UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

Seguridad en redes inalámbricas (Wi-Fi).

T E S I S

Que para obtener el título de:
LICENCIADO EN INFORMÁTICA
P R E S E N T A:
Erik Fernando García Ledesma

ASESOR: ING. OSCAR HERNÁNDEZ SÁNCHEZ

CUAUTITLÁN IZCALLI, ESTADO DE MÉXICO **2007**

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México, institución que me brindó la oportunidad de realizar mis estudios.

Al Ingeniero Oscar Hernández Sánchez, Coordinador de la carrera de Informática, quien asesoró el trabajo de investigación con paciencia, entrega y valiosos consejos que me permitieron alcanzar los objetivos de esta tesis.

En general, a los profesores que integraron el jurado, por la revisión de la información y los comentarios dirigidos al mejoramiento de la misma.

Finalmente, a todas las instituciones y bibliotecas, que contribuyeron a facilitarme el acceso a la información requerida para la elaboración de esta tesis.

DEDICATORIA

A DIOS:

Por haberme dado la oportunidad de existir, de tenerlo como guía y de darme una familia maravillosa.

A MIS PADRES:

Por haberme dado la vida y estar siempre junto a mí, brindándome el apoyo, la fuerza y la alegría para seguir adelante, además de darme una carrera para mi futuro y alejarme de los vicios.

A MIS HERMANOS:

Gracias por el apoyo y los felices momentos que hemos pasado juntos, por ayudarme a mejorar en mis estudios y sobre todo por seguir estando al pendiente de mí aún cuando ambos ya se casaron.

A toda mi familia los quiero con todo mi corazón y quiero que sepan que sin ustedes no lo hubiera logrado.

ÍNDICE

Seguridad en redes inalámbricas (Wi-Fi).

ÍNDICE DE FIGURAS

CAPÍTULO 6

CAPÍTULO 7

ÍNDICE DE TABLAS

INTRODUCCIÓN

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras y otros dispositivos mediante tecnología inalámbrica. La conexión de dispositivos mediante ondas de radio o luz infrarroja, actualmente está siendo ampliamente investigada.

Aunque las tecnologías que hacen posible las comunicaciones inalámbricas (láser, infrarrojo y radio, principalmente) existen desde hace muchos años, su implantación comercial no ha sido posible hasta fechas recientes. El gran inconveniente que ha tenido este tipo de comunicaciones ha sido la falta de un estándar que hiciera compatible los equipos de distintos fabricantes, lo cual quedó superado en 1999 con la aparición de Wi-Fi. La fuerza que a la fecha ha cobrado esta tecnología se debe, en gran medida, a las ventajas de movilidad para los usuarios y al precio competitivo que tienen en relación con las redes cableadas convencionales, entre otras cuestiones.

La seguridad de este tipo de redes preocupa a las organizaciones que cuentan con una implementación basada en redes inalámbricas. Al mismo tiempo, las empresas que no han adoptado la tecnología muestran su inquietud por no poder aprovechar los beneficios que aporta en cuanto a la productividad de los usuarios y a la reducción de costo que implica. Adicionalmente, existe cierto grado de confusión en lo que respecta a la seguridad del uso de WLAN en entornos domésticos, empresariales o urbanos.

Desde el descubrimiento de las posibles vulnerabilidades de seguridad de las redes inalámbricas, analistas, proveedores de redes, organismos de estándares y compañías especialistas en seguridad de redes, dedican parte de su tiempo a la resolución de los problemas descubiertas en la seguridad de WLAN. Esto ha dado lugar a diferentes reacciones, en lo que respecta a la preocupación por la seguridad de la tecnología (por parte de los fabricantes).

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y otras organizaciones de estándares se han encargado de redefinir y mejorar los estándares de seguridad inalámbrica de modo que la tecnología WLAN pueda hacer frente al hostil entorno de seguridad que caracteriza a este comienzo de siglo. Gracias al trabajo de estas organizaciones y líderes del sector, ahora ya se puede implementar y utilizar una WLAN con un nivel de confianza en su seguridad muy alto.

Estas limitaciones en la seguridad han conducido a la investigación y desarrollo de nuevas soluciones de seguridad, alternativas a la inicialmente existente (WEP), para proteger las redes Wi-Fi y proporcionar a las organizaciones que las utilizan la garantía que necesitan para sus sistemas y datos. La necesidad de garantizar la seguridad en el uso de las redes como elemento básico de

expansión de la digitalización de la vida económica y personal unida a la cada vez mayor presencia de las redes Wi-Fi en todos los entornos y la especial vulnerabilidad de estas hace que el área de la seguridad aplicada a estas redes constituya en la actualidad un área muy activa en la propuesta y generación de soluciones.

Para el desarrollo de la presente investigación se formuló la siguiente hipótesis: “Mediante la aplicación correcta y oportuna de los sistemas de seguridad actuales en las redes inalámbricas, esto ayudará a disminuir los riesgos y dar mayor confianza de su uso”.

Los propósitos principales de este trabajo consisten en señalar la mejoría que gradualmente se observa en la seguridad de las redes inalámbricas y ayudar a decidir la forma más apropiada de proteger la estructura de una WLAN en una organización. Para ello, se cubren áreas de especial interés como son: solución de problemas de seguridad asociados con WLAN, uso de estándares de WLAN seguros, adopción de estrategias alternativas y la selección de las opciones de WLAN adecuadas para su organización.

Dentro de la investigación teórica se organizan 7 capítulos.

El primer capítulo pretende dar una visión general de las tecnologías inalámbricas existentes, así como los aspectos que las integran como su origen, concepto, rango de cobertura, velocidades que soportan y su funcionamiento, señalando las ventajas y desventajas con relación a las redes tradicionales.

El segundo capítulo, presenta las principales instituciones que se encargan de desarrollar los estándares asociados con las redes inalámbricas, además de una pequeña descripción de los estándares más importantes de cada una.

En el tercer capítulo, se explica el significado y origen del término Wi-Fi, las ventajas y desventajas que implica su uso, después se hace una descripción de su funcionamiento y por último se señalan algunos ejemplos de dispositivos que utilizan la tecnología Wi-Fi, así como algunas de sus aplicaciones.

El cuarto capítulo se enfoca a los protocolos establecidos para la seguridad de las redes inalámbricas, abarcando sus características, principales debilidades, modo de funcionamiento y las alternativas para solucionar las vulnerabilidades acerca de la seguridad.

El quinto capítulo proporciona información que es útil para definir una estrategia de seguridad en los diferentes entornos de aplicación de Wi-Fi, considerando los beneficios al usar alternativas

como VPN, IPsec y el estándar 802.1x. Al mismo tiempo, se incluyen los principales aspectos que orientarán sobre cómo determinar cuál de las opciones de seguridad en las redes inalámbricas es la más apropiada para los diferentes tipos de organización, señalando al principio del capítulo los riesgos más comunes que podrían presentarse al usar la tecnología inalámbrica en un entorno empresarial determinado.

El sexto capítulo está orientado a la aplicación de redes inalámbricas en las empresas, describiendo el desempeño y velocidades de datos que soporta Wi-Fi, así como el rango e interoperabilidad de los dispositivos necesarios para su uso, realizando un análisis de los principales aspectos para determinar apropiadamente la selección del equipo y los componentes necesarios para su implementación.

En el séptimo, y último, capítulo se presentan algunos de los desafíos, que podrían surgir, en la tecnología inalámbrica como consecuencia de su exponencial desarrollo, después se proporcionan las características más relevantes que ofrecerán los nuevos estándares 802.11 y por último se hace referencia a los proyectos que se encuentran en una etapa de planeación y desarrollo en la actualidad para su introducción en un futuro al mercado, como la cuarta generación de teléfonos celulares, ancho de banda inalámbrico aerotransportado y la tecnología UWB.

Capítulo 1 – Introducción a las redes inalámbricas

1.1 Historia de las redes inalámbricas

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, que consiste en utilizar enlaces infrarrojos para crear una red local en una fábrica, desde entonces, las actividades hacia la investigación y desarrollo de dispositivos que hacen posible las redes de esta naturaleza se han intensificado. Estos resultados, publicados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante, tanto con infrarrojos, como con microondas, donde se utilizaba el esquema de espectro expandido. En mayo de 1985, y tras cuatro años de estudios, la Comisión Federal de Telecomunicaciones (FCC), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industriales, Científicas y Médicas) 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz para uso en las redes inalámbricas basadas en espectro expandido, con las opciones DS (Secuencia Directa) y FH (Salto de Frecuencia). La técnica de espectro expandido es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea muy pocas interferencias. La asignación de esta banda de frecuencias propició una mayor actividad en el seno de la industria y ese respaldo hizo que las WLAN empezaran a dejar ya el entorno del laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

1.1.1 La radio, el fundamento de la LAN inalámbrica

Del mismo modo en que la tecnología de radiodifusión es el fundamento de la LAN inalámbrica, los primeros trabajos en electromagnética, a su vez, representan los fundamentos de la radio. El teórico escocés James Clerk Maxwell impulsó por primera vez la noción de las ondas electromagnéticas en 1864, al postular que éstas provienen de un cambio de dirección en la energía eléctrica. Un dispositivo diseñado para producir ondas electromagnéticas mediante el cambio de la dirección de una corriente eléctrica, un proceso que se conoce como oscilación, es en esencia un transmisor.

Basándose en esto, el alemán Heinrich Hertz desarrolló un equipo en la década de 1880 que, en realidad, envió y luego recibió ondas electromagnéticas a través del aire. Este equipo era capaz de incrementar el número de ondas que se producían en un periodo determinado, su frecuencia y su velocidad de cambio u oscilación. Su

nombre, por supuesto, se convirtió en una unidad común de medida para las frecuencias, donde 1 hertz (Hz) significaba una oscilación o ciclo completo por segundo. De esta forma, las ondas electromagnéticas que son cada vez más cortas pueden ser cuantificadas o colocadas en un orden de frecuencia creciente, o en un orden de longitud de onda descendente. En la actualidad, esta cuantificación lineal se conoce como frecuencia de radio o espectro electromagnético.

Fue Guglielmo Marconi quien tomó estos primeros trabajos para dar el siguiente paso y luego llegar a una aplicación práctica. Aunque su nombre siempre estará vinculado con lo que hoy día se conoce como la radio, la transmisión de sonido, en realidad la primera aplicación fue una forma pionera de las comunicaciones de datos. Pensó que si era posible transmitir señales binarias (puntos y guiones) a través de un cable, también debería de ser posible enviar este tipo de señales a través de una onda electromagnética y usarlas como medio de comunicación.

En 1895, cuando sólo tenía 21 años, Marconi envió y recibió sus primeras transmisiones de radio, a medida que mejoró sus transmisores y antenas, las distancias se incrementaron rápida y significativamente, lo que llevó a la radio del mundo de la ciencia hacia el de la tecnología, Marconi descubrió el potencial comercial de su equipo telegráfico basado en las radiotelecomunicaciones, por lo que obtuvo su primera patente en 1896 y un año después formó en Inglaterra una compañía, la Wireless Telegraph and Signal Company Limited. Hacia 1897, el equipo telegráfico inalámbrico se usaba para las comunicaciones entre los barcos y tierra firme, además de aplicaciones terrestres que remplazaron sistemas cableados. Un año más tarde se estableció un enlace inalámbrico entre Inglaterra y Francia, y en 1901, se envió un mensaje desde Inglaterra hasta Newfoundland cruzando el océano Atlántico.

Por su parte, Thomas A. Edison fue el impulso principal de los primeros sistemas inalámbricos que se desplegaron comercialmente en Estados Unidos, lo que dio como resultado la fundación de General Electric. El trabajo de Edison se basó en el de Marconi y en el de uno de los empleados que colaboró con él, Nicola Tesla, sorprendentemente, después de muchos años de controversia, en 1899 Tesla obtuvo el reconocimiento formal de la Oficina de patentes de Estados Unidos como uno de los inventores de la radio, junto con Marconi.

Fue hasta 1923, que el gobierno de Estados Unidos inicio un proceso de dividir el espectro de frecuencias de radio en asignaciones para usos y usuarios específicos. Once años más tarde fue establecida la FCC.

Lamarr y Antheil crearon un sistema para emitir comunicaciones de radio de banda angosta a través de una banda ancha en el espectro de frecuencia, como un medio para guiar torpedos hacia sus blancos de una manera que fuera menos susceptible a las técnicas de obstrucción de frecuencias o al espionaje. La patente que apareció como resultado, premiada el 11 de agosto de 1942, fue el primer sistema de espectro expandido.

En 1981, el gobierno de Estados Unidos desclasificó la patente de Lamarr y Antheil que había expirado y dejó

de ser un “sistema de comunicaciones secreto” y a petición de la FCC, el IEEE comenzaría a estudiar las aplicaciones comerciales de las comunicaciones del espectro expandido. La fecha en que esta información fue lanzada al público no fue una coincidencia, en 1985, la FCC por primera vez asignó porciones del espectro de frecuencia de radio que las entidades industriales, científicas y médicas podrían usar sin necesidad de una licencia, a pesar de esto, los radios que se asignaron para el servicio de los sistemas de adquisición de datos inalámbricos eran dispositivos de banda angosta y no estaban basados en la tecnología de espectro expandido. No fue sino hasta 1985 cuando se establecieron las regulaciones para permitir el uso al público controlado de la tecnología de espectro expandido.

1.1.2 Las primeras LAN inalámbricas

En 1985, gracias a los cambios legales en la sección 15 de la FCC las cuales permitieron el uso de radios a través del espectro extendido en las aplicaciones comerciales, se abrió la puerta para comercializar la tecnología. Poco después de un año de que se efectuaran los cambios, se creó en Toronto una compañía, Telesystems SLW, para explotar este desarrollo. Telesystems empleó un sistema que se conoce como secuencia directa, donde una señal de banda angosta se extiende a través del ancho de banda determinado al multiplicar el ancho de la señal a través de un conjunto de frecuencias más grande. En 1988 fue introducido en el mercado el primer sistema comercial basado en la tecnología de secuencia directa en el espectro extendido (DSSS, por sus siglas en inglés). Además de incorporar DSSS, estos sistemas no operaban en una banda con licencia para los teléfonos celulares analógicos que se usan en Norteamérica, proporcionó a los fabricantes la ventaja de construir sus dispositivos libres de licencia con componentes existentes para nuevos propósitos y que originalmente estaban destinados para el uso de teléfonos celulares. En general, la operación libre de licencias mediante el uso de DSSS fue una solución ideal para distribuidores, agencias de alquiler de automóviles y aplicaciones similares en el mercado. El resultado de este sistema es similar al del salto de frecuencias, es decir, la señal de banda angosta que se extiende a través de un ancho de banda más amplio es menos susceptible a las interferencias, debido a que sólo una parte de la señal multiplicada necesita alcanzar al receptor esperado para que la transmisión sea exitosa.

Los primeros productos de Telesystems fueron diseñados como reemplazos del cableado, ya sea para conectar múltiples computadoras de escritorio con una estación de base central de manera muy parecida en la que funcionaría una red Ethernet, o para conectar las redes en edificios separados de modo semejante al que funciona un puente. Al ejecutar, NetWare de Novell, el sistema operativo de red predominante en ese momento, y al proporcionar una velocidad de datos de aproximadamente 200 Kbps, estas primeras LAN inalámbricas para entornos de oficina pequeña tenían un precio de venta de 1,500 dólares por nodo, lo cierto es que estaba muy adelantado a su tiempo y proporcionaba una relación entre precio y desempeño insuficiente para obtener el tipo de aceptación en el mercado que es necesario para sostener una compañía.

Al reconocer las ventajas de escalabilidad y consistencia geográfica de la operación del espectro extendido libre

de licencia, Telxon comenzó a ofrecer los radios sin licencia de Telesystems en sus terminales de adquisición de datos, como una alternativa para los radios de banda angosta con licencia que entonces eran vendidos principalmente por Motorola. Los radios de Telesystems estaban diseñados a fin de coincidir con las especificaciones físicas de los radios de Motorola, de manera que pudieran intercambiarse dentro de las mismas terminales de adquisición de datos.

Los clientes se dieron cuenta rápidamente de las ventajas de la nueva oferta libre de licencias y comenzó a fraguarse una migración, lo que provocó el hecho decisivo que ocurrió a principios de 1991. Wal-Mart notó el modo en que los radios libres de licencia le permitirían tener una infraestructura inalámbrica común a lo largo de todas sus operaciones en Norteamérica, elaboró una orden impresionante de 30,000 piezas a Telxon, que debió cumplir Telesystems, la orden debía de cumplirse en un periodo de 6 meses y a un precio muy bajo.

Telxon comprendió que la única manera de cumplir con los términos de entrega y de precio era que su proveedor estuviera dedicado de manera exclusiva, por lo tanto, a principios de 1991, Telxon terminó por adquirir Telesystems y entregar la orden. En 1999 Telxon agrupó su equipo de radios en la división Aironet Wireless Communications, que fue adquirida meses más tarde por el gigante en la industria de las redes, Cisco Systems.

No obstante que la operación de la banda de 900 MHz se proporcionó para una infraestructura común a través de Estados Unidos, Canadá y Australia, estaba limitada en el sentido que no estaba asignada para la operación sin licencia en otras partes del mundo. Para llegar a los mercados ubicados fuera de estas áreas, los fabricantes comenzaron a producir radios que operaban en la parte de 2.4 GHz del espectro de frecuencia que estaba disponible para la operación libre de licencia a lo largo de la mayor parte de Europa y Japón, además de Estados Unidos, Canadá y Australia. Sin importar el hecho de que la frecuencia de 900 MHz continuó siendo la banda más comúnmente usada en Norteamérica durante la primera mitad de la década de los noventa, los radios de 2.4 GHz iniciaros su proliferación a medida que la operación libre de licencia comenzó a obtener la aceptación en Europa y Japón.

A medida que la operación libre de licencia fue más popular en Norteamérica, las ondas en el aire a 900 MHz se saturaron no sólo con el equipo LAN inalámbrico sino también con los teléfonos inalámbricos que son mucho más comunes. La banda de 900 MHz comenzó a conocerse como la “banda basura”, debido a la cantidad de interferencia que impactaba en el desempeño y confiabilidad de las LAN inalámbricas. Sin embargo, finalmente, fue el movimiento hacia la estandarización lo que selló el destino de operación de la LAN inalámbrica en la banda de 900 MHz.

1.1.3 802.11: El primer estándar

En 1991, diversos fabricantes competidores como Telxon, NCR, Proxim Technology y Simbol Technologies,

emitieron al principio una solicitud de autorización del proyecto (Project Authorization Request, PAR) al IEEE, a fin de establecer un estándar interoperable para las LAN inalámbricas. Puesto que es una organización internacional, el IEEE como regla general se inclina hacia los estándares que tienen una aplicación alrededor de todo el mundo. Esta tendencia se inclinó hacia el grupo recién formado en torno a la banda de 2.4 GHz y rechazó la de 900 MHz.

Hacia 1993, los fundamentos para un estándar estaban establecidos, y en junio de 1997, el estándar 802.11 del IEEE, que tenía más de seis años en el proceso de creación, fue ratificado. Este primer estándar 802.11 proporcionaba velocidades de datos de 1 y 2 Mbps, una forma rudimentaria de cifrado de datos que, se puede decir, tiene un nombre confuso: Privacidad Equivalente al Cableado (WEP), así como la transmisión a través de las tecnologías de secuencia directa y de salto de frecuencia sobre una banda de 2.4 GHz, además de rayos infrarrojos. Los aspectos relacionados con los rayos infrarrojos de este estándar obtuvieron un pequeño impulso comercial y hoy en día representan sólo una pequeña parte en la historia del estándar.

No obstante que WEP aún se despliega, ha sido desacreditado de manera consistente como un medio viable de proteger el tráfico sobre una LAN inalámbrica. A manera de compromiso para satisfacer a los fabricantes competidores que estaban representados en el comité, tanto el salto de frecuencia como la secuencia directa en el espectro expandido fueron ratificados como medios de transmisión de radio compatibles con los estándares. Las operaciones de estas dos formas variantes competidoras son incapaces de ofrecer interoperabilidad e incluso tuvieron el efecto de interferir entre ellas y disminuir el desempeño cuando se colocaban físicamente. Los impactos de este problema dieron como resultado una confusión considerable, en especial cuando los adaptadores iniciales de la tecnología migran a los estándares actuales de velocidades más altas. Sin importar lo anterior, el primer estándar 802.11 marcó el comienzo de una nueva era y estableció los fundamentos para el siguiente estándar, 802.11b, que fue ratificado en 1999 y ofrece una velocidad de datos de 11 Mbps. Los detalles de 802.11 y los estándares asociados, se cubrirán con profundidad en el capítulo 2.

1.2 Concepto de redes inalámbricas

Hasta ahora el concepto de redes de área local (LAN) y redes de área extendida (WAN) se aplicaba principalmente a las redes fijas de datos, pero la integración de la tecnología de redes inalámbricas (WLAN) con las redes móviles, permite extender esta terminología hacia entornos móviles creando un nuevo modelo, en el que la necesidad de ancho de banda va ligada a la movilidad y a la densidad de usuarios de la zona considerada. Por lo tanto, un concepto para las redes inalámbricas es el siguiente:

- Una WLAN es una red de área local inalámbrica, que permite la comunicación de dos o más dispositivos sin el uso de cables, siendo un sistema de comunicación de datos inalámbrico flexible, utilizado como alternativa o complemento de una LAN tradicional, utilizando una interfaz inalámbrica. Las redes inalámbricas utilizan la tecnología basada en separar el espectro de las ondas de radio para

permitir la comunicación entre los dispositivos dentro del área de cobertura. Esto da a los usuarios la capacidad de moverse dentro del área de cobertura sin tener que desconectarse de la red. Este tipo de redes se diferencia de las redes convencionales principalmente en la capa física y en la capa de enlace de datos, según el modelo de referencia OSI.

Es importante señalar que al igual que una LAN, la red inalámbrica permite que los usuarios que están dentro del área de cobertura compartan archivos, impresoras y otros servicios. La mayoría de las redes WLAN utilizan tecnología de espectro distribuido. Su ancho de banda es limitado y los usuarios comparten el ancho de banda con otros dispositivos del espectro, no obstante, los usuarios pueden operar dispositivos de espectro distribuido sin autorización de la FCC (Comisión Federal de Comunicaciones).

1.3 Redes inalámbricas de datos

Una red inalámbrica de datos es un conjunto de computadoras o cualquier otro dispositivo informático, comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión, teniendo en cuenta que también existen redes inalámbricas de voz.

Para disponer de una red inalámbrica, sólo hace falta instalar una tarjeta de red inalámbrica en los dispositivos involucrados y hacer una pequeña configuración de los mismos. Una vez instalada la red inalámbrica, su utilización es prácticamente idéntica a la de una red cableada. Los dispositivos que forman parte de la red pueden comunicarse entre sí y compartir toda clase de recursos. Se pueden compartir archivos, directorios, impresoras, incluso el acceso a otras redes como puede ser Internet.

No obstante, las soluciones inalámbricas tienen también algunos inconvenientes, tienen un menor ancho de banda y, en general, son más caras que las soluciones con cable.

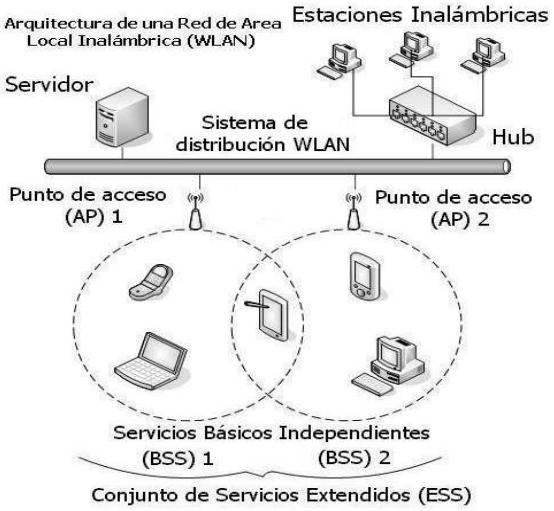


FIGURA 1. ARQUITECTURA DE UNA RED DE ÁREA LOCAL INALÁMBRICA

1.4 Tipos de redes inalámbricas de datos

Las comunicaciones inalámbricas, pueden clasificarse de distinta forma dependiendo del criterio al que se atienda. En este caso vamos a clasificar los sistemas de comunicaciones inalámbricas de acuerdo con su alcance. Se llama alcance a la distancia máxima a la que se pueden situarse las dos partes de la comunicación inalámbrica. Las comunicaciones inalámbricas se dividen en los siguientes grupos de acuerdo con su alcance:

- Las redes inalámbricas de área personal o WPAN (Redes de Área Personal Inalámbrica) cubren distancias inferiores a los 10 metros. Estas soluciones están pensadas para interconectar los distintos dispositivos de un solo usuario (por ejemplo, una computadora con la impresora).

- Las redes inalámbricas de área local o WLAN (Redes de Área Local Inalámbrica) cubren distancias de unos cientos de metros. Estas redes están pensadas para crear un entorno de red local entre computadoras o terminales situados en un mismo edificio o grupo de edificios.

- Las redes inalámbricas de área metropolitana o WMAN (Redes de Área Metropolitana Inalámbrica) pretenden cubrir el área de una ciudad o entorno metropolitano.

- Las redes globales que tienen la posibilidad de cubrir toda una región (país o grupo de países). Estas redes se basan en la tecnología celular y han aparecido como evolución de las redes de comunicaciones de voz. En comunicaciones móviles de voz se les llama 1G (primera generación) a los sistemas analógicos, 2G a los digitales, 2,5G a los digitales con soporte para datos a alta velocidad y 3G a los nuevos sistemas de telefonía celular con capacidad de gran ancho de banda.

1.4.1 Redes inalámbricas de área personal

La finalidad de estas redes es comunicar cualquier dispositivo personal (computadora, teléfono móvil, PDA, etcétera) con sus periféricos, así como permitir una comunicación directa a corta distancia entre éstos dispositivos.

Las tecnologías WPAN permiten a los usuarios establecer comunicaciones inalámbricas ad-hoc para dispositivos (como PDA, teléfonos celulares y equipos portátiles) que se utilizan dentro de un espacio operativo personal (POS). Un POS es el espacio que rodea a una persona, hasta una distancia de 10 metros. Actualmente, las dos tecnologías WPAN principales son Bluetooth y la luz infrarroja. Bluetooth es una tecnología de sustitución de cables que utiliza ondas de radio para transmitir datos a una distancia de hasta 10 metros. Los datos de Bluetooth se pueden transferir a través de paredes, bolsillos y maletines. El desarrollo de la tecnología de Bluetooth lo dirige el Grupo de Interés Especial (SIG) de Bluetooth, que publicó la

especificación de la versión 1.0 de Bluetooth en 1999. Otra posibilidad que tienen los usuarios para conectar dispositivos en un radio de acción muy cercano (1 metro o menos) es crear vínculos de infrarrojos.

Para normalizar el desarrollo de tecnologías WPAN, el IEEE ha establecido el grupo de trabajo 802.15 para las WPAN. Este grupo de trabajo está desarrollando una norma WPAN, basada en la especificación de la versión 1.0 de Bluetooth. Los objetivos principales en esta norma preliminar son baja complejidad, bajo consumo de energía, interoperabilidad y coexistencia con redes de 802.11.

1.4.1.1 Bluetooth

Bluetooth fue desarrollado en 1994 por la empresa sueca Ericsson con el objetivo de conseguir un sistema de comunicación de los teléfonos móviles con sus accesorios. En 1998 se creó el Grupo de Interés Especial Bluetooth (SIG), www.bluetooth.com, formado por empresas como Ericsson, IBM, Intel, Nokia y Toshiba, esto le dio un gran empuje a esta tecnología. El nombre Bluetooth significa en español ‘diente azul’ y procede del apodo que tenía el rey Harald Blaatlund II, un legendario guerrero danés del siglo X.

Las comunicaciones de Bluetooth se llevan a cabo mediante el modelo maestro/esclavo. Un terminal maestro puede comunicarse hasta con siete esclavos simultáneamente. No obstante, el maestro siempre puede suspender las comunicaciones con un esclavo (mediante una técnica conocida como parking) y activar la comunicación con un nuevo dispositivo esclavo. Con este sistema un maestro puede establecer comunicación con un máximo de 256 esclavos, donde sólo siete comunicaciones pueden permanecer activas simultáneamente. A este conjunto de relaciones maestro/esclavo se le llama piconet. En este entorno un dispositivo puede ser a la vez maestro de un piconet y esclavo de otro piconet. Cuando ocurre esto, al conjunto resultante se le conoce como scatternet (red dispersa).

Bluetooth utiliza la técnica FHSS (Espectro Expandido por Salto de Frecuencia) en la banda de frecuencia de 2.4 GHz. Puede establecer comunicaciones asimétricas donde la velocidad máxima en una dirección es de 721 Kbps y 57,6 Kbps en la otra o comunicaciones simétricas de 432,6 Kbps en ambas direcciones. Por otro lado, puede transmitir tanto voz como datos. Se está definiendo la versión 2.0 de Bluetooth que seguirá trabajando en alcances de 10 metros y se espera que llegue a velocidades de transmisión de hasta 12 Mbps.

FIGURA 2. DISPOSITIVOS CON TECNOLOGÍA BLUETOOTH

1.4.1.2 DECT

El estándar DECT (Telecomunicaciones Digitales Inalámbricas Mejoradas) existe desde 1992 promulgado por ETSI (Instituto Europeo de Normalización en Telecomunicaciones). El objetivo de DECT es facilitar las comunicaciones inalámbricas entre terminales telefónicos. DECT trabaja en la banda de frecuencia de 1.9 GHz y utiliza la técnica TDMA (Acceso Múltiple por División del Tiempo). La velocidad máxima actual a la que trabaja DECT es de 2 Mbps, aunque existe una propuesta de ETSI para aumentar esta velocidad hasta los 20 Mbps y conseguir alcances de hasta 17 kilómetros.

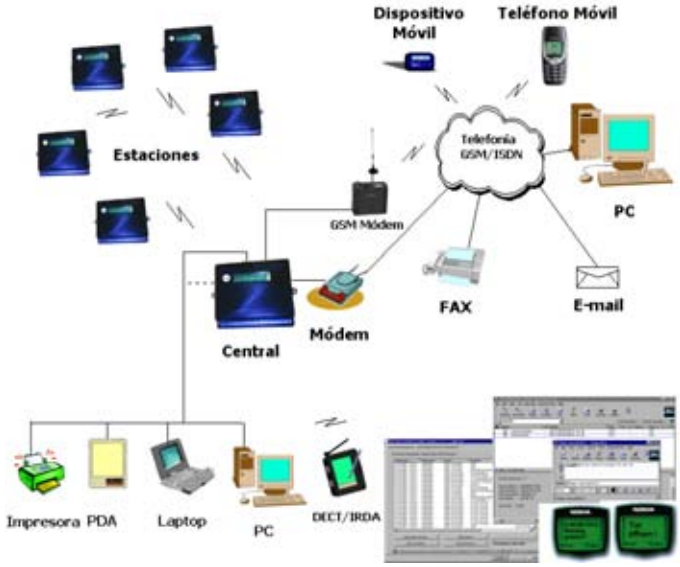


FIGURA 3. TECNOLOGÍA DECT

A pesar de que DECT podría ser un competidor de Bluetooth o, incluso, de otros sistemas inalámbricos de mayor alcance, el hecho de que trabaje en la banda de 1.9 GHz (utilizada en Europa para esta tecnología pero con barreras que regulan en Norteamérica y otras partes del mundo) y que esté muy orientada a voz le impone grandes limitaciones para competir con esas otras tecnologías.

En la idea de potenciar la tecnología DECT, en 1999 se creó en Barcelona la asociación DECT MMC (Consorcio DECT Multimedia), formada por empresas como Canon, Ericsson o Ascom, con el objetivo de potenciar el uso del protocolo DMAP (Perfil de Acceso DECT Multimedia) que permite la transmisión de datos entre dispositivos a corta y media distancia.

1.4.1.3 Infrarrojo

Los sistemas de comunicación con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja. La mayoría de los mandos a distancia de los aparatos domésticos (televisión, video, equipos de música, etcétera) utilizan comunicación por infrarrojo. Por otro lado, la mayoría de las PDA's (Agendas Electrónicas Personales), algunos modelos de teléfonos móviles y muchas computadoras portátiles incluyen un dispositivo infrarrojo como medio de comunicación entre ellos.

La tecnología infrarroja puede utilizar tres modos diferentes de radiación para intercambiar la energía óptica entre transmisores y receptores, estos son los siguientes:

- Infrarrojo de haz directo. También conocido como modo punto a punto, los patrones de radiación del emisor y del receptor deben estar lo más cerca posible, para que su alineación sea correcta. Como resultado, el modo punto a punto requiere una línea de visión entre las dos estaciones a comunicarse. Este modo es usado para la implementación de redes inalámbricas infrarrojas Token-Ring. Es la que consume menor potencia óptica, pero no ha de haber obstáculos entre las dos estaciones.

- Infrarrojo de haz cuasi-difuso. Tanto el modo cuasi-difuso como el difuso son de emisión radial, es decir, cuando una estación emite una señal óptica, ésta puede ser recibida por todas las estaciones al mismo tiempo en la célula. En el modo cuasi-difuso las estaciones se comunican entre sí, por medio de superficies reflectoras. No es necesaria la línea de visión entre dos estaciones, pero sí deben de estar con la superficie de reflexión. Además, es recomendable que las estaciones estén cerca de la superficie de reflexión, que puede ser pasiva o activa. En las células basadas en reflexión pasiva, el reflector debe tener altas propiedades reflectoras y dispersoras, mientras que en las basadas en reflexión activa se requiere de un dispositivo de salida reflexivo conocido como satélite, que amplifica la señal óptica. La reflexión pasiva requiere más energía, por parte de las estaciones, pero es más flexible de usar.

- Infrarrojo de haz difuso. En este caso el haz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. Por lo tanto la línea de visión no es necesaria y la estación se puede orientar hacia cualquier lado. El modo difuso es el más flexible, en términos de localización y posición de la estación. Sin embargo, esta flexibilidad es a costa de excesivas emisiones ópticas.

FIGURA 4. DISPOSITIVOS CON TECNOLOGÍA DE INFRARROJO

En cuanto a las ventajas de los sistemas de infrarrojos, se encuentran:

- La transmisión por rayos infrarrojos no requiere ninguna autorización especial en ningún país (exceptuando la limitación de la potencia de la señal transmitida realizada por los organismos de salud).

- Utilizan componentes económicos y de bajo consumo energético, características importantes que se han de tener en cuenta en aquellos dispositivos que deban formar parte de equipos móviles portátiles.

- Son inmunes a interferencias de los sistemas de radio de alta frecuencia.

Sus principales inconvenientes son:

- No pueden pasar objetos sólidos como paredes, rocas, etcétera. Lo que supone un freno a su capacidad de difusión. Pero al mismo tiempo, esta limitación supone un seguro contra receptores no deseados.

- Las restricciones en la potencia de transmisión limitan la cobertura de estas redes a unas cuantas decenas de metros.

- No son utilizables en el exterior debido a que agentes naturales como la lluvia, la niebla, la luz solar directa, las lámparas incandescentes y otras fuentes de luz brillante pueden interferir seriamente la señal.

El estándar original IEEE 802.11 contemplaba el uso de infrarrojos, pero nunca llegó a desarrollarse debido principalmente a inconvenientes mencionados. No obstante, no cabe duda de que los sistemas infrarrojos son de los más eficaces sistemas de comunicaciones punto a punto para corta distancia.

IrDA (Infrared Data Association) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Actualmente tiene creados dos estándares:

- IrDA-Control. Es un protocolo de baja velocidad optimizado para ser utilizado en los dispositivos de control remoto inalámbricos, por ejemplo los dispositivos como los mandos a distancia, mouse o joysticks.

- IrDA-Data. Es un protocolo orientado a crear redes de datos de corto alcance. Está diseñado para trabajar a distancias menores de 1 metro y a velocidades que van desde los 9,6 Kbps hasta los 16 Mbps. Existe una versión que extiende el alcance a 2 metros, con un alto costo de consumo energético, y otra que reduce el alcance a 30 cm, reduciendo el consumo energético a la décima parte. Existen también varios protocolos opcionales que habilitan el protocolo IrDA-Data para ser utilizado en aplicaciones específicas, por ejemplo, IrCOMM (Emulador Infrarrojo de Puerto Serie Paralelo), IrTran-P (Transferencia de Imagen Digital con Infrarrojo), IrLAN (Conectividad de Red de Área Local con Infrarrojo) o IrMC (Comunicaciones Móviles con Infrarrojo).

1.4.2 Redes inalámbricas de área local

Se llama redes inalámbricas de área local (WLAN) a aquellas que tienen una cobertura de unos cientos de metros. Las tecnologías WLAN permiten a los usuarios establecer conexiones inalámbricas dentro de un área local (por ejemplo, un edificio corporativo o campo empresarial, o en un espacio público como un aeropuerto). Las WLAN se pueden utilizar en oficinas temporales u otros espacios donde la instalación de extenso cableado sería complicada, o para complementar una LAN existente de modo que los usuarios pueden trabajar en diferentes lugares dentro de un edificio a diferentes horas.

Las WLAN pueden operar de dos formas distintas. En las WLAN de infraestructura, las estaciones inalámbricas (dispositivos con radio-tarjetas de red o módems externos) se conectan a puntos de acceso inalámbrico que funcionan como puentes entre las estaciones y la red troncal existente. En las WLAN de igual a igual (ad-hoc), varios usuarios dentro de un área limitada, como una sala de conferencias, pueden formar una red temporal sin

utilizar puntos de acceso, si no necesitan obtener acceso a recursos de red.

En 1997, el IEEE aprobó la norma 802.11 para las WLAN, que especifica una velocidad de transferencia de datos de 1 a 2 Mbps. En el estándar 802.11b, que está emergiendo como la nueva norma dominante, los datos se transfieren a una velocidad máxima de 11 Mbps a través de una banda de frecuencia de 2.4 GHz. Otra norma reciente es la 802.11a, que especifica una transferencia de datos a una velocidad máxima de 54 Mbps a través de una banda de frecuencia de 5 GHz.

1.4.2.1 Wi-Fi

El sistema que se está imponiendo en las redes locales inalámbricas es el normalizado por el IEEE con el nombre de 802.11b. A esta norma se le conoce más habitualmente como Wi-Fi (Fidelidad Inalámbrica). Con el sistema Wi-Fi se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancias de hasta varias decenas de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps.

Wi-Fi es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11, se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice como punto de acceso para acceder a Internet.

Wi-Fi es una marca de la Alianza Wi-Fi, la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11. Debido a la importancia que implica Wi-Fi se explicará ampliamente en el capítulo 3.

1.4.2.2 HomeRF

En 1998 se creó un grupo de trabajo bajo el nombre de HomeRF (Radiofrecuencia Casera) con el objetivo de desarrollar un sistema de red inalámbrica para el hogar, que utiliza el sistema FHSS como Bluetooth. Aunque el grupo inicialmente lo formaron Compaq, HP, IBM, Intel y Microsoft, posteriormente se le han ido uniendo más miembros hasta casi alcanzar los 100 a finales del 2000. Actualmente cuentan con menos miembros debido a la proliferación de otras tecnologías.

A principios de 1999, HomeRF sacó la versión 1.0 de su protocolo SWAP (Protocolo de Acceso Compartido Inalámbrico), y tiene como objetivo la conectividad inalámbrica dentro del hogar, haciendo posible que los distintos usuarios puedan compartir voz y datos entre computadoras, periféricos, teléfonos inalámbricos y los nuevos dispositivos portátiles. La versión 2.0 de este producto salió en mayo de 2001. SWAP trabaja en la banda de frecuencias de 2.4 GHz y permite configuraciones de comunicaciones punto a punto y comunicaciones con punto de comunicación central.

La versión 1.0 permite transmitir datos a 1,6 Mbps y mantener hasta cuatro comunicaciones dúplex de voz. Tiene un alcance de unos 50 metros y una potencia de transmisión de 100 mW. Utiliza un protocolo similar a IEEE 802.11 para datos y otro similar a DECT para voz. La versión 2.0 alcanza los 10 Mbps y se espera que la versión 3.0 alcance los 40 Mbps para llegar a los 100 Mbps en versiones posteriores.

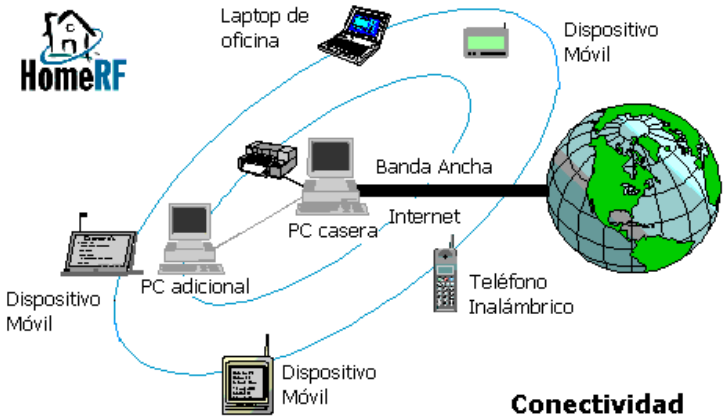


FIGURA 5. CONECTIVIDAD CON EL SISTEMA HOMERF

El Grupo de Trabajo HomeRF (HRFWG), es un grupo de compañías encargadas de establecer las normas a seguir y conseguir que los productos fabricados por las empresas integrantes de este grupo tengan una plena interoperabilidad.

Así mismo, la arquitectura del protocolo se asemeja bastante a las especificaciones que para las redes inalámbricas tienen el protocolo IEEE 802.11 en su capa física, extendiendo la capa MAC con la adición de un subconjunto de estándares DECT para proporcionar los servicios de voz. Como resultado, la capa MAC puede soportar indistintamente servicios orientados a datos tales como TCP/IP y protocolos de voz como DECT/GAP.

Actualmente, hay varios estándares y grupos de trabajo centrados en la tecnología inalámbrica del establecimiento de una red (RF). Éstos incluyen el IEEE 802.11, 802.16, y Bluetooth.

1.4.2.3 HiperLAN 1 e HiperLAN 2

HiperLAN (Red de Área Local de Radio de Alto Rendimiento) es el resultado de los trabajos de ETSI (Instituto Europeo de Normalización en Telecomunicaciones) para conseguir un estándar de red de área local inalámbrica vía radio. La primera versión de este estándar, HiperLAN 1, publicada en 1996, trabaja en la banda de frecuencias de 5 GHz y alcanza velocidades de hasta 24 Mbps.

En 1997 ETSI reconoció que HiperLAN 1 no estaba resultando viable comercialmente y creó un proyecto

llamado BRAN (Red de Acceso de Radio de Banda Ancha), el resultado se obtuvo en febrero del 2000 con HiperLAN 2. Este estándar está diseñado para ofrecer accesos inalámbricos de alta velocidad a redes ATM (Modo de Transferencia Asíncrono), a redes celulares de tercera generación, Firewire y redes IP.

La primera versión del estándar, llamada HiperLAN 1, comenzó en 1991. La meta original de HiperLAN era la alta tarifa de datos, más arriba del estándar 802.11. El estándar era en 1996 aprobado. La especificación funcional es EN300652, el resto está en ETS300836.

En 1999, se creó una asociación, HiperLAN 2 Global Forum, formada por Nokia, Tenovis, Dell, Ericsson, Telia y Texas Instrument, para promover el uso de este estándar, a pesar de ello, este sistema sigue sin alcanzar el éxito comercial deseado.

La especificación funcional HiperLAN 2 fue lograda en febrero del 2000. La versión 2 se diseña como conexión inalámbrica, rápida para muchas clases de redes. Los servicios básicos son datos, sonido, y transmisión de video. El énfasis está en la calidad de estos servicios (QoS).

El estándar cubre la comprobación, capas del control de trasmisión de datos y de la convergencia. La capa de la convergencia toma el cuidado de la funcionalidad dependiente del servicio entre DLC y la capa de red (OSI 3). Las subcapas de la convergencia se pueden utilizar también en la capa física para conectar redes del IP, de la atmósfera o de UMTS. Esta característica hace que HiperLAN 2 sea conveniente para la conexión inalámbrica de varias redes.

HiperLAN 2 ofrece velocidades de transmisión de 54 Mbps utilizando el sistema OFDM (Multiplexado Ortogonal por División de Frecuencia). Las frecuencias utilizadas son de 5.25 a 5.35 GHz para sistemas de interior a 200 mW de potencia y de 5.47 a 5.725 GHz para sistemas de exterior a 1000 mW de potencia.

1.4.3 Redes inalámbricas de área metropolitana

Se llaman redes de área metropolitana (WMAN), a aquellas redes que tienen una cobertura desde unos cientos de metros hasta varios kilómetros. El objetivo es poder cubrir el área de una ciudad o entorno metropolitano. Los protocolos LMDS (Servicio Local de Distribución Multipunto) o MMDS (Servicio Multicanal de Distribución Multipunto) ofrecen soluciones de este tipo.

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

Además, WMAN puede servir como copia de seguridad para las redes con cable, en caso de que las líneas alquiladas principales para las redes con cable no estén disponibles. WMAN utiliza ondas de radio o luz infrarroja para transmitir los datos. Las redes de acceso inalámbrico de banda ancha, que proporcionan a los usuarios acceso de alta velocidad a Internet, tienen cada vez mayor demanda. Aunque se están utilizando diferentes tecnologías, como el MMDS y los LMDS, el grupo de trabajo de IEEE 802.16 para los estándares de acceso inalámbrico de banda ancha sigue desarrollando especificaciones para normalizar el desarrollo de estas tecnologías.

1.4.3.1 LMDS

LMDS (Servicio Local de Distribución Multipunto) es una tecnología inalámbrica vía radio para comunicación entre puntos fijos. Esto quiere decir que no es una tecnología pensada para ser utilizada por terminales en movimiento. El rango de frecuencias utilizado varía entre 2 y 40 GHz dependiendo de la regulación legal del país en el que se utilice.

LMDS utiliza un transmisor central emitiendo su señal sobre un radio de hasta 5 kilómetros. Las antenas de los receptores se sitúan generalmente en la parte alta de los tejados de los edificios para procurar una visibilidad directa con el transmisor central.

Un inconveniente de los sistemas LMDS es que no existe un estándar que asegure la compatibilidad de los equipos de distintos fabricantes. En cualquier caso, en general, las soluciones LMDS no están teniendo una buena aceptación comercial.

1.4.3.2 IEEE 802.16

El Comité 802 del IEEE creó en 1999 un grupo de trabajo, el 802.16, con la idea de desarrollar un estándar de red inalámbrica metropolitana. El resultado publicado a principios de 2001 ha sido un sistema punto-multipunto que opera en la banda de frecuencias de 10 a 66 GHz. Posteriormente se empezó a desarrollar una nueva versión que opera en la banda de 2 a 11 GHz.

La norma IEEE 802.16 considera la utilización de distintos tipos de modulaciones, alcanzando distintas velocidades de transmisión: con QPSK (Modulación en Cuadratura por Salto de Fase) alcanza los 45 Mbps, con 16-QAM (Modulación de Amplitud en Cuadratura) alcanza los 90 Mbps y con 64-QAM los 150 Mbps.

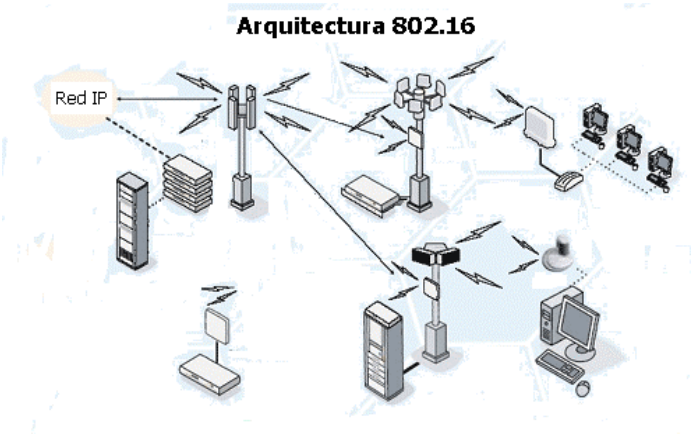


FIGURA 6. ARQUITECTURA DEL ESTÁNDAR IEEE 802.16

El estándar 802.16 (WiMAX) fue aprobado en diciembre de 2001. La tecnología 802.16 funciona de manera muy similar a la telefonía celular. El principal componente es una antena colocada en una torre con una cobertura de hasta 7,500 kilómetros cuadrados. El segundo elemento es el receptor WiMAX, que puede ser 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, dicha antena, podrá ser el punto de acceso a la red tanto de usuarios móviles como de otras antenas funcionando como repetidoras de la señal, 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.

1.4.3.3 HiperMAN e Hiperacces

ETSI se está ocupando también de sacar un estándar para redes WMAN. De los distintos trabajos realizados destacan tres proyectos:

- Hiperacces es un protocolo punto-multipunto que opera en la banda de 40.5 a 43.5 GHz y alcanza una velocidad de hasta 25 Mbps.

- HiperMAN, pos su parte, opera en la banda de 2 a 11 GHz y permite configuraciones punto a punto y en malla.

- Hiperlink está pensado para comunicaciones punto a punto de corto alcance (150 metros) con velocidades de hasta 155 Mbps operando en la banda de 17 GHz.

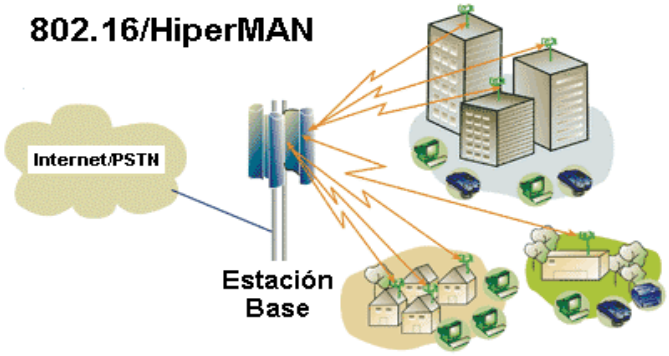


FIGURA 7. FUNCIONAMIENTO DE HIPERMAN

1.4.4 Redes inalámbricas globales

Los sistemas inalámbricos de cobertura global que existen son los sistemas de telefonía móvil. Los primeros sistemas de telefonía móvil fueron sistemas analógicos con muy pocas prestaciones para transmitir datos. Hasta finales de los años ochenta aparecieron los primeros sistemas digitales con posibilidades de transmitir datos. A esto sistemas se les ha conocido como sistemas de telefonía celular de segunda generación (2G). Éste es el caso de la tecnología europea GSM (Sistema Global para Comunicaciones Móviles) y de la norteamericana CDMA (Acceso Múltiple por División de Código).

Las tecnologías WWAN permiten a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como ciudades o países, mediante el uso de antenas en varias ubicaciones o sistemas de satélite que mantienen los proveedores de servicios inalámbricos. Los esfuerzos van encaminados a la transición desde redes 2G, algunas de las cuales tienen capacidades limitadas de movilidad y son incompatibles entre sí a tecnologías de tercera generación (3G) que seguirían un estándar global y proporcionarían capacidades de movilidad internacional. La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, y está promoviendo activamente el desarrollo de una norma global para 3G.

1.4.4.1 GSM

GSM es una tecnología estandarizada por el CEPT (Conferencia de Correos y Telecomunicaciones Europeas) a finales de los años ochenta. Su comercialización se llevo a cabo en Europa durante los primeros años de la década de los noventa y rápidamente alcanzó una cobertura global con cientos de millones de usuarios. Para conectar una computadora o PDA a un teléfono GSM, sólo hace falta un cable adaptador y el software apropiado. Un modo especial de transmisión de datos que admite GSM es el envío y recepción de mensajes cortos de texto (hasta 160 caracteres) mediante el servicio SMS (Servicio de Mensajes Cortos) desde el propio

terminal de telefonía móvil. Estos mensajes pueden intercambiarse tanto con otros terminales móviles, como con terminales de telefonía fija e Internet.

1.4.4.2 CDMA

CDMA es una tecnología desarrollada por la empresa Qualcomm. El gran mérito de esta tecnología es que supone una nueva forma de establecer comunicaciones inalámbricas multiusuario con un aprovechamiento de la capacidad seis veces mejor que TDMA. CDMA estuvo lista en 1988, aunque, posteriormente, con la ayuda de AT&T, Motorola y otros fabricantes, se desarrolló una nueva versión dual (analógica y digital) a la que se llamó IS-95, y la que ha sido la que se ha instalado en distintos países. La primera implantación de la tecnología CDMA tuvo lugar en Hong Kong en 1995. CDMA también ofrece el servicio SMS de mensajes cortos.

1.4.4.3 2,5 G

Aunque los sistemas 2G tienen ciertas capacidades de transmisión de datos, fundamentalmente se trata de un sistema que da soporte a servicios de voz. Para ofrecer servicios de datos, se ha pensado en una nueva generación de redes celulares. No obstante, mientras se desarrolla convenientemente la tecnología para poder ofrecer servicios 3G, se ha creado una ampliación de la tecnología 2G a la que se ha llamado 2,5G.

Esta tecnología de transición añade nuevas capacidades de transmisión de datos a la infraestructura de red celular existente. Existen distintas tecnologías 2,5G:

- GPRS (Servicio General de Radio Paquetes). Esta tecnología añade a las redes GSM la posibilidad de transmitir paquetes de datos. Utiliza la misma infraestructura de red que permite utilizar un conjunto de protocolos para la transmisión de paquetes de datos. La tecnología GPRS permite transmitir datos a velocidades de hasta 171 Kbps. Esta tecnología se ha implementado fundamentalmente en Europa, aunque se está expandiendo a aquellas otras regiones con sistemas GSM.

- EDGE (Velocidades Mejoradas de Datos para la Evolución GSM). Se trata de una variación de la tecnología GPRS que permite alcanzar velocidades de datos de hasta 384 Kbps. Para conseguir esto, se utiliza parte del canal de voz.

- IS-95B. Esta tecnología añade la capacidad de transmitir datos a 64 Kbps a las redes CDMA. Esta tecnología se ha implementado principalmente en Corea, Japón y Norteamérica.

- IMode. Esta tecnología desarrollada en Japón es complementaria a las redes CDMA. Permite entregar correo electrónico y navegar por los servicios ofrecidos por los proveedores de información. La velocidad de transmisión es de 9,6 Kbps.

1.4.4.4 3 G

Se puede decir que la tecnología celular de tercera generación (3G) comenzó en 1985 cuando la UIT anunció su iniciativa de crear un nuevo sistema de comunicaciones móviles al que llamó FPLMTS (Futuro Sistema Público de Telecomunicaciones Móviles Terrestres). Esta iniciativa se concretó en 1996 con la creación de IMT2000 (Comunicaciones Móviles Internacionales). El número 2000 se le puso porque se esperaba que la nueva tecnología estuviera lista para la primera década del nuevo milenio y por que la banda de frecuencia asignada era 2 GHz (2000 MGz).

El objetivo de IMT2000 es definir un marco dentro del cual puedan existir distintas tecnologías 3G, asegurándose la interoperabilidad de servicios (roaming, portabilidad, multimedia, etcétera). IMT pretende disponer de un sistema universal de comunicaciones que cubra todo tipo de redes: con cables y sin cables, terrestres y satelitales.

Después de muchas luchas entre todos los grupos de interés, finalmente se llegó a un acuerdo de tecnología única en marzo de 1999. Esta tecnología se basa en una base única, conocida como WCDMA (CDMA de Banda Ancha), desarrollada en Japón por NTT DoCoMo, sobre la que se desarrollan tres modos opcionales:

- UMTS (Sistema Universal de Telecomunicaciones Móviles). Es el estándar europeo creado como evolución de la arquitectura GSM MAP basada en WCDMA. Ofrece servicios de voz, fax, mensajes multimedia, así como servicios de datos a velocidades de hasta 2 Mbps.

- CDMA-2000. Es una evolución del estándar americano CDMA One. La particularidad de esta tecnología es que, a finales del año 2000, se convirtió en la primera tecnología 3G que ve el mercado. Los primeros en comercializarla fueron las empresas coreanas SK Telecom y KT Freetel. Esta primera versión permite transmitir datos a 300 Kbps.

- TD-SCDMA (División de Tiempo-Acceso Múltiple Síncrono por División de Código). Es una combinación de las técnicas TDMA y CDMA. Esta tecnología ha sido desarrollada por Siemens y CATT, academia china para la tecnología de las telecomunicaciones. Su mayor ventaja es que permite operar con las redes 2G.

Desde el punto de vista de la transmisión de datos, la 3G define tres modalidades de transmisión: 144 Kbps para usuarios de mucha movilidad, 384 Kbps para usuarios con movilidad limitada y 2 Mbps para usuarios sin movilidad.

1.5 Ventajas y desventajas de WLAN sobre LAN

Las redes locales inalámbricas más que una sustitución de las LAN's convencionales son una extensión de las mismas, ya que permite el intercambio de información entre los distintos medios en una forma transparente al usuario.

En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas. Enlazando los diferentes equipos o terminales móviles asociados a la red. Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 10 Mbps frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional.

Las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite. En general las WLAN se utilizarán como complemento de las redes fijas.

1.5.1 Ventajas

Ahora que las tecnologías inalámbricas, se están convirtiendo en una solución sólidamente asentada en las empresas, sus inherentes ventajas económicas y funcionales están haciendo posible que empiecen a dejar de estar presentes casi exclusivamente en proyectos de acción limitada para ser desplegadas como soluciones clave para la empresa a escala corporativa. Al mismo tiempo, su campo de aplicación, antes casi siempre reducido a sectores verticales, como almacenes, logística u hospitales, abarca ya a todo tipo de actividad.

Las ventajas principales que ofrecen las redes WLAN's son las siguientes:

- Movilidad: esta es la ventaja más fuerte frente a las redes cableadas, tanto en el ámbito empresarial como en un hogar debido al gran auge de los portátiles. Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red cableada. Su reducida cobertura puede ampliarse a través de antenas, cubriendo hasta 50 kilómetros o más. Los usuarios tienen acceso a los datos en cualquier lugar y en cualquier momento lo que proporciona un aumento potencial de productividad y servicio sobre las LAN tradicionales.

- Reducción de costos: Evita el uso de cables y costosas instalaciones. Por otra parte, tanto los puntos de acceso como las tarjetas PCMCIA tienen un costo relativamente considerable. Además los

proveedores Wi-Fi pueden ofrecer acceso de banda ancha a un precio muy inferior al del acceso tradicional. Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN cableada, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes. Si se compara con el costo de implantación de UMTS, la ventaja competitiva de Wi-Fi resulta inmensa.

- Facilidad de instalación: Basta un dispositivo como una computadora portátil o una agenda personal, equipado con tarjeta inalámbrica PCMCIA y un nodo de acceso de red. Además las redes inalámbricas se han simplificado en los últimos tiempos tanto en lo referente a la configuración como al uso. El tiempo que más consume la instalación de una red inalámbrica es la instalación de los puntos de acceso con la red local de la empresa, el cual puede durar días. Sin embargo, la implementación en redes fijas puede durar semanas.

- Robustez: Las redes basadas en cableado estructurado son por lo general más robustas frente a interferencias y condiciones adversas que las inalámbricas. Sin embargo, en ciertos entornos como en: fábricas con elevada humedad, agentes químicos agresivos, calor, etcétera. Las instalaciones cableadas pueden sufrir una rápida degradación o ser inviables. Una instalación inalámbrica adecuadamente ubicada para resguardarse de dichos entornos puede ser la alternativa idónea.

- Provisionalidad: si se va a instalar una red provisional esta es la mejor opción, por ejemplo, en ferias, oficinas temporales o crecimientos urgentes en una red ya establecida.

- Escalabilidad: Los sistemas de WLAN’s pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones especificas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red. Puede aumentarse sin límite y de forma paulatina la cobertura de la red y su capacidad de transmisión.

- Velocidad simétrica: A diferencia del ADSL, Wi-Fi es bidireccional, pudiendo recibir y enviar datos a la misma velocidad. Es por tanto útil para prestar una gran variedad de servicios que requieren idéntico ancho de banda para recepción y para envío de datos.

- Cobertura en zonas sin infraestructuras de telecomunicaciones: Wi-Fi posibilita el acceso a Internet de banda ancha a explotaciones, núcleos rurales, empresas o lugares que hasta la fecha por distintas razones han quedado al margen del despliegue de otras infraestructuras de telecomunicaciones (ADSL, cableo incluso la línea telefónica).

- Funcionamiento sin errores: En los estándares 802.11b y 802.11g, los dispositivos se comunican siempre a la mayor velocidad soportada que sea posible. Si la intensidad de la señal o las interferencias están degradando los datos, los dispositivos cambiarán su velocidad, disminuyendo a valores más bajos que no provoquen errores. Aunque esto pueda significar una reducción de la velocidad permite que la red siga funcionando.

1.5.2 Desventajas

A pesar de que esta tecnología esta en vías de desarrollo aún no ha podido eliminar las debilidades de su funcionamiento, sin embargo, en la actualidad se realizan esfuerzos por mejorar las características necesarias que permitan usar está tecnología de manera confiable. Las desventajas que presentan las redes inalámbricas son las siguientes:

- Seguridad: Sin duda su punto más débil, en primera instancia son inseguras dado que el medio de transporte es el aire. Además el sistema de cifrado que se utiliza en redes inalámbricas (cifrado WEP) está basado en algoritmos de cifrado de 40 bits. Actualmente están desarrollados sistemas de cifrado de 128 bits propios de las redes con hilos (WEP2). Existen otros sistemas de cifrado más seguros, aunque todavía no están suficientemente extendidos, ya sea por desconocimiento, como por incompatibilidad de dispositivos que no los soportan. Por otra parte, muchos usuarios (tanto particulares como empresariales) están acostumbrados a su utilización sin sistema de seguridad alguno, lo que puede ocasionar graves problemas, especialmente patentes en las intrusiones en intranets. Desde que comenzó su implantación se está mejorando constantemente los algoritmos de encriptación de datos anteriores. Aunque hace ya varios años que se detectaron las vulnerabilidades del protocolo WEP, razón por la que fue sustituido por WPA basado en TKIP (Protocolo de Integridad de Clave Temporal). Esta nueva especificación utiliza el algoritmo de cifrado AES, un mecanismo extremadamente seguro que mereció en su día la aprobación del instituto NIST (Instituto Nacional de Tecnología y Estándares). WPA 2 (Acceso Protegido Wi-Fi 2) se basa en el estándar 802.11i, y como tal constituye la propuesta de la Alianza Wi-Fi para un mercado muy convulsionado por las muchas vulnerabilidades descubiertas en los protocolos de seguridad utilizados en las redes inalámbricas. Por supuesto, esta nueva versión es compatible con WPA. No cabe duda de que la llegada de 802.11i (o WPA 2) representa una herramienta más eficaz debido al elevado nivel de seguridad que ofrece. Aun así, es necesario tener en cuenta que el algoritmo de cifrado AES requiere unas condiciones y una exigencia al hardware bastante alta, lo que significa que algunas controladoras inalámbricas antiguas no serán capaces de satisfacer los requisitos de este estándar.

- Velocidad de transferencia de datos: Las velocidades de transferencia de datos no serán típicamente tan buenas como en una red atada con alambre. Todos los usuarios de la red inalámbrica tienen que

compartir el ancho de banda (típicamente 11 Mbps ó 54 Mbps), mientras que en una LAN se consiguen velocidades de 100 Mbps.

- Alcance limitado: Las áreas que Wi-Fi puede cubrir en edificios pueden llegar a distancias comprendidas entre los 75 y 120 metros. La estructura de los edificios representan un problema importante para la transmisión a través de Wi-Fi. En áreas abiertas el alcance puede llegar a 300 metros. Esta carencia en la cobertura puede eliminarse mediante la interconexión a través de antenas.

- Protocolos de la transferencia de datos: El uso de la radio agrega ciertos gastos indirectos a cada paquete de la información intercambiado. El protocolo de control TCP/IP requiere muchos paquetes pequeños para ser intercambiado (para establecer un acoplamiento) e incluso después del acoplamiento están los datos establecidos que se transfieren en paquetes. Los gastos indirectos agregados por la radio pueden causar problemas con él “estado latente” que podría conducir al otro equipo en la red una posible desconexión y así solicitar una retransmisión. Esto puede dar lugar a una conexión mucho más lenta, mientras que el ancho de banda se sobrecarga por las retransmisiones.

- Estándares y limitaciones: Hay también limitaciones referentes a las redes inalámbricas. Todos los productos inalámbricos tienen que apoyar estándares internacionales. Las instituciones internacionales introducen prácticas y también limitan las frecuencias usadas en el equipo inalámbrico. El publicar y la puesta en práctica de regulaciones de esta clase toma tiempo. Por esta razón algunas compañías están produciendo los productos a los cuales se han aplicado patentes. Esto significa que los productos de dos compañías separadas pueden trabajar entre sí. En esta situación los productos se deben pedir solamente a partir de una compañía si esos productos se utilizan en una misma red inalámbrica. La Alianza Wi-Fi fue formada para probar y certificar estándares y para promover interoperabilidad, pero los estándares todavía se están desarrollando y los vendedores incluyen sus propias características propietarias así que la interoperabilidad es a menudo difícil de alcanzar.

- Operaciones globales: Hay también una desventaja relacionada con la operación global. En teoría, el equipo inalámbrico que se conforma con el estándar común tiene que funcionar por todo el mundo. Un dispositivo que se compra en Finlandia tiene que funcionar también en los Estados Unidos. Al menos cambiar los ajustes del adaptador para funcionar en las radiofrecuencias permitidas en otro país puede requerir la reinstalación de los conductores, que pueden estar más allá de las capacidades de muchos usuarios.

- Ancho de banda compartido: Los usuarios conectados a través de un mismo punto, comparten el ancho de banda, por lo cual la velocidad teórica comentada, puede reducirse de forma considerable si no se

ha realizado un correcto análisis de las conexiones. Por lo tanto, la velocidad obtenida está sujeta al número de usuarios conectados.

- Posibles interferencias: Wi-Fi en las versiones más extendidas (802.11b y 802.11g) trabaja en la frecuencia de 2.4 GHz. Casi todos los productos Wi-Fi mencionan las posibles interferencias en el ámbito doméstico con los populares microondas, sin embargo, en múltiples experimentos se ha comprobado que las interferencias con tales aparatos no se manifiestan. Otro posible punto de interferencia podría surgir con los dispositivos conforme a otros estándares como Bluetooth, que operan en la misma frecuencia, aunque los respectivos consorcios de normalización aspiran a solucionar estos problemas. Wi-Fi a través del estándar 802.11a, trabaja en la frecuencia de entre 5,15 y 5,35 GHz y son patentes los problemas de interferencias, fundamentalmente con las redes de satélites y redes militares. Este espectro está sumamente saturado en EE.UU. y desde el gobierno americano, se buscan soluciones para que sus sistemas de defensa liberen parte del espectro.

- Posibles repercusiones sobre la salud: No existen conclusiones claras al respecto por la frecuencia utilizada (la banda de 2.4 GHz), pero podría tener consecuencias de calentamiento (similar a los microondas). Pero la potencia de emisión es considerablemente inferior a la de sistemas como el de la telefonía móvil.

Capítulo 2 – IEEE y ETSI

2.1 Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

El 13 de mayo de 1884, el AIEE (Instituto Americano de Ingenieros Electrónicos) fue creado en Nueva York, al inicio los intereses principales del AIEE eran comunicaciones del alambre (telégrafo y telefonía) y sistemas de la luz y de energía.

La Sociedad de Radio e Ingenieros de Telégrafo y el Instituto Inalámbrico se combinaron en 1912 para formar una sociedad internacional para científicos e ingenieros, el IRE (Instituto de Ingenieros de Radio). Muchos de los primeros miembros de la IRE también eran los miembros del AIEE. El desarrollo estructural y las actividades generales de ambas organizaciones eran similares.

Después de la Segunda Guerra Mundial, las dos organizaciones se hicieron cada vez más competitivas. Al realizar actividades similares los problemas de duplicación de esfuerzos surgieron, sólo parcialmente se resolvían por comités conjuntos y reuniones. En 1961, tanto el IRE como el AIEE procuraron resolver estas dificultades por la consolidación. Un plan de fusión fue formulado y aprobado. Así, el IEEE fue formado el 1 de enero de 1963 con la fusión de AIEE e IRE.

El IEEE es una organización no lucrativa, profesional a nivel internacional para el adelanto de la tecnología relacionado con la electricidad. Tiene la mayoría de los miembros de cualquier organización profesional técnica en el mundo. El IEEE consiste en más de 365,483 miembros, incluyendo a 68,000 estudiantes en más de 150 países, 311 secciones en diez regiones geográficas, aproximadamente 1,570 capítulos que unen a miembros locales con intereses similares técnicos, 39 sociedades y 5 consejos técnicos que representan la amplia gama de intereses técnicos y más de 300 conferencias por todo el mundo cada año. Además, el IEEE produce 30 por ciento de la literatura del mundo en la ingeniería y los campos eléctricos y de electrónica informática. El IEEE cuenta con un centro de historia cuya misión es de conservar, investigar y promover la historia de tecnologías de la información y eléctricas. La mayor parte de los recursos del centro de historia están disponibles en www.ieee.org la página web de IEEE.

La misión de IEEE es promover el proceso de la ingeniería de creación, desarrollo e integración, compartiendo y aplicando el conocimiento sobre electrónica y tecnologías de la información y ciencias en beneficio de la humanidad y la profesión.

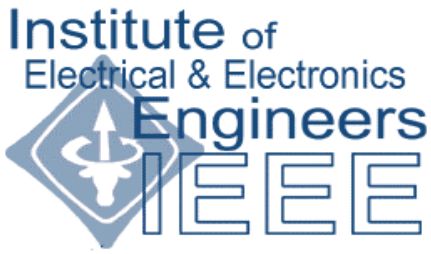


FIGURA 8. LOGOTIPO DEL INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS

El IEEE define los propósitos de la organización como científicos y educativos. En perseguir estas metas, el IEEE sirve como editor importante de diarios científicos y de un organizador de las conferencias. Es también revelador principal de estándares industriales en una amplia gama de disciplinas, incluyendo energía y energía eléctrica, tecnología de información, aseguramiento de la información, las telecomunicaciones, electrónica de consumidor, transporte, espacio aéreo, y nanotecnología. La meta de los programas de la educación de IEEE es asegurar el crecimiento de la habilidad y conocimiento entre la profesión técnica y fomentar la comisión individual a la formación permanente entre los miembros de IEEE, la ingeniería y la comunidad científica, y el público en general. IEEE, en la actualidad ofrece oportunidades educativas tales como experto IEEE, el programa de los socios de la educación, y estándares en la educación.

Otra forma de identificar el impacto de IEEE es su diccionario, publicado en intervalos de cuatro a cinco años y que en la actualidad cuenta con su séptima edición. Esta edición contiene aproximadamente 35,000 términos técnicos que se relacionan con distintas iniciativas eléctricas, computacionales y de comunicaciones pertenecientes a más de 800 estándares IEEE.

Todas las publicaciones de IEEE, incluyendo los diarios, las transacciones y los estándares son accesibles en línea para los suscriptores en IEEE Xplore. La base de datos de Xplore consiste en 1.2 millones de documentos.

En el año 2005, IEEE tenía cerca de 900 estándares activos, con aproximadamente 700 estándares bajo desarrollo. Uno de los estándares más notables de IEEE es el grupo de IEEE 802 LAN/MAN de estándares que incluye el estándar IEEE 802.3 (Ethernet) y del estándar del establecimiento de una red de la radio de IEEE 802.11. El proceso de desarrollo de los estándares de IEEE es el siguiente:

1. **Selección de los patrocinadores.** El patrocinador es la organización que asume la responsabilidad del trabajo de esbozar el documento de los estándares y asegurar su paso oportuno a través de las distintas fases de despliegue de un estándar.

2. **Emisión de la solicitud de autorización del proyecto (PAR**). La PAR es un documento conciso de tres a cuatro páginas que indica que el estándar nuevo ha sido aprobado para ser considerado dentro del IEEE. Este documento es aprobado por el Comité de Estándares Nuevos (NesCom), del IEEE. La PAR es un documento que está altamente detallado, cuando una PAR ha sido aprobada, debe ser terminada dentro de cuatro años, si el estándar requiere de un periodo más largo, se debe de adquirir una solicitud de extensión de tiempo por parte del NesCom.

3. **Aprobación de la PAR**. Las PAR normalmente son revisadas cada trimestre por el NesCom, en la mayor parte de los casos, el comité ofrece información y comentarios para las mejoras a la PAR. Esto es de mucha importancia, debido a que la PAR detalla el alcance y propósito del estándar.

4. **Organización del grupo de trabajo**. Cuando la PAR ha sido aprobada por el NesCom, se organiza un grupo de trabajo, los puestos típicos de un grupo de trabajo pueden, en general, incluir los siguientes: presidente, vicepresidente, secretario, tesorero, editor técnico, coordinador de votación y enlace de los estándares internacionales, con el fin de manejar la agenda en términos de revisión de minutas, asuntos nuevos, asuntos previos y otros aspectos. Al igual que la PAR, la duración del grupo de trabajo es de cuatro años, sin embargo, este periodo puede extenderse.

5. **Desarrollo del pre-proyecto del estándar.** El pre-proyecto del estándar debe finalizarse mediante el esfuerzo del grupo de trabajo y en general es una tarea complicada e incluso desalentadora. Debe basarse en la PAR y comienza mediante una descripción general, debido a que es muy común que existan distintos autores del pre-proyecto, la coordinación del tono, contenido y alcance está dirigida por el editor técnico y los oficiales del grupo de trabajo.

6. **Votación sobre el pre-proyecto del estándar.** El propósito de votar sobre un estándar propuesto es el de asegurar el grado más alto posible de consenso entre las partes que serán afectadas por el estándar, o cuando la votación es solamente interna en el IEEE, para asegurar el grado más grande posible de consenso que se puede alcanzar entre los distintos comités. Se considera que un pre-proyecto de un estándar ha logrado un consenso cuando el 75% de los votantes aprueba el estándar. El grupo de votación normalmente está formado por tres tipos de grupos: proveedores de tecnología, usuarios finales y otras partes interesadas que podrían o no estar asociadas directamente con el estándar propuesto.

7. **Aprobación del pre-proyecto del estándar**. Enseguida de la aprobación del estándar a través de la votación y el proceso de comentarios, se envía al Comité de Revisión (RevCom) el cual revisa todo el proceso que se ha llevado hasta esa fecha en relación con el intento de desplegar el estándar nuevo. Cuando el RevCom está satisfecho respecto a que el proceso ha cumplido con las reglas y procedimientos del IEEE, emite una recomendación de aprobación al NesCom.

8. **Publicación del estándar aprobado**. Cuando el NesCom ha aprobado la recomendación del RevCom, el estándar debe ser revisado por el editor de estándares quien comprueba que el estándar es correcto en cuanto a la gramática y sintaxis del inglés de Estados Unidos y asegura que se adhiere al formato establecido expresamente en un documento titulado Manual de estilo para los estándares IEEE. Posteriormente, la revisión final del pre-proyecto del estándar la efectúa el presidente del grupo de trabajo o un delegado asignado, con el fin de comprobar que la versión editada y formateada del pre-proyecto del estándar continúe siendo consistente con la PAR y el contenido técnico del pre-proyecto. Después de esta revisión final, el pre-proyecto se convierte en un estándar, que enseguida se distribuye a través de canales de medios normales tanto dentro como fuera del IEEE.

Además el IEEE también cuenta con un programa de premios para honrar logros en la educación, la industria, la investigación y el servicio. Cada premio tiene una misión única y criterios, y ofrece la oportunidad de distinguir a colegas, profesores inspiradores y líderes corporativos, también establece premios conjuntos con sociedades nacionales en otros países para reconocer a los individuos que han hecho aportaciones significativas en el aspecto técnico, educativo o atienden contribuciones a la profesión de la ingeniería o a la sociedad en general.

Las concesiones y honores de IEEE son las siguientes:

- Medalla de honor IEEE
- Medalla IEEE Alexander Graham Bell
- Medalla IEEE Edison
- Medalla IEEE James H. Mulligan
- Medalla IEEE por Excelencia
- Medalla IEEE Fundadores
- Medalla IEEE Richard W. Hamming
- Medalla IEEE Heinrich Hertz Medalla
- Medalla IEEE Jack S. Kilby
- Medalla IEEE Lamme
- Medalla IEEE Nishizawa
- Medalla IEEE Robert N. Noyce
- Medalla IEEE Dennis J. Picard
- Medalla IEEE Simon Ramo
- Medalla IEEE John von Neumann
- Concesión IEEE Nikola Tesla
- Concesión internacional IEEE SA
- Concesión de Steinmetz del Proteus IEEE
- Concesión del Internet de IEEE

Después de la fusión del Instituto de Ingenieros de Radio y el Instituto Americano de Ingenieros Electrotécnicos en 1963, la Medalla de honor IEEE se hizo el premio más alto del IEEE. Se otorga por realizar una contribución excepcional a la ciencia y la tecnología o una carrera extraordinaria en los campos de IEEE de interés.

2.1.1 La alianza de compatibilidad de Ethernet inalámbrico y Wi-Fi

A finales de la década de los 90, los líderes de la industria inalámbrica (3Com, Aironet, Lucent, Nokia, Symbol Technologies, etcétera) crean la Alianza Wi-Fi (antes conocida como WECA), una alianza para la compatibilidad ethernet inalámbrica, el objetivo de la Alianza Wi-Fi es el de certificar la interoperabilidad y compatibilidad de los productos de redes inalámbricas 802.11b y promover este estándar para la empresa y el hogar. Para indicar la compatibilidad entre dispositivos inalámbricos, tarjetas de red o puntos de acceso de cualquier fabricante, se les incorpora el logotipo de “Wi-Fi”, y así los equipos con esta marca, soportada por más de 150 empresas, se pueden incorporar en las redes sin ningún problema, siendo incluso posible la incorporación de terminales telefónicos Wi-Fi a estas redes para establecer llamadas de voz.

Una de las características más importantes respecto a la Alianza Wi-Fi es que está adoptando y promoviendo un estándar, que está enfocado a un campo amplio de usuarios, desde los empresariales, usuarios residenciales, áreas públicas que se utilizan intensamente como aeropuertos, hoteles, edificios recreativos, etcétera.

Es interesante señalar que Wi-Fi también trabaja con los Grupos de Interés Especial (SIG) de Bluetooth, debido a que la frecuencia de 802.11b y las frecuencias de Bluetooth son similares y ambas usan el espectro expandido. La alianza entre Bluetooth y Wi-Fi tiene como objetivo promover la capacidad de que ambos protocolos operen en un entorno físico común. En tanto que los dispositivos Wi-Fi principalmente conectarán PC’s e impresoras, el propósito de Bluetooth es esencialmente enfocarse a los productos electrónicos más pequeños, como las cámaras digitales, PDA’s y teléfonos celulares.

2.2 Estándares 802.11

En junio del año 1997 el IEEE ratificó el estándar para WLAN IEEE 802.11, que alcanzaba una velocidad de 2 Mbps, con una modulación de señal de espectro expandido por secuencia directa (DSSS), aunque también contempla la opción de espectro expandido por salto de frecuencia (FHSS), en la banda de 2.4 GHz, y se definió el funcionamiento y la interoperabilidad entre redes inalámbricas.

El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2.4 GHz, o infrarroja, con regímenes binarios de 1 a 2 Mbps. Este estándar define el Control de Acceso al Medio (MAC) y las capas físicas (PHY) para una LAN con conectividad inalámbrica. En el siguiente capítulo se realiza una descripción de la arquitectura 802.11 y de las diversas topologías incorporadas para clarificar las características únicas del

estándar de las LAN inalámbricas de tipo IEEE 802.11. La dificultad en detectar la portadora en el acceso WLAN consiste básicamente en que la tecnología utilizada es CDMA, lo que conlleva a que el medio radioeléctrico es compartido, ya sea por secuencia directa DSSS o por saltos de frecuencia en FHSS. El acceso por código CDMA implica que pueden coexistir dos señales en el mismo espectro utilizando códigos diferentes, y eso para un receptor de radio implicará que detectaría la portadora inclusive con señales distintas de las de la propia red WLAN. Hay que mencionar que la banda de 2.4 GHz está reglamentada como banda de acceso público y en ella funciona gran cantidad de sistemas, entre los que se incluyen los teléfonos inalámbricos Bluetooth.

El estándar IEEE 802.11 está orientado al desarrollo de redes de área local inalámbricas con aplicación dentro de espacios interiores. Esto no ha sido impedimento de que existan aplicaciones Wi-Fi más allá de su concepción inicial, llegando incluso a pensar en la posibilidad de dar cobertura inalámbrica a áreas metropolitanas, cubriendo por entero una pequeña ciudad. El hecho de utilizar una banda de frecuencias no regulada y la interoperabilidad entre dispositivos de diversos fabricantes, junto con la reducción de precios, ha hecho que su aplicación y expectativas de uso se hayan desarrollado enormemente. La economía en el despliegue en este tipo de redes, así como el carácter de uso “libre” del espectro, ha hecho que algunos vean estas soluciones como una amenaza, o alternativa, al servicio de acceso a Internet inalámbrico a través de tecnologías UMTS ofrecido por los operadores de redes móviles.

2.2.1 802.11 legado

Los protocolos utilizados por todas las variantes 802, entre ellas Ethernet, tienen ciertas similitudes de estructura. El estándar 802.11 de 1997 especifica tres técnicas de transmisión permitidas en la capa física. El método de infrarrojos utiliza en su mayor parte la misma tecnología que los controles remotos de televisión. Los otros dos métodos utilizan el radio de corto alcance, mediante técnicas conocidas como FHSS y DSSS, éstas utilizan parte del espectro que no necesita licencia (la banda de 2.4 GHZ).

La versión original del estándar IEEE 802.11 liberado en 1997 especifica dos tarifas de datos de 1 y 2 Mbps para ser transmitido vía infrarrojo (IR) o en la frecuencia ISM en 2.4 GHz. IR está incorporado en una parte del estándar, pero no tiene ninguna puesta en práctica real.

El estándar original también define el Acceso Múltiple de Portador de Sentido con la Anulación de Colisión (CSMA/CA) como el método de acceso de medios de comunicación. Un porcentaje significativo de la capacidad de canal disponible es sacrificado (vía los mecanismos CSMA/CA) para mejorar la fiabilidad de transmisiones de información en condiciones ambientales diversas y adversas. La herencia 802.11 rápidamente fue complementada y popularizada por el estándar 802.11b. La adopción extendida de las redes 802.11 sólo ocurrió después de que el estándar 802.11b fue ratificado y por consiguiente pocas redes corrieron en el estándar 802.11.

2.2.2 802.11a

El IEEE ratificó en julio de 1999 el estándar 802.11a (los productos comerciales que comienzan ha aparecer a mediados del 2002), que opera en la banda de 5 GHz, que con una modulación QAM-64 y la codificación OFDM alcanza una velocidad de hasta 54 Mbps, menos congestionada y, por ahora, con menos interferencias, pero con un alcance limitado a 50 metros, lo que implica tener que contar con más puntos de acceso como si se utilizará el estándar 802.11b para cubrir la misma área, con el costo adicional que ello implica. La banda de 5 GHz que utiliza se denomina UNII (Infraestructura de Información Nacional sin Licencia), que en los Estados Unidos está regulada por la FCC, el cual ha asignado un total de 300 MHz, cuatro veces más de lo que tiene la banda ISM, para uso sin licencia, en tres bloques de 100 MHz, siendo en el primero la potencia máxima de 50 mW, en el segundo de 250 mW, y en el tercero puede llegar hasta 1W, por lo que se reserva para aplicaciones en el exterior.

Mientras se desarrollaba el estándar 802.11b, la IEEE crea una nueva extensión del estándar 802.11 denominada 802.11a. Debido a su alto costo, la 802.11a suele utilizarse en redes de empresas, mientras que la 802.11b se usa más en redes domésticas.

Por otro lado, como la 802.11a y la 802.11b utilizan frecuencias distintas, ambas tecnologías son incompatibles entre ellas. Algunos fabricantes ofrecen híbridos (802.11a/b), aunque estos productos lo que tienen realmente son las dos extensiones implementadas. Las ventajas que ofrece es la velocidad máxima alta, soporte de muchos usuarios a la vez y no produce interferencias en otros aparatos. Los inconvenientes son alto costo y bajo rango de señal que es fácilmente obstruido.

2.2.3 802.11b

En el año 1999, se aprobó el estándar 802.11b, una extensión de la familia 802.11 para WLAN empresariales, con una velocidad de 11 Mbps (otras velocidades normalizadas a nivel físico son: 1, 2 y 5,5 Mbps) y un alcance de 100 metros, que al igual que Bluetooth y HomeRF, también emplea la banda de ISM de 2.4 GHz, pero en lugar de una simple modulación de radio digital y salto de frecuencia (FHSS), utiliza una modulación lineal compleja (DSSS). Permite mayor velocidad, pero presenta una menor seguridad, y el alcance puede llegar a los 100 metros, suficientes para un entorno de oficina o residencial.

IEEE 802.11b es el estándar que lidera los desarrollos actuales de WLAN. Emplea solamente la tecnología DSSS y utiliza una modulación con forma de onda CCK (Clave del Código Complementario) lo que permite alcanzar hasta 11 Mbps de velocidad.

El estándar 802.11b utiliza la misma frecuencia de radio que el tradicional estándar 802.11 (2.4GHz). El problema es que al ser esta una frecuencia sin regulación, se podían causar interferencias con hornos de

microondas, teléfonos móviles y otros aparatos que funcionen en la misma frecuencia. Sin embargo, si las instalaciones 802.11b están a una distancia razonable de otros elementos, estas interferencias son fácilmente evitables. Además, los fabricantes prefieren bajar el costo de sus productos, aunque esto suponga utilizar una frecuencia sin regulación.

2.2.4 802.11e

El estándar IEEE 802.11e, a finales del año 2005 fue aprobado cómo un estándar que define un juego de calidad de servicio para usos de una LAN, en particular el estándar 802.11. El estándar original 802.11 define otra función de coordinación que se llamó la Función de Coordinación de Punto (PCF): esto está disponible sólo en el modo "de infraestructura", donde las estaciones son conectadas a la red por un punto de acceso (AP).

Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN. Se aplica a los estándares físicos a, b y g de la familia 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y vídeo.

2.2.5 802.11f

El estándar IEEE 802.11f o el protocolo de punto de interacceso es una recomendación que describe una extensión opcional al estándar IEEE 802.11 que proporciona comunicaciones de punto de acceso inalámbricas entre sistemas de multivendedor.

Su objetivo es lograr la interoperabilidad de AP’s dentro de una red WLAN multi-proveedor. El estándar define el registro de AP’s dentro de una red y el intercambio de información entre dichos puntos de acceso cuando un usuario se traslada desde un punto de acceso a otro.

La operación del protocolo esta diseñada para la ejecución de asociación única en todas partes de un juego de servicio ampliado y para el cambio seguro del contexto de seguridad de la estación. Basado en el nivel de seguridad, las llaves de sesión de comunicación entre AP’s son distribuidas por un servidor de radio. El servidor de radio también proporciona un servicio de trazar un mapa de la dirección MAC del AP y la dirección de IP.

2.2.6 802.11g

En el 2003 apareció el estándar denominado 802.11g. El nuevo estándar 802.11g para comunicaciones inalámbricas, establece las reglas básicas para equipos WLAN capaces de funcionar a velocidades de entre 24 Mbps y hasta 54 Mbps, y al mismo tiempo compatible con los equipos 802.11b existentes que funcionan a un máximo de 11 Mbps, dado que ambos utilizan la banda de radio de 2.4GHz.

Además, al trabajar en la misma banda de frecuencia, el estándar 802.11g es compatible con las aplicaciones del estándar 802.11b, por lo que los puntos de acceso 802.11g pueden trabajar en redes 802.11b y viceversa. Las unidades 802.11g podrán trabajar también a velocidades de 11 Mbps, de modo que los dispositivos 802.11b y 802.11g puedan coexistir bajo la misma red inalámbrica.

Esta compatibilidad con versiones anteriores protege la inversión de los clientes en varios aspectos. Una tarjeta de interfaz de red IEEE 802.11g, por ejemplo, puede funcionar con un punto de acceso 802.11b y viceversa, a velocidades de hasta 11 Mbps. Para lograr velocidades más altas, de hasta 54 Mbps, tanto el punto de acceso como la tarjeta de red deben ser compatibles con el estándar 802.11g. El estándar 802.11g también especifica tipos de modulación opcionales (como OFDM/CCK) diseñados para mejorar la eficiencia en una instalación íntegramente 802.11g. En instalaciones grandes, la ventaja de tener aproximadamente los mismos alcances de transmisión efectivos es que la estructura WLAN 802.11b ya existente se puede mejorar fácilmente para lograr velocidades más altas sin necesidad de instalar puntos de acceso adicionales en muchos lugares nuevos a la hora de cubrir una zona determinada.

Las ventajas que tiene el estándar 802.11g son: la velocidad máxima alta, soporte de muchos usuarios a la vez, rango de señal muy bueno y difícil de obstruir. Los inconvenientes son alto costo y produce interferencias en la banda de 2.4 GHz.

2.2.7 802.11i

Se refiere al objetivo más frecuente del estándar 802.11, la seguridad. Se aplica a los estándares físicos a, b y g de la familia 802.11. Proporciona una alternativa al WEP, con nuevos métodos de encriptación y procedimientos de autenticación.

El estándar 802.11i, también conocido como WPA (Acceso Protegido Wi-Fi), especifica mecanismos de seguridad para redes inalámbricas (como Wi-Fi). El estándar preliminar fue ratificado el 24 de junio de 2004, y reemplaza la especificación de seguridad anterior (WEP), que mostró tener debilidades de seguridad severas. El WPA antes había sido presentado por la Alianza Wi-Fi como una solución intermedia con inseguridades WEP. El estándar 802.11i utiliza los siguientes componentes: 802.1X para autenticación (implicación del empleo de EAP y un servidor de autenticación), RSN para guardar la pista de asociaciones, y CCMP basado para proporcionar confidencialidad, integridad y autenticación de origen.

2.2.8 802.11j

El estándar 802.11j, tiene como función realizar la coexistencia del estándar IEEE 802.11a con el estándar de ETSI, HiperLAN 2. A la espera de que estas extensiones se normalicen definitivamente, algunos fabricantes

ofrecen en sus productos soluciones propietarias para mejorar la seguridad (por ejemplo, esquemas que cambian las claves de cifrado con suficiente frecuencia) o la movilidad entre canales y puntos de acceso.

El estándar 802.11a e HiperLAN 2 son muy parecidos en el nivel físico, aunque HiperLAN 2 tiene ventajas en cuanto a control de potencia y cambio automático de frecuencia en caso de interferencia. Por encima del nivel físico, sin embargo, ambos estándares tienen diferencias significativas.

Por ejemplo, el MAC del estándar 802.11a usa un protocolo de acceso distribuido con posibilidad de colisiones y los correspondientes plazos de espera y retransmisión. En cambio, el acceso en HiperLAN 2 es coordinado por el punto de acceso, que asigna recursos en el canal de radio a los terminales que quieren transmitir. Aunque el control distribuido del estándar 802.11a puede ser más adecuado para el caso de redes ad-hoc, el control centralizado de HiperLAN 2 permite regular el acceso de los terminales a los recursos de radio para ofrecer calidad de servicio.

El estándar 802.11j, por lo tanto, define los métodos uniformes que dejan al movimiento de los AP’s a nuevas frecuencias o el cambio del ancho del canal para el mejor funcionamiento o la capacidad, por ejemplo, evitar la interferencia con otros usos inalámbricos.

2.2.9 802.11t

El objetivo del estándar 802.11t es de proporcionar un juego de métodos de medida, lineamientos para un buen funcionamiento, y las recomendaciones de prueba que permitirán a los fabricantes, laboratorios independientes de prueba, proveedores de servicio, y usuarios finales, medir el funcionamiento de equipos, estándares y redes que utilicen la tecnología inalámbrica.

El estándar 802.11t proporciona una manera uniforme de probar el funcionamiento y la estabilidad de los dispositivos Wi-Fi. El proceso que se debe de seguir es el siguiente: los fabricantes de los productos Wi-Fi prueban el funcionamiento de su nuevo dispositivo, con base en el estándar 802.11t, después califican el funcionamiento del producto. Si pasa las especificaciones del estándar de manera aceptable, la Alianza Wi-Fi certifica el producto, con lo que estará listo para salir al mercado.

En conclusión, el estándar 802.11t ayudará a asegurarse de que los productos 802.11 resuelvan los desafíos y las demandas de las redes inalámbricas, y se encargará de ayudar a los usuarios elegir los dispositivos inalámbricos más rápidos y robustos.

2.3 Certificación

La importancia de tener equipos normalizados beneficia en aspectos como la eliminación de riesgos de pérdidas en los enlaces, aval de los canales de comunicación para el transporte de datos, mejora continua en la seguridad de los accesos y simplificación de la inserción de un nuevo dispositivo a una red existente. Desde abril del 2000, la Alianza Wi-Fi ha certificado la interoperabilidad de cerca de 1.500 productos. Estas certificaciones comprenden tres categorías:

- Productos Wi-Fi basados en los estándares IEEE para dispositivos de radio 802.11b, 802.11a y 802.11g, que operan en el rango de 2.4 GHz y 5 GHz. Soportan productos en modo doble o triple (802.11a, 802.11b y 802.11g).

- Seguridad en redes Wi-Fi en WPA para uso personal y empresas pequeñas y WPA 2 para grandes compañías.

- Soporte para contenidos de multimedia sobre redes inalámbricas VMM implementados en múltiples productos comerciales, se puede considerar que se ha convertido en el estándar "de facto" para las aplicaciones WLAN en decremento del estándar Hiperlan 2 del ETSI.

El certificado Wi-Fi es la única seguridad de que un producto ha pasado rigurosas pruebas de interoperabilidad que aseguran que productos compatibles de diferentes fabricantes pueden trabajar conjuntamente.

La Alianza Wi-Fi ha instituido un conjunto de pruebas realizadas por un laboratorio independiente para certificar que los productos son compatibles con otros productos con certificado Wi-Fi. La Alianza Wi-Fi que fue fundada por 3Com, Cisco, Intersil, Agere, Nokia y Symbol Technologies, en agosto de 1999 tiene como misión certificar la interoperabilidad y compatibilidad entre diferentes fabricantes de productos inalámbricos bajo los estándares IEEE 802.11b, IEEE 802.11a y IEEE 802.11g. Desde entonces Intermec, Microsoft e Intel han formado el comité de dirección de la Alianza Wi-Fi. Aquellos dispositivos con el logotipo Wi-Fi gozan de esa garantía de interoperabilidad. La relación de miembros actualizada puede ser encontrada en la página web http://www.wirelessethernet.org/pr/backgrounder.asp y la relación de los productos inalámbricos que están certificados por la Alianza Wi-Fi está disponible en la siguiente página web: http://www.wirelessethernet.org/certified_products.asp .

2.4 Instituto Europeo de Normas de Telecomunicaciones (ETSI)

El Instituto Europeo de Normas de Telecomunicaciones (ETSI) es una organización independiente, no lucrativa, desarrolladora de estándares para la industria de las telecomunicaciones (los fabricantes del equipo y los operadores de red) en Europa, con la proyección mundial. ETSI ha acertado en estandarizar el sistema de

teléfono de la célula del GSM y el sistema TETRA de radio móvil profesional. Los cuerpos de estandarización significativos de ETSI son 3GPP (para las redes de UMTS) o TISPAN (para las redes y la convergencia fijas del Internet).

ETSI fue creado por el CEPT en 1988 y es reconocido oficialmente por la Comisión de las Comunidades Europeas, ETSI es oficialmente responsable de la estandarización de las tecnologías de información y de comunicación (ICT) dentro de Europa. Estas tecnologías incluyen telecomunicaciones, la difusión y áreas relacionadas tales como transporte inteligente y electrónica médica. ETSI tiene 688 miembros, incluyendo fabricantes, operadores de red, administraciones, abastecedores de servicio, cuerpos de investigación y usuarios.

ETSI ha desarrollado el estándar GSM para la telefonía celular digital. También fue responsable de haber llevado a cabo durante los años 1991 y 1996 el proyecto HiperLAN, con el que pretendía conseguir una tasa de transferencia mayor que la ofrecida por la especificación IEEE 802.11.

FIGURA 9. LOGOTIPO DEL INSTITUTO EUROPEO DE NORMAS DE TELECOMUNICACIONES

Actualmente ETSI dispone de la especificación HiperLAN 2 que mejora notablemente las características de sus antecesoras, ofreciendo una mayor velocidad de 54 Mbps, para lo cual emplea el método de modulación OFDM y ofrece soporte de calidad de servicio. Bajo esta especificación se ha formado, el HiperLAN 2 Global Forum (H2GF), con la intención de sacar al mercado productos basados en este estándar.

En el 2005, el presupuesto de ETSI excedió 20 millones de euros, con las contribuciones viniendo de los miembros, actividades comerciales como la venta de documentos, tests y foros. De esto cerca del 40% va hacia gastos de explotación y el 60% restante se utiliza hacia programas de trabajo incluyendo centros de capacitación y proyectos especiales.

2.5 HiperLAN frente a 802.11

HiperLAN 1 fue el primer estándar europeo para redes de área local inalámbricas. Este estándar utilizaba la banda de los 5 GHz y alcanza velocidades de transmisión de 24 Mbps. HiperLAN 1 fue sustituido por HiperLAN

2, más robusto que el anterior y que permite velocidades de hasta 54 Mbps (igual que 802.11a). El estándar HiperLAN es responsabilidad del proyecto BRAN (Red Local de Banda Ancha Vía Radio) del instituto europeo ETSI.

La capa física de HiperLAN es prácticamente idéntica al estándar 802.11a. La mayor diferencia radica en la capa MAC. Mientras que IEEE 802.11a pretende ser simplemente una versión inalámbrica de 802.3, HiperLAN está diseñado de una forma más ambiciosa, soporta aplicaciones en las que el tiempo de respuesta es crítico, define interfaces de redes de tercera generación, redes ATM (Modo de Transferencia Asíncrono) y Firewire. Además, para conseguir una mejor utilización del espectro radioeléctrico, HiperLAN considera características como TPC (Control de la Potencia de Transmisión) o DFS (Selección Dinámica de Frecuencia).

Estándar	802.11b	802.11a	802.11g	HiperLAN 2
Organismo	IEEE	IEEE	IEEE	ETSI
Finalización	1999	2002	2003	2003
Banda de frecuencias	2.4 GHz	5 GHz	2.4 GHz	5 GHz
Tasa máxima	11 Mbps	54 Mbps	54 Mbps	54 Mbps
Interfaz aire	DSSS/FHSS	OFDM	OFDM	OFDM

TABLA 1. COMPARACIÓN DE LAS TECNOLOGÍAS INALÁMBRICAS PRINCIPALES

Actualmente existen dos grupos de trabajo, IEEE 802.11h y 5GSG, para considerar las compatibilidades entre HiperLAN y el estándar IEEE 802.11a. Estos grupos de trabajo esperan poder promover un nuevo estándar en la banda de 5 GHz que sea compatible no sólo para el IEEE y ETSI, sino también para el Consejo japonés MMAC (Comunicación de Acceso Móvil Multimedia). Un aspecto importante que debe conseguir es la adaptación a las regulaciones de Norteamérica, Europa y Japón.

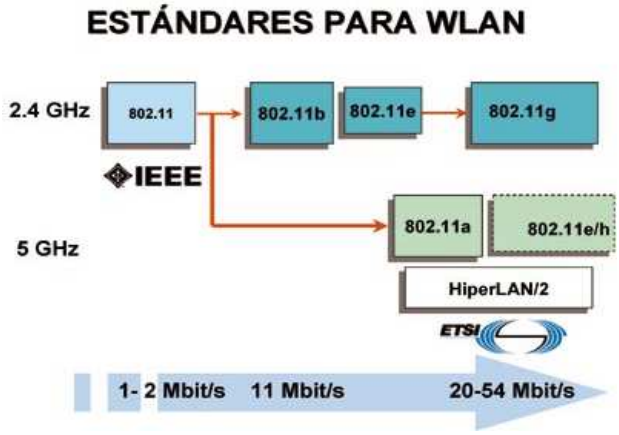


FIGURA 10. ESTÁNDARES DEL IEEE Y ETSI PARA LAS REDES INALÁMBRICAS

Capítulo 3 – Wi-Fi

3.1 Origen y significado del termino Wi-Fi

El problema principal que pretende resolver la normalización es la compatibilidad, para resolver este problema, los principales vendedores de soluciones inalámbricas (3Com, Aironet, Intersil, Lucent Technologies, Nokia y Simbol Technologies) crearon en 1999 una asociación conocida inicialmente como WECA (Alianza de Compatibilidad Ethernet Inalámbrica) y que en el año 2003 cambió su nombre a la Alianza Wi-Fi.

Wi-Fi significa “Fidelidad Inalámbrica” y es un nombre comercial desarrollado por un grupo de trabajo de comercio industrial llamado Alianza Wi-Fi. Wi-Fi describe los productos de redes de área local inalámbricos basados en los estándares 802.11 y está diseñado para que tenga un nombre más accesible para los usuarios, de la misma manera que Ethernet y Token Ring son más fáciles de aprender que 802.3 y 802.5, respectivamente. En principio, Wi-Fi fue creado para describir sólo los dispositivos con velocidades máximas de 11Mbps que operaban en la frecuencia de 2.4 GHz y que cumplían con las especificaciones 802.11b. Más tarde se decidió que Wi-Fi debería ser extendido para incluir los productos con velocidades de datos máximas de 54 Mbps que operan en las frecuencias de 2.4 GHz y 5 GHz y que están basados en las especificaciones 802.11g y 802.11a del IEEE.

FIGURA 11. LOGOTIPO DE LA ALIANZA WI-FI

3.2 Wi-Fi: Cómo trabaja

Una red Wi-Fi puede estar formada por dos computadoras o por miles de ellas. Para que una computadora pueda comunicarse de forma inalámbrica, necesita que se le instale un adaptador de red. Un adaptador de red es un equipo de radio (con transmisor, receptor y antena) que puede ser insertado o conectado a una computadora, PDA o cualquier otro equipo susceptible de formar parte de la red. De forma general, a los equipos que conforman parte de una red inalámbrica se les conoce como terminales.

Aparte de los adaptadores de red, las redes Wi-Fi pueden disponer también de unos equipos que reciben el nombre de puntos de acceso (AP o Access Point). Un punto de acceso es como una estación base utilizada

para gestionar las comunicaciones entre los distintos terminales. Los puntos de acceso funcionan de forma autónoma, sin necesidad de ser conectados directamente a ninguna computadora.

Tanto a los terminales como a los puntos de acceso se les conoce por el nombre general de estación. Las estaciones se comunican entre sí gracias a que utilizan la misma banda de frecuencias y a que internamente tienen instalados el mismo conjunto de protocolos. Aunque los protocolos que utiliza Wi-Fi están basados en las siete capas del modelo de referencia OSI, el estándar IEEE 802.11b solo define las dos primeras capas (física y enlace), el resto de las capas son idénticas a las empleadas en las redes locales cableadas e Internet y se conoce con el nombre de conjuntos de protocolos IP (Protocolos de Internet).

Los diferentes estándares, incluido IEEE 802.11, permiten que aparezcan nuevas versiones de ese mismo estándar simplemente modificando una de las capas. Esto facilita no sólo la evolución de los estándares, sino que un mismo equipo pueda ser compatible con distintas versiones de un estándar. Por ejemplo, IEEE 802.11b sólo se diferencia de IEEE 802.11 en que su capa física permite transmitir datos a alta velocidad.

Para poder describir mejor la funcionalidad de Wi-Fi se definen los siguientes conceptos:

- El modelo OSI.

Una característica común a todas las comunicaciones actuales de computadoras es el hecho de que todas ellas estructuran el proceso de comunicación en distintos niveles o capas. Cada capa se encarga de realizar una tarea específica y perfectamente coordinada con el resto de las capas. La ventaja de hacer una división por capas es que cada una de ellas puede ser normalizada de forma independiente. No obstante, la comunicación se lleva a cabo gracias al buen funcionamiento de todas las capas.

La Organización Internacional de Normalización (ISO) propuso un modelo de referencia que permitiera estructurar las comunicaciones en siete capas. A este modelo lo llamó OSI (Interconexión de Sistemas Abiertos). Las capas que componen al modelo OSI son las siguientes:

- Capa Física. Esta capa define las propiedades físicas de los componentes (frecuencias de radio utilizadas, cómo se transmiten las señales, etcétera).

- Capa de enlace. Esta capa define como se organizan los datos que se transmiten, cómo se forman los grupos de datos (paquetes, tramas, etcétera) y cómo se asegura que los datos llegan al destino sin errores.

- Capa de red. Esta capa define como organizar las cosas para que distintas comunicaciones puedan hacer uso de una infraestructura común, una red.

- Capa de transporte. Esta capa define las características de la entrega de los datos.

- Capa de sesión. Aquí se describen cómo se agrupan los datos relacionados con una misma función.

- Capa de presentación. Nos define cómo es representada la información transmitida.

- Capa de aplicación. Define cómo interactúan los datos con las aplicaciones específicas.

- Las capas que componen al estándar IEEE 802.

La norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del sistema OSI, las capas física y la de enlace. De hecho, a la capa de enlace la divide en dos, por lo que el resultado son tres capas:

- PHY (Capa Física) es la capa que se encarga de definir los métodos por los que se difunde la señal. Para hacer esto, la capa física de IEEE 802.11 se divide en dos subcapas: lo que se conoce como PLCP (Procedimiento de Convergencia de la Capa Física) y PMD (Dependiente del Medio Físico). PLCP se encarga de convertir los datos a un formato compatible con el medio físico. Por ejemplo, este formato es distinto si se trata de un medio físico de infrarrojos o de radio, mientras que PMD es el que se encarga de la difusión de la señal. Aunque las especificaciones originales del estándar 802.11 contemplan la opción de utilizar infrarrojos como medio de transmisión, no obstante, nunca ha llegado a desarrollarse este sistema debido principalmente al corto alcance que ofrece y a que no es utilizable en el exterior debido a las interferencias producidas por agentes naturales como la lluvia o la niebla.

- MAC (Control de Acceso al Medio) es la capa que se ocupa del control de acceso al medio físico. En el caso de Wi-Fi el medio físico es el espectro radioeléctrico. La capa MAC es un conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso de este espectro radioeléctrico.

- LLC (Control del Enlace Lógico) es la capa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

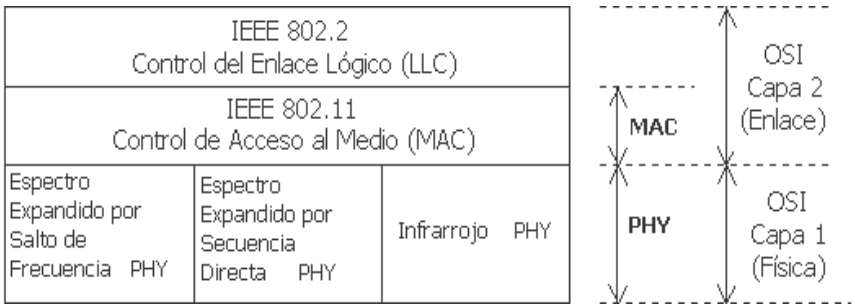


FIGURA 12. CAPAS FÍSICA Y DE ENLACE DEL MODELO DE REFERENCIA OSI

- Espectro expandido.

En cuanto a la utilización del medio radioeléctrico, la tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro expandido. Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario para la transmisión de la información. Lo que se consigue con esto es un sistema muy resistente a las interferencias de otras fuentes de radio, resistentes a los efectos de eco y que puede coexistir con otros sistemas de radiofrecuencia sin verse afectado y sin influir en su actividad. Estas ventajas hacen que la tecnología del espectro expandido sea la más adecuada en las bandas de frecuencia para las que no se necesita licencia.

Existen distintas técnicas de espectro expandido, entre las que se encuentran la tecnología CMDA utilizada en la tercera generación de la tecnología móvil. No obstante, el estándar IEEE 802.11 contempla sólo dos técnicas distintas del espectro expandido:

➢ FHSS (Espectro Expandido por Salto de Frecuencia), con las que se consiguen velocidades de transmisión de 1 Mbps. La técnica FHSS consiste en dividir la banda de frecuencias en una serie de canales e ir transmitiendo la información saltando de un canal a otro de acuerdo con un patrón de saltos conocido tanto por el emisor como por el receptor. El tiempo máximo que se debe permanecer en cada frecuencia está regulado en 400 mseg. El inconveniente de FHSS es que tiene la necesidad de sincronizar el emisor y el receptor en la frecuencia a utilizar en cada momento.

El estándar IEEE 802.11 definió en 1997 que cada canal de FHSS tuviera un ancho de banda de 1 MHz dentro de la banda de frecuencias de 2.4 GHz. El ancho de banda total disponible y, por lo tanto, el número total de canales disponibles varía de acuerdo con el marco regulatorio de cada país o área geográfica. La técnica FHSS reduce las interferencias ya que en el peor de los casos, la interferencia afectará exclusivamente a uno de los saltos de frecuencia, liberándose a continuación de la interferencia al saltar a otra frecuencia distinta. El resultado es que el número de bits erróneos es extremadamente

bajo. También proporciona algo de seguridad pues un intruso que no sepa la secuencia de saltos o el tiempo de permanencia no puede espiar las transmisiones.

Otra de las ventajas de FHSS es que permite que coexistan varias comunicaciones en la misma banda de frecuencias. Para ello, cada comunicación debe tener un patrón de saltos con distinta secuencia.

A pesar de que el estándar original IEEE 802.11 incluía el sistema FHSS, no existe ninguna instalación real que utilice este sistema. La razón es que la velocidad máxima que se consigue con la técnica FHSS es de unos 3 Mbps (aunque sólo está normalizada la velocidad de 1 Mbps). No obstante, es posible que en un futuro se consigan velocidades superiores de hasta 15 Mbps.

- DSSS (Espectro Expandido por Secuencia Directa), con la que se consiguen velocidades de transmisión de 2 Mbps. En versiones posteriores de este sistema se han conseguido velocidades superiores. La técnica DSSS se basa en sustituir cada bit de información por una secuencia de bits conocida como chip o código de chips. Estos códigos de chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits. Entre las señales que son eliminadas se encuentra el ruido y las interferencias.

  El código de chips permite al receptor identificar los datos como pertenecientes a un emisor determinado. El emisor genera el código de chips y, sólo los receptores que conocen dicho código pueden descifrar los datos. Por lo tanto, en teoría, DSSS permite que varios sistemas puedan funcionar en paralelo, cada receptor filtrará exclusivamente los datos que se corresponden con su código de chips. Por otro lado, cuanto más largo es el código de chips, más resistente será el sistema a las interferencias y mayor número de sistemas podrán coexistir simultáneamente. La norma IEEE 802.11 recoge que la longitud mínima del código de chips debe ser de 11.

  La coexistencia de sistemas no se consigue por el uso de distintos códigos de chips, sino por el uso de distintas bandas de frecuencias. Un sistema DSSS de 11 Mbps (IEEE 802.11b) necesita un ancho de banda de 22 MHz, siendo la distancia mínima entre portadoras de 30 MHz. Como el ancho de banda disponible en la banda de 2.4 GHz (en el área regulada por el FCC) es de 83.5 MHz, sólo es posible la coexistencia de tres sistemas DSSS en el mismo lugar.

A pesar de esto, en la práctica, la velocidad de 11 Mbps no es totalmente real debido a las siguientes razones:

- Las interferencias y ruidos hacen que la velocidad real baje.
- El propio protocolo consigue menos rendimiento que en sistemas cableados.
- Las conexiones a los puntos de acceso son un cuello de botella.

Por otro lado, la mayoría de las tarjetas inalámbricas de las estaciones son semidúplex (sólo contiene un equipamiento de radio), por lo que pueden transmitir o recibir, pero no ambas cosas simultáneamente.

- La técnica OFMD.

OFMD (Multiplexación Ortogonal por División de Frecuencias), con las que se consiguen velocidades de transmisión de hasta 54 y 100 Mbps. Esta técnica de gestión de frecuencias utilizada por el estándar 802.11a, divide el ancho de banda en subcanales más pequeños que operan en paralelo. De esta forma se consigue llegar a velocidades de transmisión de hasta 54 Mbps (100 Mbps con soluciones propietarias). La técnica OFMD fue patentada por los Laboratorios Bell en 1970 y está basada en un proceso matemático llamado FFT (Transformada Rápida de Fourier). OFMD divide la frecuencia portadora en 52 subportadoras, 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor.

Una de las ventajas de OFMD es que consigue una alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno. Estás ondas llegan al receptor con distinta amplitud y a distinto tiempo que la señal principal produciendo interferencias. Estas interferencias son un problema a velocidades superiores a 4 Mbps, por este motivo, se utilizan técnicas como OFMD que mitiguen este efecto. Dividir la señal en bandas más estrechas tienen más ventajas que el uso de una sola banda ancha, entre ellas mejor inmunidad a la interferencia de bandas estrechas y la posibilidad de utilizar bandas no contiguas. Se utiliza un sistema de codificación complejo, con base a la modulación por desplazamiento de fase para velocidades de hasta 18 Mbps, y en QAM para velocidades mayores.

OFMD puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite OFMD son 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

Dependiendo de la velocidad a la que se van a transmitir los datos, la norma IEEE 802.11 utiliza una técnica u otra.

Parte del motivo para utilizar OFMD es la compatibilidad con el sistema europeo HiperLAN 2. La técnica tiene buena eficacia de espectro en términos de bits/Hz y buena inmunidad al desvanecimiento de múltiples rutas.

- Modulación de la señal.

Para poder transmitir la señal vía radio, hace falta definir un método de difusión de la señal y un método de modulación de la señal. La modulación consiste en modificar una señal pura de radio para incorporarle la información a transmitir. La señal base a modular recibe el nombre de portadora. Lo que se le cambia a la

portadora para modularla es su amplitud, frecuencia, fase o una combinación de éstas. Mientras mayor es la velocidad de transmisión, más complejo es el sistema de modulación. Las técnicas de modulación utilizadas en IEEE 802.11 son las siguientes:

- BPSK (Modulación Binaria por Salto de Fase).
- QPSK (Modulación por Salto de Fase en Cuadratura).
- GFSP (Modulación Gausiana por Salto de Frecuencia).
- CCK (Modulación de Código Complementario).

Una vez emitida la señal modulada, el receptor tiene que recibir la señal, sincronizar el código de difusión y demodular la información. Los sistemas FHSS son más complicados de sincronizar que los sistemas DSSS, ya que en el primer caso hay que sincronizar tiempo y frecuencia y en el segundo, sólo el tiempo.

- MAC.

La capa MAC (Control de Acceso al Medio) define los procedimientos que hacen posible que los distintos dispositivos compartan el uso de este espectro radioeléctrico. Mientras que las distintas versiones del estándar 802.11 utilizan distintos sistemas para difundir su señal (su capa física es distinta), la capa MAC es la misma para todas ellas.

Es interesante el hecho de que la capa MAC sea muy similar a la utilizada por la red Ethernet. Ambas utilizan la técnica conocida como CSMA. No obstante, la versión cableada (Ethernet) utiliza la tecnología CD (Detección de Colisión), mientras que la versión inalámbrica utiliza la tecnología CA (Evitación de Colisión). Una colisión se produce cuando dos terminales intentan hacer uso del medio físico simultáneamente. La tecnología CD detecta que se ha producido una colisión y retransmite los datos, mientras que la tecnología CA dispone de procedimientos para evitar que se produzcan colisiones. Entre la capa MAC y la capa física se intercambian tres tipos de paquetes de datos: de control, de gestión y de información.

MAC tiene dos funciones distintas para coordinar la transferencia de datos:

- PCF (Función de Coordinación del Punto) facilita un sistema para poder transmitir el tráfico que es sensible a los retardos y que requiere un tratamiento especial evitando las demoras. A la estación que hace uso de esta función se le llama coordinador del punto (PC). El PC emite una señal guía con la duración del periodo de tiempo que necesita disponer del medio. Las estaciones que reciben esta señal no emiten durante ese tiempo.

El protocolo de la subcapa MAC para el estándar 802.11 es muy diferente del de Ethernet debido a la complejidad inherente del entorno inalámbrico. Con Ethernet, una estación simplemente espera hasta que el medio queda en silencio y comienza a transmitir. Si no recibe una ráfaga de ruido dentro de los primeros 64 bytes, con seguridad la trama ha sido entregada correctamente, esta situación no es válida para los sistemas inalámbricos.

➢DCF (Función de Coordinación Distribuida) facilita un sistema que permite compartir el medio físico (radioeléctrico, infrarrojos, etcétera) entre todas las estaciones de la red. Para ello, DCF define los mecanismos que le permiten a las estaciones negociar el acceso al medio físico, así como los mecanismos que aseguran la entrega de los datos a las estaciones. A través de DCF se transmiten los datos que no son sensibles a los retardos. La función DCF contempla un mecanismo físico y otro lógico de detección de colisión. Al mecanismo físico se le conoce como CCA (Valoración de la Disponibilidad del Canal), es muy eficiente, pero no es eficaz cuando dos estaciones de una misma red que no se ven entre ellas emiten al mismo tiempo. Esto se conoce con el nombre de problema del nodo oculto. Para evitar estos casos, se dispone del sistema lógico. Este sistema consiste en intercambiar la información del uso del medio a través de tramas de control. A estas tramas de control se les conoce como RTS (Solicitud para Enviar) y CTS (Listo para Enviar). Cuando una estación de una red va a transmitir información, primero envía una trama RTS al punto de acceso donde facilita información del destinatario de la transmisión, el remitente y el tiempo que ocupará dicha transmisión. El punto de acceso responde con una trama CTS que reciben todas las estaciones que están en el área de cobertura del punto de acceso. En esta trama CTS se incluye el tiempo de ocupación del medio, por lo tanto, las estaciones saben el tiempo que estará ocupado el medio y no intentarán hacer ninguna transmisión hasta que dicho tiempo no haya pasado.

- Los servicios.

Las redes inalámbricas IEEE 802.11 están formadas por terminales y puntos de acceso y ambos reciben el nombre de estaciones. La capa MAC define cómo las estaciones acceden al medio mediante lo que llama servicios de estaciones. De la misma forma, define cómo los puntos de acceso gestionan la comunicación mediante lo que llama servicios de distribución. Los servicios de estación de la capa MAC son los siguientes:

- Autenticación. Comprueba la identidad de una estación y la autoriza para asociarse. En una red inalámbrica no existe la conexión física, por lo que, para saber si un terminal forma o no parte de la red, hay que comprobar su identidad antes de autorizar su asociación con el resto de la red. La estación móvil prueba que sabe la clave secreta codificando la trama de desafío y regresándola a la estación base. Si el resultado es correcto, la terminal se vuelve miembro de la celda.

- Desautenticación. Cancela una autenticación existente. Este servicio da por concluida la conexión cuando una estación pretende desconectarse de la red.

- Privacidad. Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP. Este algoritmo pretende emular el nivel de seguridad que se tiene en las redes cableadas.

- Entrega de datos. Facilita la transferencia de datos entre estaciones. La transmisión de datos es la parte esencial, por lo que el 802.11 naturalmente proporciona una forma de transmitir y recibir datos. Puesto que el 802.11 está basado en Ethernet y no se garantiza que la transmisión a través de Ethernet sea 100% confiable, tampoco se garantiza que la transmisión a través del 802.11 sea confiable, las capas superiores deben tratar con la detección y la corrección de errores.

Los cinco servicios de distribución son proporcionados por las estaciones base y tienen que ver con la movilidad de la estación conforme entran y salen de las celdas, conectándose ellos mismos a las estaciones base y separándose ellos mismos de dichas estaciones, estos servicios son los siguientes:

- Asociación. Para que un terminal pueda comunicarse con otros terminales a través de un punto de acceso, debe primero estar asociado a dicho punto de acceso. Asociación significa asignación del terminal al punto de acceso haciendo que éste sea el responsable de la distribución de datos a, y desde, dicho terminal. Por lo general, se utiliza después de que una terminal se mueve dentro del alcance de radio de la estación base, una vez que llega, anuncia su identidad y sus capacidades, éstas incluyen las tasas de datos soportadas, necesarias para los servicios PCF y los requerimientos de administración de energía.

- Disociación. Cancela una asociación existente, ya sea porque el terminal sale del área de cobertura del punto de acceso, o porque el punto de acceso termina la conexión.

- Reasociación. Transfiere una asociación entre dos puntos de acceso. Cuando un terminal se mueve del área de cobertura de un punto de acceso a la de otro, su asociación pasa a depender de este último.

- Distribución. Cuando se transfieren datos de un terminal a otro, el servicio de distribución se asegura que los datos alcanzan su destino.

- Integración. Facilita la transferencia de datos entre la red inalámbrica IEEE 802.11 y cualquier otra red. Si una trama necesita enviarse a través de una red que no es 802.11 con un esquema de direccionamiento o formato de trama diferentes, este servicio maneja la traducción del formato 802.11 al requerido por la red de destino.

Los puntos de acceso utilizan tanto los servicios de estaciones como los servicios de distribución, mientras que los terminales sólo utilizan los servicios de estaciones.

Servicio MAC	Definición	Tipo de estación
Autenticación	Comprueba la identidad de una estación y la autoriza para asociarse.	Terminales y puntos de acceso
Desautenticación	Cancela una autenticación existente.	Terminales y puntos de acceso
Asociación	Asigna el terminal al punto de acceso.	Puntos de acceso
Desasociación	Cancela una asociación existente.	Puntos de acceso
Reasociación	Transfiere una asociación entre puntos de acceso o a uno mismo.	Puntos de acceso
Privacidad	Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP y WPA.	Terminales y puntos de acceso
Distribución	Asegura la transferencia de datos entre estaciones de distintos puntos de acceso.	Puntos de acceso
Entrega de datos	Facilita la transferencia de datos entre estaciones.	Terminales y puntos de acceso
Integración	Facilita la transferencia de datos entre redes WI-FI y no WI-FI.	Puntos de acceso

TABLA 2. SERVICIOS DE ESTACIONES Y DE DISTRIBUCIÓN

- La gestión.

Tanto la capa física como la capa MAC están divididas en capacidades de gestión y de transferencia de datos. Lo que se conoce como PLME (Entidad de Gestión de la Capa Física) y MLME (Entidad de Gestión de la Capa MAC), intercambian información a través de MIB (Base de Datos de la Información de Gestión), ésta es una base de datos de las características físicas (velocidad de transmisión, niveles de potencia, tipo de antena, etcétera) de las estaciones.

- El flujo de datos.

Los datos que se van a transmitir por el medio radioeléctrico proceden de las capas superiores (formato IP) y se pasan a la capa LLC (Control Lógico de Enlace), que pasa estos datos a la capa MAC, quien a su vez, se los

pasa a la capa física para su emisión. Los paquetes de datos que se intercambian entre las capas LLC y MAC se conocen como MSDU (Unidad de Datos del Servicio MAC), mientras que los paquetes de datos que se intercambian entre las capas MAC y física reciben el nombre de MPDU (Unidad de Datos del Protocolo MAC).

En la capa física, quien recibe estos datos es PLCP, quien es responsable de convertir los datos MPDU a un formato compatible con el medio físico.

- La estructura de red.

La topología de una red es la arquitectura de la red, la estructura jerárquica que hace posible la interconexión de los equipos. IEEE 802.11 y, por tanto, Wi-Fi, contempla tres topologías distintas:

- IBSS (Conjunto de Servicios Básicos Independientes). Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre los distintos terminales que forman la red. Todas las comunicaciones son directas entre dos o más terminales del grupo. A esta modalidad se le conoce también como ad-hoc, independiente o de igual a igual.

- BSS (Conjunto de Servicios Básicos). En esta modalidad se añade un punto de acceso que realiza las funciones de coordinación centralizada de la comunicación entre los distintos terminales de la red. Los puntos de acceso tienen funciones de buffer (memoria de almacenamiento intermedio) y de router con otras redes. A esta modalidad se le conoce también como modo infraestructura.

- ESS (Conjunto de Servicios Extendido). Esta modalidad permite crear una red inalámbrica formada por más de un punto de acceso. De esta forma se puede extender el área de cobertura de la red, quedando constituida por un conjunto de celdas pegadas unas a otras. Una red ESS está formada por múltiples redes BSS.

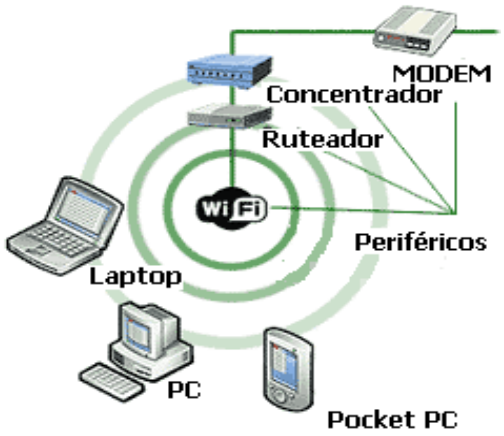


FIGURA 13. CONEXIÓN DE LOS DISPOSITIVOS MEDIANTE WI-FI

3.3 Alianza Wi-Fi

La Alianza Wi-Fi es una asociación internacional sin fines de lucro, formada en 1999, por los principales vendedores de soluciones inalámbricas como: 3Com, Aironet, Intersil, Lucent Technologies, Nokia y Simbol Technologies, conocida inicialmente como WECA (Alianza de Compatibilidad Ethernet Inalámbrica) y que desde el año 2003 es conocida con el nombre de la Alianza Wi-Fi. Formada para certificar la interoperabilidad entre productos WLAN basados en la especificación IEEE 802.11. El logotipo certificado Wi-Fi viene de la Alianza Wi-Fi e indica que el producto ha cumplido con rigurosas pruebas de interoperabilidad, para asegurar que aquellos productos de diferentes proveedores operen de manera adecuada en conjunto.

El objetivo de esta asociación fue crear una marca que permitiera fomentar la tecnología inalámbrica y asegurarse de la compatibilidad de los equipos de diferentes fabricantes.

La meta de los miembros de la Alianza Wi-Fi es incrementar la experiencia del usuario a través de la interoperabilidad del producto.

De esta forma, desde abril del 2000, la Alianza Wi-Fi certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi. Otra de las actividades de esta alianza involucra el trabajo activo en la creación de nuevos y más rígidos estándares de seguridad, como WPA, así como la proliferación de hot-spots (lugares públicos como cafeterías, hoteles y aeropuertos en donde el acceso WLAN está disponible), proporcionando productos y estándares que cubran con las necesidades requeridas para brindar un servicio de alta calidad a los usuarios finales, además de promover el uso y desarrollo de la tecnología inalámbrica Wi-Fi.

3.4 Ventajas

La popularización de la tecnología inalámbrica Wi-Fi está suponiendo un creciente interés por parte de los usuarios y de las empresas proveedoras en buscar soluciones y alternativas más fáciles de implantar a las necesidades de comunicaciones existentes o a las nuevas necesidades que puedan surgir. Las ventajas que ofrece la tecnología Wi-Fi son las siguientes:

- Bajo costo, tomando en cuenta la acción de que el precio de silicio sigue bajando, está haciendo que Wi-Fi sea una opción muy económica conectada a una red.

- Permiten a LAN’s ser desplegadas sin cables, típicamente reduciendo los gastos de despliegue de red y extensión.

- Rango de señal muy bueno y difícil de obstruir.

- Los productos Wi-Fi están extensamente disponibles en el mercado.

- Las marcas diferentes de puntos de acceso e interfaces de red de cliente son compatibles en un nivel básico de servicio. Los productos designados como certificados Wi-Fi por la Alianza Wi-Fi son compatibles e incluyen la seguridad WPA 2.

- Compatibilidad con estándares de LAN existentes.

3.5 Desventajas

Pocos desarrollos técnicos en la historia de las telecomunicaciones han tenido una aceptación social tan rápida, beneficiosa y extensa. El éxito en el mercado ha hecho que Wi-Fi sea una tecnología muy eficiente en costo. Existen muchos productos, debidamente certificados, y se están desarrollando gran número de nuevas aplicaciones y servicios. Tecnológicamente, Wi-Fi ha evolucionado desde su posición original como estándar WLAN hacia las tecnologías de acceso e incluso de móviles. Sin embargo existen algunos inconvenientes a cerca de su uso, como son:

- Baja velocidad máxima.

- Soporte de un número bajo de usuarios a la vez.

- Produce interferencias en la banda de 2.4 GHz.

- Las cuestiones de interoperabilidad entre marcas o desviaciones del estándar pueden interrumpir conexiones o bajar velocidades de rendimiento sobre los dispositivos de otro usuario dentro de la gama.

- Si no se configuran correctamente, existen problemas de seguridad.

3.6 Ejemplos de recursos Wi-Fi

La tecnología Wi-Fi hace posible que los usuarios accedan a Internet y a las redes locales de su empresa a través de banda ancha y de forma inalámbrica, tanto desde su propio lugar de trabajo como desde entornos públicos o privados de uso público.

También existen servicios Wi-Fi orientados a aquellos entornos privados de uso público (aeropuertos, hoteles, escuelas, negocios, etcétera) que quieran posibilitar a sus empleados y clientes el acceso en banda ancha y sin cables a Internet y a las aplicaciones de sus propias empresas.

Para todo ello, como ejemplo, Telefónica dispone de áreas con cobertura Wi-Fi ofrecidas por la compañía a los usuarios finales en España, en entornos de uso público, directamente o previo acuerdo con sus propietarios. Permiten a los clientes utilizar sus dispositivos equipados con Wi-Fi (PC's portátiles, PDA'S, etcétera) y acceder a través de la banda ancha tanto a Internet como a la red corporativa de la empresa de forma inalámbrica mediante el pago de una tarifa, plan mensual o a través de tarjeta prepago.

Telefónica ha apostado por la tecnología Wi-Fi a través de una serie de servicios gestionados que permiten a cualquier cliente (individuos, hogares, empresas, etcétera) acceder y construir sus redes de área local de forma inalámbrica con el máximo nivel de seguridad. Estos servicios ofrecen todas las ventajas de una red sin cables: flexibilidad, incorporación sencilla y rápida de nuevos usuarios a la red.

Existen en el mercado una gran variedad de dispositivos con tecnología Wi-Fi, teniendo en cuenta que en los siguientes puntos se mencionarán las aplicaciones para el entretenimiento, televigilancia y telefonía Wi-Fi, se señalarán algunos ejemplos de dispositivos que utilizan esta tecnología:

- Puntos de acceso para LAN inalámbrica: los puntos de acceso para grandes y pequeñas oficinas permiten establecer LAN's inalámbricas 802.11 seguras y confiables; las opciones de actualización aportan flexibilidad y protección de la inversión.

- Switches y controladores de LAN inalámbrica: los switches y controladores de WLAN proporcionan seguridad, visibilidad centralizada y administración sin discontinuidades a su red inalámbrica.

- Bridges para LAN inalámbrica: los bridges inalámbricos 802.11 para grupo de trabajo y campus conectan dispositivos cableados e inalámbricos y sustituyen de forma rentable a las líneas T1 y de fibra óptica entre edificios.

- Dispositivos cliente de LAN inalámbrica: las tarjetas PC y los adaptadores PCI y USB proporcionan soporte para LAN inalámbrica 802.11a, a las computadoras de escritorio y portátiles.

- Routers para LAN inalámbrica: los routers de LAN inalámbrica 802.11 para oficinas pequeñas y residenciales proporcionan un acceso compartido a Internet a usuarios de LAN inalámbrica y cableada.

- Servidores de impresión inalámbricos: permite compartir recursos de impresión en red entre usuarios inalámbricos y cableados.

- Antenas y cables para LAN inalámbrica: estas antenas aumentan el área de cobertura de los bridges y puntos de acceso para LAN inalámbrica de 3Com; los cables de antena ofrecen diversas opciones de

longitud; el adaptador de cable conecta un bridge de grupo de trabajo para LAN inalámbrica a una antena externa.

- Discos duros y dispositivos USB: permiten ofrecer al usuario una mayor movilidad de los datos.

FIGURA 14. DISPOSITIVOS EQUIPADOS CON TECNOLOGÍA WI-FI

3.7 Wi-Fi y entretenimiento

Linksys ofrece la gama más completa de productos y soluciones del mercado orientados a la creación de redes inalámbricas y a la integración de todo tipo de dispositivos en estas redes. La compañía pone las bases del futuro con una serie de dispositivos que interactúan entre sí y se estructuran en torno a una red inalámbrica que se convierte en la columna vertebral del hogar multimedia e interactivo. Conceptos como teletrabajo, televigilancia o videoconferencia se integran en una única red Wi-Fi que permite eliminar las limitaciones del cableado.

Linksys lleva también la movilidad al hogar donde, gracias a su tecnología, es posible acceder a la información: Internet, unidades de almacenamiento Wi-Fi y controlar diferentes dispositivos como: televisión, vídeo, DVD, consola de juegos, PC's y aplicaciones multimedia y servicios desde cualquier punto de la casa. El almacenamiento en red es otra de las novedades del hogar del futuro: un único dispositivo para toda la información de la familia: música, fotos, vídeo, juegos, aplicaciones, etcétera.

Un hogar multitemático donde es posible jugar con otros usuarios a través de Internet o enfrentarse a otro jugador sin cables en Nintendo DS, Xbox, Playstation o GameCube. También se puede acceder y mostrar en un televisor imágenes digitales o de vídeo editadas en un PC o Internet. Sin olvidar la posibilidad de enviar

imágenes en directo a través de una cámara de vídeo para Internet, que, en modo de seguridad, detecta cualquier movimiento, graba lo que ocurre y envía las imágenes por correo electrónico. Por su parte, la música digital rompe todas las barreras y se puede disfrutar y compartir entre distintos dispositivos, independientemente de dónde se haya almacenado.

Una de las características más interesantes de la nueva generación de consolas portátiles sin duda va a ser la conectividad inalámbrica. Así tanto las consolas Wii y Nintendo DS como la Sony PSP ofrecen está posibilidad, las tres con Wi-Fi, concretamente el estándar 802.11b, y la tercera además con soporte de infrarrojos. Este soporte Wi-Fi quizás se encuentre un tanto desaprovechado en la consola de Sony al estar su uso destinado al modo multijugador y a actualizar el software de la propia PSP.

Wii es el nombre de la consola de juego de Nintendo, que utiliza la tecnología Wi-Fi. La principal característica de Wii es el control inalámbrico de la consola, que es capaz de detectar el movimiento y rotación en un espacio de tres dimensiones. El mando dispone de funciones de vibración, mientras que la última versión del mando integra además un altavoz. Otro aspecto importante de la consola es el modo WiiConnect24, que permitirá recibir mensajes y actualizaciones a través de Internet con un consumo de energía muy bajo.

En el 2006, Nintendo dio a conocer información acerca del lanzamiento de la consola Wii en Japón, Estados Unidos y Latinoamérica, y confirmó que 21 juegos estarán disponibles para el 2007. Algunos ejemplos de estos juegos son: ESPN Major League Baseball, The Legend of Zelda: Twilight Princess, Madden NFL 07, Marvel: Ultimate Alliance y NFL on CBS.

Nintendo tiene aplicaciones con Wi-Fi para poder conectarse en red y jugar en línea. En este caso las opciones de conexión serán mediante hot-spots inalámbricos o a través de router, aunque Nintendo ofrece también la opción de conectar la consola a un puerto USB de cualquier computadora con Windows XP y conexión de red para no tener que comprar un router Wi-Fi si no se tiene. Otro dato destacable es que la consola de Nintendo DS podrá conectarse entre sí mediante Wi-Fi para, entre otras cosas, cargar de forma automática demos de juegos en la portátil.

La cobertura actual de zonas ADSL Wi-Fi de Telefónica supera los 1800 hot-spots, o puntos de conexión instalados en hoteles, aeropuertos, escuelas, negocios, restaurantes y zonas de entretenimiento. Nintendo destacó que dichos hot-spots se irán abriendo de forma escalonada al servicio de juego en línea Wi-Fi de Nintendo que se inaugura con el lanzamiento de Mario Kart DS.

El usuario podrá localizar el hot-spot activo más cercano a través de la web http://www.nintendowifi.com. Para acceder a Internet y jugar desde estas zonas Wi-Fi, el usuario de la Nintendo DS sólo tiene que encender su consola, elegir la opción Wi-Fi y ponerse a jugar.

FIGURA 15. CONSOLA DE JUEGO NINTENDO DS

El servicio prescinde de menús complicados y Nintendo no cobrará ninguna alta ni cuota mensual a sus usuarios. Además, la conexión Wi-Fi de Nintendo crea un entorno seguro y sin intercambio de información delicada, como detalles de tarjetas de crédito o datos personales.

Telefónica destacó que con la alianza realizada en España con Nintendo, inicia una nueva era en lo que a entretenimiento se refiere y en concreto a nuevas aplicaciones Wi-Fi. Inicialmente, esta opción de juego para Nintendo DS en línea con tecnología inalámbrica está disponible en el juego de Nintendo Mario Kart DS y en Tony Hawk's, aunque el catálogo de juegos con esta modalidad multijugador incluirá próximamente títulos como Animal Crossing: Wild World y Metroid Prime Hunters, Castlevania: Retrato de la ruina, Chronicles cristalinos de Final Fantasy y Final Fantasy III.

La PSP tiene compatibilidad Wi-Fi, que se utiliza tanto para juegos multijugador ad-hoc o a través de Internet, como para actualizar juegos, descargar contenidos adicionales o incluso navegar directamente por la web, gracias al navegador incluido en la versión 2.0 de su Firmware. También es posible en su versión 2.60 utilizar tecnología RSS para escuchar Podcast en streaming, es decir, sin descargar el archivo en la consola; y ver la televisión a través de la conexión Wi-Fi con el aparato de Sony LocationFree. Éstos son ejemplos de los juegos de la infraestructura de Wi-Fi en la consola de PlayStation: FIFA 06, NHL 06 y NBA 06.

Recién salida la XBox 360 en Estados Unidos, ya empiezan a aparecer una serie de accesorios como el Xbox 360 Wireless Network Adapter, que nos permitirá conectar nuestra consola a la red inalámbrica sin más que conectarlo al puerto USB.

Aparte de las aplicaciones de Wi-Fi para las consolas de video juego existen una gran variedad de productos para el entretenimiento de un hogar multimedia e interactivo, estos son algunos ejemplos:

- Gateway ADSL Wireless: módem de alta velocidad con conexión rápida e ininterrumpida a Internet. Se utiliza conectando los PC's mediante el router y el switch de cuatro puertos incorporados para crear una

red Ethernet y compartir la conexión con toda la casa. Cuenta con las funciones de firewall y seguridad avanzadas, permitiendo protección para los PC's, los datos y la familia.

- Puntos de acceso para PC de sobremesa y portátil: permiten configurar una red Wireless-G de alta velocidad en el hogar o la oficina. Es compatible con redes Wireless-B. Cuenta con seguridad inalámbrica avanzada.

- Servidores de impresión: dispositivo que permite compartir hasta dos impresoras con cualquier tipo de equipo de red. Es compatible con la mayoría de las impresoras paralelas y USB (1.1 o 2.0). Conecta las impresoras a la red mediante Ethernet 10/100 con cables o Wireless-G.

- Cámara IP: webcam Wireless-B que envía imagen de vídeo de alta calidad en directo a la red, sin necesidad de cables. Cuenta con un servidor web incorporado que permite ver la secuencia de vídeo desde cualquier lugar.

- Media Link: permite a los usuarios escuchar música digital desde cualquier equipo estéreo convencional. Gracias a él, se puede combinar la calidad del contenido digital con cualquier computadora o equipo de música. Permite ejecutar MP3, WMA y ejecutar listas almacenadas en cualquier computadora o cualquier otro sistema de reproducción.

- Game Adapter: funciona sin ningún tipo de controlador ni configuración en la PlayStation2, Xbox y GameCube. No necesita ni driver, ni instalación de software y funciona sobre cualquier plataforma. Así mismo, dispone de un botón exclusivo de selección de canales que permite configurar la red instantáneamente de forma sencilla.

- DVD Wireless: incluye un lector de DVD de alta progresión y cuenta con la capacidad de distribuir vídeos digitales, música y fotografías sin necesidad de cables así como cualquier otro contenido almacenado en un PC que se pueda reproducir en un televisor o en un equipo de música estéreo. Nintendo anunció el próximo lanzamiento de un producto, que se utilizará para el chat de voz de la Nintendo Wi-Fi Connection.

3.8 Televigilancia Wi-Fi

La televigilancia consiste en poder ver desde un lugar lo que está ocurriendo en otro lugar mediante la transmisión de video y audio. La tecnología inalámbrica permite situar los dispositivos de televigilancia (las cámaras) de una forma fácil y rápida, sin depender de costosas instalaciones cableadas. Por otro lado, Internet ofrece la ventaja de que las imágenes pueden ser vistas desde cualquier parte del mundo.

En el mercado existen cámaras inalámbricas Wi-Fi que permiten situar la cámara en cualquier lugar, con la sola necesidad de disponer de un enchufe de alimentación eléctrica o, en su defecto, de una batería. La señal de video se transmite vía Wi-Fi hasta la red local o Internet.

Las cámaras inalámbricas suelen disponer de un servidor web interno al que se puede acceder tanto para la configuración de la cámara como para ver su imagen. La cámara se configura como cualquier otro dispositivo inalámbrico (a excepción de las propiedades de video propias de este dispositivo). Si se dispone de varias cámaras, existen aplicaciones (como IPView) que permiten gestionarlas simultáneamente e, incluso, realizar grabaciones de las imágenes. Para determinadas aplicaciones resulta más conveniente llevar la imagen de la cámara a un servidor desde donde se ofrece al público. También existen empresas en Internet que, por un módico precio, colocan en sus servidores las imágenes de video recogidas por las cámaras web de sus clientes.

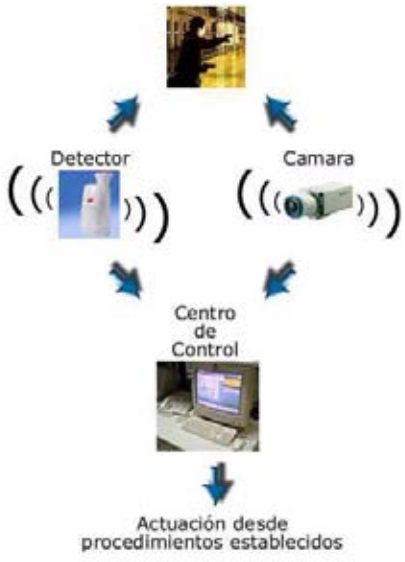


FIGURA 16. RECURSOS WI-FI UTILIZADOS PARA LA TELEVIGILANCIA

En cualquier caso, la televigilancia a través de Internet resulta una buena solución de supervisión de instalaciones y dependencias tanto para el uso particular como para la pequeña y mediana empresa y profesionales. Además, estos sistemas permiten ser combinados con el envío de mensajes de correo electrónico o llamadas al teléfono móvil en el caso de dispararse alguna alarma.

Por último, las cámaras inalámbricas tienen la posibilidad de ser instaladas sobre personas o equipo en movimiento. Esto las hace ideales para cámaras subjetivas en la retransmisión o grabación de imágenes deportivas o de aventura.

3.9 Telefonía Wi-Fi

La telefonía Wi-Fi permite establecer y mantener conversaciones telefónicas utilizando sus facilidades de movilidad, por lo que viene a ser la unión de las redes inalámbricas y de la telefonía IP.

La telefonía Wi-Fi puede tener su campo principal de aplicación en las empresas y sectores como la educación, salud, fabricación o almacenamiento, donde la movilidad de los trabajadores es un factor importante. La ventaja que ofrece la telefonía Wi-Fi frente a las comunicaciones inalámbricas de voz actuales (DECT) es que permite integrar la facilidad de transmisión de voz con la de datos y video. Adicionalmente la existencia de lugares de acceso público Wi-Fi (hot-spot) permite disponer de un servicio telefónico inalámbrico de bajo costo desde lugares públicos.

Para poder hacer uso de esta tecnología, se espera disponer tanto de terminales telefónicos específicos, como de terminales multipropósitos: PDA's y computadoras portátiles. Los terminales basados en PDA's pueden resultar muy interesantes, ya que permiten integrar las funciones de telefonía, video y datos en un solo terminal de reducido tamaño.

FIGURA 17. EJEMPLO DE TELEFONÍA WI-FI

Los retos que tienen que vencerse en la actualidad para la introducción de este servicio son tres fundamentalmente: la calidad de audio en una red abierta llena de interferencias y retardos, que actualmente no está garantizada la continuidad del servicio cuando el usuario se desplaza y la falta de seguridad de las comunicaciones Wi-Fi. A pesar de lo anterior, para todos esto puntos, existen soluciones que harán que este servicio sea posible con todas las garantías a corto y mediano plazo. En el mundo existen muchas empresas que hacen de intermediario entre Internet y la red telefónica permitiendo establecer una comunicación telefónica desde una computadora a cualquier número telefónico del mundo. Las tarifas de estas empresas suelen ser algo más altas que las de una llamada local en el lugar de destino. Generalmente suelen usar el sistema de

prepago, de forma que el usuario sólo tiene que recargar su cuenta con la cantidad que estime oportuna y podrá hablar hasta que se le agote el saldo.

Cuando se dispone de un terminal inalámbrico Wi-Fi desde donde se pretende realizar las comunicaciones telefónicas, esto implica disponer de la posibilidad tanto de realizar llamadas como de recibirlas.

Para solucionar este problema, algunos fabricantes han desarrollado un sistema que convierte las llamadas telefónicas en datos IP que pueden ser remitidos al PC del usuario o al teléfono IP por un proveedor de servicio. Para que esto funcione, el usuario tiene que desviar previamente sus llamadas telefónicas a un número de teléfono de su proveedor de servicio. Si este servicio lo presta el propio operador telefónico (por ejemplo, Telefónica), este re-encaminamiento podría realizarse de forma automática. También se puede contar con un número telefónico independiente para las llamadas a la computadora o al teléfono IP.

Cuando el usuario recibe la llamada en su terminal inalámbrico (computadora portátil o PDA), verá un icono en la pantalla que le indica que tiene una llamada telefónica en espera. El usuario puede aceptar o no dicha llamada, incluso puede navegar y hablar por teléfono simultáneamente.

En el 2003 se anunció la aparición de terminales telefónicos inalámbricos de tecnología Wi-Fi que permiten recibir y realizar llamadas telefónicas de voz siempre que sé este dentro del área de cobertura de una red Wi-Fi. Para evitar tener que llevar encima dos terminales distintos (uno Wi-Fi y otro de telefonía móvil), algunos fabricantes ya han prometido que ofrecerán terminales multimodos (GSM, Wi-Fi y PCS). Esto posibilitará que, con un solo terminal, se pueda utilizar Wi-Fi cuando sé este dentro del área de cobertura Wi-Fi y GSM o PCS cuando se esté fuera del área de cobertura Wi-Fi.

Los teléfonos Wi-Fi, al igual que los teléfonos IP o la telefonía por computadora, necesitan que se contrate los servicios de una empresa de telefonía por Internet. Estas empresas pueden ofrecer incluso un número telefónico exclusivo para las comunicaciones de voz sobre IP.

Capítulo 4 – Protocolos de seguridad en redes inalámbricas

4.1 WEP

Es el mecanismo de seguridad utilizado en las redes inalámbricas que emplean el estándar 802.11b o Wi-Fi. Está diseñado para evitar el acceso a una red por parte de intrusos que cuenten con computadoras dotadas de dispositivos inalámbricos compatibles capaces de escudriñar el tráfico que fluye a través de la red. WEP tiene como objetivos, proporcionar confidencialidad, autenticación y control de acceso en redes WLAN.

El algoritmo de codificación WEP se deriva de la tecnología RC4, un producto desarrollado por la firma RSA Associates que se convirtió en un estándar de seguridad. Originalmente estuvo basado en una codificación de 40 bits que con las impresionantes capacidades computacionales de los equipos actuales, mostró rápidamente su fragilidad en vista de que podía ser violado con relativa facilidad. Hoy en día los equipos son equipados con tecnología de 128 bits lo cual dificulta la penetración no autorizada a las redes.

El algoritmo WEP produce un número de gran longitud que no muestra un patrón predecible. El equipo origen indica al receptor en que dígito debe dar inicio y qué cantidad deberá restar a cada número en el mensaje. Un intruso que detecte el punto de inicio no podrá leer el mensaje porque desconoce el número secreto.

El administrador de la red está en capacidad de definir un conjunto de claves a cada uno de los usuarios inalámbricos basándose en un número secreto que se someterá al algoritmo de encriptado. Cualquier usuario que no disponga de una clave estará incapacitado para acceder a la red.

4.1.1 Características y funcionamiento

El sistema de cifrado WEP consiste en aplicar a los datos originales la operación lógica XOR (O exclusiva) utilizando una clave generada de forma pseudo-aleatoria. Los datos cifrados resultantes son los que se transmiten en el medio.

Para generar la clave pseudo-aleatoria, se utiliza una clave secreta definida por el propio usuario y un vector de inicialización (IV). La clave secreta es única y debe estar configurada en todas las computadoras y puntos de acceso.

La longitud de los datos cifrados excede en cuatro caracteres a la longitud de los datos originales. Estos cuatro caracteres reciben el nombre de Valor de Comprobación de Integridad (ICV) y se utilizan para que el receptor pueda comprobar la integridad de la información recibida. Esto se hace mediante el algoritmo CRC-32.

El algoritmo de encriptación utilizado es RC4 con claves, según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al IV más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El IV, en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero, ya es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Se debe observar que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

RC4, es un cifrado de flujo diseñado por Ron Rivest (quien representa a la R en el acrónimo Seguridad RSA, una compañía de seguridad de datos). RC4 (Cifrado 4 de Rivest) se puede implementar usando varias longitudes de clave. Además de usarse en WEP, RC4 se emplea en los productos de seguridad RSA y es el algoritmo base de la Capa de Conexión Segura (SSL) un protocolo de reconocimiento para proteger el tráfico a través de Internet. RC4 es el algoritmo que se selecciono para WEP debido, en parte, a su velocidad relativamente alta y su robustez. El punto es que el algoritmo RC4 se usa en forma extensa, los problemas que aparecen en WEP no se deben atribuir al algoritmo base.

El algoritmo de encriptación de WEP es el siguiente:

- Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes ICV.

- Se concatena la clave secreta a continuación del IV.

- El PRNG (Generador de Números Pseudo-Aleatorios) de RC4 genera una secuencia de caracteres pseudo-aleatorios, a partir de los datos iniciales, de la misma longitud que los bits obtenidos en el punto 1.

- Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.

- Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos de la trama IEEE 802.11.

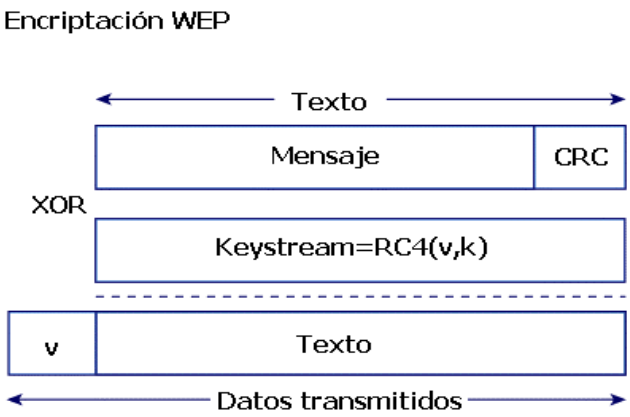


FIGURA 18. ENCRIPTACIÓN WEP

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces los datos iniciales y con ello podrá generar la clave (el keystream). Realizando el XOR entre los datos recibidos y la clave se obtendrá el mensaje sin cifrar (datos y CRC-32). A continuación se comprobara que el CRC-32 es correcto.

Una vez que llegan al destino los datos cifrados, se combina el IV con la clave secreta, distribuida a todas las estaciones, para generar la información que permitirá descifrar los datos mediante el algoritmo PRNG.

El estándar WEP proporciona el cifrado de paquetes usando claves de cifrado estáticas que comparten todos los dispositivos en la WLAN , inclusive los puntos de acceso y los clientes. Cuando se aplica a las redes relativamente pequeñas, la instalación manual de las claves WEP en cada dispositivo de cliente es una tarea abrumadora.

4.1.2 Debilidades

Uno de los inconvenientes que tiene este sistema de cifrado es que la clave secreta es estática. Una vez asignada, se configura en cada estación (por el administrador o por cada usuario) y permanece invariable hasta que se vuelva a repartir este proceso manualmente. Si se pierde una de las estaciones de la red, habría que volver a configurar una nueva clave en todas las estaciones para garantizar la seguridad. Por otro lado, el IV se transmite en abierto a todas las estaciones, el IV si cambia periódicamente.

Un IV de sólo 24 bits de longitud, un valor específico que se usa para generar el flujo de una clave será repetido cada 2^24 o 16,777,216 veces. A pesar de que esto a simple vista parece poco frecuente, un IV se usa en cada paquete enviado. En una WLAN empresarial, fácilmente podrían existir 16 millones de paquetes en el curso de un solo día. En otras palabras, la cantidad relativamente pequeña de IV disponibles limita la capacidad de la arquitectura WEP para resolver el problema de la repetición de claves. Algunos investigadores respetados

relacionados al campo, descubrieron errores en el algoritmo de programación de claves que usa WEP y afirmaron que tanto las claves de 40 como las de 128 bits de WEP pueden ser descubiertas con tan sólo la captura de 4 millones de paquetes, los cuales puede transmitir una LAN empresarial en cuestión de horas. En poco tiempo, apareció una aplicación llamada AirSnort en Internet que hizo real lo que sólo había sido teoría, mediante AirSnort, incluso un usuario casual, no sólo un pirata informático experto, puede interceptar y descifrar el tráfico WEP.

Después de que el primer ataque AirSnort fue publicado, aparecieron medios más sofisticados de atacar las redes Wi-Fi, protegidas mediante WEP. Mientras que el ataque AirSnort, es un ataque pasivo, ya que se basa en la obtención de información de la LAN, esta otra clase de ataques activos representa incluso más problemas para WEP. Entre estos ataques que se conocen como inductivos, están los siguientes:

- Los ataques de repetición. Construyen de manera incremental copias de la clave usando un bit a la vez mediante el análisis estadístico de las respuestas predecibles a los mensajes de texto simple que envía el pirata informático.

- Los ataques de modificación de bits. Son similares a los ataques de repetición en el sentido de que se basan en las respuestas predecibles de las estaciones receptoras. El pirata informático modifica un mensaje (cambia los bits) para provocar un mensaje de error cifrado en una estación receptora, el cual entonces se puede comparar con la respuesta predecible para derivar la clave a través de múltiples iteraciones.

Existen otras formas de ataques a la seguridad de la red, ya sean redes inalámbricas o cableadas, estos ataques y las maneras en las que se podrían aplicar en las WLAN son los siguientes:

- Los ataques de negación de servicio (DOS). Están diseñados para obligar que la red salga de línea, no para obtener información. En Internet, un ataque DOS se puede llevar a cabo mediante la inundación de un servidor usando una tormenta de datos como, por ejemplo, las solicitudes de inicio fingidas. El servidor es incapaz de controlar y rechazar el volumen de solicitudes y por lo tanto se satura o es incapaz de responder a las solicitudes legítimas. En las redes inalámbricas los ataques saturan la banda de frecuencia aplicable con ruido. En su forma más básica, esto se puede lograr con nada más que colocar un teléfono inalámbrico de 2.4 GHz cerca de un punto de acceso y luego iniciar una llamada. Los ataques DOS más complejos se pueden realizar en distancias más largas usando un equipo que genere una gran cantidad de energía RF a lo largo de una porción amplia del espectro, incluyendo a las bandas de 2.4 y 5 GHz.

- Los ataques de diccionario. Se basan en el hecho de que mediante algunos modelos de autenticación,

una contraseña se mantiene en secreto pero el nombre de usuario se envía en forma de texto simple y se puede interceptar fácilmente. Por lo tanto, un pirata informático, puede obtener distintos nombres de usuario y luego comenzar el proceso, generado por una computadora, de adivinar las contraseñas que usan palabras que se encuentran en los diccionarios de idiomas. Este conocido ataque de fuerza bruta puede ser exitoso debido a la capacidad que tiene el poder de procesamiento poco costoso y la realidad de que la mayoría de los usuarios son poco creativos cuando seleccionan las contraseñas. Cuando el pirata informático tiene un nombre de usuario y la contraseña asociada válida, entonces podrá entrar a la red, inalámbrica o cableada, haciéndose pasar por un usuario legítimo.

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. El IV es la parte que varía de la clave para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica cómo manejar el IV. Se indica que debería cambiarse en cada paquete de datos para mejorar la privacidad, pero no se obliga a ello. Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada paquete de datos. Y esto ocasiona que los primeras combinaciones de IV y clave secreta se repitan muy frecuentemente. Más aún si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que los paquetes de datos con igual clave se multiplican en el medio.

Por otro lado, el número de IV diferentes no es demasiado elevado, por lo que terminarán repitiéndose en cuestión de minutos u horas. El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiera nunca, pero esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etcétera) y de la carga de la red.

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los IV, lo cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla.

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido).

WEP también contempla otros problemas además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4. Como se señaló, entre los objetivos de WEP, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número del paquete de datos sin que el destino se percatara de ello.

El estándar IEEE 802.11 incluye un mecanismo de autenticación de las estaciones basado en un secreto compartido. Una estación que quiere unirse a una red, solicita al punto de acceso autenticación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió. El mecanismo anterior de autenticación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización.

WEP no incluye autenticación de usuarios, lo que incluye es la autenticación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autenticación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (replay). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

4.1.3 Alternativas al WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como WEP2. Sin embargo, debemos observar que la longitud del IV sigue siendo de 24 bits, por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera, es decir, WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autenticación de usuarios mediante 802.1x, EAP y RADIUS. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de un paquete de datos, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPN's, de la misma manera que se haría si los usuarios estuvieran conectados remotamente a la oficina. La tecnología de VPN's está suficientemente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperabilidad entre dispositivos de distintos fabricantes.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA y WPA 2 (IEEE 802.11i), es decir, que la solución recomendada a los problemas de la seguridad de WEP es cambiar a WPA o a WPA 2. Otra alternativa es utilizar un protocolo como IPsec.

4.2 WPA: La solución actual

La Alianza Wi-Fi intensificó los trabajos para crear un mecanismo que permitiera dotar a los productos certificados Wi-Fi de altos niveles de seguridad, así WPA fue introducido a principios del año 2003 y las certificaciones WPA llegaron a ser obligatorias a finales del mismo año. El resultado es que la Alianza Wi-Fi, conjuntamente con el IEEE, ha sacado al mercado un nuevo sistema de seguridad para Wi-Fi conocido como WPA (Acceso Protegido Wi-Fi).

WPA son especificaciones basadas en el estándar IEEE 802.11i que mejora fuertemente el nivel de protección de datos y el control de acceso de las redes inalámbricas Wi-Fi. La gran ventaja de WPA es que pueden aplicarse a las redes Wi-Fi existentes y que es completamente compatible con el futuro sistema de seguridad integrada proporcionado por el estándar IEEE 802.11i.

WPA se puede instalar en los equipos Wi-Fi existentes de una forma tan sencilla como instalar un pequeño software en los equipos. Una vez instalado, el nivel de seguridad adquirido es extremadamente alto, asegurándose que sólo los usuarios autorizados pueden acceder a la red y que los datos transmitidos permanecen completamente inaccesibles para cualquier usuario que no sea el destinatario.

4.2.1 Características

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización y nuevas técnicas de integridad y autenticación.

Para obtener las características antes mencionadas, WPA incluye las siguientes tecnologías:

- IEEE 802.1X. Es el estándar del IEEE para proporcionar un control de acceso en redes basadas en puertos, que se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor Triple A como puede ser RADIUS. Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

- EAP. Como se mencionó anteriormente, es el protocolo de autenticación extensible para llevar a cabo las tareas de autenticación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Protocolo Punto a Punto), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP sobre LAN).

- TKIP. Es el protocolo encargado de la generación de la clave para cada paquete de datos. Éste protocolo se encarga de cambiar la clave compartida entre el punto de acceso y el cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IV, con respecto a WEP.

- MIC (Código de la Integridad del Mensaje) o Michael. Código que verifica la integridad de los datos de los paquetes de datos, especifica un nuevo algoritmo que calcula un código de integridad de mensaje de 8 bytes con las utilidades de cálculo disponibles en los dispositivos inalámbricos existentes. El código MIC se coloca entre la parte de datos del marco IEEE 802.11 y el valor ICV de 4 bytes. El campo MIC se cifra junto con los datos del marco y los de ICV. Michael también ayuda a proporcionar protección de reproducción. Se utiliza un nuevo contador para evitar los ataques de reproducción.

4.2.2 Mejoras de WPA respecto a WEP

Las mayores ventajas que aporta WPA frente a WEP son las siguientes:

- WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2^48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de paquetes de datos (replay).

- Para la integridad de los mensajes ICV, se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

- Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

- Mejoras en el cifrado de datos mediante TKIP. Este sistema asegura la confidencialidad de los datos.

- Autenticación de los usuarios mediante el estándar 802.1x y EAP. Este sistema permite controlar a todos y cada uno de los usuarios que se conectan a la red.

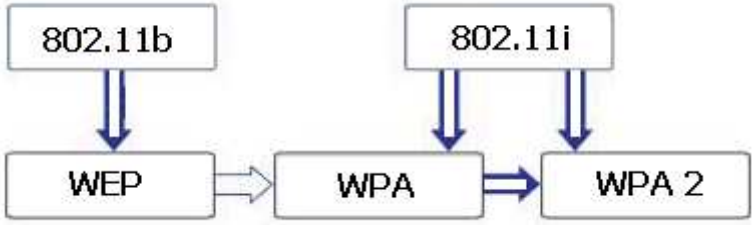


FIGURA 19. PROTOCOLOS DE SEGURIDAD

4.2.3 Modos de funcionamiento de WPA

WPA, según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un servidor Triple A y RADIUS en la red, ya que se requiere de un servidor configurado para desempeñar las tareas de autenticación, autorización y contabilidad. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

- Modalidad de red casera, o PSK. WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas,

porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

4.2.4 WPA 2 (IEEE 802.11i)

WPA 2 (IEEE 802.11i) es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN, introducido en el 2004 y a partir del 13 de marzo de 2006 el proceso de certificación WPA 2 es obligatorio para todos los nuevos dispositivos que desean ser productos certificados Wi-Fi. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA 2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa. Las diferencias de WPA 2 sobre WPA son que el algoritmo MIC fue sustituido por un código de la autenticación del mensaje llamado CCMP (Protocolo de Código de Autenticación de Mensaje), que se considera más seguro y RC4 es sustituido por AES (Estándar Avanzado del Cifrado).

WPA 2 incluye el nuevo algoritmo de cifrado AES, desarrollado por el NIST (Instituto Nacional de Estándares y Tecnología). Se trata de un algoritmo de cifrado de bloque (RC4 de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA 2. Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA 2 utiliza CCMP en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA 2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

Capítulo 5 – Seguridad

5.1 Los riesgos

La seguridad es un riesgo tanto para las redes inalámbricas como para las cableadas. Todas las tecnologías informáticas que han ido apareciendo en el mercado (desde la computadora personal hasta las redes de cualquier tipo) han sido susceptibles, de una forma u otra, de ser violadas en su integridad, confidencialidad o autenticidad de los datos que contiene.

A diferencia de las redes cableadas, las redes inalámbricas emiten señales que pueden ser fácilmente recogidas en el exterior del lugar vigilado de la red (la oficina o el hogar particular). Desde ese punto de vista, las redes inalámbricas tienen un riesgo añadido, pero este riesgo es controlable. De la misma forma que es controlable el riesgo que tiene una red cableada de que un usuario remoto y desconocido pueda entrar en ella a través de su conexión de Internet. El riesgo siempre existe sino se toman las precauciones necesarias.

Las cuatro categorías de riesgos que preocupan en el uso de cualquier tecnología de red son las siguientes:

- Pérdida del equipo.
- Infección de un virus.
- Uso equivocado por personas autorizadas.
- Uso fraudulento por personas no autorizadas.

5.1.1 La pérdida del equipo

A veces, es sorprendente la cantidad de información que podemos llegar a almacenar en el disco duro de nuestra computadora, información no sólo profesional, sino, incluso personal. No obstante, aparte del problema que supone el exponer determinada información a personas indiscretas, existe un problema adicional y es que dicha computadora podría ser utilizada para acceder a la red de nuestra empresa. Este problema existe tanto si la computadora está conectada a una red cableada como si lo está a una red inalámbrica. Perder una computadora puede convertirse en un gran problema si cae en las manos equivocadas.

Si la red es cableada, el acceso a la red se podría hacer desde cualquier parte del mundo vía Internet (si tiene las claves necesarias). En este caso, este riesgo puede eliminarse fácilmente al deshabilitar las cuentas de acceso del usuario en cuestión.

Si la red es inalámbrica, el acceso se tendría que hacer necesariamente desde una zona de cobertura. En este caso, pueden cambiarse también todos los códigos de acceso. No obstante, es cierto que, administrativamente, es mucho más sencillo eliminar una cuenta de acceso de una red cableada que cambiar manualmente las

configuraciones de acceso de todos los usuarios de la red inalámbrica (Wi-Fi no dispone de sistema automático). Sin embargo, a menos que exista algún tipo de etiqueta con identificación, la persona que consiga dicho equipo puede no disponer de ninguna pista para saber dónde se encuentra la red inalámbrica a la que se accede desde el equipo.

5.1.2 Infección por virus

Los virus son pequeños programas informáticos que pueden directamente producir daño en la computadora o ser utilizados para conseguir otros fines haciendo uso de la computadora o de la red en la que se aloja. Los virus afectan tanto a redes cableadas como inalámbricas, hasta la fecha no existe ningún virus que sea específico de redes inalámbricas.

Esto quiere decir que las medidas antivirus son idénticas, independientemente del tipo de red al que se encuentre conectada la computadora, mantener el programa antivirus actualizado y disponer de un firewall.

5.1.3 Uso equivocado por personas autorizadas

El hacer un mal uso del sistema (intencionado o accidental) por personas autorizadas a utilizarlo es una amenaza de la que es difícil protegerse. Una vez que el usuario ha pasado todos los niveles de seguridad y se encuentra dentro del sistema, es complicado controlar en detalle el uso que cada usuario hace de él.

Existen historias de empleados que han robado información de su empresa, borrado archivos, modificado información sensible o hecho cualquier otro uso malintencionado de la información. Existen más historias de empleados que de una forma no intencionada producen el mismo daño compartiendo sus claves de acceso abiertamente, introduciendo datos equivocados, imprimiendo en la impresora equivocada, enviando un mensaje de correo con información confidencial a personas equivocadas o copiando datos confidenciales a su disco duro o flexible sin las medidas de seguridad adecuadas.

Como se puede ver, estos riesgos son equivalentes tanto para las redes cableadas como para las inalámbricas. El único sistema que existe para protegerse de este riesgo es implantar una política de seguridad adecuada en la empresa, que incluya programas de formación a los usuarios y hacer seguimientos periódicos de su cumplimiento (auditorias).

5.1.4 Uso fraudulento por personas no autorizadas

Si hay un punto en el que las redes inalámbricas Wi-Fi tienen desventajas frente a las redes cableadas, ése es el riesgo de uso fraudulento por personas no autorizadas. La desventaja viene por lo que es su ventaja fundamental que cualquier usuario puede conectarse a la red desde cualquier sitio sin necesidad de conectarse

físicamente a ningún medio.

Los usos fraudulentos pueden venir por cualquiera de los siguientes caminos:

- Escuchar. Con un receptor adecuado, los datos emitidos por un usuario pueden ser recogidos por terceras personas. De hecho, existen programas como Airopeck, Airsnort, NetStumbler o Wepcrack que facilitan esta función. Estos programas descubren datos como el SSID, la dirección MAC o si el sistema WEP está o no habilitado.

- Acceder. Se trata de configurar un dispositivo para acceder a una red para la que no se tiene autorización. Esto se puede hacer de dos formas: configurando una estación para que acceda a un punto de acceso existente o instalando un nuevo punto de acceso y, a través de él, conectar fraudulentamente todas las computadoras externas que se deseen.

- Romper la clave. Consiste en intentar adivinar la clave de acceso de un usuario autorizado mediante intentos sucesivos. Un buen porcentaje de usuarios ponen sus claves siguiendo una regla (tres o cuatro letras de las iniciales del nombre, palabras concretas, etcétera). De hecho, existen diccionarios de claves. El atacante sólo tiene que tener la paciencia necesaria hasta dar con la clave correcta.

- Saturar. En este caso no se trata de intentar acceder fraudulentamente a una red, sino de dejarla fuera de servicio. El resultado es que la red no puede ser utilizada por sus propios usuarios, por lo que es un ataque a la seguridad. Para dejar inhabilitada una red inalámbrica, bastaría simplemente con saturar el medio radioeléctrico con el suficiente ruido como para que sea imposible llevar a cabo cualquier comunicación. A este tipo de ataques se le conoce también como obstrucción del servicio, DOS (Denial of Service) o jamming (literalmente, atasco).

5.2 Las debilidades de Wi-Fi

Se han hecho muchos estudios que demuestran que las redes inalámbricas IEEE 802.11 no gozan de altos niveles de seguridad. Algunos de estos estudios son los siguientes: el de la Universidad de Maryland de marzo del 2001, el de Fluhrer, Mantin y Shamir de julio del 2001 o el que un equipo de especialistas en seguridad de la Universidad de California en Berkeley (el ISAAC, Internet Security, Applications, Authentication and Cryptography) publicó en enero de 2001.

La Alianza Wi-Fi siempre ha respondido a estos informes diciendo que los ataques descritos siempre utilizan sistemas sofisticados que necesitan un esfuerzo y tiempo considerable para llevarlos a cabo. Manifiesta que WEP sigue siendo un sistema suficientemente seguro como para estar protegidos de la inmensa mayoría de los posibles intrusos. Por otro lado, WEP nunca fue diseñado para ser un sistema de seguridad total. En cualquier

caso, si se está especialmente preocupado por la seguridad ofrecida por WEP puede ser complementada con otras medidas de seguridad.

5.3 Medidas de protección

La única manera de conseguir seguridad es manteniendo unas técnicas de protección adecuadas. Hay que ser conscientes de que ninguna técnica de protección es eficaz al 100%. Siempre existe riesgo aunque sea pequeño, no obstante, a más barreras de seguridad, menor será el riesgo.

En un principio, las barreras de seguridad básicas que pueden tenerse en cuenta para cada uno de los riesgos son las siguientes:

- Pérdida del equipo. Tomar las precauciones mínimas para evitar en lo posible la pérdida o robo del equipo. No dejar grabados en el equipo los nombres de usuario y contraseña, ni tampoco dejar estos datos escritos en papeles que estén permanentemente con el equipo.

- Infección por un virus. Utilizar software antivirus. Los ataques exteriores se pueden presentar bajo tres formas: virus, gusanos y caballos de Troya. Un virus es un programa diseñado para auto-replicarse y ejecutarse sin el conocimiento del usuario. Un gusano es un programa que está pensado para auto-replicarse y difundirse por el mayor número de equipos posibles. Un caballo de Troya es un programa que aparenta ser un programa útil, pero que, realmente, se dedica a recoger información o a facilitar que el intruso tenga acceso a esa computadora o a la red en la que se encuentra. Los nuevos virus están diseñados utilizando los controles Active X y Java que incorporan los navegadores de Internet. De esta forma, estos programas pueden funcionar sin el conocimiento del usuario. El mundo de la piratería está siempre evolucionando, por este motivo, conviene mantener actualizado el software antivirus.

- Uso equivocado por personas autorizadas. Para estos casos es fundamental implantar una política de seguridad donde se defina cuáles son los puntos importantes que se deben tener en cuenta en relación con la seguridad. En este documento se hablará del uso de las claves, las copias de seguridad, etcétera. Esto debe de ir acompañado de una formación adecuada a los usuarios sobre el uso de las computadoras, las posibles amenazas a la seguridad y cómo evitarlas.

- Uso fraudulento por personas no autorizadas. A pesar de que los problemas de seguridad es un tema que tienen en mente la mayoría de los usuarios, muchas veces no se le dedica una mínima atención, por ejemplo, es habitual dejar configurados los productos en su configuración por defecto. Si hay algo que conocen los intrusos es la configuración por defecto de los equipos. Por ello, es recomendable cambiar las claves de acceso y activar las medidas de seguridad no configuradas por defecto. En el caso de WEP, por defecto, viene deshabilitado en muchos equipos. Conviene habilitarlo, así como

cambiar la identificación SSID. Otra medida en redes inalámbricas, desde el punto de vista de seguridad, es que, si se dispone de router con DHCP (Protocolo de Control Dinámico del Host), conviene tenerlo deshabilitado y asignar las direcciones IP de forma manual. Resulta también altamente recomendable la instalación del firewall. En el caso de una empresa, el firewall puede instalarse entre la red corporativa cableada y la red inalámbrica. También existen los firewall personales, éstos permiten controlar el tráfico que entra o sale de la computadora en la que se instala. Algunos de estos productos son los siguientes: Sygate Personal Firewall, BlackICE Defender de Network ICE, Norton Personal Firewall de Symantec, Tiny Personal Firewall o ZoneAlarm Pro de Zone Lab. Por último, existen programas en el mercado que permiten controlar qué usuarios se conectan a la red, permitiendo identificar los accesos no autorizados, algunos de estos productos son los siguientes: MobileManager de la empresa Wavelink, Sniffer Wireless de Network Associates o Airopeck de la empresa WildPackets.

5.3.1 La importancia de la clave de acceso

Una de las formas más simples de mantener nuestra seguridad informática es mediante las claves de acceso. En este sentido, el elegir una buena clave de acceso es fundamental. Según el CERT (Equipo de Respuesta para Emergencias Informáticas del Gobierno de los Estados Unidos), el 80% de las violaciones de computadoras son debidas al uso de claves de acceso inadecuadas. Para que las claves de acceso sean una buena protección, sólo hay que tener en cuenta las siguientes reglas:

- Que tenga una longitud mínima de seis caracteres.
- Que no sea una palabra con significado.
- Que no se corresponda con las iniciales del nombre del usuario o de la empresa.
- Que no sea una letra repetida.
- Que no esté formada por letras contiguas del alfabeto.
- Que no esté formada por teclas contiguas del teclado.
- Que mezcle letras mayúsculas, minúsculas y números.
- Cambiar periódicamente las claves de acceso.

5.3.2 Recomendaciones de la Alianza Wi-Fi

Aunque, efectivamente, no se pueda garantizar totalmente la seguridad, siempre se pueden tomar ciertas precauciones para hacer más complicado el trabajo a los intrusos. La Alianza Wi-Fi, recomienda tomar las siguientes precauciones:

- Nunca decirle a nadie la clave y, en el caso de las empresas, asegurarse que todos los trabajadores

siguen esta regla.

- Evitar en lo posible el uso de claves estáticas. Las claves hay que modificarlas frecuentemente, aunque sea una molestia.
- Utilizar un firewall.
- Examinar la red Wi-Fi frecuentemente para comprobar que no existen conexiones no autorizadas.

5.3.3 Comprobar la seguridad

Se debe de tratar de determinar las debilidades de nuestra red y de valorar el riesgo de que nuestros datos estén expuestos a terceras personas. Esto último es una tarea, que depende de la actividad a la que nos dediquemos. Sin embargo, para analizar las debilidades de nuestra red, se cuentan con herramientas interesantes. De la misma forma que estas herramientas ayudan a analizar y mejorar la seguridad de una red inalámbrica, también ayudan a los intrusos a averiguar por dónde poder atacar a la red. Por tanto, es importante sacar ventaja del conocimiento de estas herramientas. Algunos de estos productos son los siguientes: Airsnort, InternetScanner, Black Ice, Netwatcher 2000, NetSpyHunter y Network Stumbler.

5.3.4 La solución propietaria

Se conoce como solución propietaria a aquella que no está incluida en el estándar, sino que es ofrecida exclusivamente por un fabricante. En lo referente a la seguridad, si se está muy interesado en disponer de una red inalámbrica con unas buenas medidas de seguridad, en el mercado existen equipos Wi-Fi que ofrecen soluciones propietarias que permiten configurar la red con eficientes métodos de cifrado, una autenticación adecuada o sistemas automáticos de gestión de claves.

El inconveniente de las soluciones propietarias es que, al no estar incluidas en el estándar Wi-Fi, sólo funcionan en los equipos del fabricante que las incorpora. En muchos casos, esto supone que las computadoras en las que se instalan estos equipos propietarios dejan de poderse conectar fácilmente con las redes Wi-Fi que no disponen de puntos de acceso de dicho fabricante.

En general, si a la red inalámbrica se le va a dar un uso particular o se va a utilizar en la empresa para labores normales donde la seguridad no es un asunto excesivamente critico, realmente, no hará falta someterse a las limitaciones de no poder cambiar de fabricante, pero si, por ejemplo, se trabaja en el departamento de desarrollo de nuevos productos, se requiere de una alta disponibilidad del servicio o se trabaja con información de carácter personal, el disponer de medidas de seguridad puede ser fundamental.

5.4 Red Privada Virtual

El nombre de Red Privada Virtual (VPN), hace referencia a un protocolo especial que permite conectar una computadora a una red de una forma segura. Este protocolo debe instalarse en cada una de las computadoras que forman la red, no obstante, el propio sistema operativo Windows incluye las herramientas necesarias para poder llevar a cabo esta configuración de una forma fácil y cómoda.

En el mercado existen distintos protocolos que permiten crear una VPN, los más conocidos quizás sean IPSec, PPTP y L2TP.

Los sistemas operativos Windows ofrecen crear una conexión de este tipo utilizando el protocolo PPTP (Protocolo Punto a Punto Tunelado), este protocolo puede utilizarse sobre cualquier tipo de conexión (TCP/IP, NetBEUI, IPX, etcétera). La única particularidad es que una computadora de la red debe hacer las funciones de servidor PPTP (o servidor VPN). Esta computadora será la que sirva de puerta de entrada de las comunicaciones PPTP.

Una VPN cifra las comunicaciones entre la computadora del usuario y el servidor PPTP mediante un sistema que se conoce como tunelado. No importa el camino que se utilice en la comunicación (Internet, llamada directa por red telefónica, comunicación inalámbrica, etcétera), la información transmitida tendrá la garantía de no poder ser descifrada hasta que no llegue a su destino.

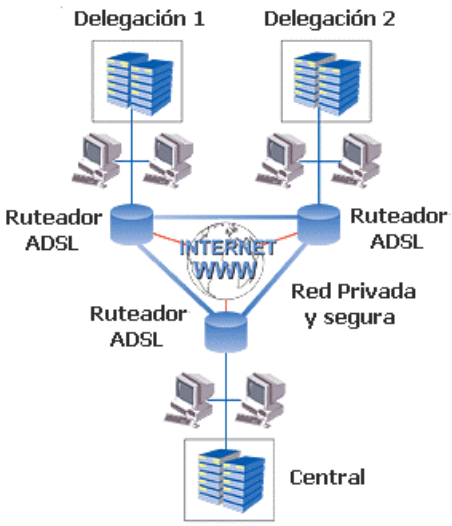


FIGURA 20. UTILIZACIÓN DE UNA RED PRIVADA VIRTUAL

Windows XP ofrece la posibilidad de utilizar protocolos más modernos que PPTP para crear una conexión VPN. Éste es el caso del estándar L2TP (Protocolo de Tunelado de Capa 2), que es utilizado en conjunción con

IPSec (Seguridad del Protocolo de Internet).

El inconveniente de las VPN es que parte de los datos transmitidos tiene que dedicarse al cifrado de los datos, por lo tanto, son redes algo menos eficientes. Si se está especialmente preocupado por la seguridad de la red, sin duda, la mejor medida de seguridad que se puede tomar con una red inalámbrica es configurar una VPN.

Además, el software necesario para crear una VPN viene incluido en Windows desde su versión 95. Por lo tanto, esta medida no tendrá ningún costo adicional, aunque si requerirá que se le dedique algún tiempo. En resumen, las ventajas que ofrece el crear una VPN son las siguientes:

- La gestión de la VPN es centralizada, escalable y eficiente.
- Ofrece seguridad a las comunicaciones inalámbricas Wi-Fi.
- Ofrece seguridad a las comunicaciones con la red local desde Internet o para cualquier otro tipo de acceso remoto.
- El software de VPN no tiene ningún costo adicional si se utiliza Windows.

5.5 Firewall

Los muros de fuego o firewall son una de las más importantes medidas de seguridad para proteger una computadora individual de los posibles ataques que pueda recibir, tanto a través de un entorno no del todo seguro como el de las redes Wi-Fi, como a través de una conexión de banda ancha a Internet.

El firewall no protege las comunicaciones, sino que protege a la computadora para que ningún intruso pueda hacer uso del disco duro o de cualquier otro recurso. Un punto de acceso o un router puede también determinar propiedades de cortafuegos para proteger los recursos de la red. Los firewall llevan a cabo su protección analizando los datos de petición de acceso a los distintos recursos y bloqueando los que no estén permitidos.

Para las aplicaciones en el hogar o en pequeños negocios, es posible que sea suficiente con las características de firewall incluidas en el punto de acceso normal. Existen puntos de acceso profesionales que mejoran fuertemente estas características. A parte de lo anterior, un firewall puede ser tanto un equipo hardware específico, como un software instalado en una computadora o servidor. Los siguientes son algunos ejemplos de equipos de hardware: Watchguard (www.watchguard.com), Webramp (www.webramp.net), Officeconnect (www.3com.com) o Sonicwall (www.sonicwall.com). Por el contrario, los siguientes son algunos ejemplos de software: Zonealarm (www.zonealabs.com), Conseal Private Desktop (www.firewall-net.com), Sybergen Secure Desktop (www.networkcomputing.com), Norton Internet Security (www.symantec.com) o Blackice Defender (www.iss.net).

5.5.1 Los filtros del firewall

El firewall toma la decisión de qué datos deja pasar y qué otros no analizando los paquetes de información. La principal diferencia entre un buen firewall y uno menos bueno es la cantidad de información que es capaz de analizar para tomar las decisiones. En la actualidad existen tres tipos de firewall:

- Filtrado de paquetes. Éstos facilitan un control de acceso básico basado en la información sobre el protocolo de los paquetes. Simplemente deja o no pasar los paquetes de acuerdo con el protocolo de comunicación que utiliza el paquete. Los routers incluidos en los puntos de acceso (o en los routers ADSL o módem) ya suelen disponer de este tipo de filtrado. El problema es que esto supone una protección mínima para el usuario.

- Servidor proxy. Se trata de una aplicación software que va más allá del simple filtrado del protocolo del paquete. Este tipo de firewall puede tomar decisiones basado en el análisis completo de todo un conjunto de paquetes asociados a una sesión que tiene el mismo destinatario. Un proxy mejora la seguridad, aunque tiene el inconveniente de hacer más lenta la comunicación. Además, son más elaborados de configurar. Algunas de las soluciones proxy del mercado son las siguientes: Microsoft Proxy Server (www.microsoft.com), Winproxy (www.winproxy.com), Sygate (www.networkcomputing.com) o Wingate (www.wingate.deerfield.com).

- Análisis completo del paquete. Éstos se basan en la misma técnica de filtrado de paquetes, pero, en vez de simplemente analizar la dirección de la cabecera del paquete, va interceptando paquetes hasta que tiene información suficiente para mantener su seguridad. Posteriormente, entrega estos paquetes al destinatario de la red interna y permite una comunicación directa entre este destinatario interno y su extremo externo. Este firewall bloquea todas las comunicaciones generadas en Internet y deja pasar aquéllas iniciadas por cualquier computadora interna. El resultado es una comunicación más fluida que con los proxy, pero la seguridad es menor.

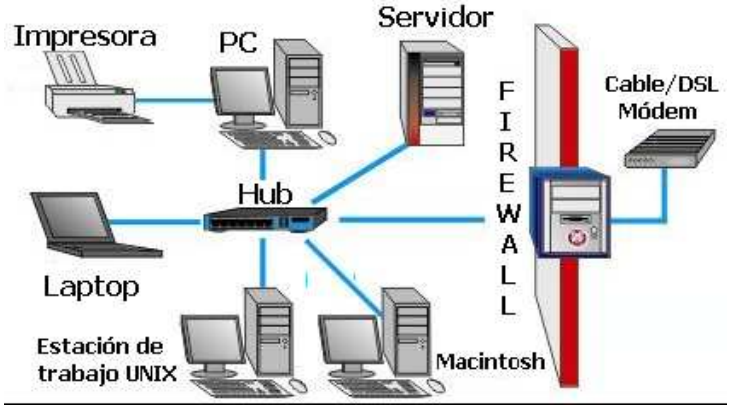


FIGURA 21. SEGURIDAD CON FIREWALL

5.5.2 Las reglas de filtrado

Las reglas de las que dependen los filtros de firewall se basan en distintos factores, condiciones o características de los paquetes de datos. Las características más comunes son las siguientes:

- Dirección IP. Tanto la dirección IP origen como destino pueden ser utilizadas para controlar los paquetes. Este tipo de filtros se utiliza habitualmente para bloquear la comunicación con ciertos servidores externos o para bloquear el acceso a Internet de ciertos usuarios.

- Nombres de dominio. Esta característica se utiliza de la misma forma que el filtrado de direcciones IP, pero basadas en los nombres de dominio en vez de los números IP, ya que los números IP de un servidor pueden cambiarse fácilmente, mientras que los nombres de dominio suelen ser más estables.

- Protocolos. Los protocolos son también una característica interesante a filtrar, por ejemplo, se puede dejar de pasar el protocolo http para permitir el acceso a páginas web, pero no permitir el protocolo telnet para impedir ejecutar comandos en computadoras remotas, el protocolo ftp para impedir la descarga de archivos potencialmente infectados de virus o el protocolo smtp para impedir que desde la computadora de un usuario se pueda crear un servidor de correo desde donde enviar correos ilegales.

- Puertos. Mientras las direcciones IP se utilizan para identificar a los equipos origen y destino de la comunicación, los puertos son unos números que sirven para identificar cada una de las aplicaciones con comunicaciones simultáneas que puede tener un mismo equipo. Generalmente, cada número de puerto se utiliza para una aplicación distinta, por ejemplo, el servicio web suele utilizar el puerto 80, Telnet el 23, o el correo electrónico POP3, el 110. Por lo tanto, filtrar los números de puertos es una forma de filtrar los servicios a los que se puede acceder o ser accedidos.

- Contenido. Los firewall pueden filtrar también los datos que contienen determinadas palabras o frases. En este caso, el firewall analiza todo el contenido de los paquetes en busca de las palabras o frases prohibidas.

PARÁMETRO	SIGNIFICADO
Protocolo	Tipo de protocolo que utiliza el paquete (TCP, UDP)
Dirección IP del destinatario	Identifica a la computadora que va a recibir el paquete
Puerto IP del destinatario	Identifica a la aplicación que va a recibir el paquete
Dirección IP del remitente	Identifica a la computadora que envió el paquete
Puerto IP del remitente	Identifica a la aplicación que envió el paquete
Contenido	Identifica el contenido de la información transmitida

TABLA 3. PARÁMETROS QUE ANALIZA UN FIREWALL

5.6 Estándar 802.1x

En junio del 2001 el IEEE aprobó el estándar 802.1x. Este estándar incluye un nuevo protocolo de seguridad conocido como EAP (Protocolo de Autenticación Extensible). Este protocolo se utiliza para controlar el acceso de los usuarios a los puntos de acceso y autenticar sus comunicaciones.

EAP se utiliza también para poder hacer una entrega segura de las claves de la sesión. Con EAP se puede generar y distribuir automáticamente las claves WEP, eliminando la pesadez de un proceso manual que iba en decremento de la seguridad.

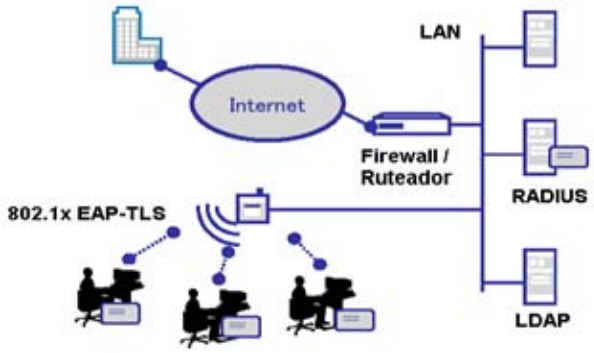


FIGURA 22. FUNCIONAMIENTO DEL ESTÁNDAR 802.1X

802.1x está siendo cada vez más aceptado por la industria, hasta el punto de que tanto Windows XP como algunos fabricantes de puntos de acceso ya lo incorporan. Por otro lado, el comité 802.11i tiene el objetivo de mejorar la seguridad de las redes inalámbricas. Uno de los puntos es el control de acceso y la autenticación (ahí es donde entra 802.1x), pero, además, incluye temas como una metodología de cifrado mejor que WEP, un mejor uso del vector de inicialización, protección contra los paquetes falsos, ataques de respuesta, etcétera.

5.7 Prácticas de seguridad Wi-Fi recomendables

En los siguientes puntos se describen las distintas herramientas de seguridad que están disponibles actualmente como: autenticación, cifrado, claves dinámicas de cifrado y los estándares WEP, WPA, WPA 2 y IEEE 802.1x, cuáles son las más adecuadas para los distintos tipos de clientes y aplicaciones. Así como los diferentes niveles de seguridad que estas herramientas y las arquitecturas asociadas, proporcionan, además de los diferentes tipos de ataques a la red junto con la manera que pueden ser mitigados.

La manera en que las WLAN Wi-Fi proporcionan a las empresas una movilidad sin precedentes y las mejoras resultantes en la eficiencia organizacional, toma de decisiones y productividad general. Sin embargo, todo esto no quiere decir nada cuando la WLAN provoca una brecha en la seguridad a lo largo de toda la empresa que finalmente impida o detenga su implementación, por el riesgo que implica una infiltración parcial o total.

Las WLAN Wi-Fi pueden tener un tremendo impacto positivo en una organización, pero también pueden tener un impacto negativo grande correspondiente, uno que ponga en riesgo la seguridad de no sólo la WLAN sino de la red entera, además de los servicios inalámbricos y cableados. Los comercios, los negocios y las tiendas de medios en general han mencionado estas preocupaciones, sin embargo, en algunos casos, han malinterpretado las WLAN, afirmando que son fundamentalmente incapaces de ofrecer seguridad. La realidad es que a pesar de que la naturaleza inalámbrica de Wi-Fi presenta problemas en la seguridad que no se encuentran en las LAN cableadas, se puede desplegar una WLAN de cualquier tamaño que proporcione un nivel general de seguridad que sea igual, o más alto, que el de una LAN cableada.

5.7.1 Autenticación

La autenticación es el proceso en que se determina que un individuo o, mejor aún, un dispositivo, es quién dice ser. Los puntos de acceso también se pueden configurar de manera que usen contraseñas, los cuales se conocen como SSID. Los puntos de acceso normalmente se distribuyen con un SSID predeterminado que es específico del fabricante, cuando este es el caso, y un adaptador de cliente tiene configurado un SSID nulo, seria capaz de asociarse al punto de acceso. Las herramientas administrativas como, por ejemplo, NetStumbler e incluso Windows XP de Microsoft, proporcionan la capacidad de registrar todos los SSID que se puedan percibir de un cliente y luego permitir que el cliente se asocie al punto de acceso seleccionado. Algunos fabricantes proporcionan la capacidad de eliminar el SSID de emisión a los puntos de acceso, esto resuelve el problema de seguridad, pero deshabilita la capacidad de que un cliente pueda encontrar la red adecuada con la cual quiere conectarse. Un SSID debe considerarse más como un nombre de red que una contraseña, debe actuar como un medio de autenticación del punto de acceso o, cuando el mismo SSID se añade a múltiples puntos de acceso de una LAN Wi-Fi entera.

Muchos fabricantes Wi-Fi proporcionan la capacidad de restringir el acceso a la LAN basándose en la tabla de direcciones MAC. La programación de direcciones MAC son los únicos identificadores numéricos que usan los fabricantes para los dispositivos LAN como, por ejemplo, las tarjetas de interfaz de red (NIC) que usan cable y las inalámbricas, al igual que los interruptores, direccionadores, concentradores y puntos de acceso. Los números de direcciones MAC son similares a los números de identificación. Mediante esta característica, puede introducir un número de direcciones MAC o un rango de direcciones MAC dentro de un punto de acceso o varios puntos de acceso, y por lo tanto, sólo permitir que los dispositivos que tienen estas direcciones se asocien, o puedan acceder a la LAN.

Cuando el usuario del dispositivo intenta obtener el acceso a la red, el dispositivo despliega su certificado a un servidor de autenticación a través de la red. Los dispositivos que contienen certificados válidos obtienen el acceso a la red. Los certificados no son nada más que un tipo de autenticación que usan los sistemas de seguridad inalámbricos para empresas.

Los nombres de usuario y contraseñas también se puede usar para el acceso a la WLAN y representan un tipo de autenticación que incluyen los sistemas de seguridad empresarial. La autenticación no se lleva a cabo en la capa de aplicación sino en la capa física, lo cual significa que el usuario que no esté autenticado no podrá obtener ningún tipo de acceso a la red. Otras contraseñas pueden ser válidas para un solo uso y se conocen como contraseñas de un solo uso (OTP), estas contraseñas, que también se conocen como tokens flexibles, se generan al escribir un número de identificación personal permanente en una aplicación que entonces genera una contraseña de un solo uso que se aplica normalmente mediante un rango de combinaciones alfanuméricas que pueden ser reconocidas por el servidor de autenticación.

Los distintos medios de autenticación se pueden usar en combinación para añadir capas de seguridad, como por ejemplo, el uso de un número de identificación personal para obtener un OTP o usar un certificado además del nombre de usuario y contraseña.

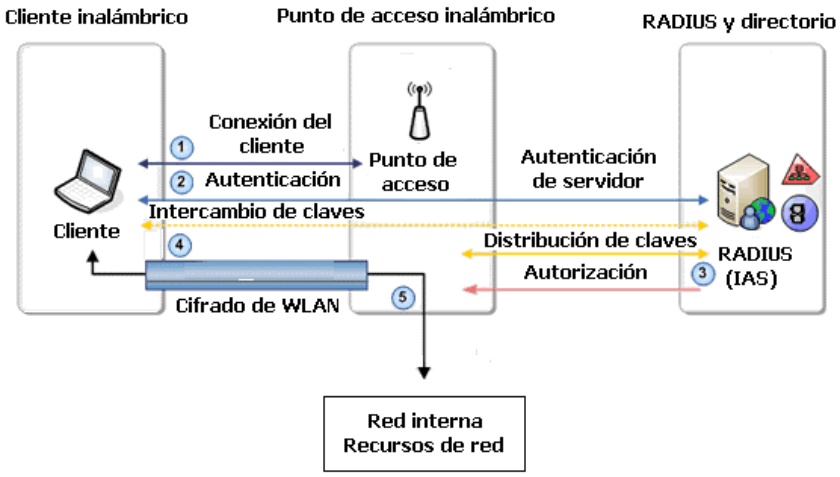


FIGURA 23. PROCESO DE AUTENTICACIÓN

5.7.2 Cifrado

El cifrado es la práctica de cambiar la información de forma que esté tan cerca como sea posible de ser imposible de leer sin la información necesaria para descifrarla. Un cifrado o algoritmo es una fórmula que se usa para generar un flujo de datos cifrados basado en una clave de cifrado. Estas claves de cifrado se pueden medir en términos de longitud, mientras más grande sea la clave, será más complicado y robusto el código. La unidad de medida que se usa para las longitudes de claves es el bit, por ejemplo, una clave de cifrado de 40 bits da como resultado 2^40 combinaciones posibles, una clave de 128 ofrece 2^128 combinaciones. El Departamento de Comercio de los Estados Unidos, trabajando en conjunto con la Agencia Nacional de Seguridad, ha impuesto restricciones en las exportaciones a las tecnologías de cifrado basados en la longitud de la clave, prohibiendo las exportaciones de muchos productos que usan claves de cifrado mayores a 64 bits

de longitud. Los productos Wi-Fi, los cuales están clasificados como productos de venta al público por el gobierno, están exentos de esta restricción y se pueden exportar incluso cuando proporcionen un cifrado sólido.

Para crear el mensaje codificado, denominado texto codificado, se combina la clave de cifrado con el mensaje original, o texto simple. Existen dos tipos principales de cifrado: el cifrado de flujo que codifica el texto simple usando 1 bit a la vez y el cifrado de bloque que fragmenta el texto simple en bloques y luego los cifra bloque por bloque. Los cifrados de flujo se consideran más eficientes y rápidos, debido a que los cifrados de bloque introducen un paso extra al proceso, el cual impacta al desempeño pero incrementa la robustez. La combinación de la clave del cifrado y el texto simple se conoce como una función OR exclusiva (con mayor frecuencia, XOR). En términos de redes, el texto simple es un solo paquete, el cual a menudo se repite debido a los errores de transmisión y a los envíos que esto implica, esta repetición frecuente de paquetes y la repetición resultante de texto cifrado proporcionan a los piratas informáticos mejores oportunidades de descubrir el código.

Una manera de resolver este problema es mediante el uso de un vector de inicialización, el cual es un valor numérico de una longitud en bits determinada que se adjunta a la clave de cifrado. A diferencia de la clave de cifrado, el vector de inicialización sufre modificaciones frecuentemente y se envía en forma de texto simple de forma tal que pueda ser reconocido tanto en las estaciones emisoras como las receptoras. La modificación en el vector de inicialización produce los cambios en el flujo cifrado, lo cual da como resultado un texto cifrado distinto aún cuando el texto simple, o el paquete, sea exactamente el mismo.

5.7.3 WEP: Cuando la equivalencia no es igual

La seguridad ha sido parte de los estándares WLAN desde que apareció el estándar 802.11 con velocidades de 1 y 2 Mbps en 1997. Debido a las velocidades de datos relativamente bajas y precios altos de los primeros tiempos, las WLAN eran simplemente un nicho tecnológico, casi exclusivamente a los mercados verticales como el de ventas y manufactura. Estos mercados están caracterizados por una cantidad relativamente pequeña de dispositivos de cliente específicos para las aplicaciones, por ejemplo, los lectores de código de barras y las terminales POS, por ubicación. Normalmente estos dispositivos no salían de las instalaciones, en 1997, las WLAN representaban una tecnología relativamente obscura, la cual sólo era importante para una cantidad pequeña de industrias e individuos. No era el fenómeno Wi-Fi actual, dada la manera drástica en que la industria WLAN ha cambiado a lo largo de este periodo tan corto, no es sorprendente que el estándar de seguridad inicial que acompañaba a los estándares WLAN haya quedado tan obsoleto.

El estándar inicial conocido como WEP, que al principio tenía la tarea de proporcionar la seguridad a las personas que enviaban información como, por ejemplo, los números de tarjeta de crédito, desde terminales POS a través de la RF. Desafortunadamente, a medida que el estándar se volvió obsoleto debido al rápido desarrollo del mercado, el término de seguridad comenzó ha ser un alardeo.

5.7.4 Autenticación 802.1x

IEEE 802.1x es un estándar ratificado por el IEEE para el control de acceso a la red basado en puertos, fue diseñado originalmente para usarse con tecnologías cableadas como por ejemplo, Ethernet. La arquitectura 802.1x está compuesta por tres partes principales: un solicitante, un autenticador y un servidor de autenticación. Cuando se aplica a Wi-Fi, el solicitante reside en los dispositivos de cliente y el punto de acceso sirve como autenticador. El solicitante normalmente es un fragmento pequeño de software que se ubica en el sistema operativo o el controlador de dispositivo que proporciona el fabricante del adaptador del cliente. El punto de acceso actúa como el portero de la LAN, permitiendo que el dispositivo de cliente obtenga el acceso a la LAN sólo después de que el cliente ha sido autenticado. Los servidores de servicio de autenticación remota de usuario por medio del acceso telefónico RADIUS, que inicialmente fueron desarrollados para la autenticación de usuarios de red remotos que usaban una conexión telefónica hacia la red a través del sistema telefónico público inseguro, fueron mejorados para autenticar usuarios accediendo a la LAN a través de un medio igualmente inseguro, ondas de radio. El proceso de autenticación de 802.1x cuando se aplica a las WLAN funciona de la siguiente manera:

1. El cliente obtiene el acceso al medio inalámbrico a través de CSMA/CA y crea una asociación con un punto de acceso.
2. El punto de acceso compatible con 802.1x acepta la asociación pero ubica al cliente en una “área de espera” sin estar autenticado, es decir, la puerta de enlace, hacia la LAN está bloqueado. El punto de acceso envía una solicitud de identificación al cliente.
3. El cliente proporciona una respuesta de identificación que tiene el nombre de usuario o un identificador específico similar que no es secreto. Al recibir la respuesta de identificación, el punto de acceso reenvía esta respuesta a través del enlace cableado hacia el servidor RADIUS.
4. El servidor RADIUS busca el ID de usuario en la base de datos. Es importante señalar que los servidores RADIUS no siempre incorporan una base de datos con ID de usuario y credenciales de autenticación, sino que acceden a estas credenciales que están en una base de datos separadas como, por ejemplo, Active Directory de Windows 2000 o la base de datos de los servicios de dominio de NT. Esto permite la centralización de la autenticación de credenciales, y por lo mismo, la disminución de la carga administrativa.
5. Una vez que el ID de usuario ha sido identificado por el servidor RADIUS, comienza un proceso de interrogación al cliente. El cliente responde a estas preguntas hasta que llega el momento de que el servidor RADIUS determina que el cliente es en realidad legítimo. Debido a que 802.1x no especifica los tipos de autenticación, dejando este aspecto a los fabricantes individuales, pueden variar los medios a través de los cuales el cliente es interrogado, responde y la forma en que finalmente es autenticado en la LAN.
6. En las WLAN, no sólo el cliente debe estar autenticado en la LAN, la LAN también debe estar autenticada en el cliente, es decir, existe la posibilidad de que un cliente se pueda asociar con un punto

de acceso que no sea parte de la infraestructura de la empresa. De hecho, los puntos de acceso ocultos pueden estar instalados por el pirata informático con el propósito de interceptar la información de autenticación del cliente. Por lo tanto, cuando se aplica la autenticación 802.1x en las WLAN, proporciona una autenticación mutua, el cliente en la red y la red en el cliente, así el cliente inicia lo que es esencialmente el proceso inverso de interrogación y respuestas con el servidor RADIUS.

7. Una vez que el cliente ha sido autenticado en la red a través del punto de acceso y el servidor RADIUS, y la red ha sido autenticada en el cliente, se abre el puerto virtual en el punto de acceso y el cliente puede comenzar a acceder a la red inalámbrica y cableada.

FIGURA 24. AUTENTICACIÓN MEDIANTE EL SERVIDOR RADIUS

5.7.5 Claves dinámicas de cifrado

A pesar de que la autenticación 802.1x resuelve las capacidades de autenticación relativamente débiles del estándar 802.11 original, no resuelve de manera directa el problema de las claves de cifrado, es decir, no resuelve los aspectos de escalabilidad o administración asociados con las claves estáticas de cifrado, las cuales son comunes a lo largo de toda la red y se almacenan en todos los dispositivos de cliente. Lo que resuelve este problema es la incorporación de un servidor de autenticación a la arquitectura. Un servidor RADIUS, o posiblemente un servidor Kerberos (un servidor de autenticación alternativo), proporciona no sólo las capacidades de autenticación, sino también la capacidad de generar claves de cifrado que son específicas para ese cliente en particular. La generación de claves centralizadas es igual cuando se administran usuarios remotos de acceso telefónico que cuando se administran usuarios Wi-Fi.

Cuando el cliente ha sido autenticado por el servidor RADIUS después de haber comparado las credenciales del cliente con las credenciales almacenadas en la base de datos, el servidor RADIUS también inicia el proceso de la generación de las claves dinámicas, este proceso de intercambio de claves se lleva a cabo durante la autenticación del cliente en la red. Se debe señalar que estas claves específicas del cliente son claves

unidifusión, que sólo se usan cuando el tráfico está dirigido a un cliente en particular. Las claves multidifusión se usan cuando el tráfico se emite a una variedad de clientes, son compartidas y tienen algunas de las mismas desventajas de las claves WEP compartidas.

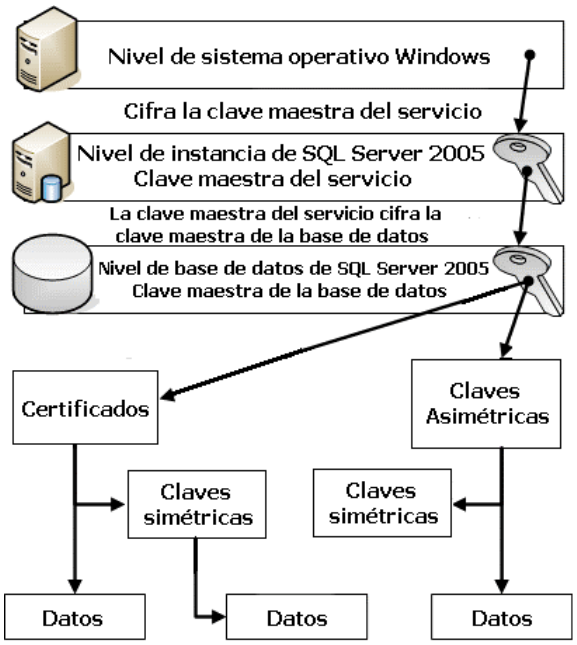


FIGURA 25. GENERACIÓN DE CLAVES DINÁMICAS DE CIFRADO

Las claves específicas de cliente no sólo son particulares para el cliente, sino también son específicas para una sesión de cliente. Mientras más corta sea la duración de la sesión, será menor el número de paquetes que se enviarán con una clave de cifrado en particular, esto significa que los piratas informáticos tendrán menos paquetes con los cuales podrán trabajar, lo cual hace que el trabajo de descubrir una clave sea mucho más difícil. Por otro lado, mientras más corta sea la duración de la sesión, será mayor el número de autenticaciones necesarias durante un periodo determinado. Dependiendo de la arquitectura y carga de la red, esto puede dar como resultado problemas en el desempeño debido a que el servidor RADIUS debe funcionar con un grado mayor de intensidad.

Al crear claves de unidifusión que sean específicas para una sola sesión y un solo usuario, la severidad de que se rompa la seguridad en el caso de que una clave sea descubierta, queda enormemente mitigada. La ruptura en la seguridad daría como resultado la desprotección de los datos de sólo ese usuario y sólo para esa sesión en particular. Esto contrasta con la pérdida de las claves de cifrado estáticas y compartidas, las cuales permiten que el pirata informático descifre paquetes de todos los usuarios y todas las sesiones tanto en el pasado como en el futuro. Estas claves dinámicas de cifrado desaparecen del dispositivo del cliente al final de una sesión o cuando el dispositivo del cliente es apagado, la pérdida de una computadora portátil ya no provocará un desastre en la seguridad.

5.7.6 WPA y WPA 2 (IEEE 802.11i)

Reconociendo la necesidad de una arquitectura de seguridad mucho más robusta y escalable para la LAN Wi-Fi, el grupo 802.11 del IEEE votó para designar un grupo de trabajo especial para la seguridad, la cual ha sido parte de una tarea del grupo dedicado a la calidad de servicio. El Grupo de Trabajo 802.11i (TGi en términos del IEEE) se formo en el año 2001.

El estándar 802.11i especifica a 802.1x, junto con el EAP, como los medios mediante los cuales los clientes Wi-Fi y las redes se pueden autenticar mutuamente. Lo que es notable acerca de EAP es que el proceso extensible del protocolo proporciona la flexibilidad de autenticar usando una variedad de maneras. Esto les ofrece a los fabricantes la libertad de ofrecer diferentes tipos de autenticación o métodos de autenticación usando tipos distintos de credenciales. 802.11i especifica RC4, el mismo algoritmo de cifrado que se usa para las claves WEP estáticas, como el algoritmo de cifrado para las claves dinámicas de cifrado de una sola sesión y un solo usuario.

5.7.7 Diferentes tipos de seguridad para aplicaciones distintas

Se han señalado una variedad de arquitecturas de seguridad distintas, cada una implementa varios medios de autenticación y claves de cifrado. Ahora, se describe la utilidad para cada una de la diferentes aplicaciones como son:

- Oficinas pequeñas

Primero, se debe hacer una distinción entre lo que son las oficinas pequeñas y las sucursales. En las primeras, la entidad es autónoma y no está conectada a través de una WLAN a la red centralizada como en el caso de una sucursal. Debido a lo anterior, una arquitectura de seguridad razonable comenzaría mediante algún nivel de autenticación. A pesar de que son bien conocidas las deficiencias de la autenticación de direcciones MAC (pueden ser fácilmente falsificadas), en realidad representan un pequeño nivel de seguridad. Es posible que los fabricantes integrarán servidores RADIUS directamente en los puntos de acceso, una característica muy útil en redes autónomas pequeñas. A pesar de que las claves WEP estáticas pueden ser descubiertas, aún se podrán usar, especialmente por la razón de que las limitaciones de escalabilidad no representan un problema en una LAN pequeña. Como los ataques a las claves están basados principalmente en la recolección de una cantidad de paquetes, lo cual en una LAN relativamente pequeña y con poco uso como el las oficinas pequeñas, la recolección de dichos paquetes requerirá de mucho más tiempo que en una LAN empresarial muy utilizada. Al modificar regularmente las claves WEP estáticas en el punto de acceso y los pocos clientes que existan, habrá mitigado en gran parte la posibilidad de un ataque.

WPA y las mejoras inherentes en TKIP (Protocolo de Integridad de Clave Temporal) son aplicables a las claves de cifrado estáticas y dinámicas, incluso las instalaciones de oficinas pequeñas deben actualizar sus sistemas a WPA o incluso a la implementación TKIP tan pronto como sea posible.

- Sucursales

Desde una perspectiva física, una sucursal puede parecer idéntica a una oficina pequeña, la principal diferencia es que poner en riesgo a una sucursal implica la posibilidad de comprometer la red empresarial completa. Sin embargo, las sucursales tienen la ventaja de poder aprovechar la infraestructura de seguridad empresarial. Para ser precisos, una sucursal puede usar una arquitectura de seguridad basada en 802.1x completa suponiendo que la autenticación a través de la WLAN proporciona un desempeño y confiabilidad aceptables. Si se despliega un método de autenticación centralizado a través de una WLAN, deberá considerar la confiabilidad del enlace y controlar las expectativas del usuario en cuanto al desempeño y la confiabilidad. Debe considerar el uso de distintos perfiles del lado del cliente como medios alternativos de autenticación local. En las sucursales más grandes, el despliegue de servidores RADIUS aislados en los sitios locales puede ser una opción, aunque existen algunos aspectos administrativos severos e implicaciones en la seguridad ocasionados por la distribución de credenciales de autenticación por medio de este método.

Los mecanismos de autenticación basados en estándares y que son más inteligentes, le proporcionarán a las sucursales una autenticación centralizada y servicios flexibles de autenticación cuando la conectividad con el servidor central no esté disponible. En las sucursales más pequeñas, puede considerar una arquitectura de seguridad basada en VPN, es decir, una arquitectura de seguridad de tipo oficina pequeña para el tráfico local mediante la invocación de un cliente VPN cuando se comunica exclusivamente a través de la RF con la LAN empresarial. Si asume que el tráfico local no sea importante y no exista el tráfico empresarial, ésta puede ser una solución efectiva.

- Empresas.

La arquitectura basada en 802.1x fue diseñada tomando en cuenta a las empresas y se aplica principalmente a este tipo de despliegue Wi-Fi. La naturaleza centralizada de esta arquitectura satisface los requerimientos administrativos, de seguridad y escalabilidad de la empresa. Los fabricantes proporcionan actualizaciones frecuentes para sus distintos componentes, haciendo que la arquitectura sea cada vez más viable para las empresas.

Existen otros enfoques de seguridad. Algunas de las organizaciones más grandes siguen luchando con las claves de cifrado estáticas, asignando prácticamente a miembros del personal para el cambio manual de las claves de miles de dispositivos de clientes individuales. Algunas organizaciones ignoran la arquitectura 802.1x,

y prefieren el enfoque VPN para la autenticación y seguridad Wi-Fi local.

- Acceso al público.

El despliegue comercial de Wi-Fi en áreas públicas como, por ejemplo, aeropuertos, hoteles, escuelas, centros de convenciones, comercios e incluso, cafeterías, representan un desarrollo de la industria. Para el proveedor de servicio, el problema principal es permitir el acceso sólo a aquellos usuarios que están autorizados, normalmente aquellos que han pagado por el uso de la red pública. Esto se traduce a la autenticación del usuario, proporcionándole los servicios para los cuales está autorizado, y luego la generación de los registros de contabilidad que se necesitan para los propósitos de facturación. Estas tres funciones están disponibles en un solo servidor llamado servidor Triple A (Servidor de Autenticación, Autorización y Contabilidad), debido a que proporciona autenticación, autorización y contabilidad. Los servidores RADIUS son un subconjunto de los servidores Triple A, lo cual significa que a pesar de que los servidores Triple A se pueden usar para las aplicaciones de proveedor de servicio, de ninguna manera están limitados a este uso y también se integran en las empresas.

Una alternativa al servidor Triple A es una puerta de enlace de selección de servicio, una herramienta que redirige un usuario a una página web específica. Mediante esta arquitectura, el usuario puede obtener el acceso a la LAN pública pero sólo podrá acceder a un solo sitio Web. Normalmente, este solicitará algún tipo de pago por el uso como, por ejemplo, un número de tarjeta de crédito para hacer una facturación de acuerdo al uso o un nombre de usuario y contraseña si se emplea un modelo de costo por membresía. En este caso, el usuario puede acceder a todo Internet después de que el proveedor de servicio ha recibido el pago. Una vez que el usuario ha obtenido el acceso a la red pública, debe entonces proporcionar su propia seguridad. Es posible que no sea necesaria ninguna medida de seguridad adicional para la exploración del Web ocasional, para los inicios de sesión en una red empresarial, una VPN se convierte en la opción lógica y también es la selección adecuada cuando los usuarios se comunican a través de Internet sobre una conexión cableada.

Capítulo 6 – Wi-Fi en las empresas

6.1 Desempeño Wi-Fi

A pesar de que los objetivos específicos de un desempeño Wi-Fi empresarial variará, existe una constante: desplegar una red Wi-Fi en áreas designadas que proporcione una cobertura confiable y ofrezca el nivel de desempeño esperado sin poner en riesgo la seguridad de la corporación.

La designación de áreas es un elemento muy importante, la gran mayoría de las empresas optan inicialmente por un despliegue WLAN limitado. Existen distintos criterios para definir la manera en que pueden estar limitados estos despliegues los cuales son los siguientes:

- Limitación del despliegue a sólo los lugares en los que es más necesario.- Esta estrategia se basa en la suposición de que cuando los usuarios de computadoras portátiles están en su área de base, por ejemplo, una oficina, cubículo o escritorio, pueden acceder a la red a través de una conexión cableada, ya sea al conectarse directamente en un puerto Ethernet o a través de un módulo de expansión. Por lo tanto, el despliegue Wi-Fi está limitado a los lugares donde las personas tienden a reunirse en un lugar retirado al de sus escritorios, en áreas como salas de conferencias, salas de juntas más pequeñas, cafeterías, salones de clase, auditorios, recepciones y otras áreas públicas similares.

- Limitación del despliegue a un edificio a la vez.- Esta limitación se presenta principalmente en los entornos universitarios, en especial en aquellas universidades donde distintos edificios o grupos de edificios tienen asignaciones diferentes, es común que se despliegue Wi-Fi mediante un método de edificio por edificio. El principal problema con este enfoque es que casi todos los estudiantes, excepto algunos, e incluso alguna parte del profesorado, pasan sus días académicos en más de un solo edificio o grupo de edificios. La experiencia ha demostrado que cuando se ha desplegado una WLAN en un solo edificio, se establece la expectativa de que se desplieguen también a lo largo de la universidad, en salones de clases, cafeterías, dormitorios y otros lugares.

- Limitación del despliegue a edificios y grupos temporales de trabajo.- En este modelo se despliega Wi-Fi no tanto por la movilidad que proporciona al usuario, sino por la movilidad que proporciona a la infraestructura. En el entorno económico y dinámico de la actualidad, es común que las organizaciones aumenten o disminuyan rápidamente su tamaño. También es común que grupos de personas que pertenecen a grupos diferentes e incluso ubicaciones, se reúnan en periodos temporales para un proyecto específico. Este fenómeno ha impulsado la creación del término redes en movimiento. En ocasiones las organizaciones empresariales despliegan una red Wi-Fi para satisfacer estas demandas. Una red Wi-Fi se puede desplegar mucho más rápidamente a lo largo de un edificio que una red con infraestructura tradicional, además de no

requerir de gastos tan altos. Cuando llega el momento de desocupar el edificio, la infraestructura de la red se puede guardar fácilmente y volver a desplegarla en otra ubicación.

- Limitación del despliegue desde el exterior hacia dentro.- En este modelo las WLAN, en especial dentro de las instalaciones pequeñas, se pueden instalar de manera remota a través del control de un contratista local o incluso un empleado de la empresa, lo que disminuye o incluso elimina la necesidad de viajar a localidades remotas.

Una vez que se ha definido la estrategia de despliegue, el paso siguiente en el proceso debe ser la definición del nivel de servicio WLAN que necesita proporcionar a los usuarios Wi-Fi. La principal pregunta que debe ser respondida es: ¿qué capacidad de salida deberá, en promedio, ser proporcionada a cada usuario de la WLAN?.

Los distintos tipos de usuarios tienen diferentes promedios en los requerimientos de la capacidad de salida, por ejemplo, los trabajadores de almacenes y puntos de venta que usan lectores de código de barras tienen requerimientos de capacidad de salida muy modestos. Los usuarios de oficina que transfieren correo electrónico, exploran el web e intercambian un documento de procesador de palabras, hoja de cálculo o archivos de presentación, tienen requerimientos más grandes, aunque también relativamente pequeños, de capacidad de salida.

Después se tiene que contemplar la planeación de la cobertura. Si el objetivo de la planeación de la capacidad es proporcionar a los usuarios lo que necesitan, el fin de la planeación de la cobertura es proporcionarles lo que necesitan donde lo necesitan. Una evaluación en sitio toma en cuenta el diseño del edificio y los materiales con los cuales fue construido (asentados en diagramas y planos de piso además de una revisión directa), los patrones de tráfico dentro del edificio, los tipos de barreras que posiblemente aparecerán en el edificio, las capacidades de rango y cobertura de los puntos de acceso que se deberán usar y la flexibilidad de esas capacidades, las tecnologías 802.11 b, 802.11a y 802.11g, y la capacidad de salida resultante para los canales disponibles para estas tecnologías, además del plan de capacidad.

Entender el efecto que distintos materiales de construcción tienen en la energía de radio representa un buen punto de inicio cuando se evalúe el edificio que se debe descubrir. Por medio de planos o, mejor aún, la inspección física directa, debe familiarizarse con los tipos de materiales de construcción que se encuentran en el edificio. En general, mientras más denso sea el material de construcción, evitará más que la energía RF pase a través de él. Este asunto de la pérdida de energía se conoce como atenuación.

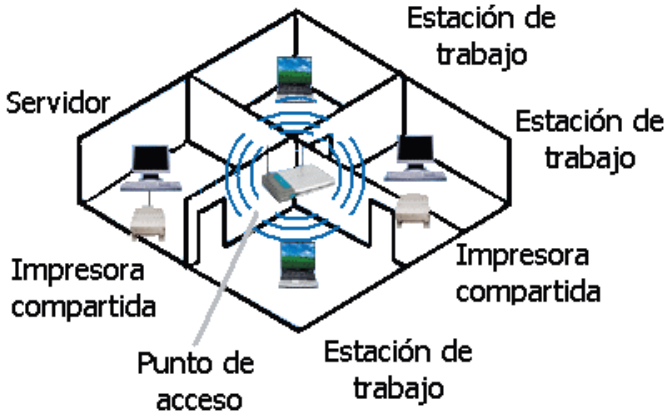


FIGURA 26. EVALUACIÓN DEL LUGAR PARA LA PLANEACIÓN DE LA COBERTURA WI-FI

Se deben seleccionar las mejores ubicaciones para la colocación de los AP y antenas que requieren de la consideración de factores distintos. Las ubicaciones óptimas desde una perspectiva de propagación pueden ser estética y económicamente inaceptables. Las restricciones en el presupuesto pueden dar como resultado puntos de acceso con rangos por debajo de los niveles óptimos y reducir las opciones de antenas. Cada edificio presentará distintos parámetros que sugerirán ubicaciones diferentes de los componentes WLAN.

Cuando se tiene un plan de capacidad y cobertura completo, puede hacer la evaluación física, en este punto, se colocan los AP's y las antenas seleccionadas en sus ubicaciones posibles y se prueba la cobertura. Además, la propagación de señales en la práctica puede ser inexplicablemente diferente de lo que es en la teoría, por lo tanto, antes de comprar el equipo e instalarlo permanentemente, es muy recomendable, o quizá imprescindible que realice pruebas de instalación en todas las ubicaciones posibles que se definieron durante el proceso de planeación de cobertura. La mayoría de los fabricantes Wi-Fi ofrecen, junto con las utilidades de los adaptadores de cliente, herramientas para la evaluación en sitio que tienen capacidades distintas. Como parte del plan de capacidad, tendrá que establecer la velocidad requerida que deberán proporcionar los AP's además de la ubicación y número de usuarios para un punto de acceso determinado. Por medio de una herramienta de evaluación en sitio, puede establecer no sólo la velocidad de datos asociada sino también la confiabilidad de esa velocidad al tomar en cuenta datos más cualitativos como, por ejemplo, la fuerza de la señal y la pérdida de paquetes. Las herramientas de evaluación en sitio con más características son NetStumbler y AirMagnet.

Por último, se debe de llevar una buena documentación respecto a las ubicaciones de los AP's, debido a que necesitará esa documentación para una referencia futura sobre cómo fue construida la red 802.11, además de que será útil para propósitos de solución de problemas y seguridad.

6.2 Velocidades de datos que soporta Wi-Fi

Aunque el equipo LAN Wi-Fi se promueve más comúnmente como dispositivos que proporcionan una velocidad

de datos máxima de11 Mbps, es importante observar que la especificación 802.11b IEEE que representa los fundamentos para que Wi-Fi soporte en realidad un total de cuatro velocidades de datos: 1, 2, 5.5 y 11 Mbps. Las bases para las cuatro velocidades de datos que proporciona el estándar 802.11b son tres tipos de modulación distintos que son los siguientes:

- Modulación de fase por desplazamiento binario (BPSK) para 1 Mbps.- Una onda analógica se puede medir en términos de su potencia, o amplitud; en términos de la cantidad de ondas por cualquier periodo determinado, o frecuencia; o en términos del momento en que la onda comienza su ciclo, o fase. Al variar de manera sistemática estos parámetros pueden alterar la codificación, y por lo tanto, la transmisión de la información. En BPSK sólo son posibles dos estados: el estado 0 ó el estado 1. Un tipo de modulación binaria como BPSK es la más básica, y por lo mismo, el tipo de modulación más sólida. BPSK usa cambios, o desplazamientos, en los tiempos de inicio de una onda para indicar cuál de los estados binarios se está codificando o manipulando. Cada trama de datos que se envía comienza con un preámbulo que establece la línea base para la transmisión y precede a la información real que se transmite. Durante el proceso de reconocimiento entre la estación que envía y la receptora, los dispositivos se sincronizan de manera que se establece una línea de base común, posteriormente, los cambios en esta línea base o desplazamientos en la fase se usan para señalar que se hizo un cambio en la transmisión de un 0 a un 1 ó de un 1 a un 0.

- Modulación de fase por desplazamiento en cuadratura (QPSK) para 2 Mbps.- Este flujo de datos no es simplemente estados binarios de 0 y 1, sino que es un conjunto de cuatro estados: 00, 01, 10 y 11. Después, estos cuatro estados se codifican con base en los cambios en los tiempos de inicio de las ondas. El encabezado de la trama, el cual también se envía usando BPSK, indica cuál es el tipo de modulación que se usará para la transmisión de la carga. La estación que envía intentará transmitir la carga usando tipos de modulación de orden más alto como QPSK, para incrementar la velocidad de datos. Este proceso de cambio de velocidad proporciona un medio automático de maximizar la velocidad de datos cuando aparecen condiciones adversas como el ruido y la distancia.

- Modulación de código complementario (CCK) para 5.5 y 11 Mbps.- Este tipo de modulación proporciona una velocidad de 5.5 Mbps y también una velocidad máxima de 11 Mbps. CCK es un tipo de modulación mucho más sofisticado que BPSK o incluso QPSK. De hecho, para alcanzar las velocidades de datos más altas, los dispositivos compatibles con el estándar 802.11b modulan la señal con BPSK y QPSK además de CCK. Con BPSK, el radio inicia con un flujo de datos de 2 bits; con QPSK, el radio comienza con un flujo de datos de 4 bits. CCK sigue este patrón exponencial al iniciar con un flujo de datos de 8 bits para alcanzar la velocidad de datos de 11 Mbps, y disminuye hasta un flujo de 4 bits cuando las condiciones dictan que se debe usar una velocidad de datos de 5.5 Mbps.

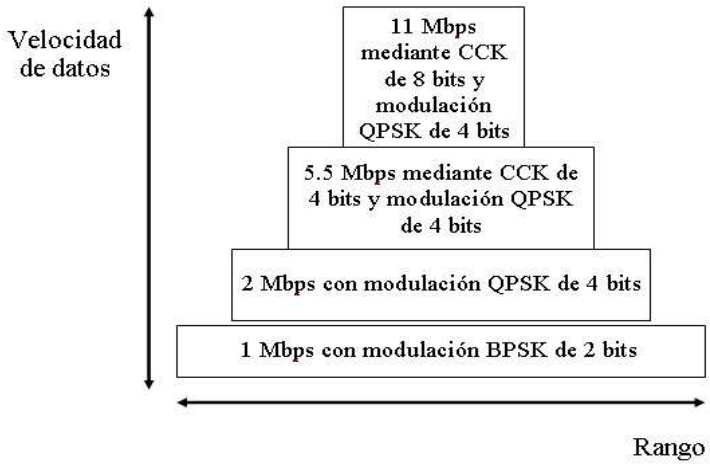


FIGURA 27. TIPOS DE MODULACIÓN QUE PROPORCIONA EL ESTÁNDAR 802.11b

Después de describir las distintas velocidades de datos que soporta el estándar 802.11b en el que se basa Wi-Fi y los tipos de modulación que proporcionan estas velocidades de datos, ahora es apropiado recomendar, o por lo menos recordar, que las velocidades de datos tienen una importancia mínima para la velocidad en la que se enviará un archivo desde un punto hasta otro. La velocidad de datos representa la velocidad con la cual viaja el paquete completo, incluida la sobrecarga de la transacción. Además, la velocidad de datos no toma en cuenta los errores en la transmisión que son lo suficientemente serios para dar como resultado un reenvío pero no son tan frecuentes para provocar un cambio a una velocidad de datos más lento. Por último, la noción de velocidad de datos es aplicable a todo el medio de transmisión, no al usuario individual que está compartiendo este medio con todos los demás usuarios en la misma célula o dominio de colisión.

6.3 Rango e interoperabilidad

El rango de un dispositivo Wi-Fi tiene una dependencia muy fuerte de los factores ambientales, lo que es especialmente importante para las instalaciones Wi-Fi empresariales: los ambientes de oficina pueden variar mucho en términos del diseño y materiales de construcción, lo que tiene un impacto sustancial en el rango. Sin embargo, las distancias que se citan en una hoja de especificaciones representan el rango alcanzado en una sola ubicación, no obstante, existen medidas más objetivas que le permitirán hacer comparaciones con más significado cuando revise las especificaciones de los fabricantes. Los elementos que contribuyen al rango de un dispositivo Wi-Fi determinado, son los siguientes:

- Potencia de transmisión.- La potencia de transmisión se puede considerar, en términos muy coloquiales, como el volumen con el que un radio puede sonar, mientras más grande sea la potencia de transmisión, será más fuerte la voz y será más grande la distancia que ésta podrá alcanzar (cuando todos los demás elementos permanecen igual). Aunque las estaciones de emisión de radio miden su potencia de transmisión en millones de watts (megawatts), los dispositivos Wi-Fi se miden en miles de watts o miliwatts (mW).

Además de los mW existe una unidad alternativa para medir la potencia de transmisión, que permite colocar a la potencia de transmisión en un contexto adecuado que usa un elemento que define el rango. Esta unidad de medida es el decibel (dB), que se asocia más frecuentemente con la medida del sonido.

- Sensibilidad de recepción.- Es una medida de la señal más débil que un radio puede recibir o demodular con éxito, estas habilidades son igual de importantes, debido a que en un radio Wi-Fi existe el requerimiento continuo de que se envíen y reciban transmisiones.. La sensibilidad de recepción se mide en dB. Los fabricantes pueden escoger la inclusión de un amplificador de ruido bajo para mejorar la sensibilidad de recepción. Por lo tanto, incluso los fabricantes que usan exactamente los mismos circuitos integrados pueden proporcionar diferentes niveles de sensibilidad de recepción debido a sus selecciones de diseño individuales.

- Ganancia de antena.- La ganancia de la antena es casi tan poco considerada como la sensibilidad de recepción en términos de su impacto en el rango. Para una antena, ganancia es la proporción de su directividad en una dirección determinada comparada en relación con alguna antena de referencia, mientras más grande sea la ganancia, será más direccional el patrón de la antena, es decir, la capacidad de transmitir y recibir energía a través de un conjunto limitado de direcciones. Con una antena teóricamente perfecta, una señal se irradiará en todas las direcciones de la misma forma, este patrón de cobertura esférico se refiere a que es una antena isotrópica. La ganancia de la antena normalmente se cuantifica en dBis (decibeles comparados con un irradiador isotrópico).

Tipo de antena	**Patrón de cobertura**	**Ancho del haz horizontal aproximado**	**Ganancia aproximada**
Omnidireccional	Omnidireccional	360 grados	Entre 2 y 12 dBis
Bastidor	Hemisférico	Entre 60 y 80 grados	Entre 3 y 9 dBis
Yagi	Direccional	Entre 20 y 40 grados	Entre 10 y 15 dBis
Disco parabólico	Haz angosto	Entre 10 y 20 grados	Entre 20 y 28 dBis

TABLA 4. VARIEDAD DE ANTENAS WI-FI

- Diversidad de antenas.- Un sistema de diversidad de antenas es aquel que tiene dos antenas o dos elementos de tipo antena integrados en un solo dispositivo RF, principalmente en el dispositivo receptor. El tipo de diversidad que se usa con mayor frecuencia en las WLAN es la diversidad espacial pasiva. El propósito de tener dos antenas no es el de duplicar la ganancia, debido a que de hecho sólo una de las dos antenas distintas (de acuerdo a su uso en 802.11) siempre es operacional en un momento determinado. Por el contrario, un sistema de diversidad de antenas, está diseñado para posicionar físicamente la antena en el mejor lugar posible para recibir una señal entrante. La diversidad de antenas para los dispositivos Wi-Fi están espaciadas de manera óptica con aproximadamente cuatro y media pulgadas una de la otra,

alrededor de la misma longitud física de una onda de radio con una frecuencia de 2.4 GHz.

- Pérdida de cable.- El cable de antena para los dispositivos Wi-Fi es normalmente el cable coaxial grueso, similar en apariencia, flexibilidad y costo al cable que se usa para las redes Ethernet. El cable de antena es ofrecido por una variedad de fabricantes y cada uno de ellos proporciona cable con distintas características de pérdida. Esta pérdida en el cable se expresa en términos de dB por pie o una proporción similar entre pérdida y distancia. A pesar de que las especificaciones de los fabricantes varían, los cables de antena están normalmente divididos en categorías de pérdida baja y pérdida ultra-baja, en las cuales el primero proporciona pérdidas de aproximadamente 6.7 dB por 30 metros y el segundo ofrece una pérdida de cerca de 4.4 dB por 30 metros.

Se puede esperar que los productos Wi-Fi de fabricantes distintos trabajen juntos, aunque no tan bien como trabajarían juntos los productos del mismo fabricante. Un sistema de múltiples fabricantes se inclinará a proporcionar una capacidad de salida y rango más pequeños que un sistema de un solo fabricante. Además proporcionará menos opciones de seguridad y otras características como, por ejemplo, la diferenciación de paquetes de voz y de paquetes de datos.

6.4 Selección de equipo y componentes WLAN

Una vez que ha decidido añadir un sistema inalámbrico a su red, necesita determinar cómo debe empezar y qué productos necesita usar. En anteriores capítulos se ha señalado la forma en que las WLAN proporcionan a las empresas mejoras generales en la productividad, basadas en la movilidad del usuario y las ventajas resultantes en la eficiencia organizacional e individual. Sin embargo, todo esto depende de la selección de los componentes adecuados que soportarán las aplicaciones deseadas y necesarias, movilidad, rangos, seguridad y otras características de red. A medida que los administradores de red se apresuran a integrar WLAN en las redes empresariales, a menudo no valoran esta tecnología y la consideran más simple de lo que realmente es.

Una WLAN correctamente seleccionada e instalada puede proporcionar un aumento drástico en la productividad a nivel individual, lo cual a su vez afecta el desarrollo general de la compañía. Sin embargo, la selección de componentes inadecuados puede dar como resultado, con la misma facilidad, un sistema que los usuarios odien, debido a los accesos y reglas de uso complejas, o un sistema que ocasione que la red sea terriblemente lenta, insegura o muy inestable.

En los siguientes puntos se señalan las distintas características y funciones que están disponibles en los productos WLAN, además de los aspectos y características a considerar para que sea posible actualizar la red en el futuro y preparar las migraciones tecnológicas como, por ejemplo, la de 802.11b a 802.11a y 802.11g. Los elementos 802.11 que tienen las mayores probabilidades de cambiar son la autenticación y el cifrado. Es decir,

se tiene que estar preparado para las actualizaciones y crecimiento continuo.

6.4.1 Definición de los requerimientos WLAN

El primer paso para diseñar cualquier red es determinar el objetivo final de la misma, como por ejemplo, las necesidades de los usuarios, para una WLAN, esto incluye la definición del área de cobertura. Antes de poder determinar lo que usted necesita, tendrá que definir por qué lo necesita. La movilidad es una de las razones más comunes para implementar una red inalámbrica, sin embargo, no se debe confundir la movilidad con la capacidad de proporcionar conectividad sin interrupciones en la LAN. Por lo tanto, al principio de la etapa de planeación debe determinar los puntos importantes en los que los usuarios estarán ubicados, además de las rutas más comunes entre las ubicaciones principales de reunión como, por ejemplo, salas de conferencias, oficinas del personal importante, laboratorios de desarrollo y lugares similares. Para este proceso es muy importante contar con un diagrama adecuado de las instalaciones que muestren la cobertura que necesita tomarse en cuenta para la WLAN.

También debe determinar las velocidades mínimas que requieren los usuarios. En relación con este aspecto, se debe tener una descripción de las aplicaciones que los usuarios ejecutan. Tal vez, cada ingeniero de red diría que todos los usuarios necesitan 100 Mbps, lo que equivale a lo que ofrece una red que usa interruptores y cables. Pero la tecnología inalámbrica no usa un medio conmutado sino un medio compartido. Por lo tanto, no todas las aplicaciones se ajustarán verdaderamente al sistema de la WLAN. Debido a que las cargas de tráfico tienden a ser variables, el diseño de red requiere que anteriormente se considere la fracción del ancho de banda disponible, lo cual es un aspecto muy importante. Esto significa que son innecesarias las redes de alta velocidad de 100 Mbps, debido a que la cantidad mínima de velocidad que se requiere generalmente aumenta a través del tiempo a medida que se integran más usuarios a una LAN.

Es poco probable que todos los usuarios de una LAN usen el mismo dispositivo. Por lo tanto, debe determinar si los usuarios necesitan dispositivos especiales en el sistema inalámbrico, por ejemplo, servidores de impresión, lectores de código de barras, tarjetas PCI, tarjetas PCMCIA o incluso teléfonos IP inalámbricos. Si es así, deberá decidir si es necesario obtener todos los dispositivos del mismo fabricante o de fabricantes distintos. Esta decisión puede ser muy importante, debido a los aspectos relacionados con la interoperabilidad. Hay que tener en cuenta que el enlace más débil en la cadena determina el nivel de desempeño, estabilidad y seguridad máximos de la LAN.

6.4.2 Migraciones de la tecnología

Es necesario que se determine la tecnología que se usará para la WLAN. A lo largo de los últimos años han aparecido distintas tecnologías WLAN, se debe considerar cuando se seleccione los componentes WLAN. Entre estos distintos sistemas se incluye a los sistemas del Foro de Interoperabilidad de la LAN Inalámbrica (WLIF),

los sistemas 802.11 de saltos de frecuencia (FHSS), sistemas de frecuencia directa de 802.11(DSSS), sistemas 802.11b, sistemas de salto de frecuencia de banda ancha (WBFH) y los sistemas 802.11a.

Inicialmente, todas las WLAN eran sistemas que estaban muy orientados a fabricantes específicos y propietarios. Las velocidades de datos de los productos WLAN disponibles se aproximaban a 1 Mbps, y los radios estaban basados en la banda ISM de 900 MHz. La disponibilidad de factores estándar estaba limitada a los puntos de acceso, tarjetas ISA y, en menor grado, tarjetas PCMCIA. Para las tarjetas PCMCIA, el consumo de energía general del cliente WLAN era alto, reduciendo el tiempo de ejecución disponible en las baterías, lo cual a su vez limitaba el grado con el cual un usuario realmente podía estar desconectado de una fuente de energía AC.

El uso principal de estas primeras WLAN era el de ventas al público y sistemas de almacén, principalmente para realizar el control de códigos de barra e inventario. El ancho de banda requerido para este tipo de aplicación era comparativamente bajo. Un problema con las primeras WLAN de 900 MHz era la cantidad limitada de países que permitían el uso de este tipo de equipo. La banda de 900 MHz no se podía usar en Europa y en mayor parte de los países de Asia, del Pacífico y Sudamérica. Sin embargo, las compañías como, por ejemplo, Ford Motor Company e IBM deseaban un sistema que se pudiera usar en todas las localidades corporativas, y debido a que esto no era posible con 900 MHz, impulsaron una solución que fuera ampliamente aceptada.

La banda ISM de 2.4 GHz se convirtió en la opción para los fabricantes WLAN innovadores, con los sistemas de 2.4 GHz aumentó la velocidad a un promedio de 2 Mbps (Breezecom Technologies, compañía fabricante de productos WLAN, incluso llegó hasta 3 Mbps). La tecnología de 2.4 GHz era permitida en más de 60 países en ese momento, y debido a las velocidades más altas y la disponibilidad global, las WLAN comenzaron a convertirse en redes más populares.

Sin embargo, aún existía el inconveniente de la interoperabilidad entre los productos. No existía ningún estándar, y por lo tanto, las WLAN estaban formadas por completo de productos propietarios que prevenían de una sola fuente. De hecho, algunas compañías que optaron por implementar las primeras WLAN terminaron creando un sistema propietario que sólo funciona con la línea de productos de un solo fabricante.

Cuando el IEEE terminó el estándar 802.11, se originó una confusión, el estándar en realidad proporcionaba soporte para dos implementaciones RF distintas, FHSS y DSSS, las cuales eran totalmente incompatibles. Esto ocasionó que algunos usuarios, no entendieran qué es lo que debían instalar, también provocó que muchos usuarios potenciales WLAN esperaran antes de realizar una instalación, debido a que no sabían cuál opción debían adoptar: FHSS y DSSS.

Estos nuevos sistemas 802.11 tenían velocidades de datos que estaban definidas con un máximo de 2 Mbps, pero la ventaja en la velocidad de datos en comparación con el formato WLIF era mínima, y por lo tanto, llevó

algún tiempo de adopción. Las ventajas principales eran que se trataba de un estándar de la industria y tenía el propósito de proporcionar interoperabilidad. Sin embargo, surgieron muchos problemas cuando se intentaba que un fabricante A trabajara con un fabricante B, y los usuarios tuvieron que aceptar la palabra de los fabricantes como única garantía para la interoperabilidad, esto también contuvo la adopción amplia de las WLAN.

En el tiempo en que los productos 802.11 comenzaron a acaparar la industria, los usuarios estaban pidiendo velocidades de datos más altas. Dos años más tarde, la industria realizó un avance enorme al llegar hasta los 11 Mbps con la terminación del estándar 802.11b y la introducción de productos con velocidades de 11 Mbps que se basaban en el estándar. La razón principal por la cuál se inicio la certificación Wi-Fi fue la de proporcionar a los usuarios la sensación de seguridad en cuanto a que los productos de un fabricante A tendrían al menos un grado de interoperabilidad con los productos de un fabricante B.

Esto ocasionó la respuesta rápida de una compañía WLAN, Proxim, lo cual dio como resultado el impulso al desarrollo de un sistema FH de velocidades más altas. Proxim solicitó a la FCC un cambio en las reglas que permitiera un nuevo sistema FH, y luego introdujo la tecnología WBFH. Esto le ofreció a FH una velocidad de datos de 10 Mbps. El problema fue que Wi-Fi, IEEE y compañías, como Microsoft y Cisco, hicieron público su deseo de no adoptar esta nueva tecnología, lo cual dio como resultado una implementación muy pequeña del uso real de WBFH.

Debido a todos los cambios en la tecnología, aún existe una confusión significativa en la industria con respecto a cuál es la mejor tecnología, qué es la interoperabilidad y lo que es actualizable. Con la velocidad de 11 Mbps además de la interoperabilidad certificada que están disponibles en el estándar 802.11b, los sistemas WLIF, FH y WBFH se extinguieron. Esto básicamente significó que los usuarios sólo tenían una opción tecnológica, 802.11b. Los avances más recientes en el mundo WLAN son las tecnologías 802.11a y 802.11g, las cuales ofrecen velocidades de datos de hasta 54 Mbps. La certificación de interoperabilidad por parte de la Alianza Wi-Fi esta disponible para ambas tecnologías, lo productos 802.11a comenzaron a aparecer en el mercado en el 2001, y los productos 802.11g están disponibles desde el 2003.

6.4.3 Definición de los requerimientos de tecnología

Antes de que podamos decidir qué tecnología debemos usar, primero debemos responder otras preguntas, a medida que se acerque a una decisión, debe hacer una lista y precisar las respuestas a las preguntas siguientes:

¿Cuáles son las aplicaciones actuales que se usarán y cuál es su requerimiento de ancho de banda por usuario?

Si desea usar la red como una conexión de red simple y para el tipo de aplicaciones normales de oficina (MS Office, correo electrónico, Internet, acceso a base de datos, etcétera), es probable que el ancho de banda de un sistema 802.11b normal sea suficiente (dependiendo de la respuesta a la pregunta siguiente).

¿Cuál es la densidad promedio y máxima de los usuarios WLAN en un área de cobertura predeterminada?, y ¿es posible que esta densidad aumente a través del tiempo?

Debe determinar cuántos usuarios estarán ubicados dentro de un área determinada, tanto usuarios rutinarios como usuarios máximos posibles. Para las aplicaciones de oficina normales, pueden obtener un desempeño razonable con una cantidad de 10 a 20 usuarios por cada punto de acceso 802.11b. Para las aplicaciones de transacciones pequeñas que implican un requerimiento de ancho de banda pequeño como, por ejemplo, la explanada de una casa de cambio o la lectura de código de barras, el número de usuarios por AP puede aumentar drásticamente. Recuerde que la capacidad de salida relacionada (que no es igual a la velocidad de datos) de un sistema 802.11b a 11 Mbps es de alrededor de 5.5 a 6 Mbps por cada AP.

¿Qué aplicaciones futuras se están considerando y cuál es el requerimiento de ancho de banda que se espera?

La respuesta a esto puede determinar si es necesario que se mueva en este momento a un sistema inalámbrico de banda ancha y velocidades altas o si puede esperar y realizar actualizaciones en el futuro. Si en este momento se decide usar 802.11b (basándose en estas preguntas), pero le será necesario migrar a un ancho de banda más alto en el futuro, la posibilidad de actualizar a 5 GHz es una solución (una vez más dependiendo de sus respuestas). Otra posibilidad es actualizar los AP’s 802.11b a 802.11g, y usar clientes 802.11g para las aplicaciones que usan más ancho de banda. Cualquiera de estas soluciones permite la migración lenta y la protección de la inversión, debido a que podrá continuar usando sus clientes 802.11b para las aplicaciones de ancho de banda bajo. Hacer una estimación a futuro de 12 a 18 meses aproximadamente le ayudará como una guía en esta parte del proceso previo de planeación.

¿A qué áreas físicas planea proporcionar el acceso WLAN?

Si desea obtener la cobertura máxima, entonces los sistemas 802.11b le proporcionarán la mejor solución. Si prefiere cubrir las áreas internas y externas, debe usar 802.11b, o limitar el uso de los sistemas 802.11a a los cuatro canales superiores (UNII-2) para el uso externo, además de la potencia de salida más baja que establece UNII-1. Los canales inferiores de 802.11a (UNII-1) sólo se deben usar para los interiores.

¿Planea usar la WLAN para condiciones VoIP portátiles, y si es así, cuántas conexiones VoIP concurrentes tendrá dentro de un área de cobertura del AP determinada?

Los teléfonos basados en 802.11 disponibles están limitados a los sistemas 802.11 DS y 802.11b. Si necesita el

ancho de banda de 802.11a para otras aplicaciones y aún desea instalar teléfonos inalámbricos VoIP, la mejor solución es un AP de banda dual, el cual proporciona un método excelente para separar el tráfico VoIP de datos (además de usar VLAN). Otro enfoque que es satisfactorio es usar dominios de colisión que estén separados virtualmente, llamados redes de área local virtual (VLAN). Los AP 802.11b y los sistemas telefónicos 802.11b actuales transportan de cuatro a siete llamadas al mismo tiempo. Cuando se agrega el tráfico de datos a estos sistemas, el número de llamadas disminuye. Los fabricantes de teléfonos 802.11b están realizando mejoras importantes a sus productos, por lo tanto debe pedir al fabricante una guía sobre el número de llamadas, el ancho de banda general y otros aspectos que considere necesarios.

¿Los AP necesitan estar colocados en ubicaciones seguras que no estén al alcance de la vista?

En los sitios de acceso público, como escuelas, edificios de salud y otros lugares públicos, normalmente los AP se mantienen en un lugar escondido y las antenas externas se usan por razones estéticas y para proteger el equipo de vandalismo y robo. Se deberá determinar si de alguna manera puede montar los AP en un área que no afecte el desempeño de la antena o requiera de antenas externas. Debe de contemplar que la banda UNII-1 requiere que la antena esté integrada al radio 802.11a, por lo tanto, las antenas externas no están permitidas.

Los AP que combinan UNII-1 y UNII-2 también requieren antenas que estén conectadas por el fabricante. El montaje por encima del material del techo puede funcionar, aunque en la mayoría de los casos, ésta no es una ubicación aceptable para la colocación de la antena, debido a que los conductos de aire acondicionado, líneas eléctricas y otros conductores de cable, además de los elementos de instalación de iluminación pueden afectar el desempeño de la antena. Además muchas regulaciones locales solicitan que el equipo que se coloca encima de los techos cumpla con ciertas regulaciones en contra del fuego y el humo, se debe de comprobar con las autoridades locales, cuáles son estas regulaciones.

¿Qué tipos de dispositivos de cliente se usarán en la WLAN?

Si desea usar dispositivos especiales como, por ejemplo, los lectores de código de barras, PDA’s, cajas registradoras, dispositivos para ubicar lugares y otros equipos parecidos, debe determinar, mediante la ayuda del fabricante de dispositivos, si es que estos dispositivos pueden proporcionar soporte para 802.11a, además de interfaces Cardbus o mini-PCI. Debido a que 802.11b sólo alcanza 11 Mbps, es perfectamente aceptable usar una interfase PCMCIA. Sin embargo, si desea usar 802.11a ó 802.11g, deberá usar el soporte Cardbus o mini-PCI, debido a que la interfase PCMCIA no es lo suficientemente rápida como para proporcionar una velocidad de datos de 54 Mbps.

¿Existe algún elemento en la construcción del edificio que interfiera con la señal RF?

Debe determinar si el edificio está construido de forma tal que RF pueda penetrar en las áreas necesarias o si

son necesarias antenas especiales para obtener la cobertura en áreas específicas. Las señales de 2.4 GHz penetran las construcciones normales de manera más sencilla que las señales de 5 GHz. Un buen método es realizar pruebas reales en el sitio con ambas tecnologías para verificar el desempeño en el entorno típico.

¿Dentro de las instalaciones se emplea algún otro equipo de 2.4 ó 5 GHz como, por ejemplo, sistemas Bluetooth, teléfonos inalámbricos, hornos de microondas, cámaras y alarmas de seguridad inalámbricas, etcétera?

Cuando otros sistemas están instalados, y se usan de manera activa, esto puede ser una razón para seleccionar una tecnología en lugar de otra. Sin embargo, también es posible que simplemente se necesite un poco de atención durante las pruebas en el sitio y la instalación para asegurar que la interferencia se mantiene en un mínimo. En muchas ocasiones, esto se puede lograr mediante la colocación adecuada de los AP's y antenas.

6.4.4 Selección de los servicios WLAN necesarios

Ahora que se ha considerado las preguntas anteriores y determinado la tecnología que desea usar, o posiblemente tenga una buena idea con respecto de lo que quiere, debe determinar qué otras funciones serán importantes para la instalación. Por lo tanto, es importante que entienda los aspectos que ocasionará el soporte de algunos de estos servicios o, en algunos casos, la falta de soporte. Esto también será una parte importante de la selección de los productos WLAN apropiados, dichos aspectos son los siguientes:

- VLAN.- Las VLAN son una característica relativamente nueva de muchos de los productos WLAN que se encuentran en el mercado actualmente. Un ejemplo, de desear contar con una VLAN sobre medios inalámbricos, es el tráfico de invitados en el sistema de una compañía. Normalmente, debe establecerse un sistema de seguridad en la WLAN para los usuarios corporativos. Cuando los invitados llegan, ofrecerles el acceso a la red no es necesariamente una tarea sencilla o incluso deseada, debido a que se deben establecer contraseñas y cuentas, además de que es posible que los usuarios cambien regularmente. Mediante el uso de una VLAN, puede proporcionar a los usuarios una VLAN que incorpore ciertos modos de seguridad (PEAP, LEAP, EAP-TLS, WPA y muchos más) y permita el acceso de red corporativa mientras proporcione una VLAN separada para los usuarios invitados con un WEP estático o quizá, sin la necesidad de WEP. Esta VLAN canalizará a los usuarios invitados sólo a ciertas áreas de la red o posiblemente únicamente a la red contaminada para el acceso exclusivo a Internet. Por medio del uso de las VLAN, ambos tipos de usuarios pueden compartir el mismo AP.

- Calidad de servicio.- QoS es un servicio necesario si usted intenta proporcionar soporte para VoIP, y también si desea diferenciar el tráfico por puerto, aplicación o usuario.

- Movilidad de IP en las subredes.- Si se desplaza de una subred a otra, cancelará cualquier tráfico que esté ocurriendo en ese momento, y, a menos que cuente con un método para la función de liberar y renovar las direcciones IP, no obtendrá la conectividad IP. La movilidad IP (IP Móvil) fue desarrollada para resolver este tipo de problemas. Por medio del uso de agentes locales y externos en la infraestructura, además de una pila de protocolos IP especial en el cliente, un cliente se podrá mover a través de distintas subredes, sin que se tenga que cambiar de direcciones IP del cliente. Sin embargo, el problema es que esta solución requiere de dos cosas: el soporte para la movilidad IP en la infraestructura, normalmente en los direccionadores, y, lo que es aún más importante, una pila de protocolos IP diferente en el cliente que proporcione soporte para las funciones de nodo móvil de IP Móvil. Un esquema más nuevo, Proxy de IP Móvil (PMIP), proporciona una solución. PMIP usa la inteligencia del AP para crear un proxy con la dirección IP del cliente, evitando la necesidad de cambiar la pila de protocolos IP del cliente con el fin de proporcionar soporte para las funciones de nodo remoto, esto permitirá el uso de cualquier pila de protocolos IP de cliente.

- Seguridad.- Debe de asegurarse que la solución de seguridad y los productos que seleccione sean compatibles, tomando en cuenta que no tendrá un nivel de seguridad más alto que el del dispositivo menos sofisticado de la red. Un ejemplo sería un edificio de servicios de salud en el cual la aplicación de los archivos de los pacientes se ejecuta en computadoras portátiles que soportan muchos modos de seguridad distintos (PEAP, LEAP, EAP-TLS, WPA y otros) pero la aplicación farmacéutica requiere de la lectura del código de barras y los lectores de código de barras pueden o no soportar la misma solución de seguridad. Por lo tanto, tenga cuidado de seleccionar los productos que soporten el método de seguridad que se ha escogido o se va ha escoger.

- Balanceo de la carga.- También deben considerar otros elementos como el balanceo de la carga y el modo activo en espera en los AP. La mayor parte de los AP de tipo empresarial de alto nivel proporcionan soporte para estas funciones, pero en algunos casos es necesario que preste atención a la forma en que estén configurados. Sin embargo, muchos de los productos de bajo nivel (productos orientados al mercado de las redes domésticas y oficinas pequeñas), a los cuales se pueden inclinar los profesionales de los servicios de información (debido a la presión de niveles administrativos más altos para reducir los costos) no soportan estos tipos de servicios.

- Interoperabilidad.- La interoperabilidad es otro aspecto que se debe considerar en la selección de productos. Debe asegurarse de que cualquier producto que seleccione cuente con la certificación Wi-Fi. Esto proporcionará al menos un nivel básico de pruebas y certificación de la interoperabilidad. También debe estar conciente de que existen distintas certificaciones Wi-Fi, por ejemplo, 802.11a, 802.11b, seguridad, calidad de servicio y otras. Los paquetes en los que vienen los productos Wi-Fi más nuevos incluyen una etiqueta de certificación de compatibilidad, la cual lista las características soportadas por el producto.

6.4.5 Selección del hardware para el punto de acceso

Existen muchos tipos distintos de diseños AP en el mercado, tanto en la forma física como en la arquitectura. La selección de la forma principal puede ser crítica en sus implementaciones y también para el soporte, mantenimiento, costo general, seguridad y confiabilidad. A continuación se examinan dos implementaciones de arquitectura principales.

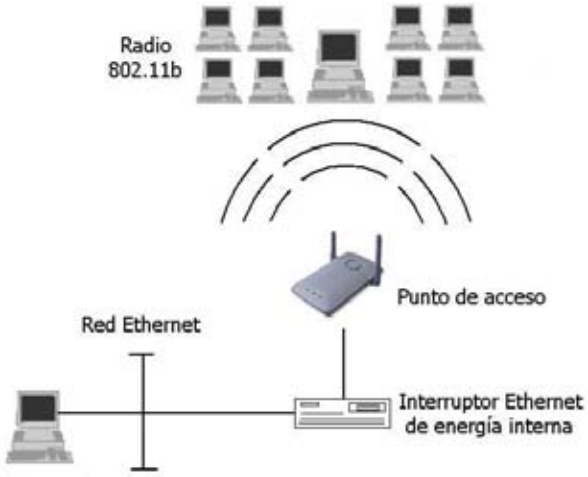


FIGURA 28. PUNTO DE ACCESO INTELIGENTE

En la arquitectura que se muestra en la figura anterior, el AP tiene bastante capacidad de procesamiento y usa su inteligencia en el extremo de la red. Se conecta directamente a la red al mismo tiempo que es un AP independiente, que no depende de ningún servidor o controlador en la red (que no sea la conectividad Ethernet) para mantener la conexión con los clientes inalámbricos. Cuando un AP falla, sólo ese AP queda afectado y los dispositivos restantes continúan operando normalmente. Sin embargo, en las instalaciones grandes, normalmente se requiere de un servidor de administración, para que proporcione el soporte, configuración y administración adecuados.

Cuando el producto se selecciona de tal manera que sus requerimientos de administración puedan incorporarse al sistema de administración WLAN que ya está en uso, la integración de la administración es muy sencilla y eficiente.

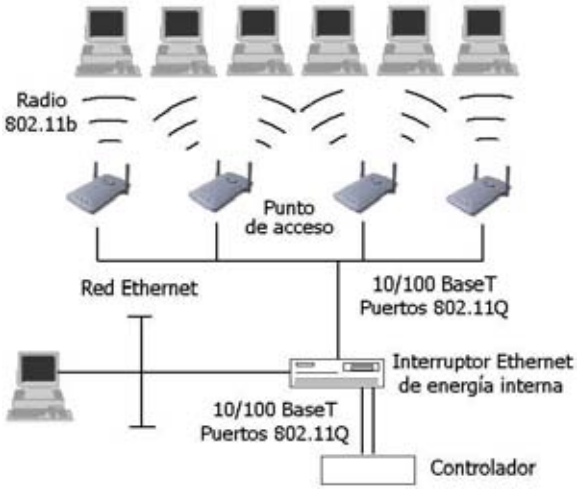


FIGURA 29. ARQUITECTURA PUNTO DE ACCESO/CONTROLADOR

El otro tipo de arquitectura de una WLAN es la que se muestra en la figura anterior, en este estilo de sistema WLAN, la inteligencia no se emplea en el AP sino en un controlador central de la red. En algunos sistemas es posible que esta configuración sea más fácil de instalar, debido a que la administración y configuración son manejadas por un solo controlador. Todo el tráfico del controlador fluye hacia el controlador, el cual administra la autenticación, seguridad, archivos de configuración y otros aspectos. El problema es que esto representa un solo punto de falla, ya que si el controlador falla, cualquier AP que esté enlazado con este controlador también fallará.

La mayoría de los AP fueron diseñados para proporcionar soporte a una sola plataforma de radio, algunos AP fueron fabricados con ranuras PCMCIA duales de manera que también se pudiera operar un segundo radio. En el momento en que estos AP se ofrecieron al mercado, tenían como fin proporcionar una ruta de migración de 900 MHz a 2.4 GHz. Sin embargo, había algunos fabricantes que prometieron duplicar el ancho de banda mediante el uso de dos radios iguales en el AP. Aunque esto implica un problema llamado insensibilización del receptor, lo cual causa un desempeño ineficiente en ambos radios.

Durante el 2003, ha aparecido en el mercado una variedad de AP's de banda dual, diseñados con la intención de proporcionar soporte tanto para 802.11b como para 802.11a de manera simultánea. Esta arquitectura se puede usar para migrar de una tecnología a otra para simplemente agregar ancho de banda al permitir a algunos usuarios de una tecnología usar otra. Sin embargo, debido a que estas arquitecturas tienen especificaciones y rangos distintos, es necesario que se considere algunos aspectos durante la etapa del diseño de la red.

La capacidad de actualización es otra característica que se tiene que tener en cuenta. Si desea usar un sistema que proporcione soporte para 802.11a, 802.11g y 802.11b debe considerar un AP que proporcione soporte para

todos los dispositivos en el mismo paquete.

La energía en línea es una característica que soportan muchos fabricantes actualmente, y puede ahorrar una cantidad tremenda de los costos de instalación, además la energía en línea tiene distintas variedades y arquitecturas. Si desea aplicar energía a su AP desde los interruptores de la red, debe investigar las opciones de energía del interruptor y también en el AP para comprobar que son compatibles. También debe considerar que es posible que algunos interruptores no tengan suficiente energía para dar soporte a los AP de banda dual, lo cual implica la necesidad de usar un inyector de energía o módulo de energía de otro fabricante.

6.4.6 Selección del producto del cliente

Debido a que la mayoría de las características de red se encuentran en el AP, el aspecto más importante que debe considerar es qué tipo de clientes se necesitarán, y quién controlará la selección de clientes. No todos los dispositivos han migrado para proporcionar soporte a 802.11a. Esto puede ser una decisión muy importante en la decisión tecnológica. Pero también debe considerar la interoperabilidad , no sólo para el lado 802.11 básico, sino también aspectos como, por ejemplo, la seguridad y QoS. Muchos de los dispositivos de cliente especializados que se encuentran en el mercado actualmente no proporcionan soporte para un rango amplio de características que son soportadas por los dispositivos tipos NIC WLAN normales. Incluso existen algunos dispositivos que aún no operan en entornos DOS, lo cual limita severamente sus capacidades de soporte. Por esta razón, primero debe seleccionar las características que son necesarias en sus sistemas y luego ir en busca de los dispositivos de cliente.

Algunos fabricantes de radios ofrecen una potencia de transmisión muy típica de 30 mW, mientras que otros proporcionan una potencia de transmisión más alta que puede llegar hasta los 100 mW. El uso de un AP de 100 mW en un extremo con una tarjeta de cliente de 30 mW da como resultado un desempeño que no es simétrico. Si es necesario que instale un AP de alto nivel de 100 mW en el sistema, es recomendable que establezca los niveles de potencia del AP que sean parecidos al de la potencia más baja de las tarjetas de cliente, esto proporcionará el mejor desempeño general de todos los dispositivos de cliente.

6.5 Caso Práctico

El presente caso práctico se basa en la Universidad Autónoma Indígena de México en la unidad Los Mochis, Sinaloa. Cuenta con un área de 500 m² de construcción, su material es de cemento y sus oficinas están construidas de tablaroca, el edificio es de 2 plantas, en planta baja cuenta con diferentes departamentos los cuales son: coordinación de unidad, coordinación general administrativa, rectoría, sala de juntas, biblioteca, centro de lenguas y unidad de recursos informáticos. En la planta alta se cuenta con los siguientes departamentos: fondo documental, oficinas generales (contraloría, soporte técnico y servicio social), sala de

asesorías, coordinación general educativa y otras oficinas (postgrado, edición y DRA), sala magna y centro de cómputo. Además la unidad cuenta con secciones de áreas verdes y una cancha deportiva.

Con el objetivo de establecer una red Wi-Fi confiable y de óptimo desempeño se consideró los siguientes aspectos: ancho de banda, frecuencia de operación, tipos de aplicaciones que van a ejecutarse en la WLAN, número máximo de usuarios, área de cobertura, material con el que están construidos los edificios, conexión de la WLAN con la red cableada, disponibilidad de productos en el mercado, planeación y administración de las direcciones IP, los identificadores de la red (SSID) y la seguridad.

Los estándares que se utilizaron en el diseño de la red Wi-Fi son el IEEE 802.11b y el 802.11g, ya que éstos son los de mayor uso en el mercado y de fácil acceso, tanto para proveedores como para clientes.

Su propósito primordial es que cada persona pueda satisfacer sus necesidades de aprendizaje aprovechando al máximo su esfuerzo y con este fin se utiliza las tecnologías de la información, que permiten superar las barreras de espacio y tiempo, con un diseño educativo basado en la personalización y acompañamiento integral del estudiante.

El proyecto se inició con un estudio de las prestaciones y limitaciones de los estándares IEEE 802.11b y 802.11g, que rápidamente llevaron a determinar que el problema principal de esta tecnología no era la velocidad sino la seguridad. Se realizo una aproximación a dicho problema desde una perspectiva independiente de los estándares y del fabricante del hardware inalámbrico.

Se realizó una valoración de las distintas soluciones que se podían adoptar para dotar a las comunicaciones inalámbricas, del nivel de seguridad que la universidad deseaba. La valoración también incluyó aspectos totalmente ajenos a la temática de la seguridad en las comunicaciones pero no por ello menos importantes como la complejidad del mantenimiento de la solución, inversión inicial, solución basada en estándares, la escalabilidad, integración con el software del punto de trabajo actual y futuro de la universidad.

Para ello se realizó un estudio de las principales marcas líderes en soluciones Wi-Fi, tales como 3Com, Linksys, Cisco, Netgear entre otros, en sus páginas web y con proveedores locales. Tomando aspectos de cobertura, compatibilidad, seguridad, costos y disponibilidad, principalmente.

Debido a los materiales de construcción de esta unidad, se propuso establecer varios puntos de acceso y antenas en diferentes partes estratégicas de la misma. Esto con la finalidad de brindar el servicio óptimo y funcional que se quiere alcanzar. Para ello se aprovechó la red cableada existente en cada una de las áreas que formaron la red Wi-Fi, para así determinar la ubicación de los dispositivos inalámbricos. Es decir, la utilización de la red inalámbrica complementa a las redes cableadas con las cuales contaba la Universidad Autónoma Indígena de México.

Para realizar la instalación de la red inalámbrica, se tuvieron que equipar a todas las computadoras de tarjetas de red inalámbricas, además de contar con los puntos de acceso 3Com modelo 8250, un ruteador VPN, un switch, una antena omnidireccional para techo 3Com de 2.5 dBi y una antena omnidireccional 3Com de 8.0 dBi para exteriores.

Después de contar con todo el equipo necesario y colocarlo en el lugar indicado, se conectaron las antenas en los puntos de acceso, el ruteador se conectó al servidor RADIUS, al servidor y a los puntos de acceso en la planta baja y se conectaron los puntos de acceso al switch en la planta alta del edificio.

Al conectar la tarjeta de red inalámbrica y el ruteador al servidor, se configuró de la siguiente manera:

Para configurar la tarjeta de red inalámbrica.- se debe de seguir la siguiente ruta: Panel de control → Conexiones de red → Conexión de red inalámbrica, seleccionar con el botón derecho del mouse y después escoger la opción de Propiedades. Aparecerá una ventana donde se debe seleccionar el protocolo TCP/IP y seleccionar la opción de Propiedades. En la ventana siguiente se configuraron los siguientes parámetros: Dirección IP (ejemplo: 192.168.110.1), Máscara de subred (es el mismo para todas las computadoras conectadas a la red, por ejemplo: 255.0.0.0) y Servidores DNS, teniendo en cuenta que sé esta configurando el servidor, en el parámetro de Puerta de enlace predeterminada se debe de dejar en blanco. Además de lo anterior se debe de configurar algunos parámetros adicionales de la tarjeta de red inalámbrica. En la Conexión de red inalámbrica se deben seleccionar las siguientes opciones: Propiedades → Configurar → Opciones avanzadas, después se abrirá una ventana donde se introdujeron los siguientes parámetros: Authentication mode: Shared Authentication, Desired SSID: el nombre de la red (no se muestra por seguridad) y WEP Option: WEP Enabled. Al tener configurada la tarjeta de red inalámbrica se configuró el ruteador proporcionando los siguientes parámetros: Dirección IP (debe de ser diferente a la dirección IP de la tarjeta de red inalámbrica, por ejemplo: 192.168.110.2), Máscara de subred, Gateway (ejemplo: 192.168.110.254), SSID, Canal (el canal que se escogió para la red es el 7, ya que es el que soportan todos los dispositivos de la red), Admin. y clave de acceso, velocidades de transmisión y modos del dispositivo.

Por seguridad la configuración del servidor RADIUS y el filtrado de direcciones MAC no se presentan dentro de la información, sólo se mencionará que al tener configurado el servidor RADIUS, se le proporcionaron los nombres de usuario y las contraseñas correspondientes. Además, se activó el acceso por filtrado de direcciones MAC de las computadoras conectadas en la red inalámbrica, con el fin de que sólo las computadoras con las direcciones MAC especificadas tengan el acceso a la red (un ejemplo de dirección MAC es el siguiente: 00:13:49:00:01:02).

Después de configurar el servidor, se pasó a configurar en todas las computadoras personales y computadoras portátiles la tarjeta de red inalámbrica de la misma forma en la que se configuró en el servidor, se debe de seguir la misma ruta: Panel de control → Conexiones de red → Conexión de red inalámbrica, seleccionar con el

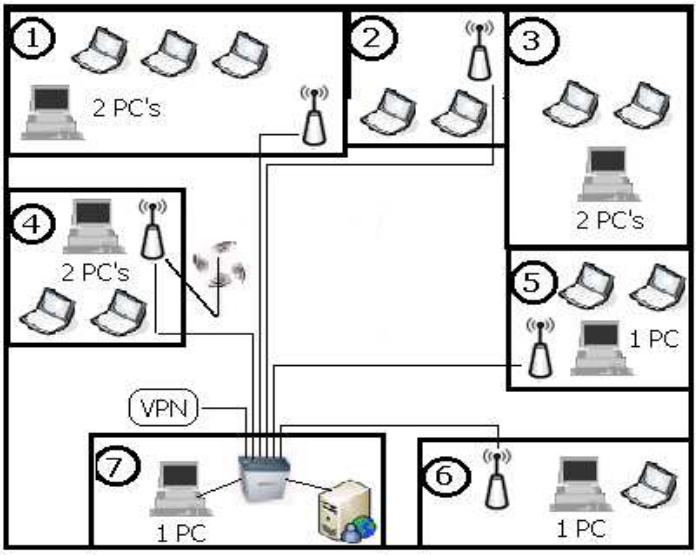
botón derecho del mouse y después escoger la opción de Propiedades. Aparecerá una ventana donde se debe seleccionar el protocolo TCP/IP y seleccionar la opción de Propiedades. En la ventana siguiente se configuraron los siguientes parámetros, teniendo en cuenta las siguientes observaciones: Dirección IP, Máscara de subred (debe de ser la misma que se estableció en el servidor y la misma para todas las computadoras que usen la red), Puerta de enlace predeterminada (se debe de poner la Dirección IP del servidor en todas las computadoras, por ejemplo: 192.168.110.1) y Servidores DNS.

Una vez que se tuvieron configuradas todas las computadoras de la red, se estableció la conexión de cada una. Para poder comprobar la conexión a la red, en cada computadora se realizó el siguiente procedimiento: en la opción de Conexión de red inalámbrica, seleccionar con el botón derecho del mouse y después escoger la opción de Ver redes inalámbricas disponibles. Al realizar el paso anterior se mostró la red inalámbrica disponible.

Al terminar de instalar y configurar la red inalámbrica, se obtuvo una velocidad de 54 Mbps y una intensidad muy buena, con la ayuda de las antenas omnidireccionales que se instalaron.

A continuación se describen algunos aspectos importantes que dieron como resultado después de la instalación de la red Wi-Fi. En la planta baja son los siguientes:

a) Coordinación de unidad.- el constante dinamismo que se tiene en este lugar, hace que la red Wi-Fi sea la solución. Se utiliza un punto de acceso 3Com modelo 8250, aprovechando el cable de la red cableada con el que cuenta esta área.
b) Coordinación general administrativa.- específicamente en la oficina del coordinador administrativo se necesito establecer un punto de acceso 3Com modelo 8250, para beneficiar al área de rectoría, esto ayudó a agilizar sus actividades, con directivos de la institución y proveedores, principalmente.
c) Rectoría.- Se beneficio por el punto de acceso ubicado en la coordinación general administrativa, ya que estas dos áreas hacen uso de funciones básicas como navegación, verificación de correo, entre otras.
d) Sala de juntas: Se estableció un punto de acceso 3Com modelo 8250, que ayudó a la interacción de información de sus participantes, para tomar decisiones en menor tiempo.
e) Biblioteca.- con la colocación de un punto de acceso, la constante búsqueda de la información por parte de los estudiantes mejoró considerablemente.
f) Centro de lenguas.- con la intención de ampliar el servicio brindado a más número de usuarios en este sitio se coloco un punto de acceso, para aprovechar la red cableada existente.
g) Unidad de Recursos Informáticos.- para poder conectar a todos los puntos de acceso en la planta baja, se instaló un ruteador VPN, el cuál se conectó con el servidor de la red.



1. Biblioteca
2. Sala de juntas
3. Rectoría
4. Centro de Lenguas
5. Coordinación General Administrativa
6. Coordinación de Unidad
7. Unidad de Recursos Informáticos

FIGURA 30. PLANTA BAJA DE LA UAIM

En la planta alta son los siguientes:

a) Fondo documental.- Se coloco un punto de acceso que mejoro la interacción con los demás departamentos y ayudo a acelerar el proceso de intercambio de información que se genera.
b) Oficinas generales.- Se instalo un punto de acceso, con el fin de agilizar los procesos de información con otras personas.
c) Sala de asesoría.- el establecimiento del punto de acceso, hizo que los asesores tengan una mayor interactividad con los estudiantes.
d) Coordinación general educativa.- Se instalo un punto de acceso en la sala de juntas de la oficina del coordinador general educativo, con la intención de cubrir las necesidades de interacción con directivos, asesores, estudiantes, entre otros.
e) Sala magna.- sin duda alguna, es una de las áreas que más se beneficio con la tecnología inalámbrica, ya que en este sitio se imparten clases de postgrado, además es un sitio de reunión tanto de personas que estudian su maestría como de estudiantes. Es por eso que el punto de acceso 3Com 8250 junto con una antena omnidireccional para techo 3Com de 2.5 dBi, les brindo el acceso a la información instantáneamente y así se pudo agilizar las labores de investigación.
f) Pasillos y áreas restantes.- Se instalo una antena omnidireccional 3Com de 8.0 dBi para exteriores, aprovechando el punto de acceso que se encuentra en el centro de lenguas.

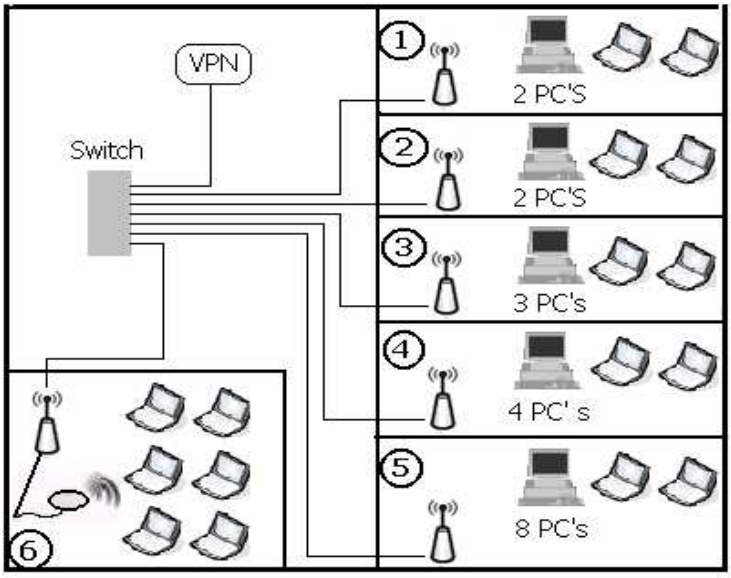


FIGURA 31. PLANTA ALTA DE LA UAIM

Se propuso en base al diseño de la red Wi-Fi, que la futura adquisición de equipos de cómputo incorpore un dispositivo de conexión inalámbrico, de esta forma no será necesaria la adquisición de cable de red, conectores, ruteadores, switches, entre otros, reflejándose ahorro en costo y tiempo de instalación. Los usuarios para poder hacer uso de la red Wi-Fi deben de contar con una laptop, PDA, pocket pc, tablet pc, entre otros, con su respectivo adaptador de red inalámbrica.

De acuerdo a las necesidades de la universidad, la línea de productos 3Com y Linksys ofrecen las características que se busco para la implementación de la red Wi-Fi, además de que son más fáciles de adquirir con proveedores locales.

En el ámbito de seguridad se estudiaron las siguientes alternativas: WEP, establecimiento de VPN's basadas en IPSec y finalmente soluciones basadas en 802.1X/EAP. De estas distintas alternativas se valoraron los siguientes puntos: la robustez y confidencialidad del proceso de autenticación, la centralización del proceso de autenticación, la integración con las bases de datos de Windows XP y Active directory, la robustez de la encriptación, la capacidad de evitar la suplantación de puntos de accesos de la red y sobre todo que la solución estuviera basada en estándares.

Para asegurar que el servicio llegue a los usuarios que se desea, se tomo una serie de medidas de seguridad que a continuación se describen:

1) Se activará el sistema de cifrado WEP en todos los puntos de acceso.

2) Todos los puntos de acceso contienen las direcciones físicas (MAC) de los dispositivos que den acceso a estos.
3) Los identificadores de red (SSID) se modificarán de forma constante y adecuada, es decir, no muy obvios, en cada uno de los puntos de acceso.
4) Se establecerá un servidor de autenticación RADIUS, el cual tendrá los nombres de los usuarios con sus respectivas contraseñas, para permitirles el acceso a la red.
5) Se instalará un ruteador VPN, para cifrar la información en túneles virtuales mediante el protocolo IPSec, para asegurar el flujo de información ante usuarios que pretendan el robo de dicha información.

Periódicamente se cambiarán las contraseñas de los identificadores de red, al igual que el del servidor RADIUS y el ruteador VPN, también se realizará monitoreo diario ante posibles intrusos que quieran invadir la red. También se realizarán presentaciones, folletos, carteles, artículos, entre otros, con el fin de dar a conocer el uso seguro y responsable de la red Wi-Fi.

La red Wi-Fi ayuda a agilizar las investigaciones de los estudiantes, por la movilidad y flexibilidad que brinda la red, además de permitirles no estar limitados a áreas de estudio fijas como lo son en la actualidad los centros de cómputo.

Conclusiones.

La posibilidad de estar conectados en cualquier lugar y en todo momento permite a los estudiantes un mayor acceso a la información, propiciando periodos más largos de actividades, dando como resultado una mayor agilidad en los procesos de aprendizaje. El personal docente tiene la posibilidad de agilizar sus procesos de investigación, elevando la productividad en el área administrativa. Además esta red Wi-Fi genera nuevas comunidades de estudio entre los estudiantes y/o asesores.

Las características que posee la red Wi-Fi, tales como la movilidad, conectividad y flexibilidad hacen de ésta, la solución a las necesidades de investigación de los estudiantes, además de favorecer el desarrollo del personal administrativo de la universidad.

Las medidas de seguridad mencionadas en este caso práctico garantizan un flujo de información seguro, además, de dar protección ante espías que pretendan beneficiarse con este servicio. La implementación y difusión de políticas de uso y seguridad aseguraron que todos los beneficiados se involucren y hagan conciencia en el uso responsable y seguro de esta red.

Capítulo 7 – El futuro de lo inalámbrico

7.1 Desafíos

Las redes siempre han tenido retos, pero éstos aumentan cuando se agrega complejidad, tal como sucede con las redes inalámbricas. Uno de los desafíos que tendrá que superar la tecnología Wi-Fi es el de la obsolescencia, aunque gran parte del futuro de Wi-Fi parece alentador, existen factores que podrían provocar problemas cuando se adquiere la tecnología, por ejemplo, se debe tener en cuenta que siempre se paga más en la actualidad de lo que valdrá en el futuro, de igual forma, si esperamos, siempre habrá algo mejor más adelante.

Otro desafío está relacionado con los cambios en la regulación que pudieran surgir. Tal vez la FCC pueda realizar algún cambio en la regulación acerca del uso de Wi-Fi, que afectará a los fabricantes de aparatos electrónicos. Esto como resultado de que los ingresos procedentes de ventas y servicios de Wi-Fi, otros estándares de red inalámbrica y aparatos electrónicos representan miles de millones de dólares.

Existen también desafíos de configuración, ya que la configuración de red continúa simplificándose, las redes inalámbricas incorporan características (en ocasiones para resolver otros retos) que se agrega a los parámetros de configuración. Por ejemplo, cuando un usuario cruza un límite de subred, la dirección IP asignada originalmente a la estación puede dejar de ser adecuada para la nueva subred. Si la transición supone cruzar dominios administrativos, es posible que la estación ya no tenga permiso de acceso a la red en el nuevo dominio basándose en sus credenciales. Para este ejemplo, la movilidad es una situación que debe pensarse muy detenidamente. La configuración puede ser un problema para el usuario móvil, ya que las distintas configuraciones de red pueden suponer un reto si la estación inalámbrica del usuario no tiene capacidad para configurarse automáticamente.

Otros desafíos que debe encarar Wi-Fi incluyen cómo mejorar las velocidades de rendimiento de procesamiento de datos, la seguridad y la calidad de servicio.

7.2 Compartir

Cada vez más usuarios optan por una red inalámbrica para conectarse en el hogar. No obstante, su puesta en marcha requiere tomar una decisión que puede ser clave, debido al desarrollo actual de las redes Wi-Fi: ¿Debe protegerse o es mejor compartir la red inalámbrica? Y en caso de compartirla, ¿se debe permitir el acceso público de forma gratuita, o es más conveniente intentar sacar un beneficio?

Por lo tanto, se debe tener en cuenta, que una red inalámbrica envía y recibe señales a través de un AP para conectar computadoras entre sí y a Internet. Un punto de acceso de una red inalámbrica es como un transmisor

de radio: retransmite señales extensivamente. A diferencia de una radio, las señales son relativamente débiles, pero algunas pueden detectarse a varias decenas de metros. No es raro que un usuario doméstico con una computadora con conexión inalámbrica capte una señal de red inalámbrica (a menudo, de forma inadvertida) procedente del punto de acceso de un vecino que se encuentre en las inmediaciones.

Las opciones son numerosas, pero en un mundo que aspira a la conexión global, la opción de compartir la red inalámbrica parece tener mucho más sentido, sobre todo si se hace de forma gratuita y se contribuye a crear una comunidad activa.

7.2.1 Acceder a WLAN de otras personas

Cada vez más usuarios de Internet disfrutan de la flexibilidad y comodidad que brinda una red inalámbrica doméstica para el acceso a Internet y la conexión a otras computadoras en el hogar. Sin embargo, además de las ventajas, las conexiones inalámbricas presentan algunos riesgos para la seguridad que debería solucionar antes de empezar a utilizarlas.

Dejar sin protección una red inalámbrica es como dejar una puerta abierta a algún vecino curioso o algo peor, a un atacante malintencionado en búsqueda de redes inalámbricas, en una práctica denominada "wardriving". Wardriving significa recorrer las calles con una computadora inalámbrica u otro dispositivo de radio para intentar localizar e identificar redes inalámbricas para infiltrarse en éstas. Los avances tecnológicos y la gran expansión de Internet en todo el mundo han hecho que esta práctica tenga mayor movilidad, resulte más accesible y rentable, y sea cada vez más frecuente, a medida que se popularizan las redes inalámbricas. Alguien que mediante wardriving consiga acceso a su red podría utilizar anónimamente su conexión a Internet, robar datos personales almacenados en la red, interceptar transferencias de archivos o, incluso, utilizar su computadora para enviar correo basura o software malintencionado cuyo origen podría ser rastreado.

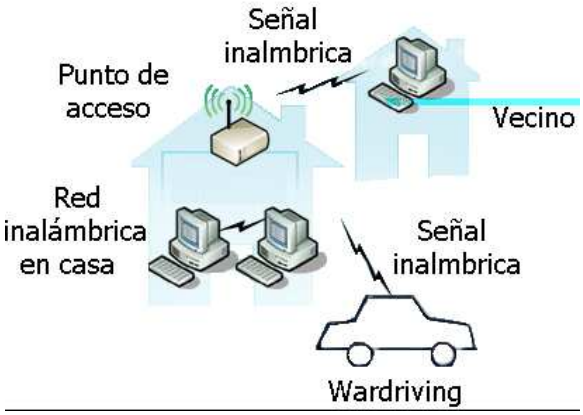


FIGURA 32. TÉCNICA WARDRIVING

Aunque quizá no le importe compartir la conexión a Internet con un vecino, tenga en cuenta que, si lo hace, éste podría tener acceso a computadoras de su red doméstica (es decir, a los archivos almacenados en esos equipos), realizar actividades ilegales en línea o dañar su sistema de algún otro modo.

7.2.2 Proporcionar acceso a la WLAN

También vale la pena ver la situación desde el punto de vista de la persona que ejecuta la red. Algunos Proveedores de Servicios de Internet (ISP) venden el servicio para una sola computadora, pero si el cliente compra e instala una puerta de enlace de banda ancha (a menudo como parte de un punto de acceso inalámbrico), no hay opción técnica para impedir que la conexión sea compartida entre varias computadoras. Si el ISP prohíbe expresamente compartir la conexión con varias computadoras y lo hacemos de todas formas, estamos violando los términos del servicio. El hecho de que mucha gente haga caso omiso de los deseos de los ISP nace porque los términos de servicio que prohíben el uso de múltiples computadoras aplican una restricción legal donde no hay limitación técnica alguna.

Ya sea como usuario potencial de redes inalámbricas abiertas o como alguien que puede compartir su conexión de Internet con otros a través de una red inalámbrica, tal vez, la gente generalmente se inclina por compartir conexiones y por modelos de empresas que reflejen los costos reales, pero cada situación es distinta, si comparte redes inalámbricas y cómo lo hace es una decisión que debe de tomar cada persona.

7.3 Disputas por el territorio

Un problema que puede surgir al utilizar las redes inalámbricas se relaciona con los usuarios sin licencia y con licencia. Los estándares de redes inalámbricas que se han mencionado utilizan el espectro sin licencia disponible para el uso general de individuos y empresas siempre que la potencia siga siendo lo bastante baja. Estos usos sin licencia de varias bandas del espectro podrían toparse con un problema: la FCC y otros cuerpos reguladores internacionales tienen usuarios autorizados con licencia, que pagan o al menos tienen garantizada la prioridad de acceso a la banda del espectro para sus propios propósitos. Estos usuarios con licencia no pueden expulsar a otros usuarios arbitrariamente, pero si pueden demostrar que los equipos sin licencia producen interferencias con sus propios propósitos con licencia, por lo tanto, la FCC o los cuerpos reguladores internacionales pueden requerir a los usuarios sin licencia que desconecten o modifiquen su uso.

Los usuarios de la banda de 2.4 GHz del estándar 802.11b, son usuarios con licencia de la parte más baja del espectro, sus equipos de radio y también los nacientes servicios de televisión independientes que utilizan las mismas frecuencias, pueden interferir o requerir la desconexión de las redes inalámbricas. Ha habido incidentes acerca de este problema, de cualquier forma, el posible conflicto sigue estando presente y es una de las razones por las que las personas que establecen redes inalámbricas de largo alcance tienen que tener cuidado para no sobrepasar las limitaciones de potencia establecidas por la FCC. Esto no es difícil si se usa

correctamente el equipo de red estándar, pero no debe suponer que puede aumentar la potencia sin sufrir ninguna consecuencia.

Otro problema es el de la interferencia, los dispositivos que utilizan las bandas sin licencia no sólo deben procurar no provocar interferencias, sino que también deben de ser muy tolerantes ante interferencias o conflictos con otros usuarios legítimos. Dado que el equipo de red inalámbrica ofrece opciones para configurar qué frecuencias se utilizarán, hay una alta probabilidad de que surjan conflictos cuando las instalaciones aumenten en densidad.

En agosto del 2002, el socio inalámbrico de espacio público de Starbucks, T-Mobile USA, se encontró dos veces en una situación similar, cuando un nuevo despliegue de red entró en conflicto con redes cercanas. En Portland, la instalación predeterminada de T-Mobile utilizó el mismo grupo de frecuencias que había estado utilizando un grupo de red comunitaria establecido anteriormente. En San Francisco, en un establecimiento Starbucks donde T-Mobile, Starbucks y Hewlett-Packard pensaban hacer un gran anuncio acerca de servicios de red ampliados, hubo un conflicto con una franquicia de Apple cercana.

En ambos casos, los problemas se resolvieron. En Portland, T-Mobile instaló un software mejor que escogía canales no utilizados. En San Francisco, la franquicia de Apple no tuvo inconveniente en cambiar de canales para la conferencia de prensa de modo que su red no apareciera como opción predeterminada. Estos problemas pueden parecer de poca importancia, pero perfilan un problema que puede terminar siendo más importante, sin una coordinación central, los conflictos de canales pueden reducir la calidad de los servicios de las redes inalámbricas.

7.4 Estándares futuros

Los estándares de la familia IEEE 802.11, fueron introducidos para establecer un conjunto de estándares comunes y seguros para la comunicación inalámbrica de datos de un dispositivo a otro, en forma muy similar en la que Ethernet (IEEE 802.3) conecta las computadoras en una LAN con cable. En la actualidad, casi todos los productos LAN inalámbricos trabajan con Wi-Fi (802.11b), un estándar que opera en la banda 2.4 GHz a velocidades de hasta 11 Mbps. Sin embargo, ya una gran cantidad de productos han comenzado a trabajar con dos nuevos estándares: 802.11a (que trabaja en la banda de 5 GHz a velocidades de hasta 54 Mbps) y 802.11g (que comparte la misma banda de 2.4 GHz a velocidades de hasta 54 Mbps).

Sin embargo, en los próximos años se espera un cambio en el mercado inalámbrico. La razón es la aparición de nuevos estándares, que prometen proporcionar a los usuarios más ventajas de las que en la actualidad ofrecen los estándares existentes.

Una tecnología que esta por surgir es WiBro o banda ancha inalámbrica en movimiento, que se considera la trayectoria natural y evolutiva para la movilidad inalámbrica y una alternativa a las redes telefónicas de alta velocidad. WiBro permitirá mantener el enlace a Internet desde un dispositivo en movimiento continuo, y lejos del hot-spot o punto de enlace a la red. Técnicamente, esta tecnología se establece en el estándar IEEE 802.16e, mejor conocido como WiMax en movimiento. WiBro ofrecerá un rendimiento de procesamiento de datos agregado de 30 a 50 Mbps y cubrirán un radio de 1 a 5 kilómetros. WiBro permitirá mantener el enlace a Internet desde un dispositivo en movimiento continuo, y lejos del hot-spot o punto de enlace a la red. La tecnología también ofrecerá la calidad del servicio que permitirá que WiBro fluya el contenido de video y otros datos de una manera confiable, esto parece ser la ventaja más fuerte sobre el estándar de WiMAX.

Otros estándares futuros que están por solucionar problemas como la velocidad de transferencia de datos y el aumento de la cobertura de la red, son los estándares: 802.11n y 802.11s respectivamente, que se describen a continuación.

7.4.1 Más rápido y compatible: 802.11n

Veintiséis compañías, entre las cuales se encuentran Intel, Cisco, Apple, Lenovo, Sony, Toshiba y US Robotics, anunciaron la formación de un grupo denominado EWC (Enhanced Wireless Consortium) que busca acelerar el proceso de desarrollo del estándar IEEE 802.11n, y promover su utilización como el estándar de la nueva generación de dispositivos para redes de área local inalámbricas.

El estándar IEEE 802.11n está a punto de ser definido completamente, y que tiene el apoyo de compañías como Intel y Cisco. El objetivo de este nuevo estándar es ofrecer redes Wi-Fi de alta velocidad (como mínimo 100 Mbps y como máximo se ha hablado hasta de 600 Mbps). Las principales características del estándar 802.11n son:

- MIMO generando canales de tráfico simultáneos entre las diferentes antenas de los productos 802.11n.
- Canales de 20 y 40 Hz (Lo que permite incrementar enormemente la velocidad).
- El uso de las bandas de 2.4 y 5 GHz simultáneamente.

Entre las características técnicas de la nueva versión del estándar del IEEE, se encuentra la compatibilidad con las versiones 802.11a/b/g, alcanzando velocidades reales de transmisión de hasta 600 Mbps.

Intel ha contribuido al desarrollo del estándar 802.11n de muchas maneras. Intel presidió al comité del grupo de tarea responsable de los documentos de la base que eran utilizados para dirigir el desarrollo del grupo del estándar 802.11n. Como parte del grupo de tarea, Intel contribuyó al desarrollo de los modelos del canal, de los

modelos del uso, de los requisitos funcionales, y de los criterios de la comparación. Intel también ha proporcionado sumisiones técnicas en tecnologías del MAC y de PHY, metodologías de la medida de funcionamiento, y metodologías de la simulación. Para la Alianza Wi-Fi, Intel ayudó al coautor de este grupo de la certificación para el alto rendimiento de procesamiento WLAN's (documento de los requisitos de la comercialización para 802.11n).

Parece ser que el 802.11n significará una verdadera revolución en el mundo del Wi-Fi, aumentando la velocidad de las redes inalámbricas de una forma increíble, acercándolas al mundo de las redes cableadas.

7.4.2 802.11s

El estándar IEEE 802.11s, es una propuesta del grupo de trabajo conocido como Alianza Wi-Mesh (www.wi-mesh.org). El borrador del estándar 802.11s define la capa física y enlace de datos para redes en malla. Esta topología aumenta la cobertura de la red y le permite estar siempre activa, aún cuando uno de los puntos de acceso falle. Se pueden agregar usuarios y puntos de acceso a la red para añadir capacidad.

Con las redes en malla no es necesario tener AP, pues todos los nodos pueden comunicarse directamente con los vecinos dentro de su rango de cobertura inalámbrica y con otros nodos distantes, mediante el enrutamiento multisalto ya mencionado. Otro beneficio importante de las redes en malla es que presentan costos de operación más bajos que las redes Wi-Fi tradicionales, ya que tienen capacidades de autoconfiguración y de re-configuración. Esto es posible mediante sofisticados protocolos que permiten el descubrimiento automático de rutas y el redescubrimiento de las mismas en caso de falla en algunos nodos. Dada esta capacidad de re-configuración, las redes en malla también resultan ser flexibles y robustas, pues la falla de uno o más nodos no impide el funcionamiento de la red y no se presenta un punto crítico de falla (como sucedería, por ejemplo, si falla el AP en una red Wi-Fi tradicional).

Las redes inalámbricas en malla es una tecnología muy nueva y con grandes posibilidades de aplicación en defensa, acceso a Internet en áreas metropolitanas, redes que permanecen poco tiempo activas (por ejemplo, recuperación en desastres o centros de convenciones), edificios donde resulta difícil la implementación de una red cableada, terrenos poco amigables y áreas rurales con grandes costos para implementar redes convencionales. Representa un tipo de infraestructura inalámbrica descentralizada, relativamente económica, muy fiable y resistente. Cada nodo necesita transmitir tan lejos como el próximo nodo. Los nodos actúan como repetidores de datos de nodos cercanos a otros equivalentes pero más lejanos. De este modo es posible implementar redes que pueden abarcar grandes distancias. La fiabilidad y resistencia se basa en el hecho que cada nodo se haya conectado a varios otros. Si un nodo cae (falla de hardware u otra causa) sus vecinos simplemente buscan otra ruta. Es posible mejorar la implementación de forma muy simple, agregando más nodos. Cada nodo puede ser un dispositivo fijo o móvil.

El estándar ofrecerá flexibilidad, requerida para satisfacer los requerimientos de ambientes residenciales, de oficina, campus, seguridad pública y aplicaciones militares. La propuesta se enfoca sobre múltiples dimensiones: la subcapa MAC, enrutamiento, seguridad y la de interconexión. Además, define sólo sistemas para ambientes en interiores, pero los principales fabricantes de equipos inalámbricos le están apostando también a sistemas en ambientes exteriores. Se prevé que la especificación final del 802.11s aparecerá publicada a mediados del 2008.

7.5 Teléfonos móviles: la próxima generación

Aunque todavía no ha despegado con la fuerza prevista la telefonía móvil basada en tecnología de 3G, fabricantes y desarrolladores de aplicaciones, así como operadores de telefonía inalámbrica ya están dispuestos a la espera de lanzar al mercado dispositivos móviles de cuarta generación.

La denominada cuarta generación de tecnología móvil (4G), que ahora está siendo desarrollada, permitiría una comunicación en dos direcciones de voz, vídeo y datos a una escala en la que antes era imposible, dieron a conocer varias compañías durante una conferencia sobre telefonía móvil 4G de Samsung.

La empresa NTT DoCoMo anunció que está realizando pruebas con teléfonos celulares de cuarta generación en Japón. Permitirán una velocidad de descarga de hasta 1 Gbps. Durante las pruebas, la empresa demostró este avance tecnológico a bordo de un automóvil que viajó a más de 60 kilómetros por hora en la isla de Jeju, al sur de Corea del Sur, en el marco del Foro 4G Samsung que se celebró en dicha localidad.

Autoridades de la empresa afirmaron que los nuevos teléfonos pueden recibir señales de hasta 100 Mbps en movimiento y hasta 1 Gbps en modo estático. Con esta última tasa de transferencia se podría descargar un DVD completo en menos de un minuto.

Las pruebas de los teléfonos 4G utilizaron un método llamado VSF-Spread OFDM que incrementa la velocidad de descarga gracias al uso de frecuencias de radio múltiple para enviar el mismo paquete de datos. Otro truco que utilizarán las nuevas redes 4G será la tecnología MIMO (Múltiple Entrada-Múltiple Salida) que permite el envío de datos a través de varias rutas distintas para incrementar el ancho de banda. Por ejemplo, MIMO podría permitir a un celular la recepción de datos desde más de una base transmisora. Esta versión mejorada de las plataformas de comunicaciones inalámbricas existentes, permitirá la conectividad con una rapidez superior a las actuales aún cuando los usuarios se encuentren lejos de las áreas urbanas y en movimiento.

Para las pruebas se usaron diversos recursos tecnológicos: factores de división variables, frecuencias ortogonales, multiplexación de código (VSF-OFCDM) , multiplexación de acceso directo para el envío de datos y aceleradores de código para agilizar todo el ancho de banda del sistema. Evidentemente la compañía ha tenido que mejorar y actualizar notablemente la infraestructura actual para soportar semejantes velocidades. Destaca

especialmente el uso de la nueva tecnología MIMO que usa más de una antena para emitir y recibir, además de mejorar considerablemente la multiplexación de la señal.

La Unión Internacional de Telecomunicaciones (UIT) definió la 4G como la tecnología de telecomunicaciones del futuro que permitirá la transferencia de datos de 1 Gbps en circunstancias normales y 100 Mbps en movimiento.

Comparado con la tecnología de tercera generación (3G), capaz de recibir y transmitir más de 2 Mbps y posiblemente 12 Mbps dentro de pocos años, la 4G es claramente mucho más rápida, de acuerdo con los reportes. Samsung espera lanzar esta tecnología al mercado para el año 2010, pero su uso comercial dependerá de los acuerdos reguladores que se decidirán el próximo año, aunque el desarrollo físico de la 4G en teléfonos celulares podría comenzar antes, a principios de 2008.

La compañía Dile 4G espera lanzar su móvil de cuarta generación en todo el mundo, que en una primera fase, los usuarios podrán utilizar el móvil desde un acceso Wi-Fi, en su casa, en su empresa o en lugares públicos, pudiendo acceder a Internet de manera económica y con una gama de acceso de servicios en línea ilimitada.

La compañía Ericsson garantiza la posibilidad de mejorar las redes de comunicaciones proporcionando banda ancha de hasta 14 Mbps. La empresa apuesta por la utilización de la tecnología HSDPA para ofrecer mayores velocidades y capacidad de acceso en las redes UMTS existentes utilizando la infraestructura ya desplegada y realizando únicamente actualizaciones de su software.

Las redes HSDPA proporcionan comunicaciones de datos de elevadas prestaciones, tanto en velocidad y ancho de banda como en rapidez de respuesta, con la seguridad e inviolabilidad en las comunicaciones inherentes a las redes GSM/GPRS y UMTS, según Antonio Campaña, director de soluciones de acceso móvil de Ericsson en nuestro país.

7.6 Ancho de banda inalámbrico aerotransportado

El ancho de banda inalámbrico aerotransportado se refiere a la idea de proporcionar servicios de redes inalámbricas permanentes utilizando aviones o dirigibles a gran altitud, que cuentan con una carga que contiene los siguientes elementos: equipo informático que permitirá la comunicación entre los diferentes componentes dentro del avión o dirigible, una antena especial que servirá para reflejar las señales del sistema satelital y de las estaciones ubicadas en la superficie terrestre para poder enviar la señal a los usuarios finales, cubriendo un área de 70 a 100 kilómetros aproximadamente, con una capacidad de transferencia de 10 a 100 Gbps, siendo una característica muy innovadora. Además de los componentes antes descritos los usuarios finales tendrán que tener una antena externa que sea proporcionada por un ISP (Proveedor de Servicios de Internet), para tener conexión a Internet. Si los proyectos, que están en un nivel de planeación para su lanzamiento, tienen

éxito, será un gran cambio en el modo en que muchos nos conectamos en la actualidad a Internet. Algunos proyectos son los siguientes:

- Angel Technologies.- (www.angeltechnologies.com) planea operar su red HALO con aviones especiales de gran altitud que trazarán círculos sobre las áreas de servicio a 15,849.60 metros de altura, muy por encima del tráfico aéreo comercial. Los aviones de la compañía tendrán pilotos que volarán alternamente para evitar la interrupción del servicio.

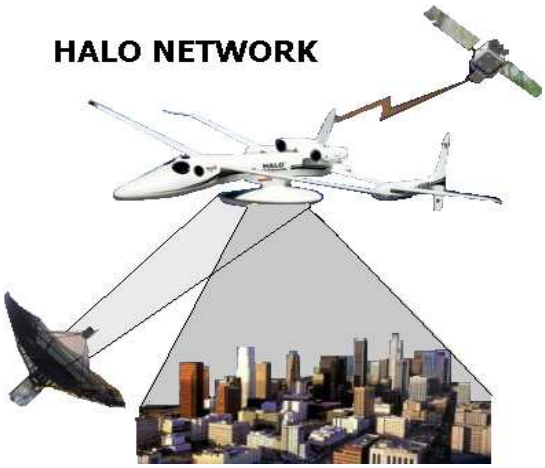


FIGURA 33. RED HALO

- Aero Vironment.- (www.skytowerglobal.com) está colaborando con la NASA para desarrollar un aeroplano llamado Helios que puede actuar como una estación de telecomunicaciones aerotransportada móvil. A diferencia de los aviones Angel Technologies, el avión Helios no utilizará pilotos y se alimentarán con energía solar, volando a una altitud de 18,288 metros, utilizando células de combustible recargables para proporcionar energía durante la noche. Se espera que el avión Helios pueda permanecer en el aire unos seis meses o más.

- Sky Station Internacional.- (www.skystation.com) planea una estrategia diferente, optando por grandes dirigibles sin tripulantes que volarán sobre una ciudad a 21,031.20 metros de altura. También utilizará la energía solar para el equipo de red que proporcione la conectividad a los clientes.

Aunque estas compañías anunciaban que empezarían a prestar estos servicios en el 2003, sus expectativas se retrasaron debido en parte por el riesgo de pérdida de capital en la industria de las telecomunicaciones y en parte, porque sigue habiendo cuestiones que no han podido resolver, por ejemplo, aunque los dos servicios sin tripulantes utilizan materiales muy ligeros, en ambos casos tienen que llevar una carga de equipo de entre 250 y 1,000 Kg que es mucha carga para caer a tierra sobre un área poblada en caso de catástrofe.

7.7 Banda ultraancha (UWB)

La tecnología UWB puede utilizarse para transmitir voz, vídeo u otro tipo de datos digitales. Su principal ventaja respecto a otras tecnologías inalámbricas radica en el hecho de que puede transmitir más datos utilizando menos potencia que el resto de sistemas disponibles. Adicionalmente, los equipos de radio necesitan menos componentes, por lo que se convierte en una solución económica.

Debido a la limitación de potencia impuesta por la FCC sobre las especificaciones de UWB, el alcance de estos sistemas es bastante reducido. No obstante, esto se convierte en una ventaja cuando se desea combinar varios radioenlaces en un espacio relativamente pequeño, como por ejemplo, una oficina o un departamento.

El funcionamiento de UWB se basa en la transmisión de secuencias de pulsos extremadamente estrechos y de baja potencia, los cuales se sitúan de forma precisa en el tiempo (desviaciones inferiores al nanosegundo). La modulación de los datos consiste básicamente en variar la posición de los pulsos empleando códigos PN (técnica de espectro ensanchado). Como resultado se obtiene un espectro de banda ancha que es mucho más resistente a interferencias, ya que éstas ocupan normalmente una fracción muy pequeña del espectro de la señal UWB. Adicionalmente, dado que las señales UWB son de baja potencia, causan muy poca interferencia al resto de señales. Por ejemplo, algunos estudios han demostrado que la interferencia de UWB sobre los sistemas GPS es inferior a las causadas por diversos equipos eléctricos como un secador de pelo, una taladro o una fuente de alimentación de PC.

FIGURA 34. FUNCIONAMIENTO DE UWB

En comparación con otro tipo de tecnologías inalámbricas, como por ejemplo WPAN/WLAN, UWB proporciona una mayor velocidad de transmisión con una gran eficiencia en potencia, lo que permite el desarrollo de dispositivos portátiles de gran autonomía. En cambio, su alcance es similar a Bluetooth, debido principalmente a las limitaciones de potencia impuestas. Eliminando estas restricciones, el alcance de UWB se estima que podría ser similar o incluso superior al proporcionado por las tecnologías 802.11. El principal campo de aplicación de UWB se orientará hacia la electrónica del hogar, por ejemplo, en la interconexión de periféricos tales como

impresoras, escáneres o monitores con la PC, o en la distribución de señales HDTV a distintos receptores de TV (Home Cinema).

7.8 Conclusiones

Desde el descubrimiento de las vulnerabilidades de seguridad de WLAN, proveedores de redes, organismos de estándares y analistas han dedicado gran parte de sus esfuerzos a la búsqueda de remedios para hacer frente a estos problemas. Muchos de estos esfuerzos han contribuido considerablemente a incrementar el nivel de seguridad inalámbrica.

Con la aparición de protocolos como WPA y WPA 2, además, de herramientas para mejorar la seguridad como el estándar 802.1x, AES, CCMP, MIC, las redes privadas virtuales, IPsec, entre otras, la seguridad en las redes inalámbricas se ha reforzado al hacer difícil las técnicas utilizadas para poder comprometer la seguridad de las mismas, por lo que en la actualidad, podemos decir que se cuenta con la tecnología y los medios necesarios para poder ofrecer soluciones para que las redes inalámbricas sean seguras, siempre partiendo de la base de que no existe la seguridad al 100%.

Respecto a la protección de la infraestructura, podemos decir, que hay que evaluar cada caso en particular donde existe o donde se pretende contar con una red inalámbrica, para poder realizar un análisis con detenimiento de las posibles deficiencias que se pudieran observar, como podrían ser: la ubicación de los AP’s, la protección física, el acceso, la configuración, etcétera.

Como se trato de explicar a lo largo de la investigación, una red Wi-Fi no es segura o insegura. Este valor dependerá en gran medida de la implementación de la misma. Evidentemente se está haciendo un gran esfuerzo, tanto en los organismos de estandarización como en los fabricantes para poder ofrecer productos que se puedan configurar con una seguridad equivalente a la de una red cableada tradicional, lo que se puede afirmar al analizar las nuevas herramientas para mejorar la seguridad como las mencionadas a lo largo de los capítulos, es que actualmente se les puede catalogar como seguras en los tres aspectos fundamentales para obtener un nivel alto de seguridad, como son la autenticación, el control de acceso y la confidencialidad.

Este decremento de la seguridad es debido en gran parte al desconocimiento de los usuarios que activan las redes inalámbricas, ya que, de acuerdo a algunos estudios realizados por parte de los interesados en la tecnología Wi-Fi, han encontrado que la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de la información. Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas, su implementación depende del uso que se vaya a dar y al entorno de la red. Debido a esto, antes de comenzar un despliegue Wi-Fi a lo largo de toda una empresa, es necesario que solicite información adicional para crear una arquitectura de seguridad más exitosa, escalable y robusta.

Entonces se puede concluir que mediante la correcta selección e implantación de los factores y elementos de seguridad que existen actualmente en las redes inalámbricas, las empresas pueden garantizar un nivel muy alto de seguridad respecto a la utilización de la red Wi-Fi, dando mayor confianza a los usuarios y eliminando los riesgos que conlleva utilizar la tecnología inalámbrica.

BIBLIOGRAFÍA

García Tomás Jesús, Raya Cabrera José Luis. Alta velocidad y calidad de servicios en Redes IP, RA-MA, 2002.

Tanenbaum S. Andrew. Computer Networks, Prentice Hall, 1996.

Carballar Antonio José. Wi-Fi Cómo construir una red inalámbrica, RA-MA,2003.

Engst Adam, Fleishman Glenn. Introducción a las redes inalámbricas, Anaya Multimedia, 2003.

Reid Neil, Seide Ron, Fuentes Zárate Jorge Omar. Manual de redes inalámbricas, McGraw-Hill Interamericana Editores, 2004.

Nichols Randall K., Lekkas, Panos C. Seguridad para comunicaciones inalámbricas: redes, protocolos, criptografía y soluciones, McGraw-Hill, 2003.

Álvarez Marañón Gonzalo, Pérez García Pedro Pablo. Seguridad informática para empresas y particulares, McGraw-Hill, 2004.

Seide Ron, Reid Neil, Fuentes Zárate Jorge Omar. Manual de redes inalámbricas, McGraw-Hill, 2004.

David Roldán Martínez. Comunicaciones inalámbricas. Un enfoque aplicado, RA-MA, 2004.

Gralla, Preston. Cómo funcionan las redes inalámbricas, Anaya Multimedia, 2006

Gast, Matthew S. Redes wireless 802.11, Anaya Multimedia, 2005.

Andrew A. Vladimirov; Konstantin Gavrilenko; Andrei A. Mikhailovsky; Eduardo Gómez Melguizo. Hacking wireless: Seguridad de redes inalámbricas, Anaya Multimedia, 2005.

http://www.wirelessdevnet.com, Wireless Developer Network.
http://www.wirelessweek.com, Wireless Week.
http://www.wi-fi.org, Alianza Wi-Fi.
http://www.ieee.org, Instituto de Ingenieros El[ectricos y Electrónicos.
http://www.ieee802.org/1/pages/802.1x.html
http://www.standards.ieee.org
http://www.standards.ieee.org/getieee802/802.11.html

http://www.standards.ieee.org/getieee802/download/802.11a-2004.pdf
http://grouper.ieee.org/groups/802/11 Grupo de trabajo de IEEE 802.11.
http://www.wi-fi.org/ opensection/protected_access.asp
http://www.wirelessethernet.org/certified_products.asp
http://www.hiperlan2.com, Instituto Europeo de Normas de Telecomunicaciones.
http://www.bluetooth.com
http://www.microsoft.com/latam/technet/articulos/wireless/pgch02.mspx
http://www.microsoft.com/latam/technet/productos/windows/windowsxp/wifisoho.mspx
http://www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx.
http://www.microsoft.com/windowsserver2003/techinfo/overview/peap.mspx. Artículo “Las ventajas de (PEAP): Un estándar usado para la autenticación de las redes inalámbricas IEEE 802.11”.
http://www.intel.com/products/mobiletechnology
http://www.compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm
http://www.homerf.org

OTRAS REFERENCIAS.

Seguridad

http://www.isaac.cs.berkeley.edu/isaac/wep-fap.pdf

http://www.eetimes.com

http://www.cs.umd.edu/~waa/wireless.html

http://www.practicallynetworked.com

Soluciones comerciales orientadas a aumentar y monitorizar la seguridad de las redes inalámbricas

Bluesocket http://www.bluesocket.com

Ecutel http://www.ecutel.com Soluciones para redes VPN

Netmotion http://www.netmotionwireless.com Soluciones para redes VPN

Herramientas que ayudan a analizar y mejorar la seguridad de una red inalámbrica

http://www.internetscanner.com

http://www.blackice.com

http://www.netstumbler.com

http://www.webattack.com/shareware/security/swantihack.shtml

http://www.wildpackets.com/products/airopeek

Herramientas para romper la seguridad de una red inalámbrica

Wepcrack: http://www.wepcrack.sourceforge.net/

Airsnort: http://www.airsnort.shmoo.com/

Aircrack: http://www.cr0.net:8040/code/network/aircrack/

Ejemplos de hardware (firewall)

http://www.watchguard.com

http://www.webramp.net

Officeconnect http://www.3com.com

Sonicwall http://www.sonicwall.com

Ejemplos de software (firewall)

Conseal Private Desktop http://www.firewall-net.com

Zonealarm http://www.zonealabs.com

Sybergen Secure Desktop http://www.networkcomputing.com

Norton Internet Security http://www.symantec.com

Blackice Defender http://www.iss.net

Telefonía por Internet

http://www.buddyphone.com
http://www.phonefree.com
http://www.ticphone.com
http://www.fonoclick.com
http://www.go2call.com
http://www.net2phone.com
http://www.pccall.com

Banda Ancha Inalámbrica Aerotransportada

http://www.angeltechnologies.com
http://www.skytowerglobal.com
http://www.skystation.com