SISTEMAS INALAMBRICOS IEEE 802

LUIS MANUEL CASTELLAR ANILLO

JEISSER DAVID PONTON MORALES

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIAS

PROGRAMA DE INGENIERIA DE SISTEMAS

MINOR COMUNICACIÓN Y REDES

CARTAGENA (BOLIVAR)

2008

SISTEMAS INALAMBRICOS IEEE 802

LUIS MANUEL CASTELLAR ANILLO

JEISSER DAVID PONTON MORALES

Monografía para obtener el título de Ingeniero de Sistemas

Director:
Ing. GIOVANNY VÁSQUEZ

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIAS

PROGRAMA DE INGENIERIA DE SISTEMAS

MINOR COMUNICACIÓN Y REDES

CARTAGENA (BOLIVAR)

2008

Nota de aceptación

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Cartagena, Enero de 2008

Cartagena de Indias, D. T y C, 23 de Enero de 2008.

Señores:
Comité Curricular
Universidad Tecnológica de Bolívar.
Ciudad.

De la manera más atenta, no permitimos presentar a su consideración y aprobación, el trabajo de grado titulado: **"SISTEMAS INALAMBRICOS IEEE 802"** elaborado por **LUIS MANUEL CASTELLAR ANILLO y JEISSER DAVID PONTON MORALES.**

Esperamos que el presente trabajo se ajuste a las expectativas y criterios evaluativos de la Universidad para los trabajos de grado.

Agradeciendo de antemano su colaboración.

Cordialmente,

LUIS M. CASTELLAR ANILLO	**JEISSER D. PONTON MORALES.**
CC: 1.047.373.122 DE CARTAGENA.	**CC: 1.128.045.207 DE CARTAGENA**

Cartagena de Indias, D. T y C, 23 de Enero de 2008.

Señores:
Comité Curricular
Universidad Tecnológica de Bolívar.
Ciudad.

A través de la presente me permito entregarle la monografía titulada: **"SISTEMAS INALAMBRICOS IEEE 802",** para su estudio y evaluación la cual fue elaborada por los estudiantes **LUIS MANUEL CASTELLAR ANILLO y JEISSER DAVID PONTON MORALES** de los cuales acepto ser su director.

Atentamente,

_____

Ing. Giovanny Vásquez

AUTORIZACIÓN

Cartagena, D. T. y C., Enero de 2008.

Yo, **Luís Manuel Castellar Anillo,** identificado con el número de cedula 1.047’373.122 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de monografía y publicarlo en el Catalogo Online de la biblioteca.

_____

Luís Manuel Castellar Anillo.

AUTORIZACIÓN

Cartagena, D. T. y C., Enero de 2008.

Yo, **Jeisser David Pontón Morales,** identificado con el número de cedula 1.128’045.207 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de monografía y publicarlo en el Catalogo Online de la biblioteca.

_____

Jeisser David Pontón Morales.

INTRODUCCIÓN

Al contrario que las redes cableadas o fijas, que requieren una conexión física a un punto terminal de red, los dispositivos de usuario asociados con redes inalámbricas, teléfonos móviles, PDAs, computadores portátiles, etc. se comunican con la red mediante transmisiones de radio. En algunos casos, las redes inalámbricas se utilizan para sustituir a las redes cableadas (de área local) preexistentes. En la mayor parte de las ocasiones, sin embargo, se emplean para facilitar la movilidad a los abonados de la red.
Existen tipos diferentes de redes inalámbricas, cada uno enfocado a un tipo particular de aplicación. Pueden ser clasificadas según el área de cobertura de radio involucrada:

PICONETS AD-HOC

También conocidas como redes inalámbricas personales, WPAN (Wireless Personal Area Network) un dispositivo actúa como master y puede haber hasta siete dispositivos slaves. Todos los esclavos deben estar situados en un radio de 10 metros del maestro. Por tanto, una piconet cubre un área pequeña, tal como una sala u oficina. Se utilizan por ejemplo, para establecer conferencias ad-hoc espontáneas entre, por ejemplo, varios computadores portátiles en una sala de conferencias. También se utilizan para interconectar varios dispositivos como un computador personal, una impresora, un escáner, una cámara digital, etc., que se encuentran distribuidas por la oficina o por la casa.

Utilizan transmisiones de radio de corto alcance entre los distintos dispositivos para comunicarse y transferir los datos. Un ejemplo de este estándar de red es BLUETOOTH [1]. Normalmente el computador posee una unidad de sistema y cada uno de los periféricos, una unidad esclava.

Ambas unidades, la de sistema y la esclava, poseen un transmisor de radio – emisor y receptor – y todas las transmisiones / transferencias de datos están controladas por la unidad de sistema. Normalmente, la velocidad de transferencia máxima está entre 400 y 700 kbps, dependiendo de si la transferencia es simétrica o asimétrica.

---

1 Tecnología de comunicación inalámbrica, que será explicada en profundidad durante el desarrollo de esta monografía, en el capítulo 1, BLUETOOTH.

REDES DE ÁREA LOCAL INALÁMBRICAS

Las redes de área local inalámbricas (WLANS) se usan ahora de manera amplia para permitir que un conjunto de computadores, tanto portátiles, como de sobremesa, se comuniquen con, por ejemplo, un servidor común o un punto fijo de acceso a la red tal como un bridge [2]. Todos los dispositivos en la WLAN están provistos de un modém vía radio con un alcance máximo típico de 100 metros. Así el rango de alcance de una única WLAN es el de una oficina grande o un laboratorio. Entonces para lograr un alcance más amplio, como por ejemplo, un campus universitario se pueden interconectar varias WLANS, utilizando, por ejemplo tecnología de Lan cableada de alta velocidad.

El uso de radio en lugar de cables fijos proporciona mayor flexibilidad cuando se cambia la situación de las mesas de trabajo, etc. Las WLANS se hacen también habituales en edificios antiguos donde la instalación de cables puede ser difícil.

Con cada WLAN existe una unidad llamada punto de acceso AP (Access point), y todas las comunicaciones tienen lugar entre los diferentes nodos inalámbricos, llamados estaciones y el AP. Así pues el AP controla todas las transmisiones de radio dentro de su red y además las comunicaciones con los AP de otras redes mediante la red troncal. Existen varios tipos de WLANS, los cuales han sido estandarizados bajo la norma IEEE 802.11. Las velocidades de transferencia típicas van de los 11 Mbps para el IEEE 802.11b hasta los 54 Mbps para el IEEE802.11a.

REDES DE RADIO CELULAR

Al contrario de las 2 descritas anteriormente, las redes de radio celular tienen una cobertura típica de todo un país, o un área más amplia siempre que los países vecinos hayan adoptado una red de radio compatible. Se diseñaron desde el principio con el fin de que una persona que disponga de un terminal compatible pueda hacer una llamada, incluyendo voz, mensajes de texto, fotos/imágenes y video, cuando este fuera de la casa u oficina. Los terminales se llaman teléfonos móviles y por este motivo, las redes de radio celular se conocen también como redes de telefonía móvil.

Las primeras redes de radio de área amplia utilizaban un único transmisor de alta potencia para cubrir un área tal como una población o una ciudad y esto daba soporte a un rudimentario servicio telefónico. Los estrictos límites en la potencia de las transmisiones de radio, sin embargo, significaban que este modo de operación no podía utilizarse para cubrir un área más grande que la

---

2 Dispositivo de interconexión de redes de ordenadores que opera en la capa 2 del modelo OSI.

de una única población. Como resultado, no fue hasta que se introdujo en Estados Unidos la primera red de radio celular a principios de los años ochenta, cuando se produjo el despegue de las redes de telefónica móvil.

En las redes celulares, el área de cobertura total deseada para toda la red se divide en un gran número de pequeñas zonas llamadas celdas. Asociado con cada celda hay un transmisor de radio de baja potencia que es suficiente solo para cubrir esa celda. El ancho de banda total que ha sido asignado a la red se divide primero en una serie de subbandas de frecuencias. En esta tecnología cada celda está rodeada por otras celdas que utilizan una subbanda diferente. Además, el empleo de celdas pequeñas implica que los equipos solo utilizan transmisiones de radio de baja potencia lo que a su vez, significa que solo se requieren baterías pequeñas y por tanto equipos más pequeños.

Asimismo se puede utilizar repetidamente el mismo conjunto de subbandas de frecuencia hasta que se alcanza la cobertura total del área requerida. Esta técnica se conoce como reuso de frecuencia y puesto que el ancho de banda de radio es un recurso muy caro, es lo que hace viables estas redes desde el punto de vista económico.

A continuación los 3 esquemas básicos de los distintos tipos de redes wireless.

Fig. 1

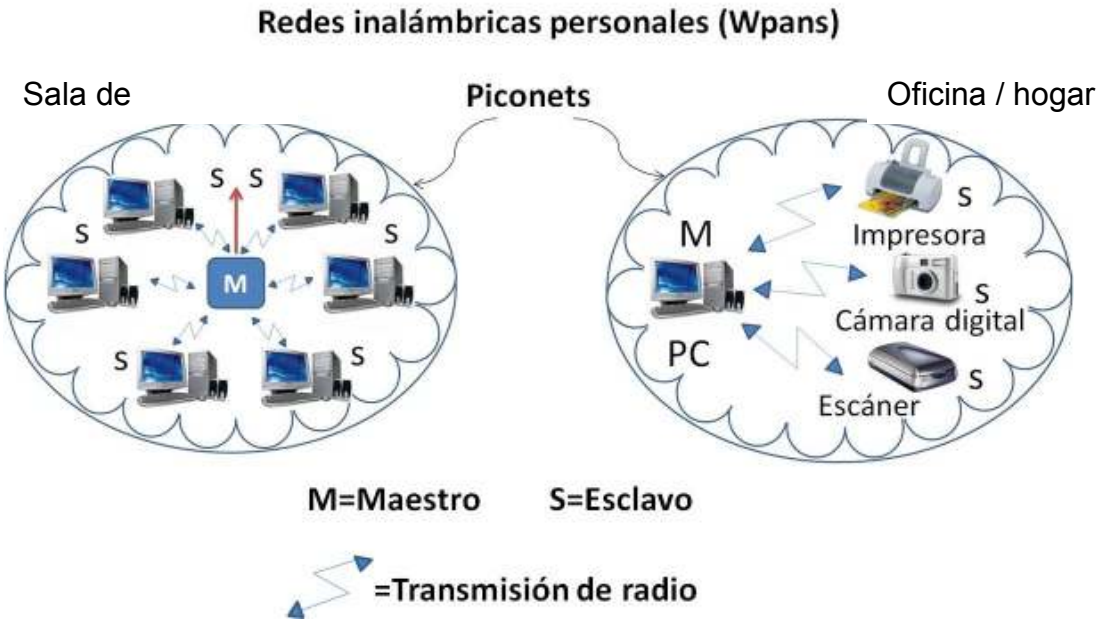
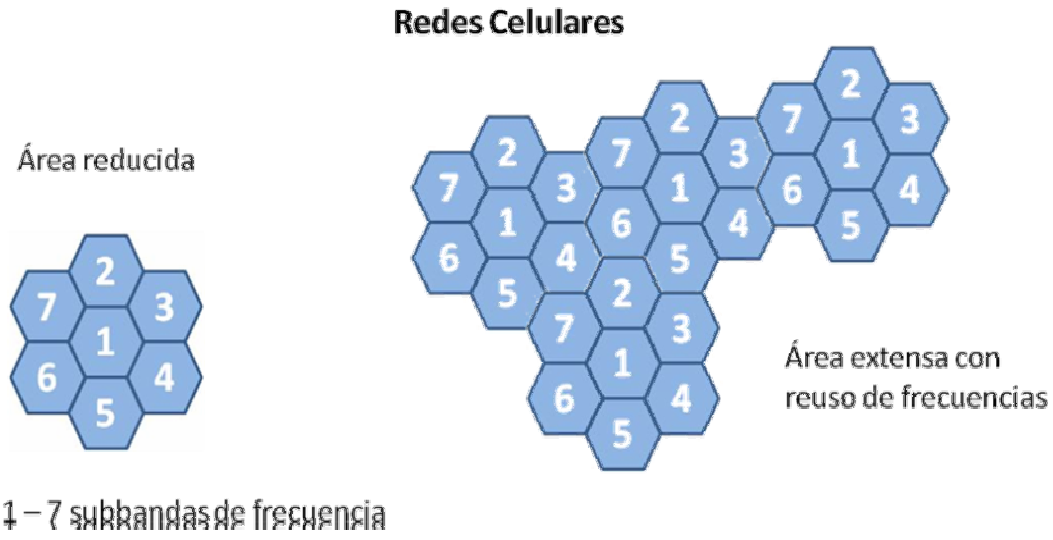


Fig. 1 extraida de STALLINGS, William. COMUNICACIONES Y REDES. Sexta Edición. Prentice Hall.

Fig. 2

Fig. 3



Actualmente, en este tipo de redes, se implanta el QoS o Quality of Services, que no es más que la prioridad de transmisión a determinados paquetes de datos dependiendo de la naturaleza de la información, voz, imagen, vídeo... la voz, por ejemplo, necesita transferencia en tiempo real, mientras que los datos contenidos en un archivo no.

Con el advenimiento de esta tecnología, todas sus ventajas y aplicaciones, también se vienen una serie de factores que ponen a prueba la vulnerabilidad

---

Fig. 2 y Fig. 3 Extraidas de STALLINGS, William. COMUNICACIONES Y REDES. Sexta Edición. Prentice Hall.

de las redes wireless. ¿Quién, de manera accidental, desde un portátil con receptor WI- FI o un PDA, no se ha topado con más de una conexión inalámbrica por el camino cuando ha realizado algún viaje? He aquí una serie de mecanismos inicialmente implementado en redes WLANS, que ayudan a proteger las redes y a evitar ciertos posibles ataques. Cabe destacar que cada uno de estos mecanismos será tratado con mayor profundidad en el capítulo de seguridad, en el desarrollo de esta monografía:

SISTEMA DE CIFRADO WEP, acrónimo de Wired Equivalent Privacy.

Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4 [3], y utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV).

Algunos Tips de seguridad:

- Todos los usuarios deben loguearse con nombre y contraseña en sus respectivos equipos al iniciar sesión.

- Todos los usuarios deben estar dados de alta en el resto de equipos con el mismo nombre y contraseña con el que inician sesión en sus respectivos equipos.

- El grupo de trabajo debe llamarse igual en los equipos de la red.

- La dirección IP tienen que pertenecer al mismo rango, excepto en redes complejas, lo mejor es tener activado el DHCP que asignará de manera automática dichas direcciones.

- La máscara debe ser la misma

- En caso d utilizar Windows XP, se debe desmarcar la opción (versión Pro de XP) de "uso compartido simple de archivos"
  (Panel de control, Opciones de carpeta, pestaña Ver, y desmarcar la casilla correspondiente "Utilizar uso compartido simple de archivos (recomendado)")

- WPA (WI- FI Protected Access), estándar desarrollado por la WI- FI alliance (WECA), que trata de ser el sustituto de WEP y es posible incorporarlo en algunos routers que no lo incorporan con una simple actualización de firmware. No obstante se pueden tomar las siguientes medidas para tratar de garantizar nuestra seguridad:

---

3 RC4, algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla (seed en inglés) para generar una secuencia de números pseudoaleatorios de mayor tamaño, con el fin de cifrarlos.

1. Deshabilitar SSID

2. Habilitar la WEP

3. Habilitar el cifrado MAC

4. Usar capas superiores tipo https

5. Usar autentificaron EAP

6. Revisar nuestra red para comprobar que no existen acceso no autorizados.

VENTAJAS DE LA UTILIZACIÓN DE REDES INALÁMBRICAS

- Movilidad. La libertad de movimientos es uno de los beneficios más evidentes las redes inalámbricas. Un ordenador o cualquier otro dispositivo (por ejemplo, una PDA o una webcam) pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de que si es posible o no hacer llegar un cable hasta este sitio. Ya no es necesario estar atado a un cable para navegar en Internet, imprimir un documento o acceder a los recursos compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.

- Desplazamiento. Con una computadora portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación. Esto no solo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio.

- Flexibilidad. Las redes inalámbricas no solo nos permiten estar conectados mientras nos desplazamos por una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red. A veces extender una red cableada no es una tarea fácil ni barata. En muchas ocasiones acabamos colocando peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conecten en la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En sitios donde pueda haber invitados que necesiten

conexión a Internet (centros de formación, hoteles, cafés, entornos de negocio o empresariales) las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

- Ahorro de costes. Diseñar o instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costes al permitir compartir recursos: acceso a Internet, impresoras, etc.

- Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o lo que es peor, esperar hasta que el nuevo cableado quede instalado.

Como bien, sabemos la tecnología en lo que respecta a las redes está cambiando y cada vez se hace mejor, ya que como hemos visto las redes de estos días son mejores, más rápidas, con mayor seguridad y lo que es de las inalámbricas; ya no hay cables. Las redes inalámbricas cada vez son mejores en todo, y además nos dan más comodidad por un aspecto importante que ya no se usan cables para conectar computadoras a una red o conectarse a Internet. En algunos casos las redes inalámbricas tienen más ventajas que las cableadas, una de ella es que cuando se visita alguna empresa que tenga red inalámbrica, las personas que tengan una laptop y tengan que utilizar el Internet ya se van a poder conectar sin necesidad del modem. Eso sí, siempre y cuando se haya configurado de esa manera para poder entrar a Internet. Se podría afirmar que en el futuro, las redes inalámbricas jugarán un papel muy importante en este mundo tecnológico, donde el objetivo principal es lograr la movilidad y expansión de servicios de internet y de comunicación en casi cualquier lugar, logrando disponibilidad y velocidad suficiente para que estemos siempre en comunicación.

Actualmente, las redes inalámbricas, están siendo muy bien acogidas por las empresas y usuarios como medio de comunicación masivo, además, las ISP también las implementan, porque estas representan menor coste de implementación y la calidad que estas puedan ofrecer es relativamente buena. El desarrollo de esta monografía se basa especialmente en 4 temáticas, donde 3 tratarán sobre las tecnologías inalámbricas actuales y de mayor utilización; las cuales son: BLUETOOTH, WI- FI y WIMAX. Se han seleccionado estas 3 tecnologías específicas, dado su funcionalidad en el mundo actual. Como son las más difundidas, es interesante estudiar factores como la funcionalidad, cobertura, costos y fallas, con el fin de estar mejor informados sobre estas tecnologías e incluso tomar una buena decisión a la hora de adquirir algún servicio sostenido sobre alguna de ellas. El ultimo a tratar será la seguridad en

las redes inalámbricas, específicamente se van a tratar los esquemas y funciones de seguridad que se implementan en las 3 tecnologías antes mencionadas.

CAPITULO 1

1.1 BLUETOOTH

La tecnología inalámbrica BLUETOOTH es un sistema de comunicaciones (Especificación industria IEEE 802.15.1), que define un estándar global de comunicación inalámbrica y de corto alcance que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura, globalmente y sin licencia. Su objetivo es eliminar los cables en las conexiones entre dispositivos electrónicos, tanto portátiles como fijos. Las características principales de esta tecnología son su fiabilidad, bajo consumo y mínimo coste. Varias de las funciones de la especificación principal son opcionales, lo que permite la diferenciación de los productos.

El núcleo del sistema BLUETOOTH consiste en un transmisor de radio, una banda base y una pila de protocolos. El sistema permite la conexión entre dispositivos y el intercambio de distintos tipos de datos entre ellos.

1.1.1VERSIONES

- BLUETOOTH v.1.1
- BLUETOOTH v.1.2
- BLUETOOTH v.2.0
- BLUETOOTH v.2.1

La versión 1.2, a diferencia de la 1.1, provee una solución inalámbrica complementaria para co-existir BLUETOOTH y WI- FI en el espectro de los 2.4 GHZ, sin interferencia entre ellos.

La versión 1.2 usa la técnica "Adaptive Frequency Hopping (AFH)", que ejecuta una transmisión más eficiente y un cifrado más seguro. Para mejorar las experiencias de los usuarios, la V1.2 ofrece una calidad de voz (Voice Quality - Enhanced Voice Processing) con menor ruido ambiental, y provee una más rápida configuración de la comunicación con los otros dispositivos BLUETOOTH dentro del rango del alcance, como pueden ser PDAs, HIDs (Human Interface Devices), computadoras portátiles, computadoras de escritorio, Headsets, impresoras y celulares.

La versión 2.0, creada para ser una especificación separada, principalmente incorpora la técnica "Enhanced Data Rate" (EDR) que le permite mejorar las velocidades de transmisión en hasta 3Mbps a la vez que intenta solucionar algunos errores de la especificación 1.2.

La versión 2.1, simplifica los pasos para crear la conexión entre dispositivos, además el consumo de potencia es 5 veces menor.
Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.

La tecnología BLUETOOTH comprende hardware, software y requerimientos de interoperabilidad, por lo que para su desarrollo ha sido necesaria la participación de los principales fabricantes de los sectores de las telecomunicaciones y la informática, conocidos como SIG (Special Interest Group), tales como: Sony Ericsson, Nokia, Motorola, Toshiba, IBM e Intel, entre otros. Posteriormente se han ido incorporando muchas más compañías, y se prevé que próximamente lo hagan también empresas de sectores tan variados como automatización industrial, maquinaria, ocio y entretenimiento, fabricantes de juguetes, electrodomésticos, etc., con lo que en poco tiempo se nos presentará un panorama de total conectividad de nuestros aparatos tanto en casa como en el trabajo.

Los dispositivos que con mayor intensidad utilizan esta tecnología son los de los sectores de las telecomunicaciones y la informática personal, como PDAs, teléfonos celulares, computadoras portátiles, PCs, impresoras y cámaras digitales. De la misma manera, BLUETOOTH intenta unir diferentes tecnologías como las de las computadoras, los teléfonos móviles y el resto de periféricos. El símbolo de BLUETOOTH es la unión de las runas nórdicas H y B.

En 1994, Ericsson inició un estudio para investigar la viabilidad de una nueva interfaz de bajo costo y consumo para la interconexión vía radio (eliminando así cables) entre dispositivos como teléfonos móviles y otros accesorios. El estudio partía de un largo proyecto que investigaba unos multicomunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance, llamado MC link. Conforme este proyecto avanzaba, se fue haciendo claro que éste tipo de enlace podía ser utilizado ampliamente en un gran número de aplicaciones, ya que tenía como principal virtud que se basaba en un chip de radio.

1.1.2 ¿CÓMO FUNCIONA?

La capa física de radio (RF) opera en la banda de 2.4 GHZ libre para ISM (banda de frecuencia industrial, científica y médica). Esta banda permite operar en todo el mundo. El sistema emplea un transmisor de salto de frecuencia para restar las interferencias y la pérdida de intensidad, y cuenta con gran número de portadoras de espectro ensanchado por salto de frecuencia (FHSS, esquema de transmisión conocido como espectro expandido por salto de frecuencias, Frecuency-hopping spread spectrum). Para minimizar la complejidad del transmisor, se utiliza una modulación de frecuencia binaria. La velocidad de símbolo es de 1 MS/s (mega símbolo por segundo), que admite una velocidad de transmisión de 1 Mbps en el modo de velocidad básica y una velocidad de transmisión aérea total de 2 a 3 Mbps en el modo de transferencia de datos mejorada (EDR).

Esencialmente BLUETOOTH utiliza 79 frecuencias de portadora distintas dentro de la banda ISM, cada una de las cuales estas separada a intervalos de 1 MHZ y ordenadas pseudo aleatoriamente con una frecuencia de 1600 saltos por segundo. Así pues, requiere un ancho de banda total de 80 MHZ. Cada portadora se utiliza para transmitir un único bit del flujo de bits usando para ello la modulación habitual por desplazamiento de frecuencia FSK (Frecuency Shift Keying). La técnica de salto adaptable mejora la coexistencia de la tecnología BLUETOOTH con los sistemas ISM estáticos (es decir, sin salto) cuando éstos se encuentran localizados.

Normalmente, varios dispositivos sincronizados por un reloj y una secuencia de salto de frecuencia comparten el mismo canal físico de radio. Uno de ellos proporciona los valores de referencia, el denominado dispositivo maestro. Los demás reciben el nombre de esclavos. Este tipo de conexión entre dispositivos es lo que se conoce como una piconet, la forma de comunicación básica en la tecnología inalámbrica BLUETOOTH.

El reloj del dispositivo maestro es el que proporciona la base de temporización en la piconet. Cada dispositivo BLUETOOTH posee una dirección única de 48 bits que se asigna a cada interfaz de radio durante el proceso de fabricación. La secuencia pseudo aleatoria usada para las transmisiones se determina, entonces a partir de la dirección del maestro. Antes que un esclavo pueda comunicarse con el maestro debe sincronizar con la secuencia de saltos de este. Para esto, el maestro envía su reloj y su dirección de dispositivo a cada esclavo alternativamente, y después de ajustar su reloj interno para sincronizarlo con el del maestro y usando su dirección de dispositivo para determinar la secuencia pseudo aleatoria que utiliza el maestro, cada esclavo se convierte en un miembro activo de la piconet. De esta forma, cada piconet tiene una única secuencia de saltos y todos los esclavos activos en la piconet saltan a la misma frecuencia de portadora del maestro en sincronía.

Existen tres clases de transceptores de radio BLUETOOTH:

- Clase 1: Tiene la máxima potencia de transmisión de 100 mw y un alcance típico de hasta 100 m (sin obstáculos)
- Clase 2: Tiene una potencia máxima de 2.5 mw y un alcance típico de 10 m
- Clase 3: Tiene una potencia máxima de 1 mw y un alcance típico de 1 o 2 m.

TABLA 1: COBERTURA DE RADIO BLUETOOTH

	Potencia máxima permitida (mW)	Potencia máxima permitida (dBm)	Rango (aproximado)
Clase 1	100 mW	20 dBm	~100 metros
Clase 2	2.5 mW	4 dBm	~20 metros
Clase 3	1 mW	0 dBm	~1 metro

1.1.3 CONFIGURACIÓN

El dispositivo que establece la piconet se convierte automáticamente en maestro y los demás serán esclavos. Puede haber hasta un máximo de siete esclavos activos simultáneamente en una única piconet. Por otra parte, un dispositivo puede ser un esclavo en espera SS (StandBy Slave) o un esclavo estacionado PS (Parked Slave). Los dispositivos que se encuentran en espera no pueden participar en la piconet. Un esclavo estacionado en cambio, no puede participar de forma activa en la piconet, pero es conocido por el maestro y puede ser reactivado por este. Generalmente estos son dispositivos que han sido puestos en modo de ahorro de energía por el maestro con el fin de ahorrar energía de las baterías del dispositivo. Todos los esclavos estacionados tienen una dirección de miembro estacionado (PMA, Parked Member Address) de 8 bits, por lo que puede haber 255 de tales dispositivos. Si ya hay siete esclavos activos, entonces un esclavo estacionado debe esperar hasta que uno de aquellos sea llevado al estado estacionado antes de poder convertirse el mismo en activo. Todos los esclavos tienen una dirección de miembro activo (AMA, Active Member Address) de 3 bits, que se utiliza por el maestro tanto para enviar bloques de datos, llamados paquetes en el estándar a un esclavo especifico como para identificar al esclavo que ha enviado un paquete de respuesta. Todas las comunicaciones se realizan a través del maestro, y las comunicaciones esclavo a esclavo están prohibidas

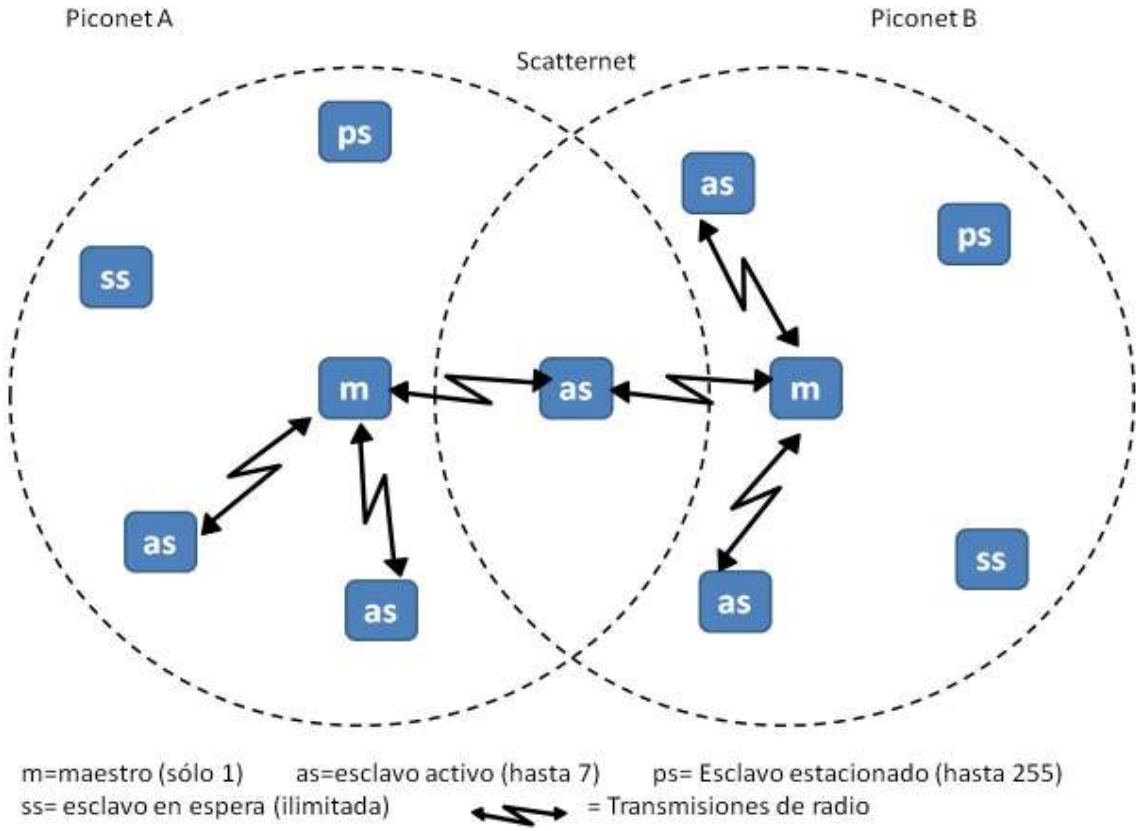
1.2. SCATTERNET

Es la unión de varias piconet en la misma sala u oficina simultáneamente, con el fin de proporcionar una mayor área de cobertura. Aquí uno de los esclavos activos está situado en la región de solapamiento de ambas piconets. sin embargo, puesto que cada piconet posee una secuencia de saltos pseudoaleatoria diferente, ambas piconets pueden funcionar simultáneamente. Así el esclavo puede ser miembro de cualquiera de las piconets, pero no de ambas al mismo tiempo. Esto se logra cuando el esclavo primeramente informa a su maestro actual de que estará inaccesible durante un determinado tiempo. A continuación procede a sincronizar con el maestro de la otra piconet de la forma descrita. Esto en la práctica conlleva a la degradación del rendimiento de cada piconet. Esto es debido a que se incrementa la probabilidad de que se use la misma frecuencia portadora simultáneamente resultando en la

corrupción del bit correspondiente dentro del flujo de bits. A continuación, un esquema básico de SCATTERNET.

SCATTERNET

Fig. 4



1.3 TRANSMISIONES DE PAQUETES EN BANDA BASE

El canal físico se subdivide en unidades de tiempo denominadas ranuras (tiempo entre saltos, 625 µs, en BLUETOOTH). Los datos intercambiados entre los dispositivos BLUETOOTH se transmiten en forma de paquetes que se emplazan en estas ranuras. Cuando la situación lo permite, se pueden asignar varias ranuras consecutivas a un único paquete. El salto de frecuencia se produce durante la transmisión o recepción de los paquetes. La tecnología BLUETOOTH consigue la transmisión bidireccional mediante la técnica de acceso múltiple o dúplex por división de tiempo (TDD), permitiendo asi ordenar las transmisiones. El procedimiento TDD seria:

El maestro envía siempre en el primer conjunto de uno, tres o cinco ranuras de tiempo de la cabecera del paquete conteniendo la dirección de miembro activo AMA, del esclavo, y el esclavo al que iba dirigido contesta entonces en el siguiente conjunto de uno, tres o cinco ranuras.

BLUETOOTH proporciona 2 tipos de servicios, llamados enlaces en el estándar. Un enlace síncrono orientado a conexión (SCO Synchronous Connection-Oriented Link) y un enlace asíncrono sin conexión (ACL Synchronous Connectionless Link). El enlace SCO está ideado para aplicaciones de voz/audio y el ACL para aplicaciones de datos en general. El enlace SCO proporciona conexión dúplex a 64kbps cuando el maestro reserva un par de ranuras consecutivas a intervalos fijos de tiempo. El estándar permite que haya tres llamadas en curso concurrentemente. Los datos asociados con aplicaciones ACL se transmiten entonces en las ranuras libres restantes. Solo puede haber en cada momento un enlace ACL entre el maestro y un escalvo y las tasas máximas de de datos son 433.9 kbps (simetrico) y 723.3 / 57.6 kbps asimétrico.

1.3.1 FORMATOS DE PAQUETES EN BANDA BASE

El formato de cada paquete, es:

- Código de acceso al canal (CAC, Channel Access Code): Se deduce a partir de la dirección de 48 bits del maestro y se utiliza para identificar la piconet.

- código de acceso de dispositivo (DAC, Device Address Code): Se deduce de la dirección del dispositivo esclavo y se utiliza por el maestro para direccionar al dispositivo.

- Código de acceso de búsqueda (IAC, Inquiry Access Code): Se utiliza para averiguar la dirección de un dispositivo vecino.

- La cabecera del paquete, está compuesta por los siguientes campos:
  Dirección Am: esta es la dirección de miembro activo (AMA) de 3 bits que identifica a cada uno de los siete esclavos activos; el valor cero se utiliza para indicar un paquete de difusión desde el maestro.

  Tipo: Indica el tipo de paquete y está determinado por la estructura del campo de carga. Por ejemplo, es posible utilizar distintos niveles de corrección de errores en recepción (FEC, Forward Error Correction) tanto para paquetes SCO como ACL, y el campo “tipo” indica la división del campo de carga entre bits de datos y o bien 0, o 1/3 o 2/3 bits de FEC.

  Flujo: Se utiliza en modo ACL para proporcionar un esquema simple del control de flujo, para enviar=1 y continuar=0

  SEQN: Es el numero de secuencia del paquete basándose en un esquema simple modulo-2 (0,1,0,1,…) y se utiliza en trafico ACL

ARQN: Se utiliza junto con SEQN para un esquema de control de errores de petición de repetición automática (ARQ, Automatic Repeat Request). el bit ARQN indica el tipo de confirmación: 1= ACK (Confirmacion positiva) y o=NAK (no confirmación)

HEC: Es un código de 8 bits de corrección de errores de la cabecera. los primeros 18 bits de la cabecera están protegidos por un código FEC con tasa 1/3 que completa la cabecera de 54 bits del paquete.

El contenido del campo de carga depende y varía según el tipo de servicio/enlace SCO y ACL y el grado de FEC que se está usando. En un enlace SCO, la carga tiene una longitud de 30 bytes y el grado de FEC puede ser 0, 2/3 o 1/3; esto es, el número de datos de usuario puede ser 30, 20 o 10 bytes respectivamente. En un ACL, la carga puede ocupar de 0 a 343 bytes. Esto incluye una cabecera (de datos) de uno o dos bytes, un byte para paquetes de una ranura y dos bytes para paquetes de tres o cinco ranuras, más un CRC de dos bytes al final. La cabecera está compuesta de un identificador (punto de acceso al servicio) para el protocolo de control del enlace lógico, que se situa inmediatamente sobre el protocolo de banda base, un campo de control de flujo y un campo de longitud que indica el numero de bytes de datos en la carga.

- Además de los paquetes SCO y ACL, existen paquetes de control. Estos incluyen:

- Paquetes de sondeo: utilizados por los maestros para interrogar a los esclavos

- Paquetes de sincronización de saltos: los envía el maestro a un esclavo para permitirle sincronizar su reloj al del maestro y su secuencia de saltos.

- Paquetes de confirmación (ACK y NAK), para su uso con el esquema de control de errores idleRQ / ARQ

1.4 PROTOCOLOS

Sobre el canal físico hay una capa de enlaces y canales con sus respectivos protocolos de control. La jerarquía de abajo a arriba de los canales y enlaces es la siguiente: canal físico, enlace físico, comunicación lógica, enlace lógico y canal L2CAP.

En el canal físico, se forma un enlace físico entre dos dispositivos que se intercambian paquetes, sea cual sea la dirección. Pero no todos los dispositivos pueden conectarse mediante un enlace físico dentro de la piconet. Se crea un enlace de este tipo entre un dispositivo esclavo y el maestro, pero dos esclavos no pueden conectarse directamente de esta forma.

El enlace físico se utiliza como medio de comunicación entre uno o dos enlaces lógicos que admiten tráfico síncrono, asíncrono e isócrono de unidifusión, y tráfico de difusión. El tráfico de los enlaces lógicos se multiplexa en el enlace físico ocupando las ranuras asignadas por el programador del gestor de recursos.

A través de los enlaces lógicos, además de los datos del usuario se transporta el protocolo de control de la banda base y las capas físicas: protocolo de gestión de enlace (LMP). Los dispositivos que están activos dentro de la piconet tienen una comunicación lógica asíncrona predeterminada para el transporte de la señalización del protocolo LMP. Es lo que se conoce como comunicación lógica ACL. Esta comunicación es la que se establece cuando un dispositivo se une a una piconet. Se pueden crear comunicaciones lógicas adicionales si resulta necesario para transportar el flujo de datos síncronos.

1.4.1 PROTOCOLO DE GESTIÓN DE ENLACE Y ESTABLECIMIENTO DE UNA PICONET

Este es el responsable del establecimiento de enlaces entre dispositivos asi como de un conjunto de funciones de gestión de dispositivos que incluyen seguridad, autenticación y cifrado, sincronización, control de energía y negociación de parámetros. Generalmente los dispositivos BLUETOOTH dependen de una batería para su alimentación y por tanto solo pueden estar en el estado activo durante un periodo de tiempo. Cada dispositivo que esta encendido pero que no forma parte de ninguna piconet está en estado de espera (standby mode). Este es el estado de mínimo consumo en el que solo está activo el reloj del dispositivo. Mientras permanece en este estado, el dispositivo puede establecer una piconet, primero pasando al modo de búsqueda y luego al modo de llamada, respectivamente.

Para crear una piconet, el usuario de un dispositivo inicia el procedimiento de búsqueda con la difusión de un paquete que contiene un código de acceso de búsqueda (IAC, inquiry acces mode). Esto es común a todos los dispositivos BLUETOOTH y consiste en una difusión consecutiva sobre 32 frecuencias portadoras, llamadas portadoras de despertador. Normalmente, los dispositivos que se encuentran en el modo espera entran periódicamente en el modo de búsqueda a la escucha de un paquete IAC en cualquiera de las portadoras de despertador. Entonces si un dispositivo detecta un paquete IAC, responde enviando un mensaje o paquete que contiene su dirección de dispositivo, clase de dispositivo y la conexión con él. En este momento el dispositivo se convierte en un esclavo y el maestro primero deduce el código de acceso al canal (CAC) y después entra en el modo de llamada.

Mientras esta en el modo de llamada, el maestro, tras establecer contacto con todos los dispositivos esclavos, procede a establecer conexiones con cada dispositivo, creando así una piconet. Inicialmente basándose en la dirección del dispositivo que ha recibido el maestro utiliza cada uno de estos para calcular el código de acceso de dispositivo (DAC) correspondiente a cada esclavo, que necesita para llamar a cada esclavo independientemente. Posteriormente el

maestro calcula la secuencia de saltos pseudo aleatorios para la piconet utilizando su propia dirección de dispositivo e informa de ello a cada esclavo. Cada dispositivo contesta, entonces sincronizando su reloj con el reloj del maestro y fijando la secuencia de saltos que ha recibido. Todos los dispositivos entran, entonces en el modo conectado.

El estado activo se compone de los modos conectado y transmisión mientras que el estado bajo consumo comprende tres modos: estacionado, retenido y escucha. En el estado activo, un esclavo se comunica con el maestro escuchando, recibiendo y transmitiendo sobre enlaces SCO y ACL utilizando la dirección de miembro activo (AMA) de 3 bits que le fue otorgada. Los tres modos de bajo consumo, ordenados por consumo decreciente son:

- Escucha: El dispositivo mantiene el AMA y continua escuchando pero no en todas las ranuras del tiempo. Asimismo, el maestro reserva un número reducido de ranuras para la transmisión de esclavos.

- Retenido: El dispositivo mantiene su AMA pero suspende cualquier transmisión ACL subsiguiente. Sin embargo, un esclavo todavía puede intercambiar paquetes SCO. Se utiliza, por ejemplo, cuando el maestro está estableciendo una conexión con un dispositivo esclavo que se está uniendo a la piconet.

- Estacionado: El dispositivo libera su AMA, permitiendo que otro dispositivo pase a activo y se le reserva una dirección de miembro estacionado PMA. El dispositivo todavía forma parte de la piconet y a intervalos fijos, llamados de señalización, resincroniza con el maestro. Todos los mensajes o paquetes son difundidos a todos los esclavos estacionados.

1.4.2 PROTOCOLO DE ADAPTACIÓN Y CONTROL DEL ENLACE LÓGICO

La capa L2CAP (Protocolo de adaptación y control del enlace lógico, “Logical link control and adaptation protocol”). Está por encima de la de banda base y se encarga de ofrecer una abstracción de canales de comunicación a las aplicaciones y los servicios. Realiza la segmentación y la unificación de los datos de las aplicaciones y la multiplexación y demultiplexación de varios canales a través de un enlace lógico compartido. La capa L2CAP dispone de un canal de control de protocolos a través de la comunicación lógica ACL predeterminada. Los datos de la aplicación enviados al protocolo L2CAP pueden transferirse a través de un enlace lógico compatible con el protocolo L2CAP.

Este protocolo solo soporta enlaces ACL, las aplicaciones de audio y voz que utilizan enlaces SCO operan directamente sobre la banda base, usando tres tipos de canales lógicos:

- Sin conexión: son canales unidireccionales y se utilizan, por ejemplo difusiones entre un maestro y sus esclavos

- Orientados a conexión: son bidireccionales y soportan calidad de servicio QoS, definida para cada sentido. los parámetros QoS incluyen tasas de datos media / pico, tamaño máximo de ráfaga, latencia y jitter.

- Señalización: son también bidireccionales y se utilizan para intercambiar mensajes de señalización entre el maestro y el esclavo por medio del protocolo l2cap.

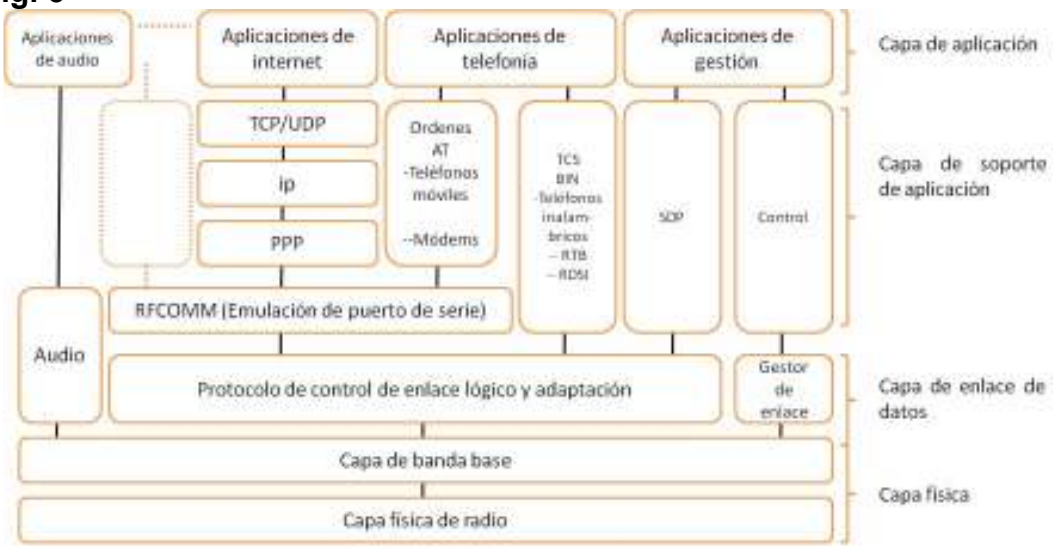
1.4.3 PROTOCOLO DE DESCUBRIMIENTO DE SERVICIOS

Como parte de sus características, los dispositivos BLUETOOTH deberían ser capaces de operar con toros dispositivos de manera ad-hoc. Para ello es necesario que un dispositivo sea capaz de averiguar qué servicios están disponibles en cada uno de los dispositivos que se encuentran dentro de su radio de acción. He aquí la función de SDD (Service Discovery Database) que mantiene el servidor. Contiene un conjunto de registros de servicios, cada uno de los cuales contiene los atributos del servicio. El SDP soporta dos funciones básicas: búsqueda de servicios e inspección. Un dispositivo cliente utiliza la función de búsqueda para localizar un servicio específico. la función de inspección la utiliza el cliente para averiguar qué servicios están soportados.

Así una vez que ha sido identificado un servicio concreto, el cliente puede solicitar sus atributos por medio del descriptor de registros de servicio utilizando los distintos protocolos que componen el perfil de una aplicación en particular.

ESQUEMA A NIVEL DE CAPAS DE LA TECNOLOGÍA BLUETOOTH Y SUS APLICACIONES

Fig. 5



TCS BIN = Especificación binaria de protocolo de control de telefonía

AT= Atención

RFCOMM= Comunicaciones para radiofrecuencia

1.5 APLICACIONES DE LA TECNOLOGÍA BLUETOOTH

1.5.1 EN CASA

Los hogares de hoy día son muy distintos a los de generaciones anteriores. Gracias a las posibilidades que brinda la tecnología, cada vez hay un mayor número de personas que traslada a casa su oficina, de forma que su vida diaria resulta más sencilla y funcional. Además, la tecnología está traspasando las fronteras del despacho y se está adentrando en otras áreas domésticas.

Los productos con tecnología BLUETOOTH permiten acabar con la maraña de cables de cualquier despacho. Ratones, teclados, ordenadores portátiles, auriculares y altavoces pueden conectarse al equipo de mesa de forma inalámbrica, lo que permite una mayor libertad y creatividad al distribuir y decorar la habitación. Por ejemplo: la impresora en una estantería o incluso en un armario. Además, con la sincronización de los contactos y los datos de la agenda entre el ordenador y los dispositivos móviles, se puede disponer de información actualizada en cualquier momento y lugar.

1.5.2 EN EL TRABAJO

Las oficinas de antes eran un lío de cables donde reinaba la confusión. Los cables de alimentación, del teclado, del ratón, de la impresora y de la PDA creaban un entorno caótico y desordenado. En algunos casos, esa maraña de cables incluso podía convertirse en un peligro. Más de uno se ha caído o enredado por cables mal puestos. Hoy día, la tecnología inalámbrica BLUETOOTH permite que la oficina sea un entorno organizado y sofisticado, con muchos menos cables a la vista. Actualmente, gracias a la tecnología BLUETOOTH, es posible sincronizar la PDA con el ordenador para tener al día la lista de contactos y la agenda, conectar los periféricos directamente a los ordenadores y moverse libremente por la oficina mientras se atienden llamadas con un manos libres, todo ello sin necesidad de un solo cable.

La tecnología BLUETOOTH no sólo acaba con el desorden en la oficina. Los dispositivos equipados con tecnología BLUETOOTH pueden conectarse en redes Ad-Hoc propias para intercambiar presentaciones o archivos, sin problemas de compatibilidad ni necesidad de acceder al correo. Además, facilitan las reuniones entre distintos grupos, ya que permiten mantener conversaciones entre varias oficinas a través de la red inalámbrica y transferir las ideas plasmadas en la pizarra directamente al ordenador.

1.5.3 EN MOVIMIENTO

Durante los desplazamientos al trabajo, a casa o a cualquier otro lugar, la tecnología BLUETOOTH permite estar comunicado permanentemente y proporciona acceso continuo a cualquier tipo de información. En el mundo de hoy, es eso lo que se espera de cualquier persona, independientemente de su papel en la sociedad: padre, estudiante o profesional que tiene que viajar a

menudo. Continuamente salen al mercado nuevos dispositivos y estándares que mejoran la comunicación móvil, y la tecnología inalámbrica BLUETOOTH a menudo es la elegida para que la conectividad inalámbrica sea una realidad.

Gracias a los móviles, PDA, portátiles, auriculares y automóviles con tecnología BLUETOOTH, podrá disfrutar de una comunicación “manos libres” mientras viaja, acceder a Internet cuando no disponga de su conexión habitual y tener siempre a mano sus datos más importantes, como los contactos o las entradas de su agenda en caso de tener sincronizado el PC con sus dispositivos móviles.

Los portátiles y demás dispositivos informáticos con tecnología BLUETOOTH pueden conectarse a móviles equipados con esta tecnología para acceder a Internet mediante redes GPRS, EDGE o UMTS. Podrá crear su propia red móvil, conectarse cuando y donde quiera y aumentar su productividad mientras se desplaza.

- Conexión sin cables entre los celulares y equipos de manos libres y kit para vehículos.

- Red inalámbrica en espacios reducidos donde no sea tan importante un ancho de banda grande.

- Comunicación sin cables entre la computadora y dispositivos de entrada y salida. Mayormente impresora, teclado y mouse.

- Transferencia de ficheros entre dispositivos vía OBEX.

- Transferencia de fichas de contactos, citas y recordatorios entre dispositivos vía OBEX.

- Reemplazo de la tradicional comunicación por cable entre equipos GPS y equipamiento médico.

- Controles remotos (tradicionalmente dominado por el infrarrojo)

- Enviar pequeñas publicidades entre anunciantes y dispositivos con BLUETOOTH. Un negocio podría enviar publicidad a teléfonos móviles cuyo BLUETOOTH (los que lo posean) estuviera activado al pasar cerca.

- Las consolas Sony Playstation 3 y Nintendo Wii traen BLUETOOTH para utilizar mandos inalámbricos.

Los dispositivos que con mayor intensidad utilizan esta tecnología son los de los sectores de las telecomunicaciones y la informática personal, como PDAs, teléfonos celulares, computadoras portátiles, PCs, impresoras y cámaras digitales.

Esta tecnología es capaz de transmitir información efectivamente hasta una distancia de 10 metros entre aparatos que utilicen transmisores "BLUETOOTH", debido que se emplea FHSS el "Hopping Pattern" de BLUETOOTH es de 1600 veces por segundo, lo cual asegura que la transmisión de datos sea altamente segura.

1.6 FUTURO DE ESTA TECNOLOGÍA

Para lograr alcanzar el objetivo de bajo consumo y bajo costo, se ideó una solución que se puede implementar en un solo chip utilizando circuitos CMOS. De esta manera, se logró crear una solución de 9x9 mm y que consume aproximadamente 97% menos energía que un teléfono celular común. Por otra parte el futuro de esta tecnología, no está muy lejano. Ya casi todo está dicho y en lo que respecta a novedades con respecto a BLUETOOTH, su futuro se centra en la aplicabilidad que se le puedan dar a diversos dispositivos, que en este momento no imaginamos, como por ejemplo sistemas de sonido completos.

1.6.1 APLICACIONES QUE POSIBLEMENTE PUEDAN UTILIZAR ESTA TECNOLOGÍA

1.6.1.1 TARJETAS BLUETOOTH: se trata de tarjetas pensadas especialmente para equipos portátiles que, integradas en el PC, permitirían al usuario llevar a cabo tareas como las anteriormente descritas (conexión de periféricos, transmisión de datos...) sin necesidad de tener que incorporar manualmente un dispositivo BLUETOOTH externo (por ejemplo USB), algo así como “BLUETOOTH de serie”. Aunque ya hay disponibles algunos en el mercado, estos modelos aún no aprovechan plenamente las ventajas que ofrece el estándar.

1.6.1.2 INCORPORACIÓN A OTROS DISPOSITIVOS ELECTRÓNICOS: esta es, quizás, una de las vías de investigación más interesantes y prácticas. Diversos fabricantes estudian la implantación de chips BLUETOOTH en varios de sus ingenios. Así por ejemplo, el usuario podrá disponer de reproductores de música BLUETOOTH con auriculares inalámbricos, acceso a Internet para descarga de temas online, etc., o de electrodomésticos activables por voz (campo conocido como domótica). Como ya se ha repetido a lo largo de todo el artículo, el límite solo está en la imaginación.

1.6.1.3 APLICACIONES JAVA: la integración de la tecnología BLUETOOTH con Java permite la generación de interfaces personalizadas para distintos tipos de usuario capaces de efectuar transmisión de datos, registros o descubrimiento de dispositivos.

1.7 A PRUEBA

Muchas son las compañías, asociaciones, entidades, etc., las que, ante el auge de la tecnología BLUETOOTH, se han ofrecido como bancos de prueba, y así

comprobar la eficacia de las propuestas más experimentales, entre las que destacan:

1.7.1 AUTOMATIZACIÓN DE PROCESOS INDUSTRIALES: todavía entre pañales, ya que los procesos industriales son muy hostiles, y BLUETOOTH tiene todavía que desarrollarse aún más para poder dar un soporte de tanto calibre.

1.7.2 BLUETOOTH Y LOS NEGOCIOS: uno de los principales objetivos que motivo el desarrollo del estándar, fue dar cobertura a nivel mundial, pensando especialmente en el ámbito de los negocios. Algunas de las propuestas más interesantes son las que hablan de acceso a Internet en los aeropuertos e incluso en compañías de trenes: el usuario podría consultar horarios, estar al tanto de las últimas noticias, revisar su mail o transmitir datos a la vez que viaja.

1.7.3 BLUETOOTH Y LA EDUCACIÓN: algunos centros educativos tales como universidades están trabajando en la implantación del estándar BLUETOOTH para facilitar el quehacer estudiantil cotidiano. En esta dirección, se ha conseguido desarrollar, por ejemplo, aplicaciones que permiten la consulta y revisión de notas a través de BLUETOOTH o la realización de ciertos cálculos, procesamiento de información con ayuda de dispositivos portátiles auxiliares (por ejemplo, PDAs).

1.7.4 DOMÓTICA: se trata de una de las aplicaciones con más futuro, tanto en el ámbito de los negocios (hostelería) como en el domestico: control de luces, persianas y puertas, sistemas de ahorro de energía, riego automático del jardín, climatización controlable mediante voz, ocio, gestión de sistemas de seguridad, etc. Las posibilidades son infinitas, y su llegada al hogar inminente. Aunque en dirección se han desarrollado ya varios estándares BLUETOOTH se destaca como una atractiva alternativa.

CAPITULO 2

2.1 WI - FI

El termino WI- FI hace referencia a las tecnologías de redes de transmisión pero de forma inalámbrica, actualmente muy utilizadas e implementadas por su facilidad, portabilidad y coste relativamente bajo. En un principio, la expresión WI- FI era utilizada únicamente para los aparatos con tecnología 802.11b, el estándar dominante en el desarrollo de las redes inalámbricas, de aceptación prácticamente universal, que funciona en una banda de frecuencias de 2,4 GHZ y permite la transmisión de datos a una velocidad de hasta 11Mbps (aunque la velocidad real de transmisión depende en última instancia del número de usuarios conectados a un punto de acceso). Teniendo en cuenta esto, WI- FI, presenta muchos estándares (ya sea 802.11a, 802.11b, 802.11g, 802.11i, 802.11h, 802.11e, con diferentes frecuencias y velocidades de transmisión).

Esta tecnología ofrece un excelente rango y un rendimiento respetable (mientras la radio puede enviar tramas por encima de los 11 Mbps, la cabecera del protocolo coloca la tasa de transferencia de datos entre 5 y 6 Mbps, sobre un par con red cableada Ethernet 10 base T). Opera usando DSSS [4] en 2.4GHZ y automáticamente selecciona la mejor tasa de transferencia (1, 2, 5.5 o 11Mbps) dependiendo de la fuerza de la señal disponible. La gran ventaja en este punto es su ubicuidad: el costo del cliente y el equipamiento del punto de acceso no es solo increíblemente barato, sino que además muchas laptop y dispositivos portátiles ahora poseen conectividad con el estándar 802.11b.

Desde entonces se pueden mover datos en tasas de transferencia mucho más rápido que el promedio de conexiones de Internet. 802.11b es ampliamente considerado como “muy bueno” para el uso general.

---

4 El método de DSSS opera en un canal determinado, luego la señal va separándose por mezcla con un código de pseudo ruido. Trabaja tomando un paquete de datos (de 0 y 1) y lo modula con un segundo modelo que es la secuencia de chipping. En 802.11 esta secuencia se conoce como el Código de Barker, está formada por 11 bits que tiene propiedades matemáticas que lo hacen ideal para modular radiofrecuencias.

TABLA 2: 802.11b FRECUENCIA DE CANALES	
Canal	**Centro de frecuencias (GHZ)**
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

Entrando mucho más en el tema de redes inalámbricas debemos remontarnos al año 1997, en el que el organismo regulador IEEE publicó el estándar 802.11 (802 hace referencia al grupo de documentos que describen las características de las LAN o Ethernet) dedicado a redes LAN inalámbricas. Dentro de este mismo campo y anteriormente, en el año 1995, tenemos la aparición de la tecnología BLUETOOTH.

Cuando la FCC (Organismo en cargado de regular las emisiones radioeléctricas), aprobó el uso civil de esta tecnología en 1997, fue que realmente empezó su verdadero desarrollo. Hoy día se conoce a WI- FI como el estándar 802.11b Y 802.11g. El primero ratificado por la IEEE como un nuevo estándar de alta velocidad para redes WLAN, llamado a veces Ethernet inalámbrico de alta velocidad o WI- FI (Wireless Fidelity). La diferencia sustancial respecto a su predecesor es que 802.11b ofrece una tasa de transmisión de hasta 11 Mbps, que puede llegar a compartirse entre doce conexiones de un mismo punto de acceso. Además, en una misma zona de cobertura pueden trabajar simultáneamente tres puntos de acceso, cada uno de ellos con un alcance para interiores de unos 90 m a 1 Mbps y de unos 30 m a la tasa máxima de 11 Mbps. La tasa de transmisión puede seleccionarse entre 1, 2, 5,5 y 11 Mbps, característica denominada DRS (Dynamic Rate Shifting), lo cual permite a los adaptadores de red inalámbricos reducir las velocidades para compensar los posibles problemas de recepción que puedan generarse por las distancias o los materiales que deba atravesar la señal (paredes, tabiques, ventanas, etc.), especialmente en el caso de interiores. En el caso de espacios abiertos, los alcances pueden aumentar hasta 120 m (a 11 Mbps) y 460 m (a 1 Mbps). El estándar 802.11g ya alcanza velocidades de 108

Mbps gracias a técnicas de aceleramiento que consiguen duplicar la transferencia teórica. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N, sin embargo, no se sabe si serán compatibles ya que el estándar no está completamente revisado y aprobado.

2.2 ¿COMO FUNCIONA?

Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio se hace referencia normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN sin cable, los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena.

La naturaleza de la conexión sin cable es transparente a la capa del cliente.

2.2.1 UN POCO MÁS

La técnica de modulación empleada es la CCK (Complementary Code Keying), codificando cada símbolo con 4 bits a velocidades de 1,375 MBd. Dado que CCK es una técnica DSSS, existe compatibilidad con los productos 802.11 originales simplemente reduciendo las velocidades de funcionamiento a 1 ó 2 Mbps. Posteriormente, un segundo esquema de codificación llamado PBCC (Packet Binary Convolutional Code) fue incluido para mejorar el alcance en el caso de tasas de 5,5 y 11 Mbps, ya que proporciona una ganancia de codificación de 3 dB.

Los sistemas basados en el estándar IEEE 802.11b se caracterizan por un conjunto de canales de 22 MHZ solapados entre sí, siendo fija la asignación de canales a cada punto de acceso. Del conjunto total de frecuencias, que en el caso de Europa es de siete, hay una combinación de canales disjuntos compuesta por los canales 1, 7 y 13. La planificación por defecto debe realizarse con estos canales, ya que aunque es posible utilizar canales

solapados, esto requiere un análisis previo bastante detallado para determinar el efecto de la perturbación producida por el canal adyacente. Como las transmisiones de 802.11b son de corto alcance, los usuarios observan una larga duración de las baterías de sus equipos, a la vez que las bajas potencias de emisión no suponen normalmente un riesgo para la salud. El nivel máximo de potencia permitido viene fijado por la norma ETSI EN 300 328, de tal manera que ésta no puede sobrepasar el valor de 100 mW (+20 dBm) de Potencia Isotrópica Radiada Equivalente (PIRE). Por otro lado, a nivel nacional, la nota de utilización UN-85 del Cuadro Nacional de Atribución de Frecuencias (CNAF) recoge las normas de uso de la banda de frecuencias de 2.400 a 2.483,5 MHZ destinada para uso común.

2.2.2 TECNOLOGIA DE CAPAS - 802.11b

Todos los equipos que implementan esta tecnología (tarjetas de red, puntos de acceso, etc.) se basan en una estructura de capas de acuerdo con el modelo de referencia OSI. La primera capa es el medio de transmisión o nivel físico. Por otro lado, la siguiente capa (nivel de enlace) define el control de acceso al medio (MAC) y el control de enlace lógico (LLC). Este último está definido por el estándar IEEE 802.2, por lo que para las capas superiores una red 802.11 es equivalente a una red Ethernet, facilitándose de este modo la interconexión entre redes heterogéneas basadas en distintos estándares del IEEE. Las tasas de transmisión que permite el estándar IEEE 802.11 son de 1 y 2 Mbps. El esquema de modulación propuesto para velocidades de 1 Mbps es BPSK, mientras que para 2 Mbps es QPSK. Sin embargo, estas velocidades significativamente inferiores a las de las redes de área local cableadas (10 y 100 Mbps) redujeron inicialmente el interés por estos sistemas.

2.2.2.1 CAPAS DEL ESTANDAR

PHY Phisical Layer (separado en PLCP y PMD)
MAC Media Access Control
LLC Logical Link Control

2.2.2.1.1 LA CAPA FISICA

- PLCP (Physical Layer Convergence Protocol): Se encarga de codificación y modulación. PLCP consiste en un encabezado de 144 bits que sirve para sincroniza, para determinar la ganancia y para establecer el CCA (Clear Channel Assessment) que es necesaria para que la capa de MAC sepa si el medio esta en uso. Este preámbulo está compuesto por 128 bits de sincronización más 16 bits llamados SFD (Start Frame Delimiter) que consiste en una secuencia fija de 0 y 1 (1111001110100000) que marca el principio del paquete. El PLCP es siempre transmitido a 1Mbps. Los próximos 48 bits son llamados Encabezado PLCP. Cuenta con 4 campos: señal, servicio, longitud y HEC ("header error check" para control de errores). La señal indica a qué velocidad se deberá transmitir (1, 2, 5.5 u 11Mbps). El campo de servicio se reserva para uso futuro. El campo de longitud indica la

longitud del paquete y el HEC es un CRC de 16bits del encabezado de 48bits. El PMD es dependiente del protocolo antes explicado.

- Preámbulo (144 bits = 128 sincronismo + 16 inicio trama).
- HEC (Header Error Control): CRC 32
- Modulación (propagación) DSSS o FHSS o IR.
- PMD (Physical Medium Dependence): Es la que crea la interfaz y controla la comunicación hacia la capa MAC (a través del SAP: Service Access Point)

Este nivel lo conforman dos elementos principales: Radio y Antena

NOTA: Aunque esto no forma parte de los conceptos de WI- FI, cuando se habla de transmisión, se deben diferenciar tres palabras:

2.2.2.1.2 Modulación: Es el método de emplear una señal portadora y una moduladora (que da forma a la anterior). Cada una de ellas puede ser analógica o digital, con lo cual se obtienen cuatro posibles combinaciones de portadora y moduladora (AA – AD – DA y DD), con las cuales se conforman todas las técnicas de modulación. WI- FI en la mayoría de los casos emplea la técnica QAM (Modulación en cuadratura de Fases con más de un nivel de amplitud).

2.2.2.1.3 Propagación: Es la forma en la cual "van saliendo" las señales al aire. Aquí es donde verdaderamente se aplican las técnicas de DHSS y FHSS. SS (Spread Spectrum) es la técnica de emplear muchas subportadoras de muy baja potencia con lo cual se "expande" el espectro útil. En cuanto a DH y FH El ejemplo típico que se emplea para estas técnicas es la analogía con una terminal de trenes, en la cual existen varios andenes. Para DH, los trenes estarían saliendo, primero el andén 1, luego el 2, a continuación el 3, 4, 5... y así sucesivamente, respetando siempre este orden. Para FH, la salida de los trenes no respeta el orden y puede ser aleatoria o acorde a un patrón determinado (WI- FI hace un muy buen uso de esto, pues en las subportadoras que recibe mucha interferencia no las usa o emplea menos cantidad de bits en las mismas).

2.2.2.1.4 Codificación: Es la asociación de bit a cada "muestra" que se obtiene. WI- FI en la mayoría de los casos emplea el código Barker [5].

---

5 el Código de Barker, está formada por 11 bits que tiene propiedades matemáticas que lo hacen ideal para modular radiofrecuencias. El código Barker genera series de objetos de datos llamados chips. Cada bit se encodea por el Código Barker de 11bits y cada grupo de 11 chips encodea 1 bit de datos.

2.2.2.2 LA CAPA DE ENLACE

La capa MAC encargada del control al acceso físico se encarga de sentir un tiempo de silencio y optar por transmitir. Luego de que el host determina que el medio ha estado sin transmisiones después de un periodo mínimo de tiempo opta por transmitir su paquete. Si el medio se encuentra ocupado el host deberá esperar. Esta capa también es responsable de identificar el origen y el destino del paquete.

Existen dos subniveles que lo conforman (MAC: Medium Access Control y LLC: Logical Link Control). Desde el punto de vista de 802.11, solo interesa hacer referencia al subnivel MAC

2.2.2.2.1 CAPA MAC: Controla el flujo de paquetes entre 2 o más puntos de una red. Emplea CSMA/CA: Carrier Sense Multiple Access / Collision avoidance.

2.2.2.2.2 EXPLORACIÓN: Envío de Beacons que incluyen los SSID: Service Set identifiers O también llamados ESSID (Extended SSID), máximo 32 carateres.

2.2.2.2.3 AUTENTICACIÓN: Proceso previo a la asociación. Existen dos tipos:
Autenticación de sistema abierto: Obligatoria en 802.11, se realiza cuando el cliente envía una solicitud de autenticación con su SSID a un AP, el cual autorizará o no. Este método aunque es totalmente inseguro, no puede ser dejado de lado, pues uno de los puntos más fuertes de WI- FI es la posibilidad de conectarse desde sitios públicos anónimamente (Terminales, hoteles, aeropuertos, etc.).

Autenticación de clave compartida: Es el fundamento del protocolo WEP (hoy totalmente desacreditado), se trata de un envío de interrogatorio (desafío) por parte del AP al cliente.

2.2.2.2.4 ASOCIACIÓN: Este proceso es el que le dará acceso a la red y solo puede ser llevado a cabo una vez autenticado.

2.2.2.2.5 SEGURIDAD: Mediante WEP, con este protocolo se cifran los datos pero no los encabezados.

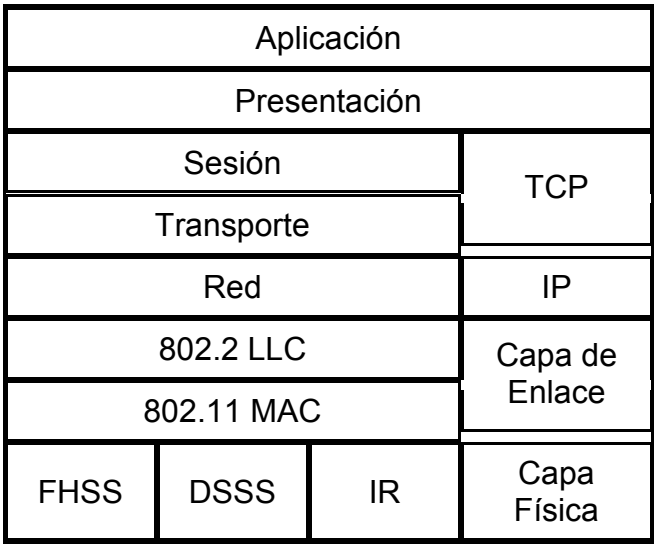
2.2.2.2.6 RTS/CTS: Funciona igual que en el puerto serie (RS-232), el aspecto más importante es cuando existen “nodos ocultos”, pues a diferencia de Ethernet, en esta topología SÍ pueden existir nodos que no se escuchen entre sí y que solo lleguen hasta el AP, (Ej: su potencia está limitada, posee un obstáculo entre ellos, etc), en estos casos se puede configurar el empleo de RTS/CTS. Otro empleo importante es para designar el tamaño máximo de trama (en 802.11 Es: mínimo=256 y máximo=2312 Bytes).

2.2.2.2.7 MODO AHORRO DE ENERGÍA: Cuando esta activado este modo, el cliente envió previamente al AP una trama indicando "que se irá a dormir", El AP, coloca en su buffer estos datos. Se debe tener en cuenta que por defecto este modo suele estar inactivo (lo que se denomina Constant Awake Mode: CAM).

2.2.2.2.8 FRAGMENTACIÓN: Es la capacidad que tiene un AP de dividir la información en tramas más pequeñas.

MODELO EN CAPAS

Fig. 6



2.3 ELEMENTOS DE UNA RED WI- FI – CONFIGURACION

Una red inalámbrica está constituida principalmente por dos tipos de equipos. Por un lado están los puntos de acceso y los routers inalámbricos, que forman a su alrededor zonas de cobertura, y por otro los equipos cliente, formados por ordenadores o periféricos dotados de adaptadores de red inalámbrica, que pueden ser PCI, USB, PCMCIA o Bridge Wireless-Ethernet.

2.3.1 PUNTO DE ACCESO

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. También se conoce como un dispositivo inalámbrico central de una red inalámbrica WI- FI que por medio de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos móviles y la transmite a través de cable al servidor de la red cableada. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados, también tienen un radio de cobertura aproximado de 100m, aunque esto varía bastante en la práctica entre un modelo y otro y según las condiciones ambientales y físicas del lugar (obstáculos, interferencias, etc.)

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El estándar 802.11 es bastante ambiguo y no define con claridad todas las funciones que debería realizar un Punto de Acceso y sólo lo describe de una manera muy superficial. Esto dio lugar a que cada fabricante lo diseñara según su criterio y, por lo tanto hoy día existen en el mercado decenas de Puntos de Acceso con características y funcionalidades muy dispares.

2.3.1.1 ¿CÓMO SE INSTALA?

Con un punto de acceso sencillo, basta con conectarlo mediante un cable de red al módem o Router ADSL. Lo normal es que no sea necesario configurar nada más, y que cualquier ordenador con adaptador WI- FI tenga acceso a la red (el ordenador detecta automáticamente la presencia de redes WI- FI). El efecto es el mismo que conectar directamente esos ordenadores al módem ADSL mediante un cable.

2.3.2 ROUTER INALAMBRICO

Es un punto de acceso inalámbrico que además cumple con otras funciones muy útiles, como un cortafuego interno para mayor seguridad, crear una red local entre los ordenadores para que se comuniquen entre sí, y la posibilidad de conectarlos a todos ellos a Internet. Son la mejor solución si se dispone de un módem de cable o un módem ADSL sin estas funciones de router, pero salen algo más caros que los puntos de acceso sencillos.

2.3.2.1 ¿CÓMO SE INSTALA?

La entrada de datos del Router inalámbrico (marcada como uplink) se conecta al módem ADSL mediante un cable de red. Por lo general también hay salidas de conexión de red por cable, que servirán si se quiere conectar un ordenador fijo al lado. El Router inalámbrico se configura accediendo a una página web. Aquí habrá que dar un nombre a la red doméstica, y también se podrán activar o desactivar funciones como el cortafuegos. Con el Router se puede crear una red local completa, en la que los ordenadores se conectan a Internet, y además se comunican entre sí para compartir archivos. Si se utilizan programas de videoconferencia, mensajería instantánea o P2P (programas de intercambio de archivos) puede ser necesario configurar parámetros especiales.

2.3.3 DISPOSITIVOS MOVILES

Los hay muy diversos como computadores portátiles (Notebooks), PDAs, teléfonos celulares. Estos tienen instaladas tarjetas PCMCIA o dispositivos USB con capacidades WI- FI y pueden, por lo tanto, recibir o enviar información a los Puntos de Acceso o a otros dispositivos de manera inalámbrica (RF). En la actualidad ya abundan los que tienen la tecnología WI- FI incorporada en el procesador (Intel, Atheros, etc.) y por lo tanto no necesitan de agregados USB o PCMCIAs.

2.3.4 DISPOSITIVOS FIJOS

Los computadores de sobremesa o fijos (desktops), las impresoras, cámaras de vigilancia, etc. también pueden incorporar tecnología WI- FI y, por lo tanto, ser parte de una red inalámbrica.

2.3.5 OTROS ELEMENTOS

También existen amplificadores y antenas que se pueden agregar, según las necesidades, a instalaciones WI- FI y sirven para direccionar y mejorar las señales de RF transmitidas

2.3.5.1 ANTENAS

Cuando trate de cubrir espacios grandes con WI- FI, encontraremos varias barreras naturales. Las principales son: árboles, metal, paredes de cemento, paredes de ladrillos y otros equipos WI- FI. Para pasar alrededor de estos obstáculos debe seleccionar la antena apropiada. Hay cuatro tipos de antenas que funcionan bien en la banda de 2.4 GHZ (WI- FI). Cada una funciona bien en su propia aplicación.

Existen principalmente cuatro tipos de antena. Omnidireccionales para zonas de cobertura en todas direcciones en torno al punto de acceso, yagi para sistemas de direccionales de apertura media o enlaces punto-multipunto, paneles para zonas de cobertura de apertura alta o enlaces punto-multipunto y parabólicas para sistemas altamente directivos.

2.3.5.1.1 OMNIDIRECCIONAL

Las antenas Omnidireccionales u Omnis irradian igualmente en todas las direcciones. Son buenas para cubrir un área grande, en donde Ud. no sabe desde donde se conectarán los clientes WI- FI. El problema de las antenas omni es que también reciben ruido e interferencia desde todas las direcciones, por lo que generalmente no son tan eficientes como antenas más direccionales.

2.3.5.1.2 SECTORIALES

Las antenas tipo Sector, irradian en una dirección cubriendo desde 180 grados hasta 60 grados, dependiendo de la aplicación. Son excelentes para aplicaciones punto - multipunto, en donde los clientes WI- FI se conectan desde una sola dirección.

2.3.5.1.3 YAGI

La antena Yagi parece una vieja antena de televisión. Tiene una parte principal de metal, cruzada por varios metales más pequeños. O un tubo de metal, con varios discos soldados. Típicamente irradian entre 15 y 60 grados.

2.3.5.1.4 ANTENA PARABÓLICA

Las antenas de tipo plato parabólico son las más direccionales de todas. Son ideales para enlaces punto a punto. Una antena parabólica de medio metro de diámetro, puede transportar una señal 802.11 hasta 30 kilómetros de distancia.

2.3.5.2 REPETIDORES

Puede usar un Router para fabricar un repetidor WI- FI. Simplemente instale dos tarjetas WI- FI, ya sean PCI o PCMCIA. Verifique que las tarjetas WI- FI permitan rutear IPs reales en modo IBSS, ya que varias tarjetas tienen esa funcionalidad bloqueada (para no canibalizar su propio mercado de puntos de acceso). O si no, puede simplemente usar masquerading para evitar ese problema.

2.3.5.3 ENLACES PUNTO A PUNTO

Puede usar un Router en cada extremo del enlace punto a punto, con una tarjeta WI- FI cada uno. Verifique que las tarjetas WI- FI permitan rutear IPs reales en modo IBSS. Para evaluar la posibilidad de una conexión punto a punto WI- FI, siga los siguientes pasos:

- Verifique que haya "línea de vista" entre los dos puntos a conectar
- Mida la distancia, usando GPS o mapas topográficos
- Calcule la pérdida de señal y las antenas necesarias.
- Use la menor cantidad de cable posible entre la antena y el Router

Cuanto mayor sea la distancia de los dos puntos a conectar, más difícil será alinear las antenas. Para distancias mayores a 10 Km, la alineación de las antenas es un trabajo en sí mismo, pero puede seguir los siguientes puntos para facilitar la tarea:

Use teléfonos celulares para comunicarse entre cada extremo durante la instalación. Ayuda tener 2 personas en cada extremo, una para manipular la antena y la otra para coordinar la comunicación con el otro extremo.

Configure los Routers antes de ir al sitio, así se sacará una duda de encima cuando este en el campo.

Use una herramienta que le permita ver la fuerza de la señal, y el ruido en tiempo real.

Manipule un extremo a la vez, cambiando cada variable lentamente hasta que vea la máxima señal y el mínimo ruido.

No toque la antena mientras mide la señal.

Una vez que su enlace está listo use WEP para evitar que gente se conecte al enlace punto a punto directamente. Si quiere proveer acceso Internet configure otro Router, preferentemente con Caching de DNS y Proxy. Esto ayuda a reducir la cantidad de tráfico que viaja por el enlace de larga distancia, baja la cantidad de colisiones de red, y mejora el enlace.

2.4 APLICACIONES DE LA TECNOLOGIA WI- FI

Se puede decir que WI- FI es una tecnología madura y consolidada que ha conseguido más de 50 millones de usuarios en aproximadamente 4 años. Los aeropuertos, hoteles y palacios de congresos (hot-spots) fueron los primeros lugares donde se instalaron redes 802.11b de forma satisfactoria. Los beneficios de WI- FI en términos de movilidad y flexibilidad, unido al aumento de velocidad y a la reducción en el coste de las tarjetas de red, lo ha convertido también en una opción muy atractiva para el mercado residencial y del pequeño negocio. Con el aumento en el uso de los ordenadores portátiles, PDAs, y demás dispositivos inalámbricos, la tecnología WI- FI tiene asegurado el éxito en el futuro.

Recientemente se pueden encontrar también en el mercado productos basados en el estándar 802.11b+, el cual consiste en una extensión de 802.11b que permite alcanzar tasas de transmisión de hasta 22 Mbps, el doble de las permitidas por 802.11b.

Las redes inalámbricas son ideales para utilizar en lugares donde diferentes equipos pueden necesitar conexión a la red en diferentes posiciones, donde no es posible realizar instalación de cable o no es recomendable, y para unir redes de varios edificios o delegaciones si existe visión directa.

2.4.1 ¿SON PERJUDICIALES PARA LA SALUD LAS REDES INALÁMBRICAS?

No se ha demostrado en todo el tiempo que llevan utilizándose este tipo de redes relación alguna con problemas de salud. La baja potencia utilizada hace inocua la tecnología para el bienestar de seres humanos o animales.

2.4.2 VENTAJAS Y DESVENTAJAS

Una de las desventajas que tiene el sistema WI- FI es la pérdida de velocidad en relación a la misma conexión utilizando cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta WI- FI en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella, las claves de tipo WEP son relativamente fáciles de conseguir para cualquier persona con un conocimiento medio de informática. La alianza WI- FI arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. Los dispositivos WI- FI ofrecen gran comodidad en relación a la movilidad que ofrece esta tecnología, sobre los contras que tiene WI- FI es la capacidad de terceras personas para conectarse a redes ajenas si la red no está bien configurada y la falta de seguridad que esto trae consigo.
Cabe aclarar que esta tecnología no es compatible con otros tipos de conexiones sin cables como BLUETOOTH, GPRS, UMTS, etc.

2.5 FUTURO DE WI- FI

La tendencia hacia fines de 2007 es a reemplazar la WI- FI por la WIMAX. Este es un nuevo estándar, que tiene mucho mayor alcance, mayor velocidad y más capacidad de cantidad de usuarios. Esta tecnología "ilumina con internet" varias decenas de kilómetros a la redonda por cada punto de acceso, a velocidades de hasta 2 megas, pudiendo soportar varios cientos de PCs y otros periféricos conectados.

2.5.1 ESTÁNDAR WI- FI - 802.11E: QOS / CALIDAD DE SERVICIO

El estándar IEEE 802.11e, es un estándar bastante nuevo. El borrador final fue aprobado en Julio de 2005 y el estándar fue ratificado a finales de 2005. A pesar de esto hasta hoy dia aun se exploran las bondades que este estándar puede ofrecer y aun está siendo objeto de estudio si implementación total. Se conoce como el estándar de QoS - Quality of Service pues busca subsanar carencias que tiene la tecnología WI- FI desde sus comienzos. Los Access Point que existían no eran capaces de priorizar el ancho de banda. Un usuario solo puede utilizar todo el ancho de banda y no hay manera de establecer prioridades para cierto tipo de tráfico como, por ejemplo, el tráfico de voz o video.

Aunque se están empezando a utilizar otros nombres como VoFI - Voice en WI-FI-, VoWLAN - Voice en WLAN, etc. Con el nuevo estándar 802.11e se pueden establecer 4 colas distintas según el tipo de servicio. La categoría más prioritaria, espera menos y la categoría menos prioritaria, espera su turno que es el cuarto. La idea es que el tráfico de voz, sea el de máxima prioridad, pues este tipo de servicios no admite demoras. Luego vendría el tráfico de video, luego el tráfico de datos más importantes y luego el resto de los datos. En este último se incluye a todos los dispositivos antiguos que no están diseñados para gestionar QoS. Es necesario conocer que si se desea implementar una Red Inalámbrica WI- FI con QoS - Calidad de Servicio - deben cumplirse varias condiciones: Los Access Points deben estar certificados para QoS y además, deben tener esta función activada. Los clientes también deben tener activada la opción de QoS y estar certificados al respecto. Las aplicaciones deben soportar QoS y deben saber asignar los niveles de prioridades que permite el estándar 802.11e al tráfico que ellas generan. Está claro que el cumplimiento de estas 3 condiciones, en la actualidad, es un poco complicado. Por ejemplo si disponemos de PDAs o de Access Points, o de computadores con chip Centrino, que tengan más de un par de años de antigüedad, seguramente no estén certificados para QoS. Lo mismo sucederá, posiblemente, con diversas aplicaciones que queramos utilizar y que deberían ser re-escritas para saber soportar QoS y asignar prioridades al tráfico.

La certificación 802.11e - QoS es voluntaria. No es obligatoria. Por lo tanto habrá equipos de gama baja, que no soporten 802.11e pero que estén certificados para los otros estándares como 802.11a, 802.11b, 802.11g, 802.11i, etc.

2.5.2 ESTÁNDARES WI- FI - 802.11K - MEDICIÓN Y GESTIÓN DE RF EN WI- FI

El estándar IEEE 802.11k se titula "Radio Resource Management" y busca incorporar varias funciones que aún no existen en los Access Point y en los clientes WI- FI. Ya se han generado 7 borradores y se espera su aprobación final para finales de este año (2007). Un gran inconveniente en la actualidad es que los dispositivos de una red inalámbrica WI- FI, se conectan a los Access Point que emiten la señal más potente. Esto no conduce necesariamente a una mejor conexión o calidad de la red. Por ejemplo en una sala de reuniones o un auditorio. El Punto de Acceso seguramente se recargará primero y luego se colapsará. Evidentemente, el uso de recursos no es eficaz.

Los dispositivos deberían aprender a cambiarse de Punto de Acceso. Para ello deberían saber medir los recursos de RF y también compartir esa información entre los Access Point y los dispositivos WI- FI. Por ejemplo cual es la carga del canal, si el canal está bloqueado, hacer un histograma del ruido, etc.

La idea final es que los dispositivos WI- FI, en vez de conectarse al Access Point que emite la señal más potente, tengan la información suficiente para saber seleccionar el Access Point más adecuado, donde haya "menos competencia". El rendimiento de los clientes de una red inalámbrica WI- FI, baja significativamente cuando hay muchos usuarios compitiendo en un Punto de Acceso. Se está trabajando con unos algoritmos que sabrán suministrar al dispositivo WI- FI "postulante" a conectarse, un listado de todos los Access Point disponibles clasificados desde el mejor hasta el peor. Una vez aprobado el estándar IEEE 802.11k, el funcionamiento será el siguiente: El Access Point le pedirá al dispositivo WI- FI que intente conectarse a la red inalámbrica WI- FI, que le informe todos los Access Point que está oyendo. El Punto de Acceso analizará esta información y luego suministrará el listado indicando cuales son los Access Point más convenientes para esa estación. Los dispositivos también podrán saber si hay nodos ocultos, y los Puntos de Acceso sabrán cuales son los confines de su celda. Según está estipulado, cuando se apruebe el estándar los Access Point y los dispositivos WI- FI se deberán poder actualizar por medio de software. Llegado el momento habrá que ver, si todos los equipos son capaces de funcionar con la actualización. Seguramente, los muy antiguos tendrán inconvenientes.

2.5.3 PROPUESTA

Una de las propuestas más llamativas actualmente, la hace AB-TEL, una compañía dedicada a la explotación de la tecnología WI- FI. Sería ofrecer canales de interacción a los clientes de un local, lo cual permitiría, por ejemplo, hacer pedidos por el móvil a los clientes de un restaurante o de un centro comercial, o la de instalar redes públicas que hicieran posible el acceso a Internet desde semáforos o edificios públicos por parte de los ciudadanos. Estas empresas en sus proyectos han intentado dar soluciones para gran parte de los problemas que presenta estas novedosas tecnologías, como la falta de

seguridad en las transmisiones inalámbricas o la poca flexibilidad a la hora de poder combinar los diferentes sistemas existentes para que cada usuario encuentre la opción que más le conviene en cada momento.

2.6 RESUMEN: como resumen final, en la tabla siguiente se detallan las características más significativas de cada uno de los estándares WLAN analizadas, en comparación con otras tecnologías inalámbricas como BLUETOOTH o UWB.

TABLA 3: CARACTERISTICAS SIGNIFICATIVAS DE LOS ESTANDARES WLAN

Estándar	802.11b	802.11a	802.11g	HiperLAN/2	BLUETOOTH	802.15.3a
Organismo	IEEE	IEEE	IEEE	ETSI	BLUETOOTH SIG	IEEE
Finalización	1999	2002	2003	2003	2002	-
Banda de frecuencias	2,4 GHZ	5 GHZ	2,4 GHZ	5 GHZ	2,4 GHZ	3,1-10,6 GHZ
Tasa máxima	11 Mbps	54 Mbps	54 Mbps	54 Mbps	1 Mbps	480 Mbps
Interfaz aire	DSSS/FHSS	OFDM	OFDM	OFDM	DSSS/FHSS	Códigos PN

CAPITULO 3

3.1 WIMAX (Worldwide Interoperability for Microwave Access)

WIMAX, en español: “Interoperabilidad Mundial para Acceso por Microondas”, es la marca que certifica que un producto está conforme con los estándares de acceso inalámbrico ‘IEEE 802.16′. Proporciona accesos concurrentes en áreas de hasta 48 km de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base. Estos estándares permitirán conexiones de velocidades similares al ADSL o al cable módem, sin cables. Se están realizando muchos esfuerzos para que este estándar sea compatible totalmente con otros anteriores, como el de WI-FI (IEEE 802.11).

La tecnología WIMAX será la base de las Redes Metropolitanas de acceso a Internet, servirá de apoyo para facilitar las conexiones en zonas rurales, y se utilizará en el mundo empresarial para implementar las comunicaciones internas. Además, su popularización supondrá el despegue definitivo de otras tecnologías, como VoIP (llamadas de voz sobre el protocolo IP).

Para promover el uso los estándares WIMAX, es necesario que los fabricantes de dispositivos electrónicos lleguen a acuerdos para desarrollar esta tecnología, dando lugar a certificaciones que aseguren la compatibilidad y la interoperabilidad de antenas, procesadores o receptores. Por ello, existe el ‘WIMAX Forum’, creado en el año 2001 que es una asociación sin ánimo de lucro formada por decenas de empresas, entre las más conocidas se encuentran Nokia, Intel, Nortel, Motorola, etc. comprometidas con el cumplimiento del estándar IEEE 802.16. y para ayudar a asegurar la compatibilidad y la interoperabilidad a través de múltiples fabricantes, algo parecido a lo que la Alianza WI-FIhace por la familia de estándares IEEE 802.11x.

El continuo e imparable progreso tecnológico, así como una sociedad cada vez más móvil y dependiente de las nuevas tecnologías, son algunos de los motivos que están induciendo profundos cambios en los actuales sistemas inalámbricos y que, al mismo tiempo, provocarán la adopción de nuevos estándares. Entre las nuevas tecnologías inalámbricas de inminente entrada en escena, WIMAX se perfila como un significativo avance tecnológico que revolucionará por completo el actual estatus de los enlaces sin cables.

Pese a su innegable funcionalidad y productividad, las redes WI-FI han estado, hasta la fecha, relegadas a entornos de escasos metros cuadrados, un panorama que promete cambiar radicalmente con la inminente aparición de la tecnología WIMAX, capaz de ofrecer conexiones de banda ancha alcanzando distancias de hasta 70 kilómetros, obviamente en las condiciones más favorables, y que supone la rampa de lanzamiento ideal para otras tecnologías en plena expansión como la telefonía sobre Internet (VoIP). Apenas han

transcurrido tres años desde que se hiciera pública su aprobación por parte del consorcio IEEE del estándar 802.16, también conocido como WIMAX, y ya comienza a convertirse en una realidad palpable. La intervención de empresas como Intel, que lo incluirá en próximas revisiones de su popular plataforma Centrino, Motorola y Nokia, entre otras muchas, augura un excelente futuro para una tecnología que complementará y dará nuevos bríos al popular estándar WI-FIy sus sucesores. Si bien el término WIMAX sólo tiene algunos años, el estándar 802.16 ha existido desde fines de la década de 1990, primero con la adopción del estándar 802.16 (10-66 GHZ) en abril de 2002 y luego con el 802.16a (2-11GHZ) en enero de 2003. A pesar del establecimiento del estándar 802.16a, el mercado del FWA (Fixed Wireless Access) nunca terminó de despegar, aunque vale la pena mencionar que durante ese período toda la industria de telecomunicaciones estuvo luchando.
Así, y en principio, este estándar 802.16 se enfocaba específicamente en el uso eficiente del ancho de banda, en la región comprendida entre los 10 y los 66 gigahercios y definía una capa de control de acceso al medio capaz de soportar múltiples especificaciones de capas físicas, desarrolladas para el uso de esta banda de frecuencia.

Poco después, ni siquiera había transcurrido un año, se llevó a cabo la primera revisión del estándar con el objeto de incorporar una rama adicional, denominada 802.16a, con la que cubrir el rango de frecuencias de los 2 a los 11 GHZ y contempla la utilización de dos técnicas de modulación, OFDM y OFDMA. Del mismo modo, en los años sucesivos también se han ido introduciendo sucesivas y significativas mejoras. Resumiendo, la última versión del estándar IEEE 802.16, la 802.16-2004 (conocida previamente como Revisión D, o 802.16d), fue ratificada en julio de 2004 e incluye la versiones anteriores (802.16-2001, 802.16b/c de 2002, y 802.16a en 2003) y cubre tanto enlaces mediante línea de visión directa (LOS, Line of Sight) como aquellos sin línea de visión directa (NLOS, Non Line of Sight) en el rango de frecuencias 2 - 66 GHZ. Como es costumbre en los estándares IEEE, sólo se regulan las especificaciones de las capas PHY (Physical) y MAC (Media Access Control). Los cambios introducidos en la norma 802.16-2004 estuvieron dirigidos al desarrollo de aplicaciones de interoperabilidad en el rango de frecuencias de 2-11 GHZ. siendo así las cosas, los actuales sistemas WIMAX se basan principalmente en dos especificaciones, el estándar 802.16-2004 de IEEE y la norma HiperMAN [6] de ETSI (European Telecommunications Standards Institute).

---

6 Se considera una alternativa europea a WIMAX y a la coreana WiBro. Estándar creado por el Instituto Europeo de Normas de Telecomunicaciones (ETSI) dirigido principalmente para proveer DSL inalámbrica de banda ancha, cubriendo un área geográfica grande

Dos enfoques similares en lo que se ha dado en llamar tecnología BWA (Broadband Wireless Access). La diferenciación de ambas es tremendamente importante por una razón. La primera está orientada a comunicaciones en las que las estaciones emisora y receptora tienen una línea de visión directa, algo similar a lo que ocurre con las emisiones infrarrojas de los mandos a distancia.

En la segunda, las bandas de frecuencia utilizadas permiten mantener la comunicación sin que ambos extremos estén directamente enfrentados, e incluso puede haber todo tipo de obstáculos que no impiden la transmisión de datos, como ocurre con las redes WI-FI actuales o con la tecnología BLUETOOTH.

La gran batalla por la hegemonía inalámbrica desde la perspectiva más optimista, las notables prestaciones y cualidades de esta innovadora tecnología de comunicación inalámbrica, así como la consolidación y certificación real de los primeros productos WIMAX, permiten pronosticar una implantación masiva a corto plazo. Consecuentemente, las consultoras más entusiastas predicen ambiciosas cotas de negocio en el pujante y creciente mercado de las comunicaciones inalámbricas. No obstante, y pese a que una de las cualidades de WIMAX son sus bajos costes de infraestructura, razón que justifica que esté especialmente indicado para llevar la banda ancha a las zonas rurales y a países subdesarrollados, han de realizarse todavía las arduas labores de las instalación de las estaciones base, concesión y asignación de licencias para el uso de determinadas banda del espectro electromagnético, así como el desarrollo y distribución de los respectivos productos. En pocas palabras, se necesita algo más, tiempo y sobre todo; mucho dinero en inversiones. Pese a ello, hay un nutrido grupo de empresas encuadradas en el WIMAX Forum (www.WIMAXforum.org), decididas a sacar el proyecto adelante.

En cualquier caso, la competencia no se va a dejar avasallar fácilmente. De un lado, la telefonía UTMS de tercera generación (3G) ya está desplegada y en funcionamiento, siendo la alternativa natural en aquellas áreas y espacios donde no exista cobertura ADSL (Cable Ethernet) o Wi-Fi, aunque su nivel de cobertura real deja bastante que desear, al menos en lo que a nuestro país concierne. Pese a todo, para tratar de contrarrestar el avance WIMAX los promotores y operadores de telefonía móvil 3G ya tienen lista una mejora de la actual tecnología W-CDMA, denominada HSDPA o 3.5G, que puede trabajar con las radio bases actuales y que supuestamente tiene picos de transmisión de hasta 10 Mbps. Un futuro que estará supeditado a las tarifas que las operadoras quieran implantar para el uso y disfrute de los nuevos servicios.

Aunque muchos prevén una dura batalla entre WIMAX y HSDPA, pensamos que ambas tecnologías, pese a ofrecer servicios y prestaciones similares, son complementarias. Mientras WIMAX tiene una orientación más específica a la transmisión de datos y cercana a las aplicaciones las informáticas convencionales, las tecnologías móviles de nueva generación seguirán apostando preferentemente por las comunicaciones de voz, aunque debidamente acompañadas con servicios de datos. Por ejemplo, la versión

móvil de WIMAX servirá a los operadores para crear redes que cubran a una ciudad y que serán utilizadas por los usuarios para acceder a Internet desde una cafetería, en casa o en sus oficinas, sin que necesariamente tengan que estar en movimiento. Mientras que los sistemas provistos de la tecnología HSDPA, podrían ser utilizadas por aquellos que quieren, por ejemplo, descarga su correo mientras viajan en un automóvil o en tren.
Así las cosas, hay quien ya augura un pacífica convergencia entre ambos contendientes tecnológicos, de tal forma que los móviles incorporen tanto UMTS (o HSDPA) como WIMAX. En este contexto, entraría en escena la tecnología UMA (Unlicensed Mobile Access) que propone precisamente los mecanismos necesarios que harían posible el uso de servicios de mensajería de datos y de voz a través de redes inalámbricas no licenciadas para el uso como sistemas de telefonía móvil. No obstante, y según vayan haciendo su aparición las primeras soluciones y dispositivos WIMAX, seremos objeto de agresivas estrategias comerciales por parte de las operadoras de telefonía móvil con la clara intención de impedir el despliegue WIMAX, el rival tecnológicamente más fuerte

La gran ventaja de la tecnología WIMAX, en su versión 802.16-204, es que puede permitir la aparición de nuevos actores en el mercado, ajenos a los operadores tradicionales o a las compañías ya instaladas y con redes. La segunda ventaja es que esta tecnología permitirá novedosos y más económicos servicios para los usuarios, siempre y cuando la competencia y el desarrollo se lleven a cabo de forma natural y sin condicionantes de ningún tipo. De esta forma, WIMAX podrá competir en igualdad de condiciones e incluso superando a sistemas como DSL, cable módem y, por qué no, UMTS.

Por último, hay que tener también presente que el hecho de que una determinada tecnología consiga un rotundo éxito depende, en multitud de ocasiones y en un gran porcentaje, más del acertado oportunismo comercial que de cuestiones puramente técnicas. Véase, por ejemplo, el caso de la VoIP, que ha ganado una tremenda popularidad entre los usuarios domésticos con la aparición de Skype pese a que existía desde 1996. Esto mismo podría ocurrir a las tecnologías inalámbricas, que existen desde hace tiempo y que podrían empezar a tener éxito con la aparición del WIMAX y, sobre todo, si el hardware y las tarifas de conexión presentan precios reducidos. Aunque mucho me temo, a pesar de las esperanzadoras perspectivas que promulga WIMAX, que los habitantes de las zonas rurales seguirán, en su gran mayoría y durante algún tiempo más, al margen de la conectividad de banda ancha. Hoy por hoy, donde no llega el ADSL tampoco suele existir cobertura 3G. No obstante, hasta ahora la Administración, en muchas partes del mundo, pero en especial en España, se ha lanzado de lleno a crear o a alentar la creación de redes WI-FI para dar cobertura de Internet a pueblos y centros que no la tenían, con WIMAX esos proyectos pueden verse reforzados. PCW

3.1.1 PRINCIPALES CARACTERÍSTICAS DE WIMAX

- Gran ancho de banda. Una sola estación de base puede admitir de manera simultánea más de 60 enlaces con conectividad tipo T1/E1 o cientos de conexiones tipo DSL (línea digital de suscriptor).

- Es independiente de protocolo. Es decir, puede transportar IP, Ethernet, ATM y otros. La clave de la compatibilidad de este estándar con otros como WI- FI (802.11), Ethernet (802.3), o Token Ring (802.5) reside en el uso de la misma capa LLC (Logical Link Controller), que actúa como interfaz de acceso a los servicios de datos que proporciona cada tecnología.

- Puede transmitir otros servicios agregados como: Voz sobre IP (VoIP), datos, o vídeo.

- Es compatible con las antenas de telefonía de tercera generación (denominadas "antenas inteligentes"), que gracias a la emisión de un haz acotado, apuntan constantemente al receptor aún en movimiento.

- En circunstancias ideales y sin obstáculos que interfieran en los enlaces establecidos, con el estándar 802.16 (WIMAX) la comunicación pueden alcanzar una distancia cercana a los 50 kilómetros y la velocidad de transferencia de los datos puede llegar a los 70 Mbps.

- Seguridad: El estándar IEEE 802.16 incluye medidas para privacidad y criptografía inherentes en el protocolo. El estándar implementa la autenticación de los instrumentos con certificados x.509 usando DES en modo CBC (cipher block chaining). También soporta algoritmos AES (Advanced Encryption Standard).

3.2 CLASES DE WIMAX

3.2.1 WIMAX FIJO

El estándar del 802.16-2004 del IEEE (el cuál revisa y reemplaza versiones del IEEE del 802.16a y 802.16d) es diseñado para el acceso fijo que el uso modela. Este estándar puede ser al que se refirió como "fijo inalámbrico" porque usa una antena en la que se coloca en el lugar estratégico del suscriptor. La antena se ubica generalmente en el techo de una habitación o en el mástil, parecido a un plato de la televisión del satélite. 802.16-2004 del IEEE también se ocupa de instalaciones interiores, en cuyo caso no puede ser tan robusto como al aire libre. El 802.16-2004 para el estándar es una solución inalámbrica tiene acceso a Internet de banda ancha que provee un ínter operable, solución de clase de transportador para la última milla. WIMAX pues acceso fijo funciona desde 2.5-GHZ autorizado, 3.5-GHZ y 5.8-GHZ exento en

la licencia se agrupa. Esta tecnología le provee una alternativa inalámbrica al módem cablegráfico, las líneas digitales del suscriptor de cualquier tipo (xDSL).

3.2.2 WIMAX MOVIL – ESTANDAR 802.16 e

El estándar del 802.16e del IEEE es una enmienda para la especificación de la base 802.16-2004 y le apunta al mercado móvil sumando portabilidad y la habilidad para clientes móviles con IEEE Los adaptadores del 802.16e para conectarse directamente al WIMAX enlazan en red del estándar. Se espera que el estándar 802.16e ha sido ratificado en 2005. El estándar del 802.16e usa Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), lo cual es similar a OFDM en que divide en las subportadoras múltiples. OFDMA, sin embargo, se pasa un paso más allá para entonces agrupando subportadoras múltiples en subcanales. Una estación del cliente solo del suscriptor podría usar todos los subcanales dentro del periodo de la transmisión, o los clientes múltiples podrían transmitir con cada uno usando una porción del número total de subcanales simultáneamente. El estándar del 802.16-2004 del IEEE mejora última entrega de milla en varios aspectos cruciales:

- La interferencia del multicamino.
- El retraso difundido.
- La robustez.

La interferencia del multicamino y retraso, mejora la actuación en situaciones donde no hay una línea de vista directo entre la estación base y la estación del suscriptor. El Control de Acceso a Medios emergente del 802.16-2004 es optimizado para enlaces de gran distancia porque es diseñado para tolerar retrasos más largos y variaciones de retraso. La especificación 802.16 acomoda mensajes de la gerencia de Control de Acceso a Medios que le permiten a la estación base interrogar a los suscriptores, pero hay una cierta cantidad de retraso de tiempo. El equipo WIMAX manejando en las bandas de frecuencia exentas en la licencia usará duplicación por división de tiempo (TDD); El equipo funcionando adentro las bandas de frecuencia autorizadas usará ya sea TDD o duplicación por división de frecuencia (FDD). El estándar del 802.16-2004 del IEEE usa a OFDM para la optimización de servicios inalámbricos de datos. Los sistemas basados en los estándares emergentes del 802.16-2004 del IEEE son el OFDM base sólo estandarizado, el área metropolitana inalámbrico enlaza en red (WMAN) plataformas. En caso de 802.16-2004, la señal OFDM está dividida en 256 trasportadores en lugar de 64 al igual que con 802.11 estándar. Como previamente indicado, el mayor número de subportadoras sobre la misma banda da como resultado subportadoras más estrechas.

3.3 REDES DEL FUTURO.

El uso exitoso de WIMAX en su versión móvil como cualquier otra tecnología, no va a depender únicamente de sus méritos tecnológicos, que por sí solos prometen bastante, sino principalmente tendrá mucho que ver la implementación temprana de los sistemas celulares de nueva generación y de la versión fija de WIMAX; la pronta disponibilidad de equipamiento, y como en todo, las condiciones propicias del mercado junto con adecuados marcos regulatorios.

Pero mientras el factor tiempo lo decide todo y como la historia puede repetirse ahora con el hermano mayor de WI- FI, conviene seguir de cerca la evolución tecnológica en los casos de éxito de las pruebas durante este año y 2007; al igual que la disponibilidad de equipo certificado e interoperable para los proyectos a mediano y largo plazo, que instituciones y compañías puedan y deban tener para no quedarse atrás en la oferta de servicios con mejores prestaciones y cobertura, complementando las que se han ofrecido con la versión fija de WIMAX que puede verse como un paso previo o independiente de la móvil en función de los requerimientos de movilidad y portabilidad de las aplicaciones y servicios.

Mientras WIMAX es desarrollada más rápidamente por la apertura e interoperabilidad propia de funcionar en frecuencias desde los 450 MHZ hasta los 5.8 GHZ en bandas libres y con licencia, así como mayores anchos de banda; HSPDA, que es promovida por el grupo 3GPP [7] , ya ha sido probada y permitirá lograr mayores tasas de transmisión que los sistemas actuales.

La versión móvil de WIMAX, entre otras ventajas, funciona con normas abiertas, lo que acelerará su desarrollo al ofrecer mayor variedad de equipos interoperables, pero con la desventaja en algunas zonas, de que la infraestructura necesaria para su despliegue no está instalada como la ya existente en los países con redes de telefonía celular de tercera generación y los sistemas UMTS (Universal Mobile Telephone System).

En el caso de México, donde empresas como Axtel y Avantel ya han empezado a ofrecer servicios con WIMAX y realizado pruebas con la ayuda de fabricantes de equipo, no sería una desventaja la falta de esta infraestructura ya que existen muchos usuarios con 3G.

---

7 3GPP: 3G Partnership Project : Esta organización realiza la supervisión del proceso de elaboración de estándares relacionados con 3G.Soporte de movilidad, además de los modos de ahorro de energía y de dormir "sleep" de los dispositivos móviles.

Lo más seguro es que las nuevas tecnologías en los sistemas celulares y WIMAX móvil se complementan en algunos escenarios, y en otros ciertamente competirán pero, finalmente, se buscará permitir a los usuarios tener acceso a Internet desde puntos fijos y mantener la comunicación al estar en movimiento en medios de transporte público o en automóviles particulares, como los recientemente habilitados en Mónaco para WIMAX.

3.4 VENTAJAS DE WIMAX MOVIL

Entre algunas de las ventajas que se espera tener y que ya se están logrando con WIMAX móvil, al usar un nuevo método de modulación conocido como SOFDMA, se pueden mencionar las siguientes:
Mejor cobertura en interiores al usar AAS y MIMO.

- Uso eficiente del espectro radioeléctrico ya que permite tener mejor throughput y cobertura (hasta 50 km.), lo cual sirve para una ampliación de las redes con WI- FI.

- Operación en un amplio rango de frecuencias de los 450 MHZ a los 5.8 GHZ (inicialmente en 2.3, 2.5 y 3.5 GHZ por ejemplo en Latinoamérica).

- Escalabilidad al poder trabajar con canales de 1.25 a 10 MHZ de ancho de banda.

- Buena eficiencia a nivel de red.

- Ofrecer excelente cobertura en esquemas NLOS (por sus siglas en inglés non line of sight), usando diferentes elementos como OFDM (Orthogonal Frequency Division Multiplexing) y soportando también línea de vista o LOS (Line of Sight).

- Soporte de IPv6, QoS, VoIP, etc. al ser un sistema basado en IP.

- La tecnología de enlace aéreo es superior al usar OFDMA (Orthogonal Frequency Division Multiplexing Access) con las llamadas “antenas inteligentes“.

- Abaratamiento de costos al permitir la interoperabilidad de equipos.

- Disponibilidad en variedad de dispositivos (tarjetas PCMCIA, mini-tarjetas, módems, PDAs, teléfonos y futuros no existentes).

- En general buen desempeño en las pruebas recientes, como las realizadas en Corea en su versión denominada WiBro (Wireless Broadband) y con compatibilidad EV-DO (Evolution-Data Optimized) vía una red IPv6.

3.5 DESVENTAJAS DE WIMAX MOVIL

Sin embargo, respecto al uso de WIMAX móvil también se pueden mencionar algunas desventajas hasta el momento:

- Implementación todavía complicada por falta de elementos para tener una red móvil administrable y operable en forma eficiente.
- La falta de un marco regulatorio adecuado, por lo que los costos de las licencias pueden tener un impacto negativo.
- Requerimiento de algoritmos y funciones de procesamiento más complejos, lo que implicaría incrementar algunos costos.
- Niveles de potencia de transmisión altos.
- La cobertura puede ser menor al utilizarse un área del espectro por arriba de los sistemas 3G.
- El lapso de tiempo que se calcula entre la ratificación de la norma y la disponibilidad de equipos puede ser de un año.
- Los handoffs todavía se consideran lentos para servicios de voz.
- El 2º laboratorio para certificación de equipos en la parte móvil, estará listo en el tercer cuarto del 2006.
- El tiempo de desarrollo y despliegue de WIMAX móvil (2006-2007) todavía puede considerarse largo si se compara con el de las tecnologías recientes de los sistemas celulares como 3GSM.

3.6 WIMAX FIJO VS WIMAX MOVIL

Nota destacada: Según un informe publicado por Juniper Research, el mercado de equipos WIMAX basados en el estándar 802.16d (versión fija) se verá estancado por la aparición de la correspondiente versión móvil (802.16e). De hecho, los primeros productos certificados para WIMAX móvil se esperan para 2007. En comparación con la versión fija, el 802.16e es un estándar superior, con enorme valor añadido en movilidad, y que además ofrece una opción de conexión fija. Según las previsiones, el WIMAX móvil triunfará a nivel de usuario, mientras que la versión fija quedará relegada a conexiones back-haul (por ejemplo, para transporte de señales WI-FI de hot-spots).

Extraído de: http://www.radioptica.com/Noticias/noticia060615.asp

3.6.1 ¿QUÉ ES WiBRO?

WiBRO (Wireless Broadband) es la versión coreana del reciente estrenado estándar Mobile WIMAX (IEEE 802.16e). Por tanto, los sistemas WiBRO están basados en los estándares 802.16-2004/802.16e y utiliza la banda de los 2,3 GHZ para ofrecer comunicaciones de datos y voz sin hilos de alta velocidad.
Uno de los objetivos principales que tiene cualquier nueva tecnología inalámbrica es optimizar la utilización del espectro. En esta línea, WiBRO utiliza una única banda de frecuencias de 9 MHZ para emitir y recibir información y la comparte por división en el tiempo (TDD-Time Division Duplex), técnica muy eficiente para tráfico asimétrico como corresponde al acceso a Internet. También utilizan la técnica OFDMA como su tecnología de acceso que combina múltiples portadoras solapadas espectralmente, pero manteniendo las señales moduladas ortogonales, de manera que no se producen interferencias entre ellas y consigue minimizar las interferencias multicamino. Además, admite diversos esquemas de modulación (QPSK, 16QAM, 64QAM) y un sistema de modulación adaptativa que permiten mejorar la eficiencia de las comunicaciones. La tecnología también incluye calidad de servicio (QoS).

3.7 ¿COMO FUNCIONA?

3.7.1 TECNOLOGÍA DE ACCESO OFDM

La multiplexación por División de Frecuencias Ortogonales, también llamada modulación por multitono discreto (DMT), es una modulación que consiste en enviar la información modulando en QAM [8] o en PSK[9] un conjunto de portadoras de diferentes frecuencias.

Normalmente se realiza la modulación OFDM tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos en la transmisión, entonces esta modulación se denomina COFDM, del inglés Coded OFDM. Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles, de portadoras equiespaciadas que forman una modulación OFDM, los procesos de modulación y demodulación se realizan en tiempo discreto. A través de esta multiplexación, La tecnología de acceso WIMAX transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias.

Debido a las características de esta modulación, es capaz de recuperar la información de entre las distintas señales con distintos retardos y amplitudes (fadding) que llegan al receptor, por lo que existe la posibilidad de crear redes de radiodifusión de frecuencia única sin que existan problemas de interferencia.

---

8 Modulación digital avanzada que transporta datos cambiando la amplitud de dos ondas portadoras. Estas dos ondas, generalmente sinusoidales, están desfasadas entre sí 90° en la cual una onda es la portadora y la otra es la señal de datos. Se utiliza para la transmisión de datos a alta velocidad por canales con ancho de banda restringido.

9 Forma de modulación angular consistente en hacer variar la fase de la portadora entre un número de valores discretos

3.7.2 RANGOS DE FRECUENCIA

WIMAX funciona en tres rangos de bandas de radio: 2,4 GHZ; 3,5 GHZ y 5,8 GHZ. Los equipos pre-WIMAX que existen en la actualidad en el país trabajan en las bandas de 2,4 y 5,8 GHZ (estas tienen permiso abierto para su uso). Sin embargo, el Ministerio de Comunicaciones no ha cedido el uso de la banda de 3,5 GHZ, que ofrece un mejor desempeño para WIMAX.

De hecho, los chips de Intel para esta tecnología funcionan solo en este espectro (de 3,5 GHZ). Carlos Hurtado [10] de Intel, afirma que "es fundamental que la ley Colombiana evolucione en este aspecto y decida pronto sobre el uso de esta banda".

Según Andrés Solano [11] de S3 Wireless, el Ministerio anunció un concurso para la cesión del derecho de uso de este espectro, "situación que todos los que promovemos el negocio WIMAX estamos esperando para continuar con los planes de expansión".

3.7.3 ESTANDARIZACIÓN

WIMAX es válido para topologías punto a multipunto y, opcionalmente, para redes en malla, y no requiere línea de visión directa. Emplea las bandas de 3,5 GHZ y 10,5 GHZ, válidas internacionalmente, que requieren licencia (2,5-2,7 en Estados Unidos), y las de 2,4 GHZ y 5,725-5,825 GHZ que son de uso común y no requieren disponer de licencia alguna. Un aspecto importante del estándar

802.16x es que define un nivel MAC (Media Acces Layer) que soporta múltiples enlaces físicos (PHY). Esto es esencial para que los fabricantes de equipos puedan diferenciar sus productos y ofrecer soluciones adaptadas a diferentes entornos de uso.

3.7.4 DESCRIPCIÓN TÉCNICA DEL IEEE 802.16

El Grupo de Trabajo IEEE 802.16 ha desarrollado el estándar de acceso inalámbrico de banda ancha punto-a-multipunto para sistemas en los rangos de frecuencia de 10-66 GHZ y el sub 11 GHZ. Dicho estándar cubre el control de acceso al medio (MAC) y las capas físicas (PHY).

Se tomaron las consideraciones necesarias para las PHY del entorno objetivo. Entre más altas sean las frecuencias, la línea de vista es obligatoria. Este requisito facilita el efecto del multipath (multidireccional), permitiendo el uso de canales más anchos, típicamente mayores que MHZ en ancho de banda. Esto le da la habilidad al IEEE 802.16 de proveer enlaces de alta capacidad en el uplink y downlink. Para el sub 11 GHZ, se requiere la capacidad de funcionar sin línea de vista.

---

10 Gerente de desarrollo de negocios de Intel en Colombia

11 Director Comercial & Mercadeo de S3 Wireless Colombia

3.7.5 El MAC del IEEE 802.16

Fue realizado para acomodar diferentes PHYs y servicios. El estándar fue diseñado para acomodar cualquier despliegue de TDD (Time Division Duplexing) o FDD (Frequency Division Duplexing), permitiendo así terminales full y half-duplex en el caso de FDD.

Fue diseñado específicamente para el entorno de acceso inalámbrico PMP. Soporta capa alta o protocolos de transporte como ATM, Ethernet o Protocolo de Internet (IP), y está diseñado para fácilmente acomodar protocolos futuros que aun no hayan sido desarrollados. Está diseñado para altas velocidades (hasta 268 Mbps en ambas vías) de la verdadera capa física de la banda ancha, mientras que provee Calidad de Servicio (QoS) compatible con ATM; UGS, rtPS, nrtPS, y Best Effort

La estructura de las tramas permite a las terminales asignarles perfiles de burst dinámicos para el uplink o downlink dependiendo de las condiciones del enlace. Esto permite la compensación entre capacidad y robustez en tiempo real, otorgando así un incremento de casi el doble en la capacidad promedio al compararse con sistemas no-adaptables, mientras mantiene una apropiada disponibilidad del enlace.

MAC 802.16 utiliza un Protocolo de Unidad de Datos (PDU) de longitud variable, así como otros conceptos, los cuales incrementan grandemente la eficiencia del estándar. Múltiples PDUs de MAC pueden ser concatenados dentro de un solo burst para evitar la sobrecarga del PHY. Adicionalmente, múltiples Unidades de Datos de Servicio (SDU) para el mismo servicio pueden ser concatenados dentro de un solo PDU de MAC, evitando la sobrecarga del encabezamiento del MAC.

La fragmentación permite a los SDUs muy grandes ser enviados a través de los límites de las tramas para garantizar la QoS de otros servicios. Y la supresión de la carga del encabezamiento puede utilizarse para reducir la sobrecarga causada por las porciones redundantes de los encabezamientos del SDU.
El MAC utiliza un esquema de auto-corrección de solicitud/concesión del ancho de banda, el cual elimina la sobrecarga y el retraso de los reconocimientos (acknowledgements), mientras que simultáneamente permite un mejor manejo del QoS que los esquemas de reconocimiento tradicionales.

Las terminales cuentan con una variedad de opciones disponibles para solicitar ancho de banda, dependiendo del QoS y los parámetros de tráfico de sus servicios. Pueden ser votados individualmente o por grupos. Incluso pueden robar ancho de banda ya asignado y realizar la solicitud para obtener más. Así mismo pueden enviar señales para ser votados, y pueden piggyback [12] solicitudes de ancho de banda.

---

12 piggyback, término que se refiere a navegar por internet de gratis, utilizando la conexión inalámbrica de algún vecino.

3.8 WIMAX EN CASA

El principal componente es una antena colocada en una torre con una cobertura de hasta 7500 kilómetros cuadrados. El segundo elemento es el receptor WIMAX, que puede ir desde una caja colocada en el techo de la casa, hasta algo tan pequeño como una tarjeta PCMCIA en una computadora portátil.

Una antena WIMAX estará conectada al proveedor de Internet (ISP) por medio de fibra óptica o cable con un alto ancho de banda (30 Mbps o más) y esa misma antena, en el modelo de la telefonía celular, podrá ser el punto de acceso a la red tanto de usuarios móviles como de otras antenas funcionando como repetidoras, sin conexión por cable alguno. De esta forma, la tecnología WIMAX permitirá enlazar zonas rurales o de difícil acceso, donde las compañías de telecomunicaciones no han colocado cables por el costo de instalación o mantenimiento.

Parte fundamental de la cobertura, estabilidad e impacto de las redes MAN apoyadas en WIMAX radicará en la frecuencia de transmisión. Existen dos alternativas:

Cuando el equipo del usuario se encuentre en una zona con varios obstáculos (edificios, árboles, cerros, etcétera) se podrá usar una baja frecuencia, en el orden de los dos a 11 GHZ. Estas frecuencias son menos susceptibles a la pérdida del enlace por algún objeto que se interponga entre la antena WIMAX y el dispositivo del usuario.
El precio por pagar para mantener la conectividad, es que el ancho de banda también será inferior a los 54 Mbps.

Si existe línea de vista, es decir, cero obstáculos entre la antena WIMAX y el equipo del usuario, se podrá optar por una mayor frecuencia, hasta 66 GHZ, con el considerable incremento en el ancho de banda. La norma 802.16 establece un tope de 70 Mbps.

A partir de las variaciones en el uso de frecuencias, es claro determinar que equipos de mayor capacidad, como es el caso de los routers, preferentemente estarán asociados a una conexión de alta frecuencia con las antenas WIMAX; y los equipos de mayor movilidad, como las computadoras portátiles, seguirán asociándose a redes WI-FI o WIMAX en menores frecuencias y anchos de banda.

Fig. 7 ESQUEMA DE FUNCIONAMIENTO WIMAX [13]

3.9 USO CRECIENTE DE LA TECNOLOGÍA WIMAX EN LATINOAMÉRICA [14]

El creciente desarrollo de las tecnologías en los países latinoamericanos, ha permitido que WIMAX tenga gran acogida y sea considerado como una de las tecnologías de acceso. A continuación una relación de implementación de WIMAX en los países latinoamericanos.

En América Latina ya se ha implementado, tanto experimental como comercialmente WIMAX en varios países.

Argentina: Millicom Argentina (ahora Ertach), Alvarion e Intel se unieron para crear en el año 2004 en Buenos Aires la Primera Red WIMAX de Latinoamérica. Actualmente, Ertach junto con VeloCom, cubren con sus servicios WIMAX casi toda Argentina gracias a la rápida expansión de este tipo de tecnologías.

Colombia: la empresa Orbitel, parte de la empresa UNE y las Empresas Públicas de Medellín ofrece comercialmente el servicio en las ciudades de Cúcuta, Cali, Cartagena, Manizales, Barranquilla, Villavicencio, Medellín, Ibagué y Bogotá. Además, TeleBucaramanga, filial de Telefónica Telecom provee una red mixta de WIMAX- WI-FI en la ciudad de Bucaramanga desde el año 2005, siendo la primera en estar en el país y Latinoamérica.

---

13 Extraído de: http://mpcinco.wordpress.com/2007/10/19/funcionamiento-WIMAX/

14 Extraído de: http://es.wikipedia.org/wiki/WIMAX

Bolivia: en Bolivia, la empresa Telecel S.A con su marca TIGO, lanzo en octubre del 2007 su nuevo servicio TIGO WIMAX dando cobertura primeramente en la ciudad de Santa Cruz de la Sierra con planes de expansión a todo el territorio boliviano.

Paraguay: en Paraguay, la empresa Telecel S.A con su marca TIGO, empezó a actualizarse de la tecnologia XL a WIMAX en noviembre de 2005 dando cobertura primeramente en area metropolitana y seguidamente expandiéndose en todo el territorio.

Costa Rica: la compañía Radiográfica Costarricense (RACSA) ofrece el servicio WIMAX desde junio del 2006. Inició comercializando el servicio desde 512 kbps en adelante para su primera etapa de implementación en el Gran Área Metropolitana (en San José y otras grandes urbes como Alajuela, Cartago y Heredia). El Instituto Costarricense de Electricidad (ICE) prevé extender el acceso inalámbrico a Internet hacia la mitad del país para los primeros meses del 2009. La red del ICE cubrirá no solamente el Gran Área Metropolitana, sino también poblaciones importantes del Pacífico Norte, Central y Sur, así como la Zona Norte y el Caribe.

Chile: Telmex inició oficialmente la comercialización de planes de Internet Banda Ancha y Telefonía, a través de la primera red inalámbrica nacional, con tecnología WIMAX a través de equipos Alcatel y Alvarion. El martes 20 de marzo de 2007. Lanzó esta innovadora tecnología en el país para las PYMES. Telmex recibió la autorización que le ha permitido desarrollar la infraestructura necesaria para ofrecer esta tecnología en Chile. Desde marzo la empresa inicia su campaña para comercializar Internet Banda Ancha y Telefonía Inalámbrica en las ciudades de Santiago, Concepción, Talcahuano, Curicó, Iquique, La Serena, Coquimbo, Linares, Ovalle, Rancagua, Talca, Temuco, Valdivia, Valparaíso y Viña del Mar. Tambien se encuentra operando en Calama, Osorno, Puerto Montt, Requinoa y Punta Arenas. La tecnología inalámbrica de Telmex esta en el 98 por ciento de las comunas de Chile, incluyendo Isla de Pascua. Telmex desde el mes de julio comenzó a comercializar esta tecnología en el sector Hogar. En octubre de 2007 Telmex amplió su tecnología WIMAX con WIMAX Movil "e". ENTEL (Empresa Nacional de telecomunicaciones) en junio del 2007 comenzó con sus primeros pasos comercializando WIMAX a las pequeñas y grandes empresas.

Venezuela: en Venezuela, Omnivisión desplegó la red WIMAX en Caracas junto a Samsung en la banda de 2.5 GHZ, sin embargo, recientemente CONATEL (ente regulador de las telecomunicaciones en ese país) asignó las bandas de 3.5 y 3.7 GHZ para el uso de esta tecnología, lo que ha retrasado un poco el lanzamiento comercial. Samsung Electronics Co. Ltd, proveedor de sistemas de Telecomunicaciones y Omnivisión C.A. operador de televisión han desarrollado el servicio WIMAX móvil en Venezuela bajo la marca MOVILMAX. El acuerdo fue firmado el 16 de diciembre 2005, convirtiendo a Omnivisión en uno de los primeros operadores en Latinoamérica en instalar servicio WIMAX móvil de Banda Ancha Personal. En enero de 2007 MOVILMAX pasó a formar

parte de la junta de directores de WCA (Wireless Communications Association International), organismo encargado de velar por los intereses de los proveedores inalámbricos que ofrecen datos a alta velocidad, Internet, servicios de voz y vídeo en espectro de banda ancha utilizando dispositivos de recepción/transmisión a lo largo del espectro de banda ancha. Actualmente esta empresa presta servicio de WIMAX movil, un estándar de última generación y que por ahora está disponible en pocos lugares del mundo.

El Salvador: en El Salvador, Telecom (del grupo América Móvil) inició el servicio de WIMAX en junio de 2007 y Telefonica Moviles ya cuenta también con su propia red WIMAX, cuyo servicio podría lanzarse antes de agosto de 2007, Salnet desplegara su red WIMAX a principios de octubre de 2007.

México: en México, AXTEL pertenece a WIMAX Forum y esta en vias de implementación. En la ciudad de Monterrey, Nuevo León (la tercera más extensa del país), habrá más de 100 puntos de acceso a Internet inalámbrico de banda ancha gratuitos en parques, jardines y bibliotecas. Además, el Parque Fundidora y la Macro Plaza, ya cuentan con conexión a internet gratis. En las ciudades de Puebla, Aguascalientes y Veracruz ya se comercializa WIMAX a través de Ultranet2go, miembro del grupo empresarial Ultra Telecom. En próximos meses Ultranet2go llegará a Coatzacoalcos, Tampico, Iguala, Cuernavaca, Xalapa y Matamoros.

Ecuador: Intel ha firmado un acuerdo con la Estación Científica Charles Darwin en Galapagos, Ecuador, para implementar un proyecto piloto de interconexión WIMAX entre las diferentes islas que conforman el archipiélago.CONATEL es el ente regulador de las telecomunicaciones en Ecuador. Operadores como SETEL y ECUADORTELECOM (recientemente adquirida por el grupo TELMEX) tienen previsto desarrollar redes metropolitanas con tecnología WIMAX en las ciudades de Quito y Guayaquil.

República Dominicana: en República Dominicana Tricom, empresa telefónica de capital privado, ha anunciado la implementación del servicio WIMAX exclusivamente a sus clientes de negocios en su primera etapa; la misma estará disponible en Bavaro, Haina y Santo Domingo Norte, Oeste y Distrito Nacional. La empresa ONEMAX ofrece servicios interactivos de voz y datos a clientes en general utilizando la tecnología WIMAX. Tambien Wind Telecom se apresta a ofrecer servicios WIMAX en este pais.

Uruguay: en Uruguay la empresa de telecomunicaciones privada Dedicado, junto a Intel están trabajando actualmente en el proyecto WIMAX para toda Montevideo y parte de la Costa de Oro, durante el 2007 el servicio podría quedar activo.

Perú: la primera empresa en instalar WI MAX en Lima (2004) TCS21S.A. E-MAX tenía 2000 usurarios a pricipios del 06 instala cobertura Basica de LIMA MTRO en setiembre 2007. Telefónica del Perú en la actualidad ya tiene más de 18 celdas de WIMAX de la marca Airspan. La empresa TELMEX PERU, ha

implementado el servicio EXPLORA también con tecnologia WIMAX, brindando paquetes integrales de Telefonia, Acceso a Internet en Banda Ancha y Transmision de datos.

Guatemala: la primera empresa en instalar WIMAX en Guatemala fue UNITEL bajo la marca Yego durante 2005, seguida meses más tarde por pruebas del servicio sin lanzamiento aun de Telecomunicaciones de Guatemala (TELGUA, parte de América Móvil).

3.10 USOS Y APLICACIONES DE WIMAX

3.10.1 AUTOMÓVILES ELÉCTRICOS CON CONEXIÓN WIMAX

Los primeros vehículos deportivos eléctricos tendrán conectividad WIMAX de serie. Los va a fabricar una empresa de Mónaco, Venturi Automobiles, que pretende así poder realizar un mantenimiento a distancia e incluso controlar la situación del coche en todo momento. Su nombre, Fétish. Tendrá dos procesadores Intel XScale encargados de controlar las baterías, un reproductor iPod y un GPS. Eso sí, el precio no ayudará a popularizar el WIMAX: un cuarto de millón de dólares.

3.10.2 SAMSUNG PRESENTA LOS PRIMEROS TERMINALES Y SISTEMAS WIBRO (MOBILE WIMAX) EN LA EXPOSICIÓN APEC IT 2005 [15]

Samsung, proveedor coreano líder en sistemas de telecomunicaciones y telefonía móvil, será una de las empresas pioneras en ofrecer la tecnología WIMAX, haciendo un avance de sus innovadores sistemas y teléfonos móviles WiBro (Wireless Broadband, nombre coreano de la marca Mobile WIMAX)

Manteniendo su tendencia de liderazgo en el sector de las telecomunicaciones, presentó en la exposición APEC IT 2005, además de una amplia gama de aplicaciones, tales como acceso banda ancha, hogar digital, video telefonía, VOD y navegación, los primeros sistemas y teléfonos móviles WiBro & endash;versión coreana de la marca Mobile WIMAX- del mundo: los modelos H1000 (con aspecto de teléfono móvil) y M8000 (con aspecto de PDA).

El modelo WiBro H1000 destaca por su diseño en forma de concha que ofrece la posibilidad de apertura horizontal y vertical de su teclado QWERTY. Su amplia pantalla de 2.2 pulgadas optimiza las prestaciones de e-mail e Internet del teléfono. Además, el H1000 tiene cámara dual (2 megapixels y VGA) y la función de TV Output (salida directa a TV). En cuanto al modelo WiBro M8000, se trata de un elegante teléfono de tipo PDA equipado con un teclado QWERTY que facilita el uso del servicio de email. Además, Samsung lanzará una tarjeta WiBro PCMCIA para equipos portátiles y PCs de sobremesa.

---

15 Nota extraída de: http://www.tecnoWIMAX.com/category/WIMAX-movil/

Kitae Lee, Presidente y CEO del Negocio de Telecomunicaciones de Samsung afirma: “Estamos orgullosos de presentar los primeros terminales WiBro del mundo y los últimos teléfonos DMB a los asistentes al encuentro APEC IT 2005. Los servicios WiBro empezaron a comercializarse en Corea a partir del año 2006. De esta manera, Samsung liderará este mercado, ofreciendo productos innovadores a sus consumidores, y dará un paso más allá en el compromiso de la compañía por facilitar la vida de sus clientes.”

3.10.3 EXPECTATIVAS FINALES SOBRE ESTA TECNOLOGIA

IEEE 802.16e, el WIMAX móvil Aunque con la publicación oficial del estándar 802.16-2004 se asentaron las bases para el despliegue inicial de la nueva tecnología de acceso de banda ancha sin hilos, las expectativas finales de WIMAX van más allá de ser un sistema de tipo ADSL inalámbrico para entornos urbanos y rurales. Realmente los promotores de este proyecto persiguen la ambiciosa meta de que WIMAX sea la tecnología inalámbrica que unifique el mundo de la telefonía móvil y las redes de datos. Con este objetivo, en diciembre 2002, fue creado el Grupo de Trabajo IEEE 802.16e para mejorar y optimizar el soporte para la combinación de las capacidades de comunicación tanto fijas como móviles en frecuencias por debajo de los 6 GHZ. Cumpliendo el calendario previsto, el pasado 7 de diciembre de 2005 se realizó la ratificación oficial del nuevo estándar WIMAX Móvil (802,16e). La nueva versión del estándar introduce el soporte de la tecnología SOFDMA (una variación de la técnica de modulación OFDMA) el cual permite un número variables de ondas portadoras, que se añade a los modos OFDM y OFDMA ya existentes. Además, IEEE 802.16e ofrece un soporte mejorado de las tecnologías MIMO (Multiple Input Multiple Output) y AAS (Adaptive Antenna Systems). También, incluye mejoras para la optimización del consumo de energía para los dispositivos móviles y con ello disminuir con ello el tamaño del módem CPE (Customer Premise Equipment), así como extensas características de seguridad.

Por último, también existen los grupos de trabajo de IEEE 802.16f e IEEE 802.16g que se encargan de las interfaces de administración de la operación fija y móvil. Donde esta ultima constituye la puerta de entrada para lograr la tan esperada red de la nueva generación, la cual debe permitir desarrollar toda la gama de servicios IP multimedia de nueva generación (comunicaciones VoIP nueva generación, video comunicación, mensajerías integradas multimedia, integración con servicios IPTV, domótica, etc.) así como la evolución, migración en términos más o menos de sustitución o emulación de los actuales servicios de telecomunicación. Cabe aclarar que para lograr llegar a NGN, también hay que tener muy en cuenta la implementación de un servicio complejo a nivel fijo y sobretodo siempre centrado hacia la integridad de los datos.

CAPITULO 4

4.1 SEGURIDAD EN LAS REDES INALAMBRICAS

Como se sabe, la seguridad en redes inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado. Asimismo se toma esta medida de aseguramiento para redes de mayor cobertura como WIMAX. En este capítulo se explicaran métodos de autenticación y aseguramiento para las redes inalámbricas en general.

Los tres aspectos fundamentales que se deben tener en cuenta al analizar e implementar una red inalámbrica segura, son:

- Autenticación
- Control de acceso
- Confidencialidad

4.2 MECANISMOS DE SEGURIDAD

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle.
Existe el término “wardriving”, que se refiere a la acción de recorrer una ciudad para buscar la existencia de redes inalámbricas y ganar acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes.

El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable). Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica.

4.2.1 SISTEMA DE SEGURIDAD A TRAVÉS DE UN DMZ

Un DMZ, o zona desmilitarizada, es un concepto de protección. Define típicamente donde poner servidores que accedan a Internet. En otros términos, un servidor de Web o el servidor del correo es a menudo fijo a en un DMZ. Esto

le permite a cualquier usuario de Internet acceder los recursos asignados en el servidor, pero si el servidor esta fuera del DMZ, un Hacker no podrá usar la computadora Hackeada para investigar el resto de la red. Técnicamente, un DMZ realmente es nuestra propia pequeña red, separada de la red interior, y separada del Internet. Este concepto es muy útil y costoso pero de igual forma es una alternativa muy implementada en las grandes empresas por el nivel de seguridad que puede ofrecer siempre y cuando sea bien implementado.

Un cortafuego protegerá el DMZ de las amenazas externas. Sin embargo, debido a que el servidor se debe comunicar al mundo externo, el cortafuego se configurará para ignorar muchos tipos de conexiones. Además de aislar los servidores, el DMZ es configurado para ser fácilmente accesible a los usuarios de la red interna. Esto es realizado por el hardware y software del cortafuego que normalmente vienen con un puerto ubicado al lado sólo para colocar un DMZ. Por ejemplo, NetScreen tiene tres puertos: uno para la conexión a Internet, el segundo para la conexión interna, y el tercero para un DMZ en que un hub o switch puede conectarse para permitir múltiples servidores.

Este mismo puerto podría usarse para conectar un punto de acceso que realmente nada más que un hub/switch inalámbrico. Haciendo esto, usted está poniendo el WLAN básicamente en una zona semi-confiada que se espera que sea atacada por los Hackers. Operando con la mentalidad de que su WLAN ya podría ser atacada, se puede planear más apropiadamente a quien y a que se le permite acceder la red interna. Sin embargo, mientras este tipo de protección ayuda a proteger los recursos internos, no protegerá a los usuarios de la red inalámbrica. Por consiguiente, el DMZ debe ser simplemente una parte de su plan de seguridad inalámbrico, es decir, serviría como refuerzo a implementaciones de seguridad que se deben tener en cuenta para los usuarios de la red.

4.2.2 LOS MÉTODOS DE SEGURIDAD TERCERISTAS

Al usar las medidas de seguridad como las que se venían hablando, ayudarían a asegurar la WLAN, el hecho simple es que esto no es suficiente para la seguridad en ambientes dónde se necesita mayor privacidad. Para situaciones como ésta, hardware y/o software adicional pueden ser implementados mediante productos terceristas. Integrando estos productos con las tecnologías existentes, la WLAN puede convertirse prácticamente impenetrable.

4.2.2.1 LOS CORTAFUEGOS

En pocas palabras, una WLAN debe ser considerada insegura y como parte del Internet público. Así que si se diseña una red inalámbrica con esta perspectiva, se debe usar un cortafuego para separar a los usuarios de la red inalámbrica de los usuarios internos.

Un cortafuego puede hacer mucho para eliminar las amenazas de seguridad. Dependiendo de cómo esté configurado y que tipos de políticas se estén usando, un cortafuego puede bloquear eficazmente todas las peticiones entrantes que no están autorizadas. Esto crea una barrera física contra los

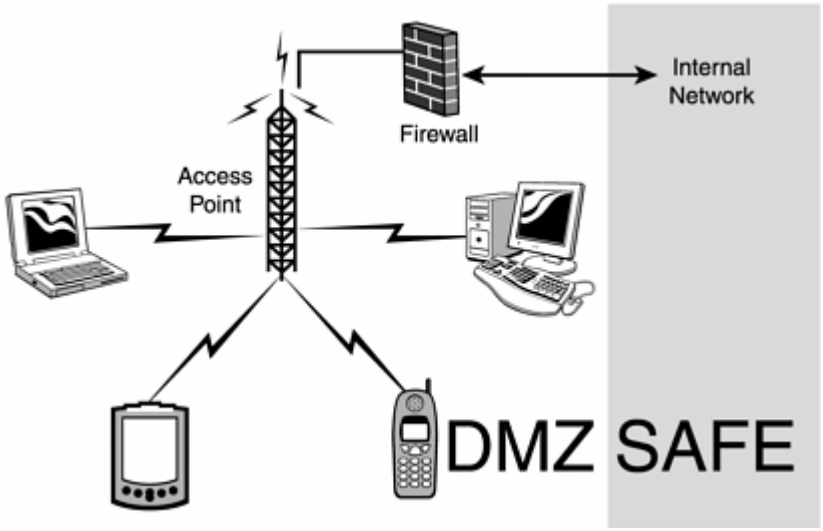
Hackers que podrían tener control sobre la red inalámbrica y podrían estar intentando abrir una brecha hacia la red interna.

Al seleccionar un cortafuego para la parte inalámbrica de su LAN, la mejor opción es usar un cortafuego del hardware especializado, o simplemente usar uno de los cortafuegos principales que protejan la conexión existente a Internet. Debido a que el punto de acceso debe estar ubicado fuera de un DMZ, puede conectarse simplemente al puerto de DMZ en cualquier de los cortafuegos más grandes.

Con esta perspectiva, es importante configurar correctamente las políticas de seguridad en el cortafuego. Uno de los problemas más comunes con el complejo equipo es la posibilidad de desconfiguración. La razón por la cual se recomienda usar un cortafuego especializado ya que uno mismo podría configurarlo para bloquear todo, y luego dejar correr estas configuraciones. Aunque es posible que el cortafuego principal corporativo del Internet, sea la opción menos atractiva. Además, un usuario base de la red inalámbrica probablemente será muy menor, lo que le permite al administrador mantener un nivel más íntimo de administración de las políticas y configuraciones usadas para controlar a los usuarios.

Fig. 8

WLAN USANDO UN CORTAFUEGO CON UNA DMZ [16]



16 imagen Extraída de: Maximum Wireless Security

4.2.2.2 LAS VPNs

Al hablar de los cortafuegos, también vale la pena mencionar las VPNs. Una VPN es una red virtual, encriptada, que se construye encima de una red existente. Esto también está conocido como tunneling, porque el flujo de datos encriptados es fijo y se mantiene dentro de una conexión normal y sin encriptar. Una VPN extiende la red interior segura fuera al usuario remoto. Por consiguiente, el usuario inalámbrico remoto existe en ambas redes al mismo tiempo. La red inalámbrica permanece disponible, pero un túnel de VPN se crea para conectar al cliente remoto a la red interior, mientras también hace que todos los recursos de la red interior estén disponibles.

La razón por la cual se habla de VPNs con cortafuegos es porque estos suelen integrarse a una aplicación o paquete de software. Debido a esto, un cortafuego puede configurarse para bloquear completamente todas las peticiones entrantes, con la excepción de clientes de VPN autorizados. Esto no sólo asegurará una medida fuerte de seguridad al punto de acceso, sino que también proporcionará una medida adicional de seguridad a los usuarios de WLAN, incluyendo sus datos.

La encriptación usada por la mayoría de las aplicaciones de WEP tiene debilidades. Un Hacker con una computadora portátil y una lata de Pringles para una antena puede sentarse dentro de la zona de la radiación de la WLAN y puede capturar la información suficiente para vulnerar la contraseña del WEP. Teniendo esta contraseña, el hacker puede configurar su computadora para capturar todos los datos que viajan a través del aire. Después de haber obtenido la contraseña de encriptación, este puede descifrar todos los datos WEP-protegidos y puede "ver" la información. El correo electrónico, documentos, y contraseñas pueden ser espiados de esta manera.

Sin embargo, usando la encriptación de VPN además de la encriptación de WEP, un hacker tendría que descifrar los datos dos veces. La primera capa es crackeable de encriptación del WEP, y la segunda es la capa robusta de encriptación de la VPN. Por tal motivo un hacker no podría descifrar tan fácilmente el password, certificado, o la clave de la tarjeta inteligente de la VPN, la tasa de éxito para crackear el tráfico de VPN será muy baja.

Aunque usando tanto VPN como WEP queda definitivamente a su criterio, hay un mayor inconveniente. El problema se genera como resultado del proceso adicional causado por el encriptando y descifrado de los datos dos veces: primero de WEP, y entonces del VPN. Usando WEP con VPN en un cortafuego/ access point propiamente configurado afecta la velocidad de transmisión y rendimiento en un 80%. En otras palabras, tomaría 10 minutos para enviar un archivo en una VPN con WEP habilitado, pero tomaría sólo 2 minutos sin la encriptación. Este impacto puede tener consecuencias serias en

la conectividad de la red, y eliminar el entusiasmo del usuario final por la conexión inalámbrica.

Además, usar VPN en una red inalámbrica requiere que el software del cliente sea instalado en cada maquina por usuario. Este requisito crea problemas para los usuarios finales. Por ejemplo, la mayoría del software de VPN es escrito para la plataforma de Windows. Esto significa Macs, las computadoras basadas en nix, y las palmtop no se podrían conectar a la WLAN. Aunque éste no podría ser un problema para la mayoría de los hogares y negocios pequeños, esto solo podría tener un impacto serio en las corporaciones que crecen rápidamente.

4.3 SEGURIDAD EN BLUETOOTH

4.3.1 MODOS DE SEGURIDAD

Hay tres modos primarios de seguridad.

4.3.1.1 MODO 1: SIN SEGURIDAD

Todos los mecanismos de seguridad (autenticación y cifrado) están deshabilitados. Además el dispositivo se situa en modo promiscuo, permitiendo que todos los dispositivos BLUETOOTH se conecten a él.

4.3.1.2 MODO 2: EN LA CAPA L2CAP, NIVEL DE SERVICIOS

Los procedimientos de seguridad son inicializados después de establecerse un canal entre el nivel LM y el de L2CAP. Un gestor de seguridad controla el acceso a servicios y dispositivos. Variando las políticas de seguridad y los niveles de confianza se pueden gestionar los accesos de aplicaciones con diferentes requerimientos de seguridad que operen en paralelo.
Su interface es muy simple y no hay ninguna codificación adicional de PIN o claves.

4.3.1.3 MODO 3: EN EL NIVEL DE LINK

Todas las rutinas están dentro del chip BLUETOOTH y nada es transmitido en plano. Los procedimientos de seguridad son iniciados antes de establecer algún canal. Aparte del cifrado tiene autenticación PIN y seguridad MAC. Su metodología consiste en compartir una clave de enlace (clave de linkado) secreta entre un par de dispositivos. Para generar esta clave, se usa un procedimiento de “pairing” cuando los dos dispositivos se comunican por primera vez.

4.4 DEBILIDADES DE LA SEGURIDAD

4.4.1 GENERALES

- No está demostrada la fuerza del generador pseudoaleatorio del procedimiento “challenge-Response”. Se podrían producir números estáticos o repeticiones periódicas que redujeran su efectividad.

- PINs cortos son permitidos. De hecho se puede elegir la longitud del PIN, que va de entre 1 a 16 bytes. Normalmente los usuarios los prefieren muy cortos.

- No hay una forma “elegante” de generar y distribuir el PIN. Establecer PINs en una red BLUETOOTH grande y con muchos usuarios puede ser difícil, y esto lleva normalmente a problemas de seguridad.

- La longitud de la clave de cifrado es negociable. Es necesario un procedimiento de generación de claves más fuerte.

- En el caso del modo 3, la clave maestra es compartida. Es necesario desarrollar un esquema de transmisión de claves mejorado.

- No existe autenticación de usuarios. Sólo está implementada la autenticación de dispositivos.

- No hay límite de intentos de autenticación.

- El algoritmo de cifrado por bloques E0 es muy débil. Más tarde se analiza.

- La autenticación es un simple “challenge-response” con hashes. Según esta diseñado, el esquema es vulnerable a ataques “Man in the Middle”.

- Los servicios de seguridad son limitados. Servicios de auditoria, de no repudio, etc, no están implementados.

4.4.2 VULNERABILIDADES DEL CIFRADO.

Dejando aparte de que el cifrado es opcional, veremos que además acaece de varias vulnerabilidades.
El algoritmo de cifrado por bloques E0 es débil. Aunque se perfilaba como relativamente seguro hace pocos años. Su sistema de creación del Stream para el cifrado es mucho más complejo, y soluciona los problemas de reutilización de claves como el que tiene el RC4 del wifi (802.11b). Sin embargo, como con todos los algoritmos de cifrado, su seguridad va cayendo paulatinamente.

Aunque E0 permite longitudes de clave que van desde 1 hasta 16 bytes (8-128 bits), Jakobbson y Wetzel presentaron un ataque con complejidad matemática de O(2^100) (esto es el equivalente a reducir la longitud de clave efectiva de 128 a 100 bits).

Posteriormente Fluhrer y Lucks presentaron otro ataque que requería desde O(2^73) hasta O(2^84), dependiendo de la cantidad de keystream capturado.

Hasta aquí podríamos decir que las posibilidades de ataque de recuperación de la Clave de Cifrado no eran efectivas, considerando que para conseguir un O(2^73) había que tener unos 14.000 gigas de keystream.
Pero luego los ataques se fueron perfeccionando, hasta que en 2004, Yi Lu y Serge Vaudenay presentaron un nuevo ataque de correlación, que resuelve en O(2^37) con una cantidad de keystream consecutivo de 64 gigas, mejorándolo en el CryptoAsia 2004 a 2^40 operaciones simples solo con los primeros 24 bits de 2^35 frames.

Uso parcial del reloj. Como hemos visto, el reloj del dispositivo maestr es un parámetro de entrada para la generación del Stream de cifrado. Aunque parece que por un fallo de diseño el bit más significativo de su valor es ignorado, permitiendo este hecho entre otras cosas ataques tipo Man in The Middle.

Los datos cifrados pueden ser manipulados. Incluso con el cifrado más fuerte, las características de los cifrados de Stream permiten que los datos interceptados en un ataque Man in The Middle puedan ser convenientemente manipulados dependiendo de la cantidad de texto cifrado conocida. Así es posible por ejemplo manipular cabeceras IP.

4.4.3 VULNERABILIDADES DE LA SEGURIDAD.

Son debidas principalmente a prácticas de codificación errónea en el desarrollo de los servicios RFCOMM, al desconocimiento de los protocolos de seguridad BLUETOOTH y demás (OBEX), y a la reutilización de servicios antiguos para protocolos diferentes.

4.4.3.1 PERMISOS IRMC

IrMC define los permisos de acceso para los objetos comunes.
Hay objetos visibles aunque el servicio sea “no emparejado”.
Servicios abiertos intencionadamente.

4.4.3.2 ERRORES DE PILA

- Buffer Overflows.
- Fallos en la implementación de servicios como en el chequeo de la longitud de datos o la integridad de paquetes en OBEX, o terminaciones NULL.

4.4.3.3 SERVICIOS OCULTOS

Servicios con los más altos privilegios se dejan abiertos pero escondidos.
Canales traseros para hacerle la vida más fácil a otros dispositivos.
Acceso completo al comando AT, y por lo tanto a todo el dispositivo.

4.5 SEGURIDAD EN REDES WI-FI

La seguridad en redes WI-Flabarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquéllos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).
Para las WLANs, el primer paso en el endurecimiento de la seguridad es enfocarse en el punto de acceso. Puesto que el AP es lo más fundamental en la transferencia de datos de LAN inalámbricas, debemos asegurarlo, ya que es la parte de la solución, en lugar del problema.
Estos “hoyos” en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red alámbrica a la cual se conecta. La tabla siguiente contiene los mecanismos de seguridad usados en redes WLAN, así como las ventajas y desventajas de cada uno de ellos.

4.5.1 MECANISMOS DE SEGURIDAD PARA REDES WI-FI

TABLA 4.

Mecanismo de seguridad	Descripción
Especificación original 802.11	Utiliza tres mecanismos para proteger las redes WLAN: - SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para accesar a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía

	(beacon). - Filtrado con dirección MAC (Control de Acceso al Medio): restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico. - WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación WI-FIexige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.
802.1X	Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que

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

Tabla extraída de:
http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm

4.6 MÉTODOS DE AUTENTICACIÓN EN LAS REDES INALÁMBRICAS

4.6.1 AUTENTIFICACIÓN POR MAC

El AP comprueba la MAC del cliente antes de permitir el acceso. Las MAC pueden configurarse tanto en el AP como en un ACS. En este momento el Àccess Point, por ejemplo un Aironet de Cisco utiliza un servidor RADIUS para autentificar las MAC de los clientes en los SSID's correspondientes. La dirección MAC de un cliente legítimo puede ser capturada por un atacante. Las tarjetas Orinoco (y todas las que tienen un chipset prism) permiten la modificación de su MAC. Con este sistema se podría establecer un filtro que obligase a utilizar encriptación en SSL o a nivel de aplicación (pop3s, imaps, SSH, HTTPS) y HTTP.

4.6.2 AUTENTIFICACIÓN EAP

Protocolo extensible de autentificación. Es un protocolo que sirve para adaptar a las redes inalámbricas protocolos ya establecidos y otros nuevos. Este sistema requiere siempre un ACS. EAP utiliza dos WEP como claves de sesión que las partes implicadas acuerdan durante la autentificación y que se cambia con una frecuencia que determina el administrador del AP. Un WEP es para el tráfico broadcast y otro se establece para cada cliente de manera que los clientes no pueden escucharse mutuamente. Yo considero que este mecanismo es muy seguro. La política de filtros para esta autentificación podría ser completamente abierta.

4.6.3 EAP-MD5

Mediante EAP se autentifica realizando un intercambio de claves "cifradas" por MD5. El autentificador puede ser nombre de usuario y contraseña o una dirección MAC. Linux y WinXP pueden asociarse por este método. Con WinXPSP1 desaparece la autentificación EAP-MD5 que es sustituida por EAP-MS-CHAPv2 aún no soportada por algunos equipos, como el freeradius.

4.6.4 EAP-TLS

TLS: Seguridad en la capa de transporte. La autentificación se realiza mutuamente mediante certificados. Con este sistema tanto el ACS como el cliente deben demostrar su identidad. Sólo WinXPSP1 soporta este método. WinXP lo hace defectuosamente. Esta configuración es para el AP "raíz". La red se extiende fácilmente manteniendo estas configuraciones sin más requerimientos que asociar correctamente los puntos de acceso que funcionan como repetidores.

4.6.5 OTROS MÉTODOS DE SEGURIDAD

4.6.5.1 TKIP (Temporal Key Integrity Protocol):

Al contrario que WEP, utiliza claves de sesión dinámicas de 128 bits, para cada usuario, cada sesión y cada paquete. Los usuarios deben acceder a través de un servidor de autentificación, típicamente un RADIUS. Una vez autentificados mutuamente el servidor genera una clave “master” que transmite de manera segura al cliente y que será utilizada para enviar el resto de claves auxiliares

que serán utilizadas durante esa sesión. Esta propuesta aparece a finales de 2002, también se basa en RC4, pero propone tres mejoras importantes:

4.6.5.2 COMBINACIÓN DE CLAVE POR PAQUETE: La clave de cifrado, se combina con la dirección MAC y el número secuencial del paquete. Se basa en el concepto de PSK (Pre-shared Key). Esta metodología, genera dinámicamente una clave entre 280 trillones por cada paquete.

4.6.5.3 VI (Vector de inicialización) de 48 bits: Esta duplicación de tamaño implica un crecimiento exponencial del nivel de complejidad, pues si 24 bits son 16 millones de combinaciones, 48 bits son 280 billones. Si se realiza un gran simplificación (pues el caso es más complejo) y se divide 280 billones sobre 16 millones, el resultado es: 17.500.000, por lo tanto si un VI de 24 bits se repite en el orden de 5 horas en una red wireless de una mediana empresa, entonces un VI de 48 bits = 5 x 17.500.00 horas = 87.500.000 horas = 3.645.833 días = 9.988 años, es decir se repetiría después de la Guerra de las Galaxias. Ya se pone complicada la cosa.

4.6.5.4 MIC (Message Integrity Check): Se plantea para evitar los ataques inductivos o de hombre del medio. Las direcciones de envío y recepción además de otros datos, se integran a la carga cifrada, si un paquete sufre cualquier cambio, deberá ser rechazado y genera una alerta, que indica una posible falsificación del mismo.
Desafortunadamente TKIP, no está contemplado aún en la totalidad de los productos.

MIC (Message Integrity Check) : Se trata de un sistema que garantiza que un paquete no ha sido modificado en tránsito.

Con WPA desaparece el problema de las claves compartidas, ya que una clave “master” distinta es recibida por cada usuario cada vez que RADIUS acepta sus credenciales. Con este sistema el administrador puede aceptar o eliminar usuarios del sistema sin necesidad de cambiar todas las claves.
Con WPA tenemos las tres cuestiones que definen la seguridad resueltas de manera robusta:

- RADIUS provee la autentificación.
- TKIP la privacidad.
- MIC la integridad.

4.6.5.5 SOHO (Small Office and Home Office)
Los usuarios que no deseen usar un servidor de acceso pueden seguir utilizando el sistema de clave compartida, ya que WPA lo permite, aunque sin necesidad de preocuparse por los problemas de seguridad de WEP.

Hasta la fecha la única vulnerabilidad que se ha descrito referente a WPA se refiere a sistemas que han sido establecidos con SOHO y claves PSK demasiado cortas y/o vulnerables a ataques por diccionario.

4.7 SEGURIDAD EN REDES WIMAX

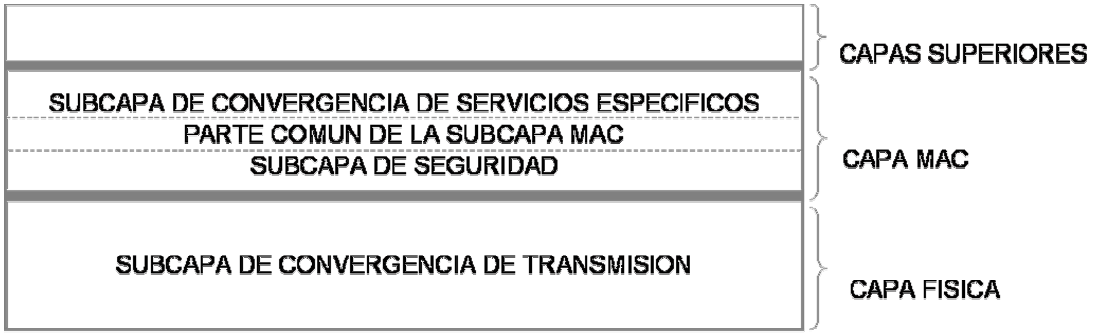
Como cualquier otra red de comunicación al servicio de empresas y usuarios individuales que desean mantener su información segura, los sistemas WIMAX necesitan aplicar medidas para asegurar la privacidad de sus usuarios finales y prevenir del acceso a información confidencial o sensible a personas que no están autorizadas.

Desde que los sistemas WIMAX utilizan el interface radio como medio de transmisión, la pregunta que conviene hacerse es cómo prevenir que los intrusos no intercepten información sensible y confidencial transmitida por ondas hertzianas ya sea en banda libre o banda licenciada.

Tanto los clientes como los operadores deberían sentirse protegidos y confiar en que su sistema es privado y seguro, y que las medidas apropiadas están disponibles para minimizar los riesgos de seguridad, incluyendo:

Fig. 9

ESTRUCTURA DE UNA RED WIMAX/BWA



Escuchas/espionaje: interceptar información de forma intencional cuando se está transmitiendo.

Privacidad: Asegurarse de que la información transmitida es solamente leída por los destinatarios a los que va dirigida.

MAC Spoofing: evitar que un atacante copie las direcciones MAC de CPE legítimas con el fin de conseguir el acceso a la red.
Robo del Servicio: prevenir que los agresores puedan acceder a Internet u otros servicios utilizando CPE robadas y advirtiendo a los usuarios legítimos de obtener los servicios de forma gratuita.

4.7.1 PRINCIPALES CONSIDERACIONES

El estándar WIMAX requiere de las mejores características de seguridad en su clase, lograda gracias a la adopción de las mejores tecnologías disponibles actualmente. Las características de seguridad son independientes al tipo y a la topología de la red de acceso. En este sentido, el estándar aborda las cuatro áreas principales a tener en cuenta: cómo prevenir el uso clandestino de la conexión wireless; denegación de servicios para unidades robadas o utilizadas de forma fraudulenta; suministrar servicios sólo a los usuarios finales específicos; y cumplir con la Gestión de Acceso Seguro.

Respecto a cómo prevenir la utilización clandestina de la conexión wireless, la clave está en la encriptación.

La seguridad WIMAX soporta dos estándares de encriptación de calidad, DES3 y AES, que es considerado tecnología de vanguardia. Básicamente, todo el tráfico en redes WIMAX debe ser encriptado empleando el Counter Mode con Cipher Block Chaining Message Authentication Code Protocol (CCMP) que utilizan AES para transmisiones seguras y autenticación de la integración de datos.

CCMP, es complementario al TKIP y representa un nuevo método de encriptación basado en AES (Estandar de encriptación avanzada), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC – MAC. Asi como el uso del TKIP es opcional, la utilización del protocolo CCCMP es obligatorio si se esta utilizando 802.11 i

Fig. 10

ENCRIPTACIÓN CCMP [17]

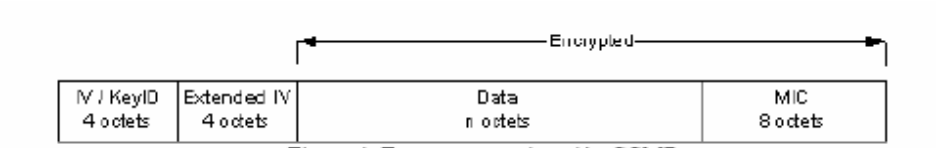


Figura 4: Estructura encriptación CCMP

CCMP utiliza un IV de 48 bits denominado número de paquetes (PN) utilizado lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

17Extraido de: http://documentos.shellsec.net/otros/SeguridadWireless.pdf

4.7.2 AES - ADVANCED ENCRYPTION STANDARD

Es uno de los mas modernos métodos de encriptación seleccionado por el gobierno americano para reemplazar a su estándar DES. Es bastante fuerte, y realmente está bajo la revisión para la próxima versión inalámbrica 802.11 norma (802.11i). De hecho, aunque aun no es oficialmente soportado por todos los hardware de WLAN, ciertos fabricantes han empezado a implementarlo

4.7.3 AUTENTICACION END TO END

La autenticación end-to-end del método PKM-EAP (Protocolo de Autenticación Extensible) es utilizada de acuerdo con el estándar TLS de encriptación de clave pública.

El estándar define un proceso de seguridad dedicada en la estación base para los principiantes. Del mismo modo, también hay unos requerimientos de encriptación mínimos para el tráfico, así como para la autenticación end-to-end -lo último que es adaptado desde la especificación del interface del servicio de datos sobre cable (DOCSIS) BPI y el protocolo de seguridad. En relación al suministro de servicios sólo a los usuarios finales específicos, la autenticación - basada en certificados digitales X.509- es incluida en la capa de control de acceso a los medios y da a cada usuario 802.16 receptor su propio certificado incorporado, más otro para el fabricante, permitiendo a la estación base autorizar al usuario final. La privacidad de la conexión es implementada como parte de otro subnivel MAC, la capa de privacidad. Ésta se basa en el protocolo Privacy Key Management que es parte de la especificación DOCSIS BPI.

4.8 CONCLUSIONES SOBRE LA SEGURIDAD EN REDES INALAMBRICAS

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

El sistema WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, tiene distintas debilidades que lo hacen no seguro, por lo que deben buscarse alternativas.

Tanto la especificación WPA como IEEE 802.11i solucionan todos los fallos conocidos de WEP y, en estos momentos, se consideran soluciones fiables.

La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos. Mientras no se descubran problemas de seguridad en WPA, esta implementación puede ser suficiente en los dispositivos para los próximos meses.

La apuesta de seguridad del IEEE para sustituir al desafortunado WEP, 802.11i, todavía está pendiente de ser estudiada en profundidad por investigadores debido a que sus especificaciones no son públicas.

5. CONCLUSION

Después de una larga investigación sobre 3 tecnologías inalámbricas del estándar IEEE 802, se puede concluir que el costo relativamente bajo, y la comodidad que ofrece la implementación de este tipo de redes, ha hecho que su uso sea cada vez más frecuente en ambientes de difícil acceso, es decir, a lugares donde instalar una red cableada de comunicación representa un alto coste o simplemente es imposible de instalar por las condiciones del lugar, distancias, etc.

BLUETOOTH es una tecnología inalámbrica de corto alcance, con varias utilidades; especialmente para uso doméstico por lo que se hace atractiva su implementación en muchos artículos y electrodomésticos caseros y de uso personal, como son teléfonos celulares, consolas de videojuegos y equipos reproductores de música. Con esta investigación se logró conocer la estructura y el funcionamiento básico de BLUETOOTH, las ventajas de su utilización, etc. Son varias las aplicaciones que esta tecnología puede ofrecer y su uso tiende a ser cada día más fuerte

De WI–FI se pude concluir que a pesar de haber empezado como la tecnología inalámbrica revolucionaria, se quedó corta en cuanto a cobertura se refiere, pues dio paso a otra aun mas actual y de mayor cobertura llamada WIMAX.

WI–FI es la tecnología inalámbrica ideal para implementarse en áreas relativamente cortas, como son campus universitarios, oficinas, etc. Actualmente es muy utilizada y no hay indicios de que desaparezca totalmente, aunque con el advenimiento de tecnologías de banda ancha inalámbrica móvil y redes de nueva generación NGN, lo más probable es que la utilización de WI-FI disminuya considerablemente.

Las tecnologías de comunicación tienden al uso masivo de redes inalámbricas a lo largo y ancho de grandes ciudades e incluso entre lugares lejanos, sin duda la llegada de tecnologías como WIMAX y las consecuentes a esta como WIMAX móvil e incluso las que vienen más adelante, han cambiado el concepto de funcionalidad que anteriormente existía sobre las redes inalámbricas e incluso el pensamiento de que las redes inalámbricas no iban a reemplazar a las cableadas, ha ido cambiando sustancialmente y aunque todavía está lejos de ser una realidad si se piensa en una implementación hibrida, aprovechando al máximo las ventajas que la red cableada y la inalámbrica poseen. El mundo actual se dirige hacia un ambiente de total comunicación, es decir estaremos conectados a la red desde que salgamos de la casa hasta que lleguemos al trabajo, al restaurante, a otra ciudad, y todo esto gracias a las posibilidades que las soluciones inalámbricas del estándar IEEE 802.11 ofrecen.

Actualmente se han logrado velocidades relativamente altas e incluso ya en el mundo existen muchas ISP que prestan el servicio de Internet banda ancha inalámbrica y los clientes se sienten contentos con esto, también existen múltiples métodos de seguridad para las redes inalámbricas, que cada vez garantizan mas la fiabilidad de estas redes, dado que el medio de transmisión es el aire, se hacía mucho más fácil la captación de información por parte de terceros. Hoy día acceder a la información que se transmite por la red inalámbrica es más difícil

6. RECOMENDACIONES

Debido a que la información sobre las 3 tecnologías inalámbricas del estándar IEEE 802 descrita en esta investigación es básica, es recomendable citar y consultar otras fuentes diferentes a las que se consultaron en este trabajo. También se recomienda conocer al menos el funcionamiento básico de las redes inalámbricas para que así se pueda entender con claridad la información descrita en el documento y poder hacer un buen uso de los conocimientos que se pueden adquirir.

El tema de las redes y las tecnologías es muy cambiante y a diario surgen nuevas propuestas y estándares que hacen mas robusto el funcionamiento de las redes inalámbricas es por esto que se recomienda investigar constantemente y en fuentes actualizadas sobre las tecnologías inalámbricas para así mejorar y actualizar el contenido presentado en esta monografía. El estudio de estos temas lo llevan a cabo profesionales en sistemas, electrónica, comunicaciones en redes y afines.

Dado el costo de implementación y la dificultad del acceso que hay en nuestra ciudad a los equipos necesarios para implementar una red inalámbrica ya sea de corto o largo alcance, se hace pertinente simular con herramientas como son software y asistir a laboratorios de redes donde se cuente con la infraestructura adecuada para así poner en práctica los conocimientos adquiridos a lo largo de este investigación. No está de más recalcar que con buenas bases de conocimiento sobre el tema se pueden implementar soluciones inalámbricas a nivel empresarial, educativo y doméstico.

7. GLOSARIO

AES - Advanced Encryption Standard / Estándar de Cifrado Avanzado: También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En Octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) norteamericano como estándar de cifrado reemplazando al hasta entonces estándar DES.

Acceso Remoto: Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.

Access Point (AP) - Punto de Acceso (PA): Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

Ad Hoc: Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad Hoc".

Algoritmo de Encriptación: Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales. Cada algoritmo utiliza bloques de distintos tamaños.

Antena: Dispositivo generalmente metálico capaz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia que punto emitan la señal podemos encontrarlas direccionales u omnidireccionable.

Autenticación: Proceso en el que se da fe de la veracidad y autenticidad de un producto, de unos datos o de un servicio, así como de la fiabilidad y legitimidad de la empresa que los ofrece.

Autorización: Proceso por el que se acredita a un sujeto o entidad para realizar una acción determinada.

BLUETOOTH: Estándar de comunicación inalámbrica que utiliza FHSS, capaz de transmitir a velocidades de 1 Mbps a una distancia de 10 metros entre aparatos (normalmente portátiles, impresoras, monitores, teclados, ratones, etc....) que implementen esta tecnología ya que su FHSS/Hopping Pattern es de 1600 veces por segundo, lo que asegura transmisiones altamente seguras. En cuanto a su implementación Bluetooth utiliza el término piconet. Un piconet

es un grupo de 2 u 8 aparatos que utilizan "BLUETOOTH" que comparten el mismo rango que es utilizado por un "Hopping Sequence", a su vez cada piconet contiene un aparato principal ("master") que es el encargado de coordinar el "Hopping Pattern" del piconet para que los demás aparatos ("slaves") sean capaces de recibir información.

Clave de Encriptación: Serie de números utilizados por un algoritmo de encriptación para transformar plaintext (texto sin encriptar que se puede leer directamente) en datos ciphertext (encriptados o cifrados) y viceversa.

Cliente o Usuario Inalámbrico: Toda solución suceptible de integrarse en una red wireless como PDAs, portátiles, cámaras inalámbricas, impresoras, etc.

Confidencialidad: Calidad de secreto, que no puede ser revelado a terceros o personas no autorizadas.

Cortafuegos o Firewall: Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc.

Denegación de Servicio (DoS) - Denial of Service: Se trata de una ofensiva diseñada específicamente para impedir el funcionamiento normal de un sistema y por consiguiente impedir el acceso legal a los sistemas para usuarios autorizados.

DES: Algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmo DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

EAP - Extensible Authentication Protocol / Protocolo de Autenticación Extensible: Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros.
Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

RADIUS - Remote Authentication Dial-In User Service: Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISPs) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

Sniffers: Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información. Los sniffers no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos.
Algunas herramientas sniffers conocidas son: WepCrack, Airsnort o NetStumbler, entre otras.

SSID: Identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

Tarjeta de Red Inalámbrica: Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB

TKIP - Temporal Key Integrity Protocol / Protocolo de Integridad de Clave Temporal: Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

VPN - Red Privada Virtual / Virtual Private Network: Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos SEGURIDAD EN REDES DE ÁREA LOCAL INALÁMBRICA, ESTÁNDAR DE SEGURIDAD IEEE 802.11i sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (LAN).

Wardriving: Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos wireless. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc.

WEP - Wired Equivalent Privacy: Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que

recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

WLAN - Wireless Local Area Network / Red de Área Local Inalámbrica: También conocida como red wireless. Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

WPA - Wi-Fi Protected Access / Acceso Wi-Fi Protegido: Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

BIBLIOGRAFIA

ROB FLICKENGER, Building Wireless Community Networks, Second Edition: Editorial O´reilly. Junio de 2003. Pags 182.

¿Qué es WIMAX? [En línea]. http://blogWIMAX.com/que-es-WIMAX/. (consulta: 10 de Diciembre, 2007).

FERNANDEZ, Ramón Alfonso, MCSE (Microsoft Certified Systems Engineer). WIMAX Un nuevo horizonte en las comunicaciones inalámbricas [en linea]. http://www.idg.es/pcworldtech/mostrarArticulo.asp?id=293637928&seccion=movilidad. 01/07/2006, Disponible en la Web. (Consulta: 11 de Diciembre, 2007).

Redes inalámbricas [En linea]. http://www.tredess.com/espanol/faqs/FaqRI.htm. (Consulta: 3 de Diciembre, 2007)

TecnoWIMAX Weblog sobre tecnología WIMAX. [En linea]. http://www.tecnoWIMAX.com/category/WIMAX-movil/. 10/12/2005, Disponible en la web. (Consulta: 12 de Diciembre, 2007)

FERNANDEZ, Alcántara Azael. WIMAX móvil. La historia de despliegue puede repetirse. [En línea].http://www.enterate.unam.mx/Articulos/2006/mayo/WIMAX.htm. Mayo de 2006, Disponible en la web. (Consulta: 11 de Diciembre, 2007)

GARCIA CORREA, Francisco José. LA PRÓXIMA GENERACIÓN DE REDES, NGN, UN TRAYECTO HACIA LA CONVERGENCIA. [En línea]. http://sociedaddelainformacion.telefonica.es/jsp/articulos/detalle.jsp?elem=3188. 13/09/2006, Disponible en la web. (Consulta: 12 de Diciembre, 2007)

Red de siguiente generación. [En línea]. http://es.wikipedia.org/wiki/Red_de_siguiente_generaci%C3%B3n. Disponible en la web. (Consulta: 11 de Diciembre, 2007)

CUELLAR RUIZ, Jaime. REDES INALÁMBRICAS, ESTÁNDARES Y MECANISMOS DE SEGURIDAD [En linea]. http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm. 08/2004, Disponible en la web. (Consulta: 14 de enero, 2008).

ALAPONT MIQUEL, Vincent. SEGURIDAD EN REDES INALAMBRICAS [En Línea]. http://documentos.shellsec.net/otros/SeguridadWireless.pdf. Disponible en la Web. (Consulta: 16 de Enero, 2008).

BARAJAS, Saulo. PROTOCOLOS DE SEGURIDAD EN REDES INALÁMBRICAS. [En Línea]. http://www.saulo.net/pub/inv/SegWiFi-art.htm. Disponible en la Web. (Consulta: 16 Ener, 2008).

TANEMBAUM, Andrew S. REDES DE COMPUTADORES. Pearson Educación, México 2003.Ed. Prentice Hall. Págs. 912.

ANEXO 1 ELEMENTOS BASICOS EN EL DISEÑO DE UNA RED WIRELESS

Al momento de diseñar una red inalámbrica es importante tener en cuenta aspectos básicos, con el fin de proponer un modelo de red que cumpla con las expectativas requeridas; los elementos a considerar son:

1. Como primera medida se debe tener en cuenta el número de usuarios que se conectaran a la red, esto ayuda a determinar el tipo de dispositivos a implementar y que cubran las especificaciones. Por ejemplo; un Access Point.

2. Dependiendo de la cobertura de la red inalámbrica y la distancia a la que se encuentren los usuarios que van a hacer parte de la red, así deben adquirirse los dispositivos necesarios para que el servicio funcione sin mayores contratiempos. Existen muchos dispositivos, por ejemplo antenas diseñadas para un tipo de situación específica, como el rango de cobertura y alineamiento de la señal.

3. El tipo de usuario y el entorno de operación que va a tener la red inalámbrica son factores muy importantes, ya que esto va a determinante al momento de emplear niveles de seguridad cuando se este diseñando la red. Sin embargo toda red inalámbrica por naturaleza es insegura y se deben tener en cuenta la utilización de algunos métodos de seguridad, ya sean hardware (Firewalls, DMZ, etc.) o programados (Protocolos de encriptación).

ANEXO 2 COMPARACION ENTRE BLUETOOTH, WI-FI Y WIMAX

TECNOLOGIAS	BLUETOOTH	WI- FI	WIMAX
Licencia	no	no	Si/no
Cobertura	10-12 m	300 m	40-70 km
Banda Frecuencia	2.4 GHZ	2.4-5 GHZ	2-11 GHZ
Velocidad	1-3 Mbit/s	11-54 Mbit/s	124 Mbit/s
Ventajas	Velocidad y Precio	Velocidad y Precio	Velocidad y Alcance
desventajas	Bajo alcance	Bajo alcance	Interferencias
Aplicaciones	Tarjetas, aplicaciones JAVA, educación, negocios, uso domestico, teléfonos celulares	Educación, empresarial, entornos de alcance relativamente corto	Teléfonos celulares de nueva tecnología, entornos metropolitanos y de largo alcance