de usuarios de redes inalámbricas, principalmente por los bajos precios de los dispositivos. Puede utilizarse a nivel mundial, en las regiones en donde se encuentra asignada la banda de 2.4 GHz para ser usada por el 802.11. Tiene como desventajas que tampoco tiene incorporada la capacidad de QoS. La principal desventaja es la interferencia que puede darse debido a que la frecuencia que utiliza la comparte con dispositivos que utilizan radio frecuencia para transmitir, y otras tecnologías inalámbricas, lo que puede causar una saturación de la frecuencia causando un gran nivel de interferencia.

1.2.3 802.11g

Es el estándar mas difundido y mas utilizado actualmente. Trabaja sobre la banda de los 2.4 GHz, al igual que el 802.11b, pero además ofrece una tasa de transmisión de 54 Mbps, como el 802.11a. El incremento en la velocidad de transmisión se da debido a que se realizó una extensión de la capa física (PHY). Incorpora las técnicas de modulación OFDM y CCK, además de una nueva tecnología llamada Codificación Binaria Convolucional de Paquetes (PBCC, *Paket Binary Convolutional Coding*) que brinda tasas de enlace más altas.

Cuando un dispositivo 802.11b entra en un punto de acceso 802.11g, todas las conexiones bajan su velocidad para adaptarse al nuevo dispositivo.

Tiene casi las mismas ventajas y desventajas que el 802.11b, además de tener las siguientes ventajas: tiene las mejores características de los dos estándares anteriores (la tasa de transferencia y la disponibilidad mundial). Tiene una compatibilidad con los estándares anteriormente utilizados. Entre sus desventajas están que tiene un número restringido de canales de transmisión, y que aún no ha sido totalmente adoptado por los desarrolladores de productos inalámbricos.

1.3 Otros estándares definidos

Además de los estándares mencionados en el apartado anterior, en el IEEE se crearon grupos de trabajo para desarrollar estándares que complementaran la especificación de los estándares a, b y g. Algunas características agregadas son: seguridad, definición de servicios e interoperabilidad.

1.3.1 802.11c

Es un estándar que especifica las características que debe tener un punto de acceso para poder funcionar como un puente (*bridge*) al tener múltiples puntos de acceso (ESS).

Esta definido a nivel de la capa MAC. Aunque éste estándar ya se completo no tiene una gran importancia para la implementación de las redes, ya que los dispositivos ya lo tienen incorporado.

1.3.2 802.11d

Especifica los requerimientos necesarios para la utilización del estándar 802.11 en diferentes países. Trabaja sobre la capa física.

La importancia de este estándar es debido a que en cada país las frecuencias se utilizan de diferente forma y para diferentes servicios. Se pretende tener un estándar para que el 802.11 pueda ser utilizado sobre diferentes dominios reguladores a nivel mundial.

1.3.3 802.11e

Es una extensión sobre el estándar 802.11 que introduce el concepto de Calidad de Servicio (QoS, *Quality of Service*). Este concepto se refiere a la transmisión de audio y video. Mejora las capacidades de los estándares 802.11a, b y g, además de asegurar una compatibilidad con los productos existentes. Trabaja sobre la capa MAC, para poder reconocer requerimientos específicos y así priorizar el envío de los flujos de audio y video.

Debido a que está definido sobre la capa MAC, será independiente de cada implementación y será compatible con los productos existentes.

1.3.4 802.11f

Cuando se desarrollo el estándar 802.11 fueron omitidas algunas características para brindar una mayor flexibilidad sobre el estándar. Una de las características no definidas es la que especifica el grado de interoperabilidad de los puntos de acceso de distintos fabricantes.

Este estándar provee la información necesaria para que los PA's de diferentes desarrolladores puedan trabajar conjuntamente, en funciones como el *roamming*.

1.3.5 802.11h

Es una extensión del estándar 802.11a y se basa en agregar algunas características a este estándar para que pueda ser utilizado en Europa, en donde actualmente se utiliza HyperLAN. En este estándar se introducen dos conceptos: Selección de Frecuencia Dinámica (DFS, *Dynamic Frecuency Selection*) que permite hacer cambios de frecuencias al encontrar otras redes operando sobre la misma frecuencia, y Control de la Energía de Transmisión (TPC, *Transmit Power Control*) que restringe el uso de energía por parte de los dispositivos. Esta definido como una extensión sobre la capa PHY del 802.11a.

1.3.6 802.11i

Es un estándar que pretende mejorar las características de seguridad utilizadas por el 802.11, en el que se utiliza Privacidad Equivalente a la Cableada (WEP, *Wired Equivalent Privacy*).

La mejora se realiza a través del uso del Protocolo de Clave de Integridad Temporal (TKIP, *Temporal Key Integrity Protocol*). Mejora la capa MAC del 802.11 en aspectos de seguridad. Incluye el manejo y distribución de claves (RADIUS), la encripción (AES) y la autenticación. Para más información sobre la seguridad en el estándar 802.11 vea el apéndice A.

1.3.7 802.11IR

Es la especificación del estándar 802.11 para el medio infrarrojo. Soporta tasas de transferencia de 1 a 2 Mbps. No se encuentra difundido, y no es muy utilizado, ya que no ofrece muchas ventajas en comparación con los estándares que utilizan radio frecuencia. La única ventaja significativa puede ser la seguridad ofrecida por el medio sobre el que trabaja.

1.3.8 802.11j

Es una extensión del estándar 802.11 para las regulaciones japonesas. Permite usar el 802.11a en los diferentes espectros asignados por el gobierno japonés:

- 4.900 – 5.000 GHz
- 5.000 – 5.100 GHz
- 5.150 – 5.250 GHz

1.3.9 802.11k

Pretende estandarizar la medición de los recursos utilizados por los estándares 802.11a, b y g. Sirve para realizar mediciones sobre las condiciones de las redes y hacer diagnósticos para encontrar errores. Se estandariza la recolección de datos, especificando que datos recolectar y como recolectarlos.

1.3.10 802.11m

Es un estándar para mejorar o corregir los estándares existentes, especificando el mantenimiento de las redes inalámbricas.

1.3.11 802.11n

Es un estándar de la siguiente generación. Brinda un rendimiento elevado, además de hacer que el estándar 802.11 satisfaga mejor las necesidades. Se obtiene una alta velocidad de transmisión, que puede llegar a los 100 Mbps. La meta de este estándar es llegar a tasas de transferencia mayores que los 150 Mbps a través de un canal de comunicación 802.11. El trabajo sobre éste estándar aún esta en proceso, pero dentro del proceso se pretenden realizar cambios en las capas física y MAC.

1.3.12 802.11r

El grupo del 802.11r se encuentra trabajando en reducir el tiempo cuando un dispositivo sale de la cobertura de un punto de acceso y pasa a la cobertura de otro, dentro de un Grupo de Servicios Extendidos (ESS). La mejora de estos tiempos es crítica para aplicaciones en tiempo real, como lo son las de video y voz, especialmente en dispositivos móviles en los que se espera que los clientes hagan *roamming* frecuentemente. La terminación de este estándar puede facilitar la introducción del servicio de voz sobre Wi-Fi (Vo Wi-Fi).

1.3.13 802.11s

Este estándar se esta desarrollando para permitir que los puntos de acceso o celdas de diferentes desarrolladores puedan autoconfigurarse dentro de una infraestructura en una topología inalámbrica de multi-saltos. Esto crearía una topología en malla que podría abrir nuevos mercados para aplicaciones en el estándar 802.11. También se busca que el estándar pueda trabajar con diferentes requerimientos funcionales dentro de diversos escenarios.

2. ESTÁNDAR 802.16

2.1 BWA

Acceso de Banda Ancha Inalámbrico (*Broadband Wireless Access*). Se espera que sea una de las tecnologías primarias al brindar acceso de banda ancha. Las tecnologías existentes actualmente son DSL, cable módem y fibra óptica. El motivo de querer pasar de las alternativas cableadas a BWA es que tiene muchas ventajas con respecto de éstas. Las ventajas que provee BWA son:

- Puede ser implementado y desplegado rápidamente, ya que no es necesario realizar la infraestructura de cableado necesaria para prestar servicios como la transmisión de datos, video y voz.
- Puede llegar a lugares que eran inalcanzables por las otras alternativas, ya que el costo o complejidad del despliegue es demasiado alto.
- Su implementación implica un costo menor.
- Ofrece una alta escalabilidad.

Debido a que es una tecnología necesaria, el siguiente paso para su adopción es la estandarización. El Grupo de Trabajo del IEEE 802.16 en Estados Unidos y el Proyecto BRAN del ETSI en Europa, son algunas de las diferentes entidades que se encuentran trabajando para lograr la estandarización. Estas entidades han colaborado en la división de rangos de frecuencia para las diferentes regiones a nivel mundial. La tabla II muestra la asignación de las frecuencias para algunas áreas y algunos países.

Tabla II. Espectros para redes inalámbricas de banda ancha

País	10 GHz	18-24 GHz	24 GHz	26 GHz	25-27 GHz	27.5-29.5 GHz	28 GHz	31 GHz	38 GHz
Norte América									
USA									
Canadá									
Asia/Pacifico									
Australia									
Japón									
Corea									
Malasia									
Nueva Zelanda									
Filipinas									
Singapur									
Taiwán									
Tailandia									
Centro y Suramérica									
Argentina									
Bolivia									
Brasil									
Chile									
Colombia									
Ecuador									
México									
Paraguay									
Perú									
Venezuela									
Europa, Este Medio, África									
Checoslovaquia									
Francia									
Alemania									
Hungría									
Irlanda									
Israel									
Holanda									
Noruega									
Polonia									
Rumania									
Sudáfrica									
España									
Reino Unido									

Fuente: Doug Gray. ***WW spectrum allocations for BWA***. Pág. 2.

2.2 Especificación del estándar 802.16

Con la intención de mejorar la especificación del estándar 802.11, el IEEE creo el grupo de trabajo 802.16, para definir la forma en que se realizan las comunicaciones dentro de una red inalámbrica de área metropolitana.

2.2.1 Historia

El proyecto para la creación de este estándar inicio en 1998, pero el trabajo de desarrollo fue realizado entre el 2000 y el 2003. El objetivo era hacer que el acceso a la banda ancha inalámbrica fuera mas barato y mayormente difundido, además de una mayor disponibilidad, a través de un estándar para Redes de Área Metropolitana Inalámbricas (*Wireless MAN*).

El estándar 802.16 define la especificación de la interfaz para WMAN. Este estándar para acceso inalámbrico provee el enlace para la última milla de conexión. Pero tiene el inconveniente de requerir línea de vista (LOS) para entablar la comunicación.

La primera versión fue aprobada en Diciembre del 2001. Esta versión utiliza el ancho de banda entre las frecuencias licenciadas de 10 – 66 GHz. Soporta grandes tasas de transferencia para una estación en distancias de hasta 50 kms, manejando servicios de voz, video y datos, aunque en la práctica se espera que las tasas de transferencia decaigan al mismo tiempo que la distancia de transmisión aumente.

Debido a que esta tecnología utiliza un rango más grande de frecuencias, soporta una gran variedad de arquitecturas de implementación. También es independiente del protocolo utilizado para la transmisión, ya que puede utilizar IPv4, IPv6, ATM, Ethernet y otros.

Los operadores de telefonía 3G lo ven como un fuerte competidor, ya que la capacidad de transmisión de datos es superior, y al brindar los servicios de video y voz tiene un gran potencial en la comunicación inalámbrica, aunque se espera que los primeros dispositivos de hardware salgan al mercado y sean adoptados en el año 2005.

A este estándar también se le conoce por el nombre de WIMAX (*Wireless Interoperability Microwave Access*, Interoperabilidad de Acceso Inalámbrico por Microondas). En el año 2001 se creó el Foro WiMAX, y tiene por objeto las siguientes funciones:

- Promover el despliegue a gran escala de las redes inalámbricas de banda ancha que operan sobre los 2 GHz, utilizando un estándar y certificando la interoperabilidad entre los productos y las tecnologías.
- Permitir la interoperabilidad entre los fabricantes de equipo basado en los estándares 802.16 (al igual que la Alianza Wi-Fi lo hace para el 802.11).

Utiliza TDMA (Acceso Múltiple con División de Tiempo) para realizar la transmisión por el medio físico, en lugar de utilizar CSMA/CA, utilizado por el 802.11. Esto se debe a que CSMA/CA no trabaja correctamente sobre grandes distancias.

TDMA le otorgando espacios de tiempo a cada nodo dentro de la red, y así evita el problema de tener colisiones en el medio de transmisión. También utiliza DAMA (Demanda de Asignación de Acceso Múltiple). DAMA asigna capacidad a múltiples estaciones en función de los cambios que se produzcan en las necesidades y en la demanda.

Intel ha llamado a WIMAX (802.16) “Lo mas importante desde el mismo Internet”.

2.2.2 Componentes de una red 802.16

Una red WIMAX se encuentra formada por dos elementos básicos para realizar la interconexión: las estaciones base, que juegan el papel de los puntos de acceso en las redes Wi-Fi; y las estaciones suscriptoras, que son similares a las estaciones para estas mismas redes.

2.2.2.1 Estación base

Es la radio central (transmisora/receptora) que mantiene las comunicaciones con dispositivos móviles dentro de un rango definido. Provee conectividad, administración y control sobre las estaciones suscriptoras. Tiene las siguientes características:

- Interfaz de respaldo (Gigabit Ethernet)
- Sub-bloque de CPU (administra, autentica)
- Interfaz aérea (capas física y MAC)
- Soporte voz y datos

2.2.2.2 Estación suscriptora

Incluye antenas montadas sobre techos, conectadas a interfaces internas o externas. Proveen conectividad entre el equipo suscriptor y las estaciones base. Debe tener las siguientes características:

- Interfaz de host (Ethernet)
- CPU (SDRAM, Flash)
- Interfaz aérea (capas física y MAC, RF y componente analógicos)
- Soporte para voz y datos

2.2.3 Topologías de red

Existen dos formas de interconectar dispositivos inalámbricos a través del estándar 802.16, y estas son las topologías de red en malla y red punto a multipunto. Cada una de ellas ofrece características especiales, en base a los servicios y al propósito de la conexión que se establece entre un conjunto de dispositivos.

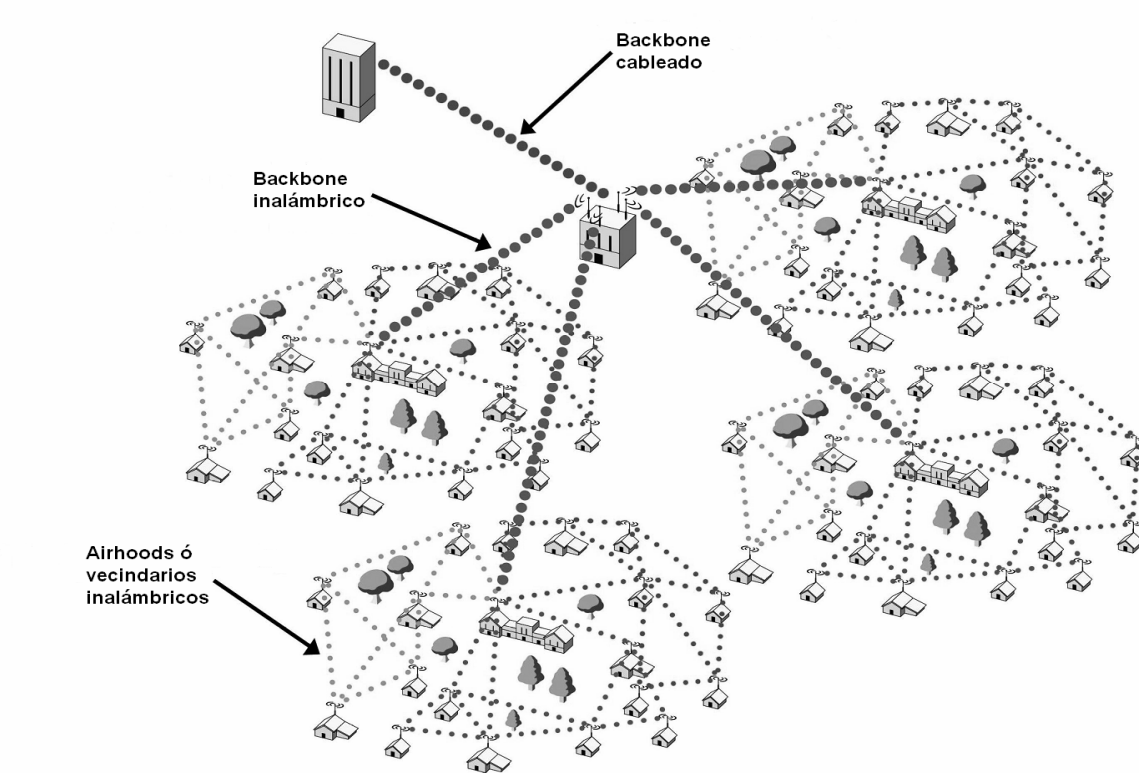
2.2.3.1 Redes en malla

Cada dispositivo dentro de una red en malla recibe y transmite su propio tráfico (funcionando como un *router*). Además, cada dispositivo tiene la capacidad de determinar automáticamente cuando debe ajustar la red (como cambiar de un nodo a otro para realizar la comunicación). Tiene la ventaja de que es fácil de implementar y es escalable. Puede tener dos formas de implementación:

- Omni. Utiliza antenas que pueden transmitir sobre cualquier dirección, haciéndolas menos complejas.

- Direccional. Utiliza solo ciertas direcciones de transmisión. Mas complejo, pero minimiza la interferencia.

Figura 3. Esquema de una red en malla



Fuente: Carolina Gabriel. ***Examinig the hotzone***. Pág. 12.

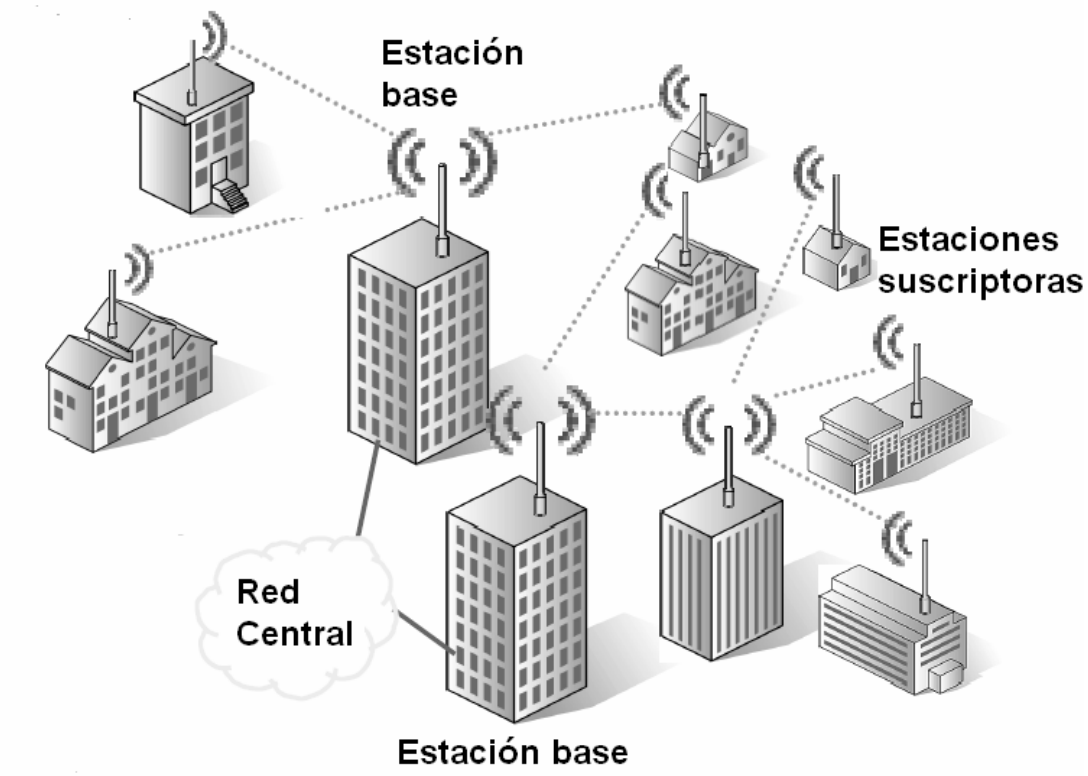
La figura 3 muestra un ejemplo de una red en malla, comunicada por *backbones* inalámbricos y cableados.

2.2.3.2 Redes punto a multipunto

Utiliza antenas de amplia cobertura para realizar la comunicación (del lado de las estaciones base) y antenas altamente direccionables (del lado de los suscriptores). Las estaciones base son colocadas centralmente sobre torres o edificios altos para que pueda llegar a todos los suscriptores.

Esta configuración permite utilizar circuitos de *full-duplex* para su comunicación, a través de FDM (Multiplexado por División de Frecuencia) y utilizar *half-duplex* a través de TDM (Multiplexado por División de Tiempo).

Figura 4. Esquema de una red punto a multipunto



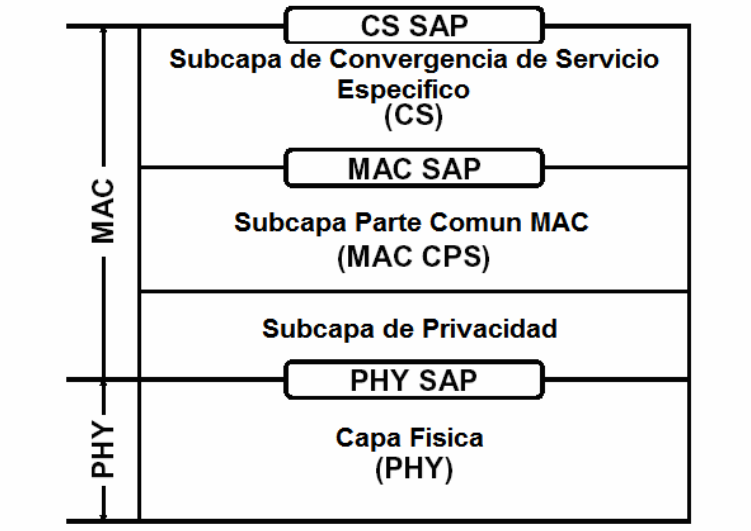
Fuente: Roger Marks. ***IEEE 802.16 working group on broadband wireless access***. Pág. 5.

En la figura 4 se puede apreciar una topología punto a multipunto, con cada estación base brindándole la conexión al conjunto de estaciones suscriptoras que se encuentran dentro de su rango.

2.2.4 Capas

En el estándar 802.16 se definen las capas física y MAC (igual que en el 802.11). Debido a esta especificación, el resto de capas no sufre ningún cambio. La figura 5 muestra la estructura de las capas definida por el 802.16.

Figura 5. Diagrama de las capas del 802.16



Fuente: Joon Yoo. ***IEEE 802.16 standards & drafts***. Pág. 13.

2.2.4.1 Capa MAC

Esta capa define como pueden comunicarse las estaciones base y las estaciones suscriptoras sobre la banda. Define las funciones de transmisión de datos en marcos y controla el acceso al medio inalámbrico compartido.

Tiene las siguientes características:

- Soporta las topologías de punto a multipunto y de malla.
- Es independiente de los protocolos.

- Tiene subcapas de convergencia.
- Es orientada a la conexión.
- Provee calidad de servicio (QoS).
- Soporta diferentes capas físicas.

2.2.4.1.1 Subcapa de convergencia de servicio específico

Provee transformación o mapeo sobre datos de redes externas recibidos a través del punto de acceso de servicio. Esto incluye clasificar las unidades de datos de servicio y asociarlas al flujo adecuado identificado por el identificador de la conexión. El flujo de servicio es unidireccional y es proveído por una QoS particular.

Para que pueda ser interoperable, se requiere que sea específica para cada servicio, por lo que se encuentra dividida en:

- Capa de Convergencia ATM. Puede crear conexiones dinámicamente, utilizando Caminos Virtuales (VP, *Virtual Path*) y Canales Virtuales (VC, *Virtual Channel*). Soporta totalmente QoS.
- Capa de Convergencia de Paquetes. Soporta todos los protocolos basados en paquetes como el IPv4, IPv6, Ethernet, Modo de Transferencia Síncrono (STM, *Synchronous Transfer Mode*) y VLAN's. Las capas son específicas para el tipo de paquete que utiliza.

2.2.4.1.2 Subcapa parte común MAC

Especifica la forma en que se comparte el medio físico de transmisión de una manera eficiente. Se utiliza el flujo de servicio para administrar QoS.

Provee el acceso al sistema, la asignación del ancho de banda, el establecimiento y el mantenimiento de las conexiones. Se aplica QoS para la transmisión de los datos sobre la capa física. Utiliza DAMA-TDMA para *uplink* (transmisiones hacia la estación base) y TDM para *downlink* (transmisiones desde la estación base). También realiza la función de direccionamiento, utilizando los 48 bits de la dirección MAC.

2.2.4.1.3 Subcapa de privacidad

Provee seguridad y privacidad a los suscriptores sobre la red, encriptando la información que viaja a través de la conexión entre las estaciones base y las estaciones suscriptoras. También evita el robo del servicio, autenticando a los suscriptores sobre las estaciones base. Esta formada por:

- Protocolo de encapsulación. Define un conjunto de algoritmos de criptografía y reglas para aplicar estos algoritmos a los PDU's de la capa MAC.
- Protocolo de administración de claves. PKM (*Privacy Key Management*). Sirve para distribuir de forma segura las claves para los suscriptores.

2.2.4.2 Capa física

En esta capa se define el medio a través del cual se transmitirá la información, se especifica la banda de frecuencia, el esquema de modulación, las técnicas de corrección de errores, la sincronización entre los transmisores y los receptores, la tasa de transferencia y la estructura de Multiplexado por División de Tiempo (TDM, *Time Division Multiplexing*). Tiene tres objetivos:

- Soportar la transferencia de datos, pasando las señales a las capas superiores (MAC).

- Soportar interacciones entre las subcapas relacionadas al control de la capa.
- Administración de sus funciones.

Tiene diferentes especificaciones para la modulación:

- SC (*Single Carrier*)
- SCa (Interfaz Aérea de *Single Carrier*)
- OFDM (Multiplexado por División de Frecuencia Ortogonal)
- OFDMA (Múltiple Acceso por División de Frecuencia Ortogonal)
- HUMAN (Red de Área Metropolitana No Licenciada de Alta Velocidad)

2.2.4.2.1 WirelessMAN-SC

- Opera sobre las bandas licenciadas del rango entre 10 y 66 GHz.
- Requiere de línea de vista.
- Soporta TDD, FDD, TDM y TDMA.
- Utiliza perfiles de despliegue adaptativos.
- Canales de ancho de banda de 20, 25 o 28 MHz. Permite asignar mas frecuencias.

2.2.4.2.2 WirelessMAN-SCa

- Trabaja con las bandas licenciadas entre 2 y 11 GHz.
- No requiere de línea de vista para operar.
- Soporta TDD, FDD, TDM y TDMA (igual que SC).
- Modulación de *single carrier.*
- Utiliza perfiles de despliegue adaptativos (como el BPSK, QPSK, 16 QAM, 64 QAM y 256 QAM).

- Trabaja con canales de ancho de banda de 1.75, 3.5 y 7 MHz.
- Tiene menos asignaciones por operador.
- Disminuye el multicamino.

2.2.4.2.3 WirelessMAN-OFDM

- Utiliza TDMA como técnica de acceso.
- Trabaja con las bandas licenciadas entre los 2 y los 11 GHz.
- No requiere de línea de vista.
- Multiplexado por frecuencias. Utiliza un tamaño de 256 puntos de transformación.
- Perfiles de despliegue adaptativos (QPSK, 16 QAM y 64 QAM).
- Canales con ancho de banda de 1.75, 3 y 7 MHz.

2.2.4.2.4 WirelessMAN-OFDMA

- Utiliza las bandas licenciadas entre 2 y 11 GHz.
- No requiere de línea de vista.
- Puede utilizar *duplex* TDD y FDD.
- Utiliza multiplexado por división de frecuencia, con un tamaño de 2048 puntos de transformación. Además, los transportadores activos se dividen en conjuntos o subcanales.
- Se le puede asignar a un transmisor uno o mas subcanales.
- Acceso múltiple a través de direccionamiento a múltiples transmisores.

2.2.4.2.5 WirelessHUMAN

- Utiliza las bandas no licenciadas entre los 2 y los 11 GHz, principalmente el rango entre 5 y 6 GHz.

- Utiliza canales de ancho de banda de 10 o 20 MHz.
- Selección Dinámica de Frecuencia (DFS, *Dynamic Frequency Selection*).
- Es similar a OFDM, pero transmite con menos poder para reducir los riesgos de interferencia.

2.3 Estándares definidos

El IEEE en la creación del estándar 802.16 trabajó de manera similar a cuando se definió el 802.11. Para su especificación se crearon grupos específicos para cada área, dependiendo del propósito de cada estándar. De esta manera surgió un conjunto de estándares que aportan diferentes características a WIMAX.

2.3.1 802.16a

Abarca las bandas licenciadas desde los 2 a los 11 GHz. No requiere de línea de visión (como el estándar original) y es más barato, con tasas de transferencia más pequeñas. Soporta el esquema para redes en malla, en el que los suscriptores se comunican entre ellos en lugar de utilizar una estación base 802.16a. Esta es una de las razones por las cuales ha aumentado la promoción del estándar, ya que es una forma muy flexible de brindar servicios a través de redes de área metropolitana inalámbricas.

Se pretende que sea la tecnología a utilizar para llevar Internet inalámbrico de alta velocidad a lugares a los que solo llegaban las alternativas cableadas con costos mas elevados. Esto hace que sea un fuerte competidor para las conexiones a través de líneas T1, DSL y por cable.

2.3.2 802.16b

Es una extensión del estándar original, certificada en Enero del 2003. Utiliza la frecuencia de 2 – 11 GHz, permitiendo conexión sin línea de visión. Puede manejar tasas de transferencia de 124 Mbps. Esto constituye un gran beneficio para la implementación de redes inalámbricas, ya que permite tener mas estaciones conectadas a un solo punto de acceso. Desde su creación ya ha empezado a ser adoptada como la tecnología inalámbrica dominante (en banda ancha).

Además tiene un rango ampliado de transmisión, que puede llegar a los 50 kms y puede utilizar frecuencias tanto licenciadas como no licenciadas. Puede utilizar topologías punto a multipunto o de malla. Puede soportar varios servicios simultáneamente, incorporando características de QoS.

2.3.3 802.16c

Especifica y estructura conjuntos de pruebas y brinda los propósitos de las pruebas sobre los distintos protocolos. También se relaciona con la interoperabilidad, brindando información detallada de los perfiles del sistema y especificando las combinaciones de las opciones.

2.3.4 802.16d

Fue diseñado para utilizar frecuencias autorizadas y no autorizadas sobre áreas que se encuentran dispersas geográficamente. Las frecuencias se encuentran en el rango de 2 – 11 GHz. Mientras que las frecuencias más altas ofrecen un ancho de banda mayor, también requieren de línea de vista, ya que tienen una longitud de onda más pequeña.

Es una combinación de los estándares 802.16a, b y c. Soporta cientos de conexiones y puede operar hasta 50 KMs, con velocidades hasta los 75 Mbps.

2.3.5 802.16e

Debido a que las primeras versiones del 802.16 son para redes fijas, fue necesario iniciar el trabajo sobre un estándar que permitiera la movilidad de los dispositivos, aprovechando las capacidades inalámbricas. Fue así como surgió el 802.16e, que es una extensión al estándar original para incluir movilidad.

Este estándar puede ser la mayor amenaza para los operadores de celulares de 3G, pero aún así, algunas grandes empresas de telefonía celular, como Nokia, se encuentran interesadas en el desarrollo del estándar, ya que puede significar un nuevo flujo de ingresos, ya sea a nivel de estaciones base o a nivel de telefonía.

2.3.6 802.16f

Es un grupo formado recientemente, y que trata acerca de las redes con topología de malla. Esta topología puede ayudar a mejorar la cobertura para las estaciones. Las redes con topología de malla permiten que los datos viajen de punto a punto, sobrepasando los obstáculos que encuentren, ya que cada dispositivo es inteligente y funciona como un *router*, y puede encontrar la mejor ruta para llegar a su destino.

2.3.7 802.16.2

Fue publicado en el 2001 y especifica la práctica recomendada para cubrir la operación de múltiples sistemas diferentes de banda ancha, dentro del rango de frecuencia de 10 – 66 GHz. Especialmente se enfoca en el rango entre los 23.5 y los 43.5 GHz.

2.3.8 802.16.3

Define la interfaz aérea para sistemas licenciados operando sobre la banda de los 2 a los 11 GHz.

3. ANÁLISIS COMPARATIVO ENTRE WI-FI Y WIMAX

3.1 Características

En los capítulos anteriores ya se han descrito los detalles técnicos de los estándares 802.11 (Wi-Fi) y 802.16 (WiMAX). A continuación se mostraran las características que brinda cada uno de ellos, tomando en cuenta que existe una familia de estándares definidos para ambos estándares.

3.1.1 802.11

Inicialmente exploraremos las características principales del estándar 802.11, utilizado para las conexiones de redes inalámbricas de área local. Es importante mencionar que la utilización de este estándar nos permite comprobar en la práctica, que las características definidas concuerdan con su especificación.

3.1.1.1 Escalabilidad

Brinda una flexibilidad en las bandas de frecuencia que puede utilizar, aunque el rango no es muy grande (2.4 – 2.483 GHz). Pueden utilizarse diferentes topologías de red, lo que permite que se adapten a diferentes necesidades en las empresas. El crecimiento de estas redes es sencillo, porque no es necesario realizar una infraestructura cableada para aumentar el número de usuarios.

3.1.1.2 Cobertura

Debido a que es un protocolo para redes WLAN, la cobertura que brindan apenas alcanza los 100 m, aunque diferentes fabricantes han encontrado la forma de aumentar este rango, pero perdiendo las bases de la estandarización.

3.1.1.3 Rendimiento

Es capaz de utilizar diferentes algoritmos para la modulación de la frecuencia, dependiendo de la capa física que se utilice. Cada método de modulación de frecuencia tiene diferentes características que pueden ser utilizadas para diferentes necesidades. Son capaces de brindar una alta confiabilidad en la transmisión, aunque no aseguran altas tasas de transmisión o que no exista perdida de información (aunque es muy reducida).

3.1.1.4 Calidad de servicio (QoS)

En la definición del estándar original no existe QoS, pero debido al crecimiento de las redes 802.11 y a la demanda de los servicios de transmisión de video, audio y datos, fue necesario que se incorporara a los productos 802.11. Debido a la necesidad de QoS se creo el estándar 802.11e, en el que se definen las bases para su incorporación y compatibilidad con productos existentes en el mercado y con redes implementadas.

3.1.1.5 Seguridad

Utiliza varios protocolos, pero aún existen algunos problemas para lograr la misma seguridad que se tiene con las redes cableadas:

- WEP (*Wireless Equivalent Privacy*)

- WPA (*Wireless Protected Access*)
- 802.1X
- 802.11i

3.1.1.6 Movilidad

Esta es una característica muy importante en las redes inalámbricas y uno de los objetivos que se buscan para pasar de una red cableada a una red inalámbrica. El estándar 802.11 tiene la capacidad de ser móvil, permitiendo servicios como el *roamming*, para poder pasar de un punto de acceso a otro sin perder la conexión hacia la red.

3.1.2 802.16

Ahora es necesario revisar algunas de las características del estándar 802.16, a fin de poder realizar el análisis comparativo entre los dos estándares. Aunque las características que se mencionan a continuación solo han sido obtenidas en base a la especificación del estándar, ya que aun no ha sido utilizado en situaciones reales.

3.1.2.1 Escalabilidad

Brinda flexibilidad en cuanto a los canales de banda ancha, lo que hace que la implementación y el mantenimiento de las redes se realice de una manera sencilla. Además, es capaz de utilizar espectros de frecuencias autorizadas y no autorizadas, por lo que existe una gran gama para seleccionar la banda a utilizar. El operador tiene la capacidad de decidir como realizar la división y asignación sobre el espectro que utiliza.

Al utilizar sectores angostos, puede aumentar el número de usuarios, manteniendo un buen alcance y un buen desempeño. Para escalar la red, el operador puede utilizar el mismo espectro, dividiéndolo en mas sectores para crear los niveles de aislamiento apropiados entre las estaciones base.

3.1.2.2 Cobertura

Utiliza tecnologías que brindan un rango de cobertura creciente, entre ellas, la topología en malla y antenas inteligentes. Cuando se mejora la tecnología y se reduce el costo, es posible aumentar la cobertura y el rendimiento utilizando múltiples antenas para enviar o recibir la información con una cobertura mejorada en ambientes extremos.

3.1.2.3 Rendimiento

Los esquemas de modulación de datos que utiliza permiten que el rendimiento tenga un gran aumento sin perder los rangos de cobertura o de eficiencia de la señal, que siguen manteniéndose altos. La modulación puede llegar a ser dinámica, permitiendo cambiar de un algoritmo a otro, si el primero no puede llegar a establecer un enlace para las estaciones involucradas.

3.1.2.4 Calidad de servicio

Se refiere a los servicios de transmisión de voz, video y datos. Estas son características importantes en los mercados en evolución de las redes inalámbricas. Es por esto que estas características se encuentran incluidas en el estándar original y en sus variantes. Para poder brindar estos servicios es necesario contar con redes que tengan un bajo tiempo de retardo (tasas de transmisión altas).

Las características de petición y otorgamiento de la capa MAC permiten brindar niveles de servicio similares a los de T1 o de “mayor esfuerzo”, ya sea para negocios o para hogares, todos basados en la misma estación base.

3.1.2.5 Seguridad

WIMAX incluye en su definición características de seguridad como la privacidad y el encriptamiento. Con esto se pretende lograr transmisiones seguras al tener autenticación y encripción de los datos. Utiliza algunos algoritmos similares a los del 802.11, pero con versiones mejoradas para brindar una mayor seguridad.

3.1.2.6 Movilidad

El estándar original 802.16 no incluye características de movilidad. Son redes de banda ancha inalámbrica, pero son redes fijas. En el estándar 802.16a tampoco se incluyen estas características, pero se encuentra en desarrollo el estándar 802.16e, en el que se definen las características de movilidad, con lo que se cumple uno de los objetivos de las redes inalámbricas.

3.1.3 Resumen de las características

A continuación se muestra una tabla de resumen, que contiene lo más importante de las características expuestas anteriormente.

Tabla III. Resumen de características

Característica	802.11	802.16
Tasa de Transferencia	54 Mbps	100 Mbps
Tecnología de Modulación	OFDM	OFDM
Acceso al Medio	CSMA/CA	DAMA-TDMA
QoS	No soportado. En progreso el estándar 802.11e para soportarlo.	Soportado
Cobertura	100 mts.	50 km.
Frecuencias	2.4 GHz	2-11 GHz
Seguridad	WEP. En progreso el estándar 802.11i para mejorarlo. WPA y 802.1X	Triple DES, RSA, Llave Publica
Movilidad	Soportada	No soportada. Se encuentra en proceso el estándar 802.16e.
Escalabilidad	Escalable	Altamente escalable

3.2 Aplicaciones

Cada estándar cuenta con diferentes características, y estas hacen que cada uno de ellos cubra mejor alguna solución requerida en cuanto a redes inalámbricas se refiere.

3.2.1 Aplicaciones del 802.11

Tiene algunas aplicaciones principales y algunas otras que no son tan comunes pero que pueden utilizar implementaciones de redes 802.11:

- Redes para negocios y corporaciones
- Redes para hogares
- Aeropuertos
- Cafeterías / Internet
- Universidades

- Cámaras de seguridad
- Control de inventarios
- Ordenes de restaurantes

Además, es muy útil para implementaciones de redes en espacios compartidos, como salones de conferencia en los que los usuarios ya no tienen que competir por las conexiones cableadas, sino que pueden compartir el acceso inalámbrico, y en lugares difíciles de cablear. Este estándar también es una parte importante del mercado del Acceso Publico de Banda Ancha, proveyendo acceso temporal a Internet con altas velocidades, muy utilizado en hoteles, aeropuertos, cafeterías, universidades, librerías, etc.

3.2.2 Aplicaciones del 802.16

El estándar 802.16 esta diseñado principalmente para llevar conexiones a lugares que no pueden ser alcanzados a través de medios cableados. Algunas aplicaciones en las que puede utilizarse son:

- Acceso de banda ancha por demanda.
- Acceso de banda ancha residencial (cubre los lugares que no son alcanzados por cable ni DSL).
- Campus universitarios de gran tamaño.
- Distribuidores de Internet.

El potencial de las redes inalámbricas de banda ancha, basadas en el protocolo 802.16, incluye nuevos servicios que antes solo podían ser proveídos por sistemas DSL, cable módem y 3G. Permite brindar acceso a Internet de banda ancha, teniendo la posibilidad de que sea acceso móvil o fijo, con altas velocidades de conexión.

3.3 Ventajas y desventajas

Las redes inalámbricas, ya sean LAN o MAN, deben brindar por lo menos las siguientes ventajas:

- Movilidad. Los usuarios pueden acceder a los recursos de la red sin estar físicamente en una localidad que tenga conexión a la red, ya que puede hacerlo desde cualquier ubicación siempre que ésta se encuentre dentro de los rangos de transmisión de la red.
- Rapidez de instalación. La rapidez con que se puede hacer una instalación de una red inalámbrica aumenta, ya que no es necesario realizar cableado estructurado o hacer modificaciones sobre las instalaciones físicas o sobre las eléctricas.
- Flexibilidad. Las topologías de red para las redes inalámbricas permiten que sea mas fácil modificar la estructura de la red según sea necesario.
- Escalabilidad. Las topologías de red también son fácilmente adaptables a las necesidades de las empresas, y pueden pasar de ser redes pequeñas o punto a punto, a redes de gran tamaño y con una infraestructura compleja.

3.3.1 Ventajas del 802.11

Estas son algunas de las ventajas que presenta el estándar 802.11 y que pueden determinar el rumbo que seguirá esta tecnología:

- Completa estandarización y aceptación a nivel mundial.
- Precios bajos.
- Facilidad de implementación.
- Interoperabilidad entre productos de diferentes fabricantes.

3.3.2 Desventajas del 802.11

Otro factor que puede significar el crecimiento o disminución en el uso de este estándar son las desventajas. A continuación aparecen algunas de ellas:

- Tiene muchas variaciones para agregar nuevas características a la versión original o a las más utilizadas.
- Tiene rangos de transmisión muy bajos, tomando en cuenta que las tasas de transferencia también son bajas.
- No se asegura un nivel de seguridad alto con los protocolos utilizados.
- No permiten brindar servicios de QoS, debido a las tasas de transferencia requeridas para la transmisión de voz y video a través de la red.

3.3.3 Ventajas del 802.16

Para que este estándar pueda penetrar el mercado de las redes inalámbricas debe brindar algunas ventajas que lo hagan atractivo al mercado. Estas son algunas ventajas:

- Al contar con el soporte de la estandarización las economías de escala permiten reducir los riesgos monetarios
- Los operadores no se encuentran atados a un solo proveedor, ya que las estaciones base son interoperables con estaciones suscriptoras de diferentes fabricantes.
- Equipo de menor costo y con un mayor rendimiento.
- Creación de innovaciones rápidamente.

3.3.4 Desventajas del 802.16

Es importante considerar las desventajas que implican el uso y la implementación de rede WIMAX. Estas son las desventajas a tomar en cuenta:

- Falta de estandarización.
- Interferencia entre las bandas que utiliza con otras tecnologías o servicios.

3.4 Medición de los beneficios

Para justificar la implementación de redes inalámbricas, y para cualquier otra tecnología que se encuentre en planes de implementación, es necesario utilizar algunos métodos para la medición de los beneficios que se obtendrían al utilizar la nueva tecnología. Existen diferentes métodos para calcular los beneficios, pero todos ellos son importantes para que los directores ejecutivos tomen la decisión de cambiar a una red inalámbrica y determinar que tipo de red es la que llena las expectativas de la empresa, brindando mayores beneficios e implicando un costo menor.

3.4.1 Retorno de inversión (ROI)

En este método se realizan mediciones sobre los ahorros de tiempo y las ganancias en la productividad que son obtenidas al utilizar redes inalámbricas. La dificultad de utilizar el método ROI es cuantificar los beneficios que se obtendrán. El caso del costo es algo directo, tangible que puede utilizarse como métrica, pero los beneficios tienen que ser traducidos cuidadosamente a una métrica similar a la de los costos, para poder realizar una comparación en base a los mismos términos.

3.4.1.1 Caso de estudio: ROI en Intel

"TI Intel, con la ayuda de Finanzas Intel, encontraron que las LAN inalámbricas brindan un Retorno de Inversión positivo en una amplia gama de escenarios de uso y segmentos de usuarios." [1]

El plan desarrollado por Intel consistía en asignar cantidades de dólares a cada componente de la ecuación del ROI:

ROI = Beneficios de productividad – Costos iniciales – Costos de mantenimiento

Para obtener los datos apropiados para realizar los cálculos se realizaron encuestas, entrevistas y monitoreo de los primeros usuarios de las WLAN's, obteniendo los ahorros de tiempo por día logrados con ellas. Después crearon segmentos basándose en los datos obtenidos: administración de ingeniería/productividad, manufactura, ventas, marketing y soporte, y así lograron obtener las ganancias de productividad reales. También fue necesario calcular las ganancias de productividad de cada usuario y luego por cada año.

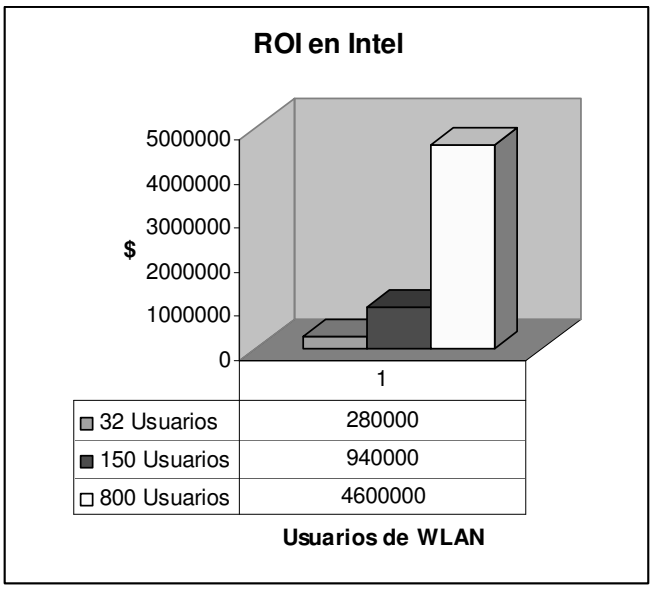
Al obtener las ganancias por usuario por año, se utilizaron otros factores que afectan este valor como el valor del dinero a través del tiempo, impuestos y depreciación. También se incluyeron los costos iniciales para infraestructuras de diferentes tamaños.

Al finalizar el estudio en Intel, se determino que al tener mas usuarios para las WLAN's aumenta el ROI, por lo que resulta rentable pasar de una red cableada a una red inalámbrica.

[1] Doug Busch, Vicepresidente y CIO de Intel

Con los datos obtenidos, y siguiendo un proceso de estimación, se llego a obtener la grafica mostrada en la figura 6, en la que aparece el número de usuarios para una red inalámbrica y el ROI obtenido para cada categoría.

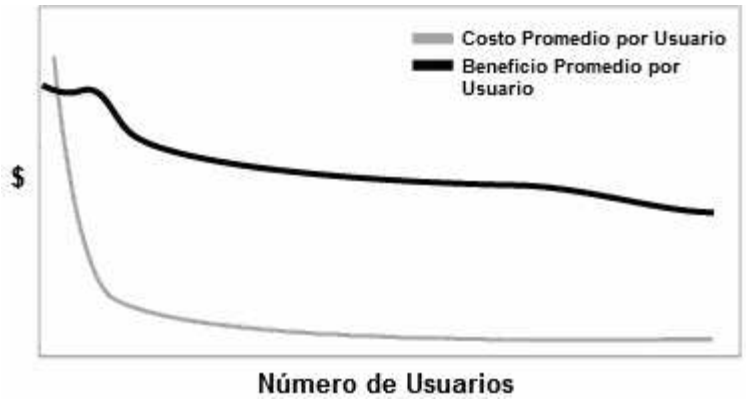
Figura 6. Retorno de Inversión en Intel utilizando WLAN's



Fuente: Doug Busch. **Retorno de inversión en Intel utilizando WLAN's**. Pág. 2.

Además de notar que el ROI aumenta a medida que aumentan los usuarios, también se pudo comprobar que el costo promedio por usuario disminuía, inicialmente de manera drástica, y alcanzando una estabilidad más adelante. La figura 7 muestra la relación entre el número de usuarios, el costo promedio por usuario y el beneficio promedio obtenido por usuario.

Figura 7. Beneficios y costos por usuario en una WLAN



Fuente: Telecom. **Como calcular el ROI de las WLAN**. Pág. 3.

3.4.1.2 Pasos para realizar un estudio de ROI

A continuación se presentan los pasos necesarios para llevar a cabo un estudio en el que se determina el retorno de la inversión que se obtendrá al implantar una nueva tecnología:

1. Basándose en la ecuación del ROI, se asignan cantidades monetarias a cada uno de los elementos que la forman. Para obtener estas cantidades se realizan estudios sobre la empresa, que pueden ser entrevistas, cuestionarios, encuestas y observación activa (si ya se encuentra implantada la red).
2. Encontrar los ahorros en el tiempo que se obtendrán al pasar a una red inalámbrica. Después de encontrar el tiempo que se ahorra se encuentra el valor monetario equivalente para ese tiempo.
3. También es necesario realizar la medición de la productividad, ya que se espera obtener una mejora en productividad debida al ahorro de tiempo. También se le asigna una cantidad a este aumento en la productividad.

4. Se determinan los costos iniciales para la implantación de la red dentro de la empresa. Estos costos son fijos y dependen del tamaño de la red que se desea implantar.
5. También es necesario tomar en cuenta los costos de soporte y mantenimiento. Para ello se debe considerar el tiempo de vida que tendrá la red.
6. Teniendo ya los datos anuales por usuario, se calculan para el tiempo de vida que tendrá la red.
7. Se analizan los resultados para saber la rentabilidad que tendrá implantar la red inalámbrica dentro de la empresa. El análisis debe de realizarse a largo plazo, abarcando desde el inicio de la implantación, la migración hacia esta tecnología si fuera necesaria, todo el tiempo útil, el mantenimiento y el deshecho de la solución.

Según el estudio de Intel, al aumentar los usuarios aumenta el ROI, justificando así su implementación. Sin embargo, este estudio fue realizado para redes LAN inalámbricas, por lo que no toma en cuenta a las redes WMAN. El realizar un estudio para las WMAN para encontrar el ROI presenta un mayor grado de dificultad, ya que no existen muchas implementaciones de estas redes, pero tomando en cuenta las características superiores con respecto a las redes WLAN, se esperaría que los beneficios en productividad y en tiempo fueran mayores, además de tomar en cuenta los rangos de transmisión mayores, permitiendo enlazar empresas ubicadas en diferentes localidades. El único factor que podría afectar el ROI de las WMAN es el precio de los dispositivos, que es mayor al de los dispositivos WLAN, implicando un mayor costo inicial y disminuyendo el ROI.

3.4.2 Economías de escala

El estándar 802.16 permite crea economías de escala, que reducen la cantidad monetaria de riesgo. Debido a que los dispositivos tienen una plataforma común sobre la que se basan los productores y distribuidores de dispositivos, permiten que se reduzcan los costos de los dispositivos. También permiten tener una mas rápida innovación mejorando los precios y el rendimiento, que no podían ser logrados por arquitecturas propietarias.

Otro factor que contribuye a las economías de escala es la interoperabilidad de las estaciones entre múltiples productores de dispositivos 802.16, ya que la interoperabilidad se encuentra definida dentro del estándar y el Foro WIMAX certifica esta interoperabilidad entre los productos de distintos vendedores.

El concepto de la estandarización para las redes inalámbricas es de gran importancia porque reduce los costos a través de la integración y de economías de escala, que permiten una mayor producción, lo que implica dispositivos menos costosos.

3.5 Tendencias

Para determinar la importancia de estas redes dentro del mercado de las telecomunicaciones, o al menos para realizar una estimación, es necesario conocer cuales son las tendencias de cada tecnología. Una de ellas se encuentra alcanzando una etapa de madurez, mientras que la otra aun esta en su fase inicial de crecimiento.

3.5.1 Crecimiento

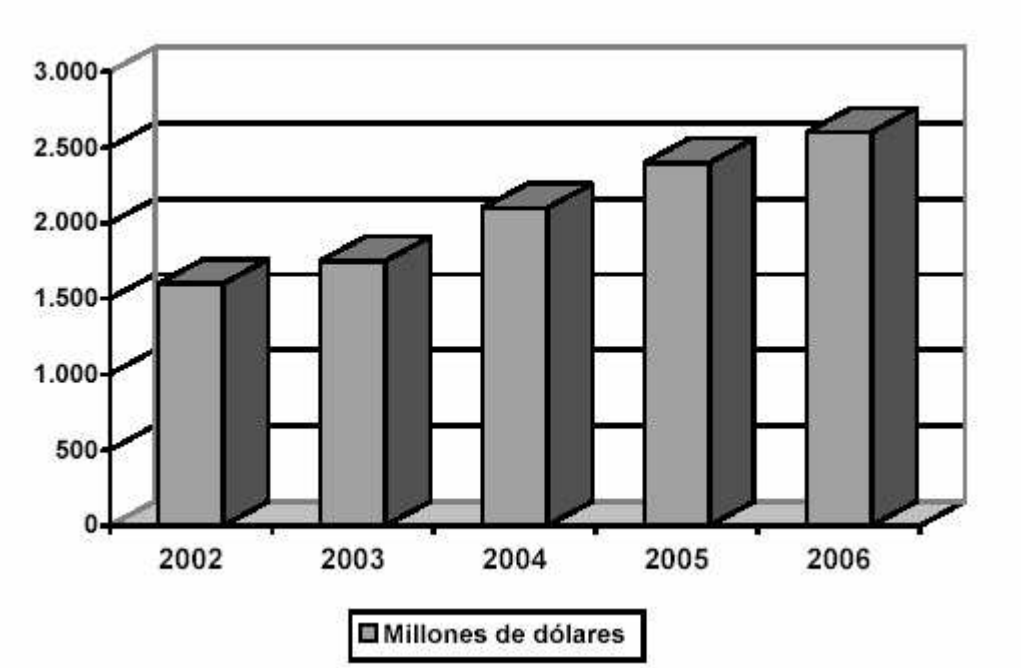
Se ha obtenido un crecimiento en el uso de la tecnología WLAN para poder brindar acceso inalámbrico a Internet, siendo una variante para las tecnologías cableadas que actualmente brindan este servicio. De acuerdo a Frost & Sullivan el mercado creció un 43% en 1999 y se estima que llegue a $1.8 billones para el año 2006.

Gracias a la reciente adopción del estándar 802.11g, se ha dado un incremento en el mercado de WLAN's durante el año 2003. El Grupo Dell'Oro registro $419 millones en ingresos totales en el mercado, incluyendo puntos de acceso, *bridges*, *gateways* y NIC's para el 802.11b y g. Los ingresos del 802.11g aumentaron un 48% para llegar a un del 24% de los ingresos del mercado total, al mismo tiempo que los ingresos del 802.11b disminuyeron.

El crecimiento que se ha dado en la utilización de redes inalámbricas a partir del 2002, año en el que se tuvo un volumen de ventas de aproximadamente $1600 millones, solo tiene un inconveniente, las empresas aún no confían plenamente en las soluciones de seguridad utilizadas actualmente. Pero con la creación de nuevos protocolos de seguridad, la adopción de estas redes tendrá un mayor crecimiento llegando hasta el 2006 como punto máximo (según los estudios realizados).

En base a datos estadísticos se pudo obtener la grafica mostrada en la figura 8, que muestra el volumen en dólares generado por las redes inalámbricas durante algunos años, mostrando también un pronóstico para el año 2006. En la grafica parece existir un crecimiento, pero al llegar a su punto de madurez, este crecimiento se tornara en disminución, dando paso a nuevas tecnologías, como WiMAX.

Figura 8. Volumen generado por las soluciones inalámbricas



Fuente: Jay Kuo. ***Multimedia over Wi-Fi: challenges and opportunities***. Pág. 12.

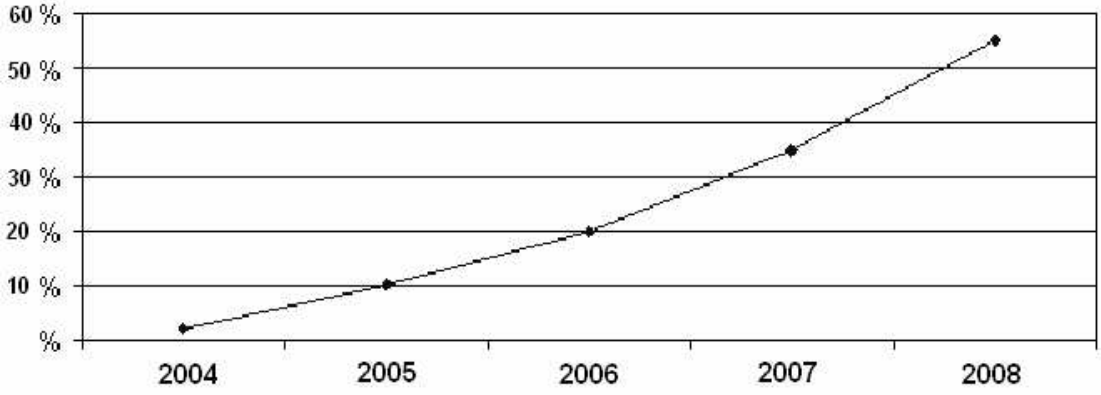
Acerca de WiMAX, se habla de las posibilidades que presenta esta nueva tecnología, aunque su adopción aún este a algunos años de darse, es necesario que los proveedores de servicios empiecen a tomarla en cuenta, y tomar decisiones al respecto, ya que las tendencias del mercado indican que será la tecnología inalámbrica dominante dentro de unos años. La planeación de estrategias que incluyan esta tecnología ya ha comenzado, y los fabricantes de productos ya se están preparando para tener disponibles los dispositivos 802.16 cuando este estándar sea ratificado por la comunidad de usuarios de redes inalámbricas.

Gracias al fuerte apoyo que WiMAX ha recibido de Intel, ha emergido rápidamente de entre las tecnologías para BWA. Actualmente, algunas tecnologías propietarias de WiMAX ya están siendo desplegadas por los proveedores en los Estados Unidos, Asia y Europa.

Aunque la adopción a nivel mundial se ha retrasado debido a que los vendedores no tenían un estándar sobre el cual basarse, al contrario de Wi-Fi, que ha logrado un gran crecimiento y una buena aceptación por parte de los fabricantes. El tener un estándar ayuda a bajar los costos de producción y a promover la interoperabilidad entre los fabricantes, factores que son considerados de alta importancia para la incursión en el mercado.

Tomando en cuenta las características de WiMAX y los factores que se han dado para la incursión en el mercado de redes inalámbricas, se han hecho estimaciones para conocer el grado de penetración que tendrá esta tecnología a un corto plazo, obteniendo los resultados mostrados en la figura 9.

Figura 9. Tasa de penetración de WiMAX



Fuente: Telenium. Giga group analiza las principales tendencias en el mercado de movilidad. Pág. 2.

3.5.2 Futuro

Como se ha visto a través de datos y pronósticos, determinar el futuro de estos estándares dependerá de que tan bien se adapten a los requerimientos de las empresas, y que tanto puedan evolucionar junto a ellas.

3.5.2.1 802.11

Según un estudio realizado por el Grupo Dell'Oro, el mercado para las redes 802.11 aumentara en un 23% en el año 2004, con un crecimiento continuo durante el año 2005. Sin embargo, este crecimiento comenzará a disminuir después del año 2005, llegando a un punto máximo en el 2006. Para el año 2007 se espera que inicie el periodo de declinación para este mercado.

3.5.2.2 802.16

A pesar de que de los productos WiMAX solo algunos se encuentran en el mercado actualmente, los estudios indican un gran crecimiento en el uso de esta tecnología para los siguientes 10 años, a diferencia de Wi-Fi, que se espera tenga su punto más alto para el año 2006.

De acuerdo a un estudio realizado por BWCS y Consultaría Senza-Fili, se encontró que los servicios basados en tecnologías como WiMAX valdrán $3.7 billones para el 2009. En el estudio se estima que estos servicios tendrán el 3.6 % de todas las conexiones de banda ancha para el mismo año (en los Estados Unidos).

En el reporte *Wi-Fi, WiMAX and 802.20: The Disruptive Potential of Wireless Broadband*, Monica Paolini, autora del mismo, indica que WiMAX se presenta como el dominador del mercado BWA. Ella dijo: "A través de los últimos meses, hemos visto un crecimiento en los vendedores y proveedores de servicios basando su peso sobre WiMAX como el estándar líder para el acceso de banda ancha inalámbrico". Prueba de ello es que Navini, una empresa desarrolladora de productos inalámbricos, se unió al Foro WiMAX después de apoyar durante un largo tiempo al estándar 802.20.

Finalmente, el reporte concluye que la adopción a gran escala de BWA no se dará sino hasta el 2007. Los años siguientes servirán para realizar pruebas e implementación a pequeña escala de las tecnologías como WiMAX.

4. METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UNA RED WIMAX

4.1 Factores a considerar para la implementación

Existen varios factores que tienen que ser considerados para llevar a cabo la implementación de una red WiMAX. Existen los factores tecnológicos, legislativos, sociales y culturales que pueden influir en la implementación, o incluso en la aceptación de una nueva tecnología.

4.1.1 Leyes

La SuperIntendencia de Telecomunicaciones (SIT) es la encargada de velar por el cumplimiento de los artículos establecidos en la Ley General de Telecomunicaciones. En esta ley se establece la creación de la SIT y las funciones que tiene a su cargo.

La Ley General de Telecomunicaciones esta formada por 101 artículos y se encuentra dividida de la siguiente manera:

1. DISPOSICIONES GENERALES
2. ÓRGANO COMPETENTE
    a. Superintendencia de Telecomunicaciones
    b. Normas Generales de Actuación
3. CONDICIONES DE OPERACIÓN
    a. Régimen de Operación
    b. Requerimientos
    c. Interconexión de Redes

d. Acceso a Recursos Esenciales
e. Procedimiento para Resolver Conflictos en torno al Acceso a Recursos Esenciales
f. Plan de Numeración
g. Selección de Operador de Red

4. ESPECTRO RADIOELÉCTRICO
    a. Disposiciones Generales
    b. Bandas de Frecuencias Reguladas
    c. Bandas de Frecuencias Reservadas
    d. Bandas de Frecuencias para Radioaficionados
    e. Transformación del Uso de las Bandas de Frecuencias del
    f. Espectro Radioeléctrico.
5. FONDO PARA EL DESARROLLO DE LA TELEFONIA
6. SOLUCIÓN DE CONFLICTOS ENTRE PARTICULARES
7. INFRACCIONES Y SANCIONES
8. RECURSOS CONTRA RESOLUCIONES

4.1.2 Frecuencias

Mundialmente se dividió el espectro de frecuencias y estas fueron asignadas a cada país para que las entidades respectivas se encargaran de hacer la distribución dentro del país. La entidad encargada de realizar esta división es la Unión Internacional de Telecomunicaciones, que definió el Reglamento de Radiocomunicaciones.

En Guatemala existe la SIT que es la entidad encargada de la distribución de frecuencias para los operadores. De acuerdo a la Ley General de Telecomunicaciones, existe una clasificación para las bandas de frecuencias del espectro radioeléctrico:

- Bandas de frecuencias para radioaficionados
- Bandas de frecuencias reservadas
- Bandas de frecuencias reguladas. Estas son las que hay que tomar en cuenta para las redes inalámbricas. Para utilizarlas es necesario adquirir previamente los derechos de usufructo, según lo especificado en la Ley General de Telecomunicaciones. Existe un inventario de estas frecuencias en donde se puede ver a quienes fue concedido cada rango de frecuencias y cual es la cobertura sobre la que puede utilizarlo.

4.1.3 Disponibilidad de dispositivos

Los dispositivos certificados por el estándar 802.16 aún están en desarrollo. Algunos han sido sacados al mercado para realizar pruebas o prototipos de implementaciones de estas redes, pero aún no se encuentran distribuidos comercialmente.

Los dispositivos saldrán al mercado durante el primer semestre del año 2005, aunque se espera que su adopción comience a darse a partir del segundo semestre, por lo que aún falta tiempo para poder utilizar esta tecnología en nuestro país.

4.1.4 Integración con la tecnología actual

El estándar 802.16 fue diseñado para que pudiera ser compatible con los dispositivos 802.11 que existen actualmente, para que no fuera necesario cambiar todos los dispositivos al hacer una migración hacia la nueva tecnología.

Las empresas que actualmente prestan servicios para redes inalámbricas pueden seguir utilizándolos y pueden surgir nuevas empresas, ya que cuando llegue el nuevo estándar a nuestro país, y con él los nuevos dispositivos, pueden integrarse con las infraestructuras de red actuales sin perder la interoperabilidad. En cambio, se obtiene una mejora en la cobertura de los servicios y se logra una mejor comunicación. Empresas que actualmente tienen redes 802.11 pero que tienen varias localidades dispersas en diferentes regiones pueden utilizar una topología 802.16 para integrar las diversas localidades con un método alternativo a las infraestructuras cableadas.

4.2 Análisis de factibilidad

El análisis de factibilidad sirve para saber si es posible realizar el despliegue de redes inalámbricas y específicamente WiMAX en nuestro país. En este estudio se toman aspectos como los técnicos, económicos y de impacto que pueden afectar o promover la entrada de estas redes al país.

4.2.1 Factibilidad técnica

Las redes WiMAX no son totalmente independientes de las redes Wi-Fi. En cambio, pueden cooperar para lograr una mejor interconexión. Es por ello que deben considerarse las implementaciones actuales de WLAN's y a las empresas proveedoras de este tipo de redes, ya que ellas cuentan con la experiencia de trabajar con redes inalámbricas, además de que el estándar 802.16 y sus especificaciones son compatibles e interoperables con los dispositivos 802.11 (y sus variantes).

Los dispositivos 802.16 aún se encuentran en producción, mientras que algunos de sus estándares aun esperan la certificación, y saldrán al mercado para el año 2005 (mayormente durante el segundo semestre de este año). La posibilidad de implementar una red 802.16 se pospondría hasta la llegada de estos dispositivos al mercado. Sin embargo, actualmente ya se encuentran en el mercado los dispositivos 802.11, por lo que puede iniciarse el proceso de despliegue de Redes Inalámbricas de Área Local, para que al llegar los productos 802.16 ya se cuente con una infraestructura, así como una industria de servicios inalámbricos en nuestro país.

El ultimo factor a considerar seria la obtención de los dispositivos que actuaran como clientes. Es necesario realizar estudios sobre la utilización de dispositivos inalámbricos en nuestro país, sin tomar en cuenta teléfonos celulares anteriores a los 3G (que no tienen capacidades de navegación por Internet). En base a estos estudios se puede pronosticar el crecimiento que se tendrá en el uso de estos dispositivos para conocer aproximadamente como estará el mercado de las comunicaciones inalámbricas cuando lleguen a nuestro país los dispositivos 802.16.

4.2.2 Factibilidad económica

La incursión en el mercado de las WMAN resultaría en una gran inversión para las empresas. Pero como se vio en el capitulo 3, los beneficios obtenidos con esta tecnología son positivos, si se llevan a cabo correctamente, y pueden ir aumentando al aumentar también el numero de usuarios conectados a la red.

Debido a que cada empresa es diferente y podría tomar diferentes acercamientos para entrar al mercado, es necesario que cada una de ellas realice estudios como la determinación del ROI o del TCO (Costo Total de Propiedad) para decidir finalmente la rentabilidad de proveer servicios de red inalámbricos.

También es necesario determinar los precios a los que se brindaran los servicios, ya que con estos precios se deben de cubrir los gastos de instalación y mantenimiento, pero no deben de ser tan altos como para afectar la suscripción de usuarios para recibir los servicios.

4.2.3 Factibilidad humana

La implementación de las redes inalámbricas en general no supone una gran cantidad de personal, ya que su nivel de escalabilidad y su fácil implementación hacen que el personal sea reducido. Solo si se requiere crear una infraestructura compleja puede requerirse de mas personas para llevar a cabo su implementación.

Para poder implementar estas redes se requiere que las personas tengan un alto conocimiento en los aspectos de redes, redes inalámbricas, informática, electrónica y eléctrica. Esto provocaría que se diera un aumento en el nivel de educación, ya que crearía una gran cantidad de empleos y las personas aspirantes a ellos deben de tener los conocimientos anteriormente mencionados.

4.2.4 Factibilidad de mercado

Es importante destacar que en Guatemala existen 5 empresas proveedoras de servicios telefónicos celulares, y que ellas son las que probablemente podrían incursionar inicialmente en el mercado de las redes 802.16. Otro grupo que puede entrar al mercado son los actuales proveedores de redes 802.11.

Después de que exista un mercado competitivo para las redes WMAN podrían disminuir las barreras de entrada, promoviendo la entrada de nuevos competidores al mercado, lo que provocaría la obtención de costos competitivos y de una mejor calidad hacia los usuarios.

4.2.5 Estudio de impactos

El estudio de impactos nos ayuda a determinar de que manera se verán afectados el ambiente, la cultura, la economía; en general, el país, al utilizar una tecnología como WiMAX.

4.2.5.1 Impacto ambiental

Las transmisiones sobre redes inalámbricas se realizan utilizando radio frecuencia, y en algunos casos utilizando comunicación infrarroja, lo que implica un aumento de señales electromagnéticas en el ambiente.

Se han realizado algunos estudios para comprobar que tan dañino puede ser para una persona estar expuesta a este tipo de señales. Los resultados han sido variados, por lo que no se ha concluido una respuesta exacta.

Sin embargo, se considera que no pueden ser más dañinos que la utilización de teléfonos celulares o de un horno de microondas. Es necesario hacer conciencia a los futuros usuarios sobre los posibles riesgos, y profundizar mas en los estudios para encontrar los riesgos, si en realidad existen.

4.2.5.2 Impacto social

Si se realiza la implementación de una WMAN en nuestro país los usuarios podrían obtener varios beneficios como:

- Contar con un método para comunicarse más fácilmente, y posiblemente a un menor costo. Esta comunicación va mas allá de la comunicación que se obtiene con los teléfonos celulares, ya que se podrá transmitir voz, video y datos.
- Promover el crecimiento en el uso de Internet llegando a lugares a los que antes no podía llegarse con alguna infraestructura cableada, lo que promovería también que empresas guatemaltecas incursionaran en negocios por Internet (e-bussiness, e-commerce, m-commerce, etc.).
- Promover el uso de la tecnología dentro de nuestro país, para mejorar aspectos como la educación, el entretenimiento, la información, la salud, la seguridad, etc., brindando posibilidades de estar comunicado desde cualquier lugar (dentro del rango de cobertura) de una forma transparente.
- Los actuales proveedores y los proveedores potenciales de Internet podrían invertir en esta tecnología en lugar de seguir utilizando redes de cableado de los diversos tipos, aumentando así su productividad y reduciendo los costos (economías de escala).

- Mejorar el nivel general de la población al lograr tener un acceso a información no solo de nuestro país, sino también del extranjero, logrando comunicaciones en diversos idiomas. Esto podría implicar un crecimiento en las exportaciones de productos nacionales.
- Promover la creación de nuevos servicios móviles, y aprovechar al máximo la competencia en el mercado de teléfonos celulares que existe actualmente, incentivando a los proveedores a incursionar en esta nueva tecnología.
- Creación de una industria dentro del país. La industria de redes inalámbricas. Esto también permite la creación de nuevos empleos para las personas con conocimientos suficientes para desempeñarlos.

4.2.5.3 Impacto cultural

Actualmente se cuenta con una gran cantidad de usuarios de dispositivos móviles, aunque mayormente son teléfonos celulares. Pero desde hace algunos años se ha venido dando este crecimiento de usuarios, lo que significa que han aceptado de buena manera el uso de estos dispositivos. En nuestro país no existen proveedores de redes inalámbricas actualmente. Hasta el año 2004 han comenzado a darse movimientos para la implementación de estas redes. Las redes inalámbricas que existen en nuestro país mayormente son redes dentro de empresas, no comerciales para el publico, por lo que no se puede saber con exactitud el impacto cultural, aunque tomando en cuenta el caso de los teléfonos celulares, podemos concluir que al implementar una Red de Area Metropolitana se daría una buena aceptación por parte de los usuarios, siempre y cuando los precios no sean muy elevados y haya un grupo de proveedores que creen un mercado competitivo.

4.2.6 Resultado del análisis

Los resultados del análisis de factibilidad muestran que es muy posible llevar a cabo la implantación de WMAN's dentro del país, aunque se iniciarían los movimientos para este mercado a partir del segundo semestre del 2005. Pero depende de las empresas que estén dispuestas a realizar las inversiones para utilizar la tecnología WiMAX y para poder proveer los servicios inalámbricos.

Además de ser factible la utilización de redes WiMAX, resulta ser una innovación necesaria en nuestro país ya que los beneficios que se obtendrían pueden llevar a mejorar la situación tecnológica, económica y cultural del país. Incluso en los países industrializados se obtendrían beneficios que hacen que esta tecnología tenga un fuerte apoyo y se trabaje arduamente para lograr su estandarización.

4.3 Implementación

Considerando que el análisis de sensibilidad nos revela que si puede realizarse la implementación de redes WiMAX, y el estudio de impactos nos indica que el país y sus integrantes no se verán afectados de gran manera por esta tecnología, es necesario crear un plan para llevar a cabo la implementación.

4.3.1 Aspectos a considerar

El primer aspecto a considerar antes del plan son las opciones que brinda WiMAX, en términos de servicios, topologías de red, estándares y dispositivos que utiliza.

4.3.1.1 Servicios

El primer aspecto que debe considerarse para seleccionar el tipo de red que mejor se adapta a las necesidades de la empresa es el tamaño de la empresa. Después se debe de considerar que servicios de red se brindaran a los usuarios que formaran parte de la red. Los servicios pueden ser como un servidor de Internet (ISP), servir como puente para interconectar varias redes que se encuentran en distintas localidades, conectar empresas de gran tamaño, transmisión de video o de voz en tiempo real, etc. Para cada una de estas aplicaciones, la conexión recibirá un numero limitado de usuarios que puede variar, requerirá de una tasa de transferencia determinada, tener la capacidad de llegar a grandes distancias, o contar con métodos de seguridad en diferentes niveles.

4.3.1.2 Selección del esquema de red

Existen dos topologías o esquemas de red que pueden ser usados para implementar una red 802.16. La selección del esquema de red depende del entorno sobre el que se va a realizar la conexión. El estándar 802.16a no provee conexiones sin Línea de Vista. Esto implica que cuando se realice un plan de implantación es necesario seleccionar estratégicamente la ubicación de cada estación base. Para solucionar este problema puede utilizarse la topología de redes en malla, en la que cada estación suscriptora se conecta a la estación base que sea mas optima. En un ambiente en el que se tiene libre Línea de Vista puede utilizarse una red con topología de punto a multipunto.

Con la movilidad brindada por el estándar 802.16e puede prestarse el servicio de *roamming*, para el que se adapta mejor la topología punto a multipunto para mantener la comunicación y el paso de una estación base a la otra sea más sencilla.

4.3.1.3 Selección del estándar a utilizar

Actualmente, solo esta certificado por el IEEE el estándar 802.16a, sobre el que se están basando la mayoría de dispositivos WiMAX, por lo que la selección de un estándar se encuentra limitada. Cuando se certifique el estándar 802.16e, la selección dependerá de la solución requerida. Este nuevo estándar proveerá movilidad a las estaciones suscriptoras, por lo que funciona idealmente para dispositivos de pequeño tamaño dentro de una empresa. No seria recomendable para un servicio de proveedor de Internet o para interconectar varias localidades, ya que podría provocar que muchos usuarios no autorizados accedieran a la red. El 802.16a sirve mejor para redes que pueden utilizarse en entornos públicos o de gran acceso, en los que existe un mejor control sobre los usuarios que se conectan a la red.

4.3.2 Requerimientos de hardware

Los requerimientos de HW para llevar a cabo la implementación de redes 802.16 constan de las estaciones base y de las estaciones suscriptoras. Pero también es necesario contar con Puntos de Acceso para las WLAN y que los clientes tengan tarjetas o interfaces basadas sobre el estándar 802.11. Los grandes fabricantes de dispositivos WiMAX se encuentran desarrollando estos dispositivos que llegaran al mercado para el año 2005, por lo que no existen características específicas de cada producto.

El foro WiMAX certifica los productos elaborados para redes WMAN, por lo que éstos deben cumplir con las características especificadas en la definición del estándar.

4.3.3 Plan de implantación

El despliegue de redes WiMAX aún no ha tenido un gran crecimiento, y las únicas implementaciones existentes son solo pruebas realizadas para verificar el funcionamiento del estándar. Aún no existen redes que sean aplicables para alguna empresa o servicio real. Es por eso que no existe una metodología o plan de implantación para estas redes.

A continuación se desarrolla un plan que puede ser utilizado para la adopción e implantación de redes 802.16 en un entorno como el existente en nuestro país, que no cuenta con una industria de redes inalámbricas ni con muchos proveedores de servicios 802.11:

1. Seleccionar el estándar, la topología, los servicios, etc. Para este punto es necesario considerar los aspectos tratados en el inciso 4.3.1 en donde se indican las opciones existentes que pueden seleccionarse de acuerdo a las necesidades de utilización de la red.
2. Definir que entidades participaran en la implementación (estaciones suscriptoras y estaciones base). Al identificarlas se puede diseñar un modelo de la implementación de la red.
3. Dividir la implantación en fases que van a ir creciendo gradualmente, desde WLAN's hasta WMAN's. Es necesario comenzar implementando redes de menor tamaño, para luego unirlas e ir formando redes mas grandes hasta llegar al diseño realizado en el paso 1.

4. Crear un programa de seguridad que involucre tanto el estándar 802.11 como el 802.16. En el Apéndice A se tratan los aspectos de seguridad referentes a los estándares 802.11 y 802.16. En este apéndice también se menciona la importancia de contar con seguridad dentro de las redes, que problemas tienen los métodos de seguridad existentes y cuales son los posibles ataques que pueden sufrir las redes inalámbricas.
5. Colocación de PA's del estándar 802.11. De acuerdo a la división de las redes, el dispositivo básico para crear WLAN's son los Puntos de Acceso. Es necesario colocarlos estratégicamente para que pueda aprovecharse al máximo su potencial.
6. Realizar pruebas de conexión (cobertura, velocidad, # de usuarios) y de seguridad (autenticación, encriptación) sobre las WLAN's. Al tener colocados los PA's deben realizarse pruebas para verificar que su instalación concuerda con lo especificado en el diseño de la red.
7. Colocación de estaciones base del estándar 802.16. Cuando se ha asegurado la funcionalidad de las WLAN's individualmente, se deben colocar las estaciones base, que son el elemento básico de comunicación en las redes WMAN, para que sirva como puente o router entre las diferentes WLAN's.
8. Configurar las capas física y MAC, además del canal de comunicación por el que se transmitirá la información entre los equipos. Es necesario configurar las frecuencias sobre las que trabajaran los marcos y el secuenciamiento que utilizaran. También se deben configurar los servicios que se incluyeron en el paso 1 (QoS).
9. Se realiza una adaptación entre la capa de red y la capa MAC del 802.16 para que se cumpla con el modelo OSI para la comunicación entre redes.

10. Realizar pruebas de conexión y de seguridad sobre las WMAN's. De igual forma que en cada WLAN, es necesario verificar que exista conectividad entre cada una de ellas al incorporar la red WMAN a la estructura.
11. Al terminar la implantación es necesario crear un plan para auditar la red. La auditoria de la red se refiere a controlar los accesos a la red y la utilización de los recursos de la misma. El plan de auditoria es necesario para verificar que solo las personas autorizadas accedan a los recursos y que solo accedan a los recursos sobre los que tienen permiso.
12. Capacitación de las personas que utilizaran la WMAN. Es necesario capacitar tanto a los usuarios como a los administradores. Los administradores deben conocer los modos de funcionamiento de las redes (802.11 y 802.16), las características descritas en su definición y los métodos de seguridad utilizados. Los usuarios deben de ser capacitados en aspectos básicos de las redes inalámbricas, que le permitan realizar conexiones con otros dispositivos dentro de la red y utilizar sus recursos. Es necesario que los usuarios conozcan la importancia de la información de conexión que ellos poseen, para que no pueda ser utilizada por personal no autorizado.
13. Ejecutar la auditoria y monitoreo de la red para asegurar su funcionamiento y su desempeño. Se debe contar con personal capacitado para llevar a cabo la auditoria y el monitoreo de la red. Es importante que además de los accesos a la red se verifique que se encuentra funcionando de acuerdo a su especificación y que no se dan problemas de conexión. También debe de verificarse el desempeño de la red, ya que las tasas de transmisión pueden descender a medida que aumenta la distancia sobre la que se desea realizar la comunicación.

14. Mantener actualizado el software de los dispositivos, en caso de que surjan mejoras de seguridad o del manejo de la comunicación. Actualmente están en desarrollo nuevos métodos de seguridad que pueden ser incorporados a través de actualizaciones de software o de reemplazo de hardware. También están siendo desarrollados nuevos dispositivos para asegurar la interoperabilidad con los estándares que recientemente han sido certificados por el IEEE.

CONCLUSIONES

1. El estándar 802.11 ha sido aceptado mundialmente y está ganando constantemente más adeptos, con lo que se coloca de manera estable en el mercado.

2. Las características para brindar la conexión de la última milla hacen que el estándar 802.16 sea un fuerte competidor para las tecnologías cableadas utilizadas actualmente.

3. La estandarización del 802.16 y sus variantes puede ser un obstáculo para su incursión definitiva en el mercado, ya que hasta el momento sólo la versión (a) se encuentra estandarizada.

4. El estándar 802.16 no reemplazará al 802.11, sino que lo complementará, para tener una mayor cobertura, y aprovechar el equipo que actualmente es el más usado.

5. El crecimiento del 802.16 no hubiera sido posible si no hubiera existido una aceptación del estándar 802.11, ya que a partir de su crecimiento comenzaron a aparecer nuevas tecnologías para redes inalámbricas.

6. Las características de calidad de servicio (QoS) y de seguridad se encuentran implementadas en el 802.16, lo que lo hace ganar una ventaja sobre el 802.11, que no las incluye dentro de sus características básicas.

RECOMENDACIONES

1. Crear una cultura en la que se utilicen redes inalámbricas, así como sus servicios, para que la integración de las redes WiMAX sea más sencilla, y exista una menor resistencia al cambio.

2. Desarrollar planes estratégicos en los que se incluya la adopción del estándar 802.11, además de la integración del 802.16 a la infraestructura tecnológica de las empresas.

3. Desarrollar planes de seguridad tanto a nivel tecnológico como a nivel humano, tomando en cuenta los métodos existentes actualmente, además de los métodos que aún se encuentran en desarrollo.

4. Antes de tomar la decisión de utilizar una red inalámbrica, realizar un estudio sobre los beneficios, los costos y la factibilidad de la implantación.

5. Apoyar e incentivar la creación de estándares para redes inalámbricas, ya que esto permite una reducción de costos, disminuyendo la creación de productos propietarios.

BIBLIOGRAFÍA

1. Arbaugh, William A. Y otros. Your 802.11 wireless network has no clothes. Estados Unidos: s.e., 2001. 13pp.

2. Brenner, Pablo. A technical tutorial on the IEEE 802.11 protocol. 1997. 24pp.

3. Carney, William. IEEE 802.11g new draft Standard clarifies future of wireless LAN. 2002. 5pp.

4. Chang, Dean y Subir Varma. Wimax rolls interop guidelines for 802.16a. 2003.

5. Cohen, Beth y Debbie Deutsch. 802.16: a look under the hood. Wi-Fi Planet. 2003.

6. Cox, John. Calculating costs of WLANs. Network World Fusion. 2004.

7. Fellah, Adlane. WiMAX, NLOS and Broadband Wireless Access (Sub-11Ghz) Worldwide Market Analysis 2004-2008. 2ª ed. Canada: s.e., 10pp.

8. Fora, Pau Oliva, (In)seguridad en redes 802.11b. Matarowireless. 2003. 34pp.

9. Gabriel, Caroline. WiMAX: the critical wireless Standard. 33pp.

10. Gómez, Catherine y otros. Estudio de Factibilidad. Colombia: s.e., 2000. 14 pp.

11. Grima, Brian. Wi-Fi Protected Access. Wi-Fi Alliance. 2002. 3pp.

12. Hayes, Vic. Tutorial on 802.11 to 802. 1996. 16pp.

13. IEEE. IEEE 802.16's Published Standards and Drafts. 2004.

14. Incrementar la productividad mediante WLANs. Wireless Mundi. 2003.

16. Intel. Accelerating wireless broadband. 2003. 6pp.

17. Intel. Can going wireless really be simple?. s.l. 12pp.

18. Intel. IEEE 802.16* and WiMAX. 2003. 8pp.

19. Intel. Linking productivity gains to return on investment. 2002.

20. Intel. Which WLAN is right for you. 2004.

21. Intel. Wireless LAN deployment considerations. 2004.

22. Intel. Wireless LAN productivity cases. 2004.

23. Johnston, David y Hassan Yaghoobi. Peering into the WiMAX spec. 2004.

24. Louazel, Benoit. Implementation of IEEE 802.16a in GloMoSim/QualNet. 2004.

25. Marks, Roger. IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access. 2002. 12pp.

26. Raichura, J.P. WiMAX/IEEE 802.16* technology briefing. 35pp.

27. Salvador, Dave. Picking the right topology. Extreme Tech. 2003.

28. Scheurich, Christoph. Wireless: An Overview. s.l.

29. Shakouri, Mohammad. Capitalazing on the WIMAX market opportunity. 2004. 17pp.

30. SIT. Ley general de telecomunicaciones. Guatemala: s.e., 1998. 33pp.

31. Tropos networks. 802.11 Technologies: Past, Present and Future. 2004.

32. Unión Internacional de Telecomunicaciones. La invasión de los sistemas Wi-Fi. 2003.

33. Wimax will dominate broadband wireless market in 2006. 2003.

34. Yoo, Joon. IEEE 802.16 standardas & drafts. 2003. 52pp.

A. SEGURIDAD EN REDES INALÁMBRICAS

La seguridad es un tema muy importante cuando se trabaja con cualquier tipo de redes que interconectan diversos dispositivos. En las redes cableadas se ha logrado alcanzar un nivel de seguridad alto en el que el acceso a las redes queda restringido sólo a los usuarios que tienen asignado este acceso. A medida que avanza el tiempo se ha logrado cubrir una gran cantidad de los problemas en la seguridad de estas redes y así evitar los ataques que pueden ser aplicados a ellas. Sin embargo, en las redes inalámbricas aún se desarrollan métodos para alcanzar un nivel de seguridad alto, que sea de una efectividad similar a la seguridad de las redes cableadas.

A.1 Seguridad en Wi-Fi

El manejo de la seguridad es un aspecto importante en las telecomunicaciones, y las redes inalámbricas no son la excepción. Ahora veremos los aspectos básicos de seguridad para redes inalámbricas de área local.

A.1.1 Aspectos básicos

Cuando se tiene una WLAN es necesario cumplir con ciertos aspectos básicos de seguridad para limitar el acceso de los usuarios a los recursos de la red. Son características mínimas que debe brindar una red inalámbrica.

A.1.1.1 Autenticación

La autenticación es necesaria para restringir el acceso a la red. Cada usuario que quiere utilizar los recursos de la red, primero debe autenticarse, demostrando que tiene autorizado el acceso a ellos. Existen dos métodos para realizar la autenticación: Sistema abierto y Llave compartida.

A.1.1.1.1 Autenticación por sistema abierto

Es el método de autenticación que es predeterminado para el protocolo 802.11. Este método autentica a cualquier usuario que solicite la autenticación. Consiste en que el cliente que desea conectarse a la red envía una solicitud de autenticación con su ID y el PA le devuelve una respuesta, ya sea exitosa o rechazada.

A.1.1.1.2 Autenticación por llave compartida

Cuando un cliente se quiere conectar a un PA, los dos equipos deben tener la misma llave. Utiliza un método estándar de petición de autenticación en el que se utiliza una llave secreta. La diferencia con el método de sistema abierto consiste en que se utiliza la llave para encriptar los paquetes de autenticación. Este método es menos utilizado, ya que en los ataques a las redes 802.11 se capturan los paquetes encriptados y a partir de éstos los atacantes pueden obtener la llave de encriptación WEP y conectarse a la red.

A.1.1.2 Propagación de la señal

Se refiere al rango de cobertura que tienen los PA's. Al administrar efectivamente la propagación de la señal se logra que sólo puedan conectarse usuarios que se encuentren dentro del área de cobertura, lo que hace más difícil para las personas no autorizadas entrar a la red, ya que físicamente deben estar dentro de esta área. Al extender el área de cobertura más allá de los límites deseados puede hacer que la red sea más vulnerable a ataques de usuarios externos.

A.1.1.3 Identificador del conjunto de servicios (SSID)

El SSID es un identificador de la red, que identifica el área cubierta por uno o más PA's. Los PA's se encuentran transmitiendo su SSID para que los usuarios puedan recibirlo. Los usuarios deben tener configurado el SSID del PA al que desean conectarse. Cuando un usuario se conecta a la red, son comparados los SSID del PA y del dispositivo cliente. Si se determina que no son iguales, la conexión es rechazada. Este método no asegura la limitación de las conexiones, ya que envía los paquetes con el SSID sin encriptar, haciendo fácil para cualquier atacante obtenerlo y configurarlo en su propio dispositivo.

A.1.1.4 Encriptación

Encriptar significa transformar la información para que no viaje tal y como es. Se utilizan llaves para transformar la información para que no pueda ser leída sin tener la misma llave. Para redes 802.11 existen los métodos WEP y el Protocolo de Integridad de Llave Temporal (TKIP).

En WEP se utiliza una llave estática de 40 bits. En TKIP la llave no es estática, y es de 128 bits, mejorando el método WEP. También existe la Verificación de la Integridad del Mensaje (MIC) que está diseñada para prevenir la captura de paquetes, para que éstos no puedan ser alterados o reenviados. MIC consiste en funciones matemáticas utilizadas en el transmisor y el receptor y luego se comparan los resultados. Si el resultado no concuerda, el paquete es desechado.

A.1.1.5 Privacidad

Debido a que la señal viaja por un medio físico abierto, las conexiones a la red no están limitadas físicamente, solamente por la configuración de los PA's. La información puede ser capturada por cualquier persona con dispositivos inalámbricos y con software de administración de red. La única medida de privacidad que existe es la encriptación de los paquetes, aunque las llaves de encriptación pueden ser encontradas a partir de la captura de paquetes.

A.1.2 Métodos

El estándar 802.11 fue diseñado junto con algunos métodos para brindar seguridad, y otros fueron agregados al darse cuenta que los métodos actuales no eran suficientes para brindar el alto nivel de seguridad requerido.

A.1.2.1 WEP (*Wired Equivalent Privacy*)

Es un protocolo utilizado para brindar seguridad a las redes inalámbricas. Consiste en encriptar la información en las capas física y MAC. Está basado en el algoritmo RC4, que es un algoritmo simétrico (utiliza las mismas llaves para cifrar y descifrar) utilizando llaves de 64 bits (la llave consiste de 40 bits, y el vector de inicialización (IV) consiste de los otros 24 bits).

En su especificación en el estándar 802.11 se definieron las siguientes características:

- Encripción. Permite enviar información de una manera más segura, considerando la dificultad de desencriptarla sin tener la llave. Mientras más grande es la llave, mayor la dificultad de obtenerla.
- Autosincronización. No existe pérdida de paquetes, y no es necesario realizar una configuración o control adicional sobre los paquetes, ya que contienen la información suficiente para poder ser recuperados y desencriptados en el orden correcto.
- Eficiente. No afecta el desempeño en la transmisión de información y tampoco afecta su integridad.
- Exportable. Al utilizar un tamaño de llave similar puede utilizarse en varios países sin cambiar su especificación.

Su funcionamiento está definido de la siguiente manera:

- Se transmite la llave entre las estaciones que se comunicarán por el medio inalámbrico. La transmisión debe realizarse a través de un medio seguro.
- Se genera una semilla con la llave de 40 bits y el vector de inicialización de 24 bits. Esta semilla se utiliza de entrada para el Generador de Números Seudo Aleatorios (PRNG).

- El PRNG genera octetos de números seudo aleatorios.
- A cada PDU a transmitir se le aplica un XOR con la cadena de octetos generada, produciendo el PDU cifrado.
- El PDU cifrado se concatena con el vector de inicialización y se transmite por el medio inalámbrico.
- El receptor lee el vector de inicialización y lo concatena con su llave para producir una semilla que introducirá en su PRNG.
- El PRNG del receptor genera una cadena igual a la generada por el transmisor, y aplicando un XOR al PDU cifrado con la cadena generada se obtiene el PDU original.

A.1.2.2 802.1x

Este estándar fue diseñado originalmente para redes cableadas. Se basa en los servidores de autenticación RADIUS. También es conocido como Control de Acceso a la Red basado en Puertos. Utiliza el Protocolo de Autenticación Extensible (EAP) y RADIUS para autenticar a los usuarios. Esta infraestructura permite que los usuarios se autentiquen con un servidor central. Cuando el servidor acepta la autenticación de la identidad del usuario, envía información al usuario y a los PA's para que puedan conectarse entre ellos. Se utiliza una conexión de confianza, en la que cada participante se autentica hacia el otro, asegurando la conexión con los PA's de la red. Además, asegura la generación y distribución continua de llaves de encriptación. Estas llaves dinámicas reducen el riesgo de determinar la llave de encriptación al obtener información capturando paquetes, ya que la llave cambia cada cierto conjunto de paquetes.

A.1.2.3 VPN (*Virtual Private Network*)

Esta implementación de redes fue diseñada para redes cableadas. Se utiliza para proveer seguridad a comunicaciones remotas a través de Internet. Cuando un usuario utiliza un túnel VPN, la información es encriptada hasta llegar al *gateway* VPN, que se encuentra antes del PA.

Los atacantes no pueden utilizar la información que se obtiene de la VPN, ya que se encuentra encriptada, aunque se recomienda encriptar también la ruta entre el *gateway* y el VPN. Esta opción de seguridad es muy recomendada para soluciones empresariales. Cuando una VPN se instala adecuadamente, extiende el nivel de seguridad a un nivel similar a las redes cableadas.

A.1.2.4 802.11i

Este nuevo estándar, desarrollado por el IEEE, pretende cubrir los aspectos cubiertos en el 802.1X y en EAP, mejorando las características de seguridad de cada uno de ellos. Entre sus nuevas características se diseñaron nuevos esquemas de encriptación y métodos dinámicos de distribución de llaves.

Como las otras soluciones posteriores a WEP, el 802.11i también pretende solucionar los problemas y vulnerabilidades encontradas en WEP, ya que las llaves que utiliza son dinámicas en lugar de estáticas, además de ser de un mayor tamaño (128 bits). Utiliza TKIP como protocolo para generar llaves temporales. Al utilizar llaves temporales, cada estación cliente conectada a la red utiliza diferentes llaves de encriptación a través del tiempo.

Al utilizar TKIP se reduce la posibilidad de encontrar la clave que se está usando para encriptar los datos, y aunque fuera encontrada sólo podría usarse mientras la llave se encuentre dentro de su período útil para esa estación. En este nuevo estándar no se utiliza el mismo método de encriptación que en WEP, sino que es sustituido por el Estándar de Encriptación Avanzada (AES). Este algoritmo se basa en utilizar llaves de longitud variable, que pueden ser de 128, 192 o 256 bits. El inconveniente con este nuevo estándar consiste en que no es totalmente compatible con los dispositivos 802.11 actuales. Requiere de nuevos dispositivos que soporte el estándar.

A.1.2.5 WPA (*Wi-Fi Protected Access*)

Este es un nuevo estándar, que aunque no pertenece al 802.11, está basado en dicho estándar para cubrir las deficiencias que se tienen con WEP. WPA se deriva del estándar 802.11i, por lo que será compatible con los productos certificados para este estándar.

Una de las ventajas de WPA es que consiste en una actualización del software, en contraste con el 802.11i que requiere de nuevo hardware. Mejora las características de encriptación de la información y de autenticación existentes en WEP.

Además, WPA cuenta con el apoyo de la Alianza Wi-Fi, quienes ya certifican productos que utilizan WPA. De acuerdo a su especificación, WPA cubre todas las vulnerabilidades conocidas en WEP, convirtiéndolo en una gran mejora en seguridad para las redes 802.11. De igual forma que el 802.11i, WPA utiliza TKIP para la generación de claves temporales. Como método de autenticación utiliza el 802.1X junto con el Protocolo de Autenticación Extensible (EAP).

Utiliza en conjunto estos métodos con los que se logran crear niveles, como una jerarquía de seguridad, a la que se le añade una comprobación de los mensajes (MIC) para evitar la falsificación de los paquetes.

A.1.2.6 WPA2

También utiliza TKIP, 802.1X y EAP, de la misma forma en que son utilizados en WPA. Sin embargo, se añade un nuevo esquema de encriptación de datos (AES). Este esquema permite que exista seguridad entre los clientes que se encuentren en una topología ad hoc. Utiliza un algoritmo de autenticación mutuo, en el que ambas partes que desean realizar una conexión deben autenticarse mutuamente, para que cada una de ellas esté segura de que está estableciendo la comunicación con la estación correcta. Está diseñado para mejorar la seguridad de los dispositivos 802.11 y sus variantes, haciéndolo compatible con los productos existentes.

Debido a que se deriva de la versión original de WPA, WPA2 permite que la transición de la versión 1 a la 2 sea sencilla. También permite trabajar en modo mixto, esto significa que puede configurarse para utilizar cualquiera de las dos versiones, dependiendo de las características requeridas. Se asegura que con esta selección de versiones no se comprometerá la seguridad de la red.

A.1.2.7 Otros métodos de seguridad

Existe un conjunto de métodos que son propietarios y que han sido desarrollados por grandes fabricantes, que no se encuentran dentro de la especificación de ningún estándar de seguridad. Debido a que son métodos propietarios de cada empresa, no existe interoperabilidad, sólo entre productos de la misma empresa.

A.1.2.7.1 Infraestructura de autenticación y privacidad WLAN (WAPI)

Es un estándar creado por la Administración de Estandarización de China (SAC) en el año 2003. Como el resto de soluciones creadas después de WEP, WAPI sirve para mejorar las características de seguridad de éste. Este estándar sólo es utilizado en China, en donde se requiere que todos los dispositivos inalámbricos cumplan con él. Paul Nikolich, presidente del comité de estándares para LAN y MAN del IEEE 802 dijo: "Creemos que la implementación obligatoria de protocolos WAPI fragmentará sin necesidad el mercado mundial de productos WLAN". Al expresar esto, Nikolich muestra su preocupación por la falta de estándares, ya que esto elimina el concepto de economía de escala, implicando un costo más elevado para los usuarios de redes inalámbricas.

A.1.2.7.2 Control de acceso a una red cerrada

Es un mecanismo para controlar el acceso a la red desarrollado por Lucent. Con este método puede seleccionarse la forma de operar de la red. Puede encontrarse abierta o cerrada. En una red abierta, se permite que cualquier usuario pueda acceder a la red. En una red cerrada, sólo los usuarios que conocen el nombre de la red (SSID) pueden acceder a ella.

A.1.2.7.3 Listas de control de acceso (ACL)

Este método se basa en las direcciones MAC de las estaciones cliente. Cada PA tiene un límite de usuarios que pueden estar conectados a él, y estos usuarios deben estar especificados en una lista conteniendo las direcciones MAC de cada uno de ellos.

Sólo pueden acceder los usuarios cuyas direcciones MAC se encuentren en la lista del PA. Si una estación quiere conectarse a la red y su dirección MAC no se encuentra en el listado, entonces se rechaza el acceso a la red.

A.1.2.7.4 Administración de llaves

Este método sólo es utilizado por algunos de los mayores fabricantes de productos 802.11. No es muy confiable, ya que en algunas implementaciones se utilizan métodos de seguridad que tienen vulnerabilidades conocidas que pueden ser explotadas por quienes atacan la red. Su mejor desempeño se presenta cuando se utilizan diferentes llaves para cada usuario, pero deben establecerse períodos de duración para las llaves, tomando en cuenta que las llaves sólo pueden ser cambiadas manualmente.

A.1.3 Vulnerabilidades

La primera vulnerabilidad de una red inalámbrica consiste en que la información viaja libremente a través del aire, y no sobre un medio de difícil acceso. Esto implica que cualquier persona con los dispositivos adecuados puede acceder a la información.

El método WEP fue el primero utilizado para cubrir los problemas de seguridad en las redes 802.11. Pero al utilizar este método se encontraron ciertas vulnerabilidades. Con la creación de nuevos métodos de seguridad se intentan solucionar las vulnerabilidades de WEP.

Debido a que los métodos creados recientemente cubren los problemas de WEP, las vulnerabilidades que pueden darse en una red 802.11 son las de este método. Con el resto de métodos aún no se han reportado vulnerabilidades que deban ser solucionadas.

A.1.3.1 Problemas con la autenticación

En las redes 802.11 existen diferentes métodos de autenticación, pero ninguno de ellos asegura que la información no puede ser falsificada por un atacante que ha capturado los paquetes enviados entre una estación cliente y un PA. Si una persona puede capturar los paquetes (con un *sniffer*), es posible que pueda obtener la información necesaria para que pueda autenticarse al PA, y así acceder a la red.

A.1.3.2 Problemas con la encriptación

En este punto existen varios problemas. El primero es que el tamaño de la llave utilizada es solo de 40 bits. Esto hace que el número de combinaciones para encontrar la clave no es tan grande como en 802.11i y en WPA. El segundo problema es el método de encriptación que utiliza (RC4). En el artículo *Weaknesses in the Key Scheduling Algorithm of RC4,* publicado por Fluhrer, Martin y Shamir en el 2001, muestran cómo puede realizarse un ataque pasivo para determinar la llave completa a partir de un texto cifrado. El tiempo para determinar la llave es relativamente corto y crece de forma lineal, sin importar el tamaño de la llave o del vector de inicialización (VI). Además de este ataque, existe la posibilidad de desencriptar la información sin contar con la llave secreta. Esto se debe a que puede obtenerse el VI por medio de un sniffer, ya que en la definición del 802.11, el VI debe viajar tal y como es.

Conociendo el VI puede cancelarse el XOR aplicado para realizar la encriptación y así obtener el mensaje original.

El tercer problema que se encuentra es que la llave es estática, o sea que no cambia a través del tiempo. Esto significa que si una persona es capaz de descifrar la clave de WEP, puede utilizarla para desencriptar todos los paquetes de la red, ya que la llave no cambiará, a menos que se haga manualmente.

A.1.3.3 Otras vulnerabilidades

Las vulnerabilidades mencionadas anteriormente son aspectos técnicos de las redes inalámbricas. Sin embargo, también existen vulnerabilidades creadas por los usuarios y administradores de dichas redes:

- No habilitación de los métodos de seguridad disponibles. Hay ocasiones en que la red cuenta con los mejores métodos de seguridad, pero no son habilitados o son configurados incorrectamente, lo que hace que su potencial no sea aprovechado.
- Tarjetas en modo ad hoc. Esto puede permitir que otros usuarios puedan obtener credenciales de autenticación, así como robar información. Cuando una tarjeta se encuentra en modo ad hoc, los métodos de seguridad no pueden prevenir el robo de información.
- Ingeniería Social. Existen personas capaces de obtener información de los usuarios de una red utilizando métodos para engañarlos y así poder autenticarse como ellos. También existen usuarios que comparten su información de autenticación con otras personas, sin saber la importancia de esta información.

A.1.4 Ataques

Basándose en las vulnerabilidades descritas anteriormente, los *hackers* han encontrado la forma de atacar las redes inalámbricas. Aunque algunos ataques son pasivos y no afectan el desempeño de la red, otros pueden falsificar la identidad de los usuarios o de los PA's, utilizar información robada, hacer que un PA no pueda aceptar peticiones de conexión, etc.

A.1.4.1 Ataque basado en ACL

Este ataque puede aplicarse cuando se utiliza el método de Listas de Control de Acceso en los PA. Este método restringe el acceso a la red sólo a los clientes que tienen direcciones MAC registradas. El ataque consiste en utilizar un *sniffer* de paquetes para obtener la dirección MAC de algún cliente. Después, se modifica la dirección MAC de la estación atacante por la MAC obtenida en el *sniffer*. Entonces la estación atacante aparece ante el PA como una estación cliente válida. Para esto es necesario que la estación a la que se está sustituyendo no debe estar conectada a la red.

A.1.4.2 Descubrir SSID

Un método de seguridad utilizado es el de ocultar el SSID del PA, para que no pueda ser obtenido por algún atacante. Para que un atacante pueda obtener un SSID oculto, primero debe esperar a que un cliente realice una petición de conexión. Después, utilizando un *sniffer*, se puede obtener el SSID en el paquete que solicita la autenticación. Después de descubrir un SSID, ya se pueden realizar intentos de conexión a la red.

A.1.4.3 Negación de servicio (DoS)

En este caso, el atacante se hace pasar por el PA, de igual forma que en el caso anterior, utilizando un *sniffer* para obtener la dirección MAC del PA y luego asignándola a la estación atacante. Después de esto, los clientes intentarán conectarse al atacante, quien envía notificaciones de desasociación para negarles el acceso a la red.

A.1.4.4 *Man in the middle* (Hombre en Medio)

Este ataque es similar a los de falsificación de identidad como el de ACL o DoS. La diferencia de este ataque es que el atacante se coloca lógicamente entre el PA y el cliente, haciéndoles creer a ambos que están conectados entre ellos, cuando en realidad los dos se conectan con el atacante, quien falsifica la identidad de los dos. Toda la información entre ellos pasa por el atacante.

A.1.4.5 ARP *poisoning* (Envenenamiento de ARP)

Este ataque se da cuando la red se encuentra en una topología de infraestructura. Consiste en envenenar la caché de ARP de un sistema dentro de la LAN cableada. Esto permite realizar un ataque *Man in the Middle* en la WLAN. En este caso, el atacante envía paquetes de tipo ARP hacia las estaciones de la LAN, en los que envía información necesaria para que el tráfico se redireccione hacia él. Si se utilizan *switches*, puede evitarse creando VLAN's o utilizando tablas de ARP estáticas en todas las estaciones.

A.2 Seguridad en WiMAX

La seguridad en WiMAX ha sido un factor importante para que muchas empresas apuesten por qué ésta será la tecnología predominante en las redes inalámbricas dentro de algunos años, ya que incorpora métodos que brindan un nivel de seguridad similar al de las redes cableadas.

A.2.1 Aspectos básicos

Al igual que las WLAN's, las WMAN's deben cumplir algunos aspectos básicos de seguridad, que son importantes para su adopción como un estándar para redes inalámbricas.

A.2.1.1 Autenticación

En el 802.16 se utilizan certificados x.509 versión 3 para realizar la autenticación. Estos certificados digitales garantizan la identidad de los dispositivos 802.16 dentro de la red. Estos certificados están formados por el número de serie, la dirección MAC, el nombre del fabricante y la autoridad que firmó el certificado del fabricante de los dispositivos, haciéndolos robustos por la cantidad de información contenida en ellos.

Los certificados actúan en los dispositivos 802.16 de la misma forma en que las direcciones MAC actúan en los dispositivos Ethernet.

Esta especificación es parte de la capa Parte Común MAC. Cuando un usuario quiere autenticarse hacia una estación base, ésta revisa que el usuario tenga autorización para conectarse y acceder a los servicios de la red.

Si la estación base determina que sí tiene autorización, envía una clave de autorización encriptada con la llave pública del usuario.

A.2.1.2 Confidencialidad

Este es uno de los factores más importantes de seguridad dentro de las redes 802.16, ya que pueden utilizarse sobre bandas de frecuencias no licenciadas. Es por eso que se utilizan métodos de encriptación, para asegurar la confidencialidad de la información entre los elementos de la red. Utiliza el algoritmo simétrico AES para realizar la comunicación. Pero para poder utilizarlo es necesario que ambas partes conozcan las bases para la comunicación. Estas bases deben de establecerlas utilizando un método asimétrico de encriptación, como la llave pública.

A.2.1.3 Integridad

La integridad se refiere a que la información no es alterada de ninguna manera y llega al receptor tal y como fue enviada por el emisor. La integridad se asegura a través de firmas digitales y funciones de hash. Los fabricantes de dispositivos pueden firmar digitalmente el software que utilizan sus dispositivos para asegurar la funcionalidad y que no ha sido alterado.

A.2.2 Métodos

Los métodos utilizados para la seguridad en el 802.16 están definidos en Docsis. Entre ellos se encuentran los siguientes:

- DES en modo Encadenamiento de Bloque Cifrado (CBC) para encriptar los paquetes que son transmitidos.

- Protocolo PKM para autorizar a las estaciones suscriptoras a transmitir llaves entre ellas y las estaciones bases. Utiliza certificados y métodos de llave pública RSA para autenticar las estaciones suscriptoras.

A.2.3 Vulnerabilidades

En la definición del estándar 802.16 se encuentran especificados todos los métodos de seguridad que utiliza, incluso cuenta con una subcapa encargada para manejar la privacidad. Utiliza métodos basados en niveles de seguridad, lo que hace que sea más seguro que los métodos para las redes 802.11. Incorpora métodos de encriptación más robustos, con llaves de mayor tamaño y que varían con el tiempo, además de certificados y firmas digitales, y métodos de autenticación mejorados.

Debido a todas las características descritas anteriormente, además que aún no existen implementaciones públicas de este tipo de redes, hacen que el encontrar vulnerabilidades para los métodos de seguridad sea más complicado. Pero de igual manera como se encontraron los problemas del método WEP para el 802.11, que estaban basados en las matemáticas, también sería posible encontrar similares problemas para los métodos más avanzados utilizados en 802.16, contando con el conocimiento matemático suficiente, además de las herramientas para poder demostrarlo.

A.2.4 Ataques

Debido a que no se han encontrado las vulnerabilidades existentes en este protocolo, y aún no hay redes sobre las que se puedan practicar ataques, tampoco existen ataques conocidos para este estándar.

A.3 Buenas prácticas de seguridad en redes inalámbricas

Los siguientes son algunos de los puntos que deben considerarse para tener los aspectos básicos de seguridad al utilizar una red inalámbrica:

- Habilitar todos los métodos de seguridad para redes inalámbricas posibles.
  - Apagar los PA's cuando no se encuentren en uso.
  - Ajustar el poder de las salidas de los PA's.
  - Deshabilitar cualquier SSID nulo.
  - Utilizar filtrado de MAC.
  - Utilizar el método WEP para encriptar datos.
  - Utilizar el IPSec.
- Actualización contínua de dispositivos, métodos de seguridad o software.
- Utilizar métodos de seguridad físicos o en otra capa (como los *firewalls*).
- Especificar a los usuarios de estas redes cuáles son las vulnerabilidades que poseen, mostrando las posibles amenazas.
- Informar a los usuarios sobre la mejor forma de crear *passwords* para que éstos sean más difíciles de encontrar.
- Crear una conciencia sobre los usuarios acerca de la importancia de la información de autenticación, y sobre no compartir dicha información con otras personas.
- Utilizar herramientas de administración para monitorear la red.
- Planear efectivamente la colocación del equipo *wireless.*

B. ECOSISTEMA TECNOLÓGICO

Es un modelo conceptual creado para entender la evolución tecnológica, tomando como base el concepto de sistema dinámico. Este concepto indica que un sistema es un conjunto de componentes relacionados entre si, que buscan un fin común, y que tienen algún método de control. Además, este sistema forma parte de un sistema mayor, y es influenciado por fuerzas del entorno. A partir de este concepto, tenemos que un ecosistema tecnológico es un modelo que nos muestra una tecnología específica, los elementos que la componen, tecnologías con las que interactúa y factores externos que influencian el crecimiento de la tecnología.

Este modelo se basa en pronósticos tecnológicos, estudios de la evolución tecnológica y las investigaciones actuales en innovación. A este modelo se le denominó ecosistema, ya que se basa en el concepto original de ecosistema: un hábitat para una variedad de especies diferentes que coexisten, se influencian entre ellas y son afectadas por un conjunto de fuerzas externas. La evolución de estas especies afecta al ecosistema y se ve afectada por la evolución de otras especies.

B.1 Elementos del ecosistema tecnológico

Existen dos tipos de elementos que conforman un ecosistema tecnológico: los roles y las relaciones. Los roles que se pueden identificar son:

- Componentes
- Productos y aplicaciones
- Soporte e infraestructura

Las relaciones que existen entre cada uno de estos roles son llamadas caminos de influencia.

B.2 ¿Por qué se creo el modelo?

La creación de este modelo surgió de la necesidad de realizar mejores predicciones sobre aspectos tecnológicos, tomar ventaja sobre las inversiones y oportunidades del mercado, y mantener o hacer crecer las cuotas del mercado. También se pretende que con este modelo se unifiquen los numerosos métodos que existen actualmente para realizar pronósticos en el área de la tecnología, que van desde extrapolación analítica de tendencias, hasta paneles de discusión de expertos en la materia. A la única conclusión que se puede llegar a partir de todos estos métodos es que realizar un pronóstico sobre la evolución tecnológica es extremadamente complejo y difícil.

Al utilizar este modelo, podremos observar la evolución de una tecnología en específico, las redes WiMAX, y así poder apreciar de mejor manera cuál es el camino o la tendencia que sigue la adopción de esta nueva tecnología, y podremos anticiparnos de mejor manera a las siguientes etapas del ciclo de vida de la tecnología.

B.3 Pasos para crear un ecosistema tecnológico

Para desarrollar un modelo de ecosistema tecnológico es necesario seguir una serie de pasos, que van desde el propósito del modelo hasta un diagrama evolutivo de la tecnología que estamos modelando. El listado de pasos es el siguiente:

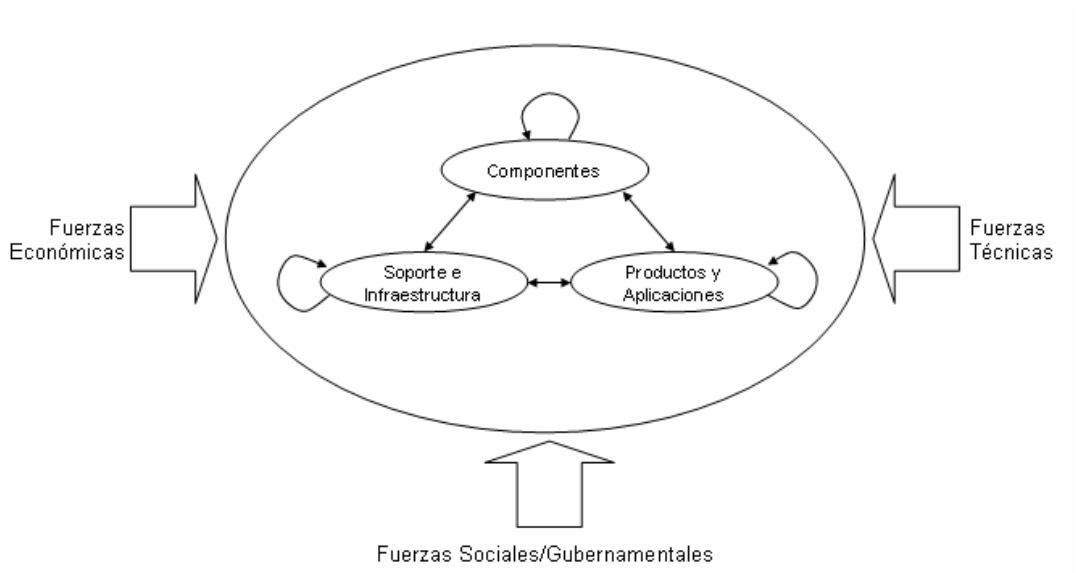
1. Establecer el propósito del modelo. Es importante conocer cuál es la motivación del modelo, así como también, qué es lo que esperamos obtener al finalizar su construcción.
2. Encontrar las tecnologías participantes que pueden influenciar o verse influenciadas por la evolución de la tecnología que se está estudiando. Para este paso es necesario:
    - Identificar la tecnología sobre la que se enfoca el modelo. Es el punto de enfoque o de partida para mapear el ecosistema, además de servir como contexto para identificar tecnologías relacionadas
    - Identificar tecnologías competentes. También es necesario identificar cualquier otra tecnología que forme parte del entorno de la de enfoque, siendo complementaria o sustituta en proveer la misma función o servicio.
3. Identificar las relaciones que existen entre las tecnologías identificadas. Es importante no sólo identificar las relaciones, sino también la naturaleza de las mismas. Las tecnologías pueden influenciar o ser influenciadas por otras, estar formadas o formar parte de alguna otra, y complementar la definición de otras.
4. Identificar los roles que tiene cada tecnología.
    - Componentes. Son utilizados como componentes en una tecnología más compleja. Cuando una tecnología funciona como componente, la tecnología más compleja depende de la primera para funcionar.
    - Productos y aplicaciones. Identifican tecnologías que usan componentes para realizar un conjunto de funciones o para satisfacer un grupo de necesidades. Estas tecnologías tienden a competir con otras que tienen el mismo rol.

- Soporte e infraestructura. Este rol identifica las tecnologías que trabajan en conjunto, en colaboración con otras tecnologías. Las tecnologías en este rol le dan un valor agregado a las tecnologías a las que les brindan soporte.

5. Identificar las fuerzas del ambiente externo que pueden impactar en los resultados de la evolución tecnológica. Se identifican principalmente tres tipos: fuerzas sociales y gubernamentales, fuerzas económicas y fuerzas tecnológicas.

En la figura 10 se muestra un diagrama que representa a grandes rasgos cómo se encuentra estructurado un ecosistema tecnológico.

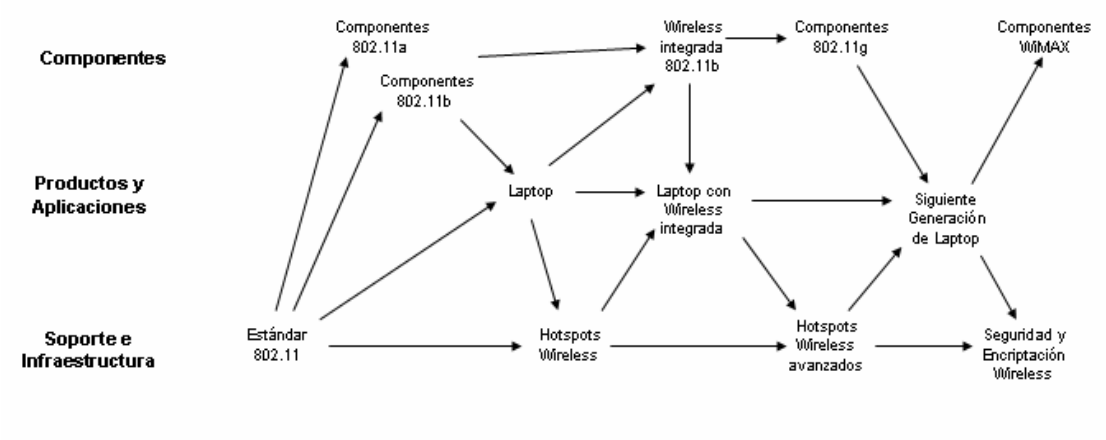
Figura 10. Esquema general del ecosistema tecnológico



Fuente: Jesse Bockstedt. ***Technology roles in an ecosystem model of technology evolution***. Pág. 13.

En la figura 11 aparece un ejemplo de un ecosistema tecnológico para la tecnología Wi-Fi (redes inalámbricas de área local). En el diagrama aparecen identificadas las tecnologías, las relaciones existentes entre ellas y la clasificación a la que pertenecen.

Figura 11. Ecosistema tecnológico de Wi-Fi



Fuente: Jesse Bockstedt. ***Technology roles in an ecosystem model of technology evolution***. Pág. 17.

B.4 Ecosistema tecnológico para WiMAX

Siguiendo el proceso definido en el punto anterior, se desarrolla el modelo del ecosistema tecnológico para la tecnología WiMAX.

B.4.1 Establecer el propósito del modelo

El propósito de realizar este modelo es pronosticar el futuro de la tecnología WiMAX. La tendencia que ha seguido Wi-Fi, según lo que se vio en el ecosistema tecnológico desarrollado para este estándar, demuestra de muy buena manera la forma en que ha evolucionado, hasta llegar a ser el punto de conexión con WiMAX.

De la misma manera, se busca determinar la forma en que WiMAX evolucionará, y cuáles pueden ser las futuras tecnologías a las que puede ayudar o servir de base para su implementación.

B.4.2 Encontrar tecnologías participantes

Como se vio en la descripción del ecosistema, es necesario identificar a las tecnologías, tanto la de estudio, como las que se relacionan con ella.

B.4.2.1 Definir la tecnología de enfoque

En base al propósito del modelo podemos determinar que la tecnología de enfoque es WiMAX. Esta tecnología define el contexto del modelo y es el punto de partida para determinar el resto de factores dentro y fuera del ecosistema.

B.4.2.2 Definir las tecnologías competentes

En este paso se identifican cuáles son las tecnologías relacionadas con WiMAX. Estas tecnologías son las que influencian su evolución, las que la conforman como elementos y las que pueden verse afectadas en algún momento.

B.4.3 Identificar las relaciones

Los tipos de relaciones que pueden existir entre dos tecnologías son:

- Asociación. Indica que las tecnologías se encuentran asociadas de una manera complementaria.
- Dependencia. Indica que de las tecnologías relacionadas, una depende de la otra.
- Influencia. Indica que una tecnología influye sobre la otra. La influencia puede ser negativa o positiva para el crecimiento, o evolución de una de ellas.
- Estructural. Indica que la estructura de una tecnología se encuentra formada por otras tecnologías.

B.4.4 Clasificar las tecnologías por sus roles

En este punto ya hemos identificado a todas las tecnologías participantes en el ecosistema y las relaciones entre ellas. Ahora es necesario categorizar cada tecnología en los distintos roles. La tabla IV muestra el resultado final de la categorización de las tecnologías.

Tabla IV. Tecnologías identificadas para el ecosistema tecnológico

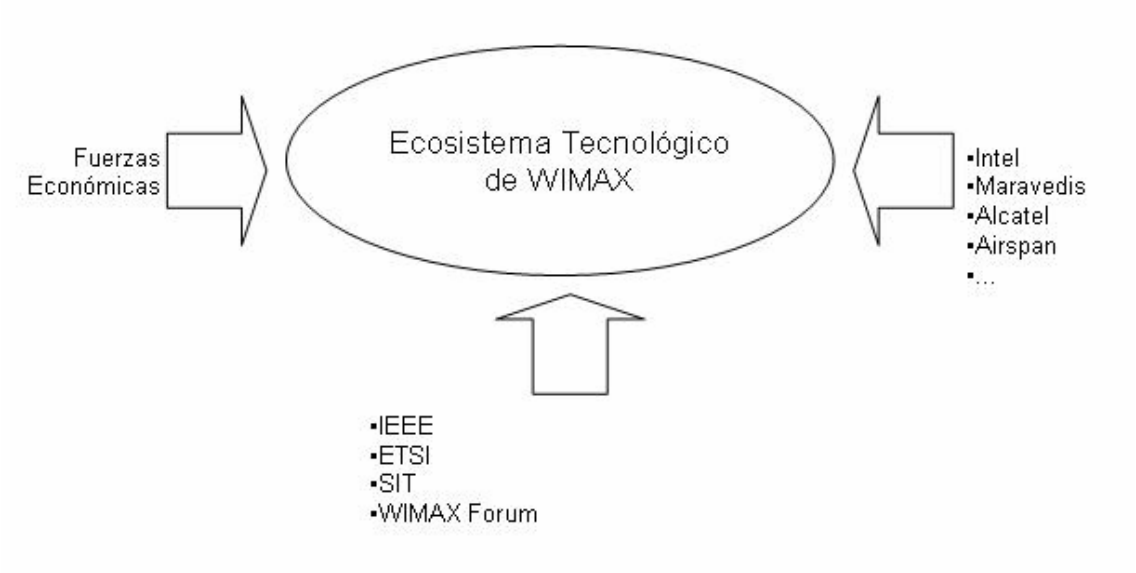
Tecnología de enfoque	WiMAX
Tecnologías competentes	HyperMAN
	DSL
	Fibra óptica
	T1
Componentes	RF (*Radio Frecuency*)
	IR (*Infra Red*)

	CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*)
	TDD (*Time División Duplex*)
	FDD (*Frecuency División Duplex*)
	TDMA (*Time División Multiple Access*)
	FDM (*Frecuency Division Multiplex*)
	TDM (*Time Division Multiplex*)
Productos y aplicaciones	Wi-fi (*Wireless Fidelity*)
	HyperLAN
	AP (*Access Point*)
	CPE (*Customer Premise Equipment*)
	BS (*Base Station*)
	SS (*Subscriber Station*)
	DSSS (*Direct Sequence Spread Spectrum*)
	FHSS (*Frecuency Hopping Spread Spectrum*)
	802.11j
	802.11i
Soporte e infraestructura	802.16e
	802.20
	802.21
	BWA (*Broadband Wireless Access*)

B.4.5 Identificar las fuerzas externas

Las fuerzas externas son factores que se encuentran fuera del entorno del ecosistema tecnológico. Estas fuerzas pueden ser específicas para cada región o país. En la figura 12 se muestra el esquema general del ecosistema tecnológico de WiMAX, junto con algunas fuerzas externas genéricas.

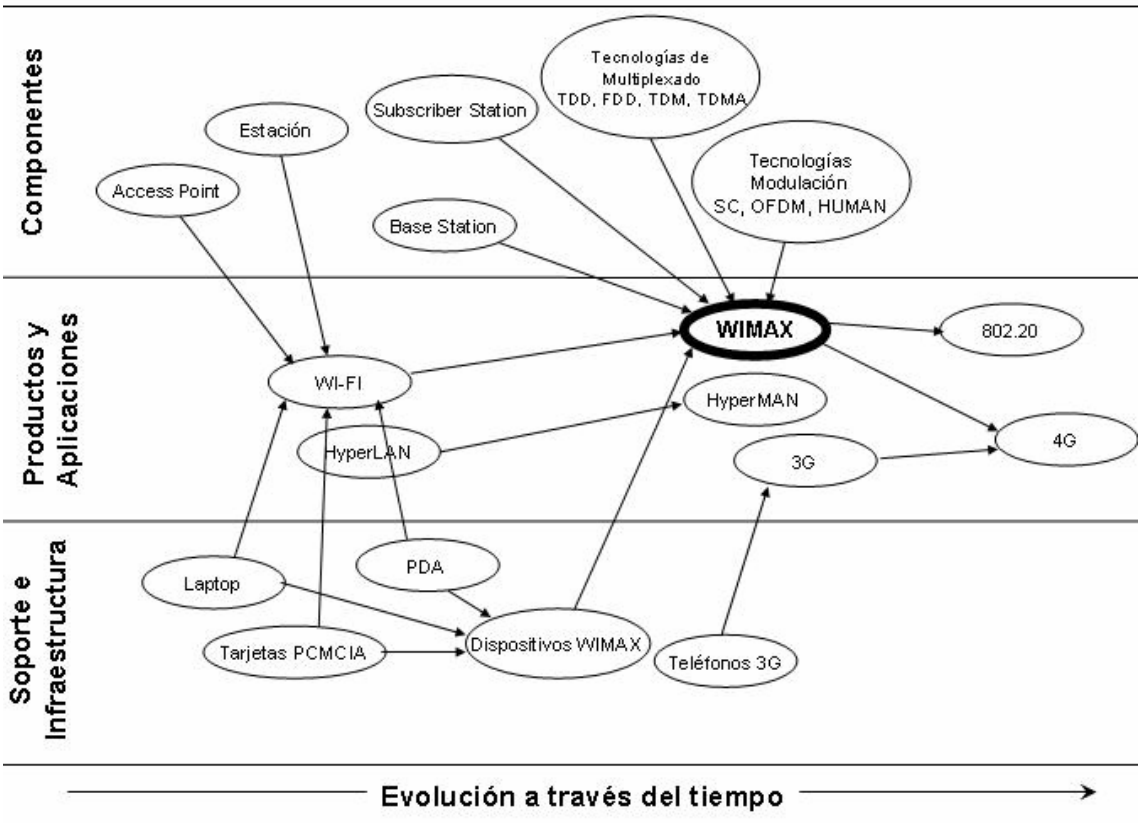
Figura 12. Esquema general del ecosistema tecnológico de WiMAX



Fuente: José Alberto Córdova Paz. 13/09/2005.

Finalmente, tomando todos los elementos identificados en los pasos anteriores, llegamos al modelo final en el que se muestran de manera gráfica cómo se relacionan las diferentes tecnologías. Otro factor importante del modelo es que muestra la evolución a través del tiempo, y cuáles pueden ser las futuras tendencias de la tecnología. El modelo final aparece en la figura 13.

Figura 13. Ecosistema tecnológico de WiMAX



Fuente: José Alberto Córdova Paz. 13/09/2005.

El modelo final obtenido nos muestra a WiMAX como tecnología de enfoque. Se puede apreciar la evolución a través del tiempo, que se ha dado desde el estándar Wi-Fi hasta WiMAX, y cómo este estándar puede ser el precursor de tecnologías como 4G y el estándar 802.20 para dispositivos móviles. También pueden apreciarse tecnologías que compiten con el estándar 802.16, como lo es HyperMAN que evolucionó del estándar HyperLAN. También podemos observar las tecnologías de modulación y multiplexación de la señal que forman parte de WiMAX, así como las estaciones base y las estaciones suscriptoras. Finalmente, podemos observar los dispositivos inalámbricos que pueden ser utilizados con WiMAX, brindándole al estándar un valor agregado.