UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

EVALUACION DE SEGURIDAD EN REDES WI-FI

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

MIGUEL ANGEL ESPINOZA TELLO

PROMOCIÓN
1989 - II

LIMA – PERÚ
2008

EVALUACION DE SEGURIDAD EN REDES WI-FI

A Miguel y Esther, mis padres,
Yanet, Adriana y Ayax, mi familia, por todo
el apoyo que recibí para culminar este trabajo

SUMARIO

El presente trabajo consta de seis capítulos. En el primero se describe el entorno actual en el que se desenvuelve la Tecnología WI-FI, recopilación de notas periodísticas locales relacionadas con los riesgos de seguridad de redes inalámbricas y la proyección de esta tecnología hacia el futuro.

En la segunda parte se describe los fundamentos de la tecnología Wi-Fi, el Estándar 802.11, su estructura en la capa física del modelo OSI, la estructura de una trama Wi-FI y los servicios ofrecidos por el Estándar 802.11.

La tercera parte describe los Fundamentos de Seguridad Wi-Fi y los diferentes métodos de protección existentes como encriptación de Datos, WEP, WPA y TKIP.

En el cuarto capítulo se analiza las vulnerabilidades, formas de ataque o intrusión a redes Wi-Fi tales como el ataque del falso intermediario y ataque de Denegación de Servicio.

En el quinto capítulo se compara las modalidades de seguridad existentes y se describen los pasos necesarios para la protección de una red existente.

Finalmente el sexto capítulo se describen los accesos públicos y se proponen recomendaciones para proteger, empresas, hogares y medidas de protección del usuario móvil.

INDICE

INTRODUCCIÓN

El objetivo de este trabajo es analizar la tecnología WI-FI desde el punto de vista de la seguridad y brindar directrices básicas para asegurar una red con puntos de acceso inalámbrico así como también dar pautas a los usuarios finales para que adopten medidas de protección en este escenario emergente.

No es muy difícil demostrar el poco conocimiento de las organizaciones y usuarios de los sistemas de información e Internet, o la poca importancia que se da a esta tecnología que ya forma parte del entorno. Los escasos reportes periodísticos locales dan una muestra de ello, esto es lo que se aborda en el primer capitulo.

En los últimos años han emergido y proliferado nuevas tecnologías, dentro de las cuales destacan las tecnologías inalámbricas como WI-FI, WIMAX, GSM, Bluetooth, Infrarrojos (IrDA), etc. Los dispositivos inalámbricos constituyen una de las grandes revoluciones de este siglo, sin embargo este trabajo solo esta limitado a la tecnología Wi-Fi y los estándares existentes. Por lo que los fundamentos de esta tecnología y la seguridad relacionada a ella se describen en los dos siguientes capítulos.

Las tecnologías inalámbricas (Wireless, en inglés) favorecieron en gran parte el crecimiento de otro fenómeno que es la movilidad. Esta ha cambiado en el último par de años, sin que muchos lo perciban, la estructura y la topología de las redes empresariales, junto con ellos también creció la vulnerabilidad, por lo que en los dos últimos capítulos se comparan los métodos de seguridad existentes, políticas a definir y medidas de protección.

Mi agradecimiento a la FIEE y a la UNI y todos los compañeros que me ayudaron a obtener información.

CAPITULO I
MOTIVACION

Por muchos años la tecnología de redes LAN inalámbrica Wi-Fi o 802.11 fue considerada como una tecnología interesante pero no una tendencia principal. Esto ha cambiado. Ahora desde una persona común hasta las grandes compañías, no solamente los adictos a la tecnología y los expertos en IT, ven los beneficios prácticos de esta tecnología. El crecimiento explosivo de accesos inalámbricos instalados en el medio trajo consigo las ventajas de movilidad para el usuario, ahorro en infraestructura de cableado, etc., pero también los riesgos o brechas de seguridad en las redes, ataques, virus, intrusión, sustracción o alteración de información son algunos de estos riesgos.

No estamos capacitados para detectar cuando estamos sufriendo un ataque en una red Wi-Fi. La forma de ataque más simple es la conexión a un punto de acceso desprotegido. Estos puntos de acceso inalámbricos propagan un mensaje que revela su presencia para todos los que están dentro de su rango de alcance. Si la seguridad no esta implementada, el enemigo podría conectarse como un usuario autorizado. Reportes periodísticos han escrito artículos acerca de conducir en la ciudad con una laptop y conectarse directamente dentro de LAN's inalámbricas desprotegidas de muchas empresas. Esta práctica se ha denominado "war driving", con la laptop unida a un dispositivo GPS van marcando la posición de redes vulnerables. Existe también otro término conocido como "warchalking" que consiste en dejar señales en el piso o en las paredes en lugares donde se ha detectado acceso a una red Wi.-Fi. Estos ejemplos muestran que tan vulnerables pueden ser las redes Wi-Fi a menos que se hayan habilitado medidas de seguridad. Aún si no nos interesa ser espiados y solamente usamos el computador para navegar por Internet, no podemos asumir que estamos a salvo si no se han habilitado medidas de seguridad.

1.1 Escenario actual en el Mundo

Es una espera epidémica que ocurrirá a muchos expertos en seguridad. Mientras muchos Gerentes IT hoy están ocupados asegurando sus redes de cableado fisico, sus empresas han gastado billones en tecnología inalámbrica. A finales del 2006, las empresas en Estados Unidos habían invertido $60 billones de dólares en servicios y seguridad de comunicaciones inalámbricas; y el 80 por ciento de la fuerza de trabajo en Estados Unidos ya usaba alguna clase de dispositivo inalámbrico, incluyendo celulares y dispositivos móviles de computación. Estas eran buenas noticias para la productividad del empleado, pero malas noticias para compañías mal preparadas para afrontar las brechas de seguridad en redes y los virus.

Globalmente ha existido una falta de funcionalidad y de madurez de la infraestructura. Y, esa es la única razón por la que los virus de hoy nos han causado mas daño. Pero esto pronto va a cambiar. Los analistas de la industria predicen dramáticos incrementos en el uso de dispositivos portátiles inalámbricos y la proliferación de nuevos capacidades móviles. Esperan ver 5.9 billones de celulares, asistentes personales digitales (PDA's) y aplicaciones de Internet equipadas con capacidades inalámbricas a finales del 2008, con esto, se obtiene una epidemia a gran escala en los centros de trabajos.

Para muchos gerentes IT, el mundo inalámbrico puede ser un nuevo territorio. Muchas empresas han visto que proteger sus procesos inalámbricos contra los virus informáticos es solo una pieza de un complicado rompecabezas que pueden dar a omitir. Pronto tendrán que enfrentar amenazas que podrían causar daños a gran escala.
Por ende, para de proteger contra los virus y las brechas de seguridad en el futuro, los vendedores de seguridad de redes inalámbricas (aún gigantes como IBM) están ocupados desarrollando productos para este fin. Adicionalmente, dentro de las aplicaciones y en los dispositivos, están resolviendo problemas en el ámbito de red inalámbrica.

1.1.1 Visión General de Seguridad en redes inalámbricas

En los mercados donde los dispositivos inalámbricos son ampliamente usados, hasta hoy, la mayoría de los ataques inalámbricos han ocurrido fuera de U.S. No obstante, hubo un virus que lo hizo sobre dispositivos portátiles, fue conocido como el virus Liberty.

Por ejemplo algunos usuarios de PDA's recibieron lo que ellos pensaron era un programa que les permitiría jugar cierto juego de manera libre. Sin embargo, este lanzo un virus que borró todos los datos del dispositivo cuando hicieron doble clic en el link o enlace.

Sin embargo los virus no han afectado a los usuarios que regularmente guardan una copia de seguridad de la información de sus PDA's en sus computadores personales. No obstante, han ocurrido problemas más serios en el mundo, en la forma de virus y / o código malicioso que forzó a los teléfonos a discar números particulares, interceptó las transmisiones y perpetuaron el robo de datos.

Disfrazado como un mensaje corto, un virus fue distribuido en Escandinavia. El virus deshabilitaba los botones del celular cuando un usuario recibía el mensaje. Para reparar sus equipos, los usuarios tuvieron que llevar los equipos a sus proveedores de servicio.

Se han escrito nuevos tipos de código malicioso que fuerzan a los dispositivos inalámbricos a efectuar llamadas a celulares, porque muchos de ellos tienen capacidades telefónicas. Un incidente en Japón captó la atención de los operadores inalámbricos y las compañías de software en todo el mundo. Los usuarios de NTT DoCoMo's, un servicio popular I-mode (internet móvil) recibieron un e-mail que simulaba formar parte del sitio Web. Cuando los usuarios dieron clic sobre el link, sus teléfonos automáticamente marcaron el número de emergencias japonés. Afortunadamente, podían detenerlo antes que sea tarde; pero, esto podía apagar un sistema 911 con consecuencias de vida o muerte. Por ejemplo, virus similares pueden ser desencadenados y afectar los Centros de Atención al Cliente de una empresa, o causar que los teléfonos marquen un numero de la serie 900. Si un virus se extiende a todos los trabajadores móviles acumulando cargos importantes, la corporación puede ser seriamente afectada.

La amenaza de robo de información, es talvez más alarmante para los negocios. Para prevenir la interceptación de información según esta siendo transmitida, todos los estándares de transmisión inalámbrica incluyen seguridad de fábrica, pero son conocidas por ser falibles. La tecnología de encriptación diseñada para detener la amenaza de

sniffing, ha sido incluida por los desarrolladores de standards, tales como el Protocolo de Aplicación Inalámbrica (WAP en inglés) y el standard inalámbrico LAN 802.11b.

Dado que la red inalámbrica esta esencialmente en cualquier lugar, la amenaza de sniffing es un problema inherente a lo inalámbrico. Los sniffers deben tener acceso a una parte fisica de la red para romper una red de cableado. El problema es, con lo inalámbrico, que no necesitan estar en la red. Pueden estar dentro de un automóvil en el exterior con un transmisor.

Cuando investigadores de la Universidad de California en Berkeley resolvieron como romper esta encriptación, el standard LAN inalámbrico ampliamente usado, 802.11, cayó abatido. Dado que los desarrolladores manejaron la seguridad de las redes inalámbricas desde el principio y están trabajando para mejorarla antes que las redes inalámbricas sean más penetrantes, hay algo de esperanza.

Las empresas también tendrán que asegurar sus transacciones inalámbricas. Habrá ataques sobre los mismos dispositivos, pero luego se enfocarán rápidamente sobre las transacciones.

Según se desarrollen mas capacidades en los dispositivos, se espera que estas amenazas crezcan mas seria y frecuentemente. Típicamente debe mirar hacia el pasado para predecir el futuro. También, nuevas amenazas posibles aparecerán cada vez que haya un avance en la tecnología.

Cada vez que las compañías de software liberan tecnologías populares en el entorno de PC, la gente los usa para escribir código malicioso. Lo mismo se espera con respecto a lo inalámbrico. Por ejemplo, un programa de Windows puede ejecutarse actualmente en un dispositivo Windows CE, pero CE aun no soporta macros. Entonces, la habilidad del virus para expandirse es nula, porque el dispositivo no soporta macros.

No obstante, los dispositivos inalámbricos están desarrollando otras capacidades. Al comienzo, los dispositivos PDA solamente almacenaban una lista de contactos. Pero,

hoy son pequeños dispositivos de computación. Existe mas chance de cosas siendo utilizadas de manera inapropiada, según se crea mas funcionalidad.
Muchos virus han sido regionales hasta ahora. Pero crece la amenaza de expansión de virus alrededor del globo, según las regiones del mundo empiezan a estandarizar las tecnologías inalámbricas.

Adicionalmente, existe un gran potencial para la expansión de virus entre PC's y dispositivos móviles (los cuales podrían habilitar muy rápidamente la expansión de virus), porque en estos últimos se están soportando mas capacidades. Entonces las mismas aplicaciones podrán ejecutarse en PC's y dispositivos portátiles. Entonces los virus se expandirán fácilmente por e-mail o programas que sincronizan las PC's y dispositivos portátiles. Una versión de java ya es soportada por la mayoría de teléfonos inalámbricos.
Lo que realmente esta siendo fácilmente disponible, son más productos y medidas de seguridad en redes inalámbricas. Aun así, la incertidumbre sobre como manejar las posibles amenazas esta previniendo a las empresas de utilizar y desplegar la tecnología inalámbrica.

Aunque todavía, muchas empresas tienen que enfrentar incidentes de seguridad en sus redes de cableado. Y, es muy difícil para los gerentes IT mantenerse actualizados con los nuevos desarrollos porque ambos, los mundos de cableado e inalámbrico cambian rápidamente. Es un tremendo reto para los gerentes IT comprender el espacio y los incidentes, y que soluciones existen para manejarlos.

Muchas empresas aún no están preocupadas en protegerse contra los virus, porque los virus para redes inalámbricas aún no se han esparcido. También, muchas empresas no han oído mucho acerca de virus para redes inalámbricas, por ende, no es un problema real en este momento. Dado que los datos de dispositivos inalámbricos pasan a través del FireWall corporativo, seguridad inalámbrica adicional no es necesaria, porque la información no será valiosa para nadie más.

Por ejemplo en Final Mile Communications (http://www.finalmile.com), una compañía de servicios profesionales, los trabajadores de campo usan teléfonos Nextel para

recibir tickets de problemas y reportar el status al centro de despachos. Ellos aún no han visto ningún virus, pero cuando el virus se presente, será un serio problema de tratar.

Parece haber mas preocupación acerca de la posibilidad de que los datos sean apropiados por otras compañías. Determinando que es aceptable y que no, la primera decisión que una empresa debe tomar cuando implementa un sistema inalámbrico seguro es el modelo de seguridad.

Es muy importante, porque es parte del problema. Por ejemplo, en las redes de cableado, la encriptación basada en infraestructura de clave pública no ayudó porque es dificil de usar. Una empresa que desea dar a sus trabajadores de campo acceso a datos importantes esta apuntando a tener trabajadores más eficientes. Sin embargo, se ha negado la ventaja de ir a través de la seguridad de una red inalámbrica, si es que esta introduce más error y toma más tiempo el usarlo. Se debe tomar un enfoque holístico.

Al mercado están entrando mas productos que pretenden ofrecer seguridad de redes inalámbricas de extremo a extremo (end-to-end) que empieza con el dispositivo e incluye el software que ejecuta las aplicaciones. Dando así a las empresas más opciones que cubran sus necesidades específicas. Uno de los problemas más simples no ha sido ampliamente manejado: Si el dispositivo se pierde o es robado, pocos dispositivos móviles tienen mecanismos para proteger la información almacenada en ellos. Tal que solamente el propietario pueda acceder a los datos almacenados. Hoy existen algunos productos pioneros que las empresas pueden añadir a los dispositivos de usuario para encriptación de datos.

Por ejemplo el producto F-Secure (http://www.f-secure.se) tiene software de encriptación y antivirus para computadores de bolsillo (Pocket PC), Palms y dispositivos Symbian. F-Secure ofrece motores antivirus para gateways WAP a nivel de operador. Un ejemplo mas es Trend Micro (http://www.trendmicro.com) que tiene software antivirus para dispositivos y seguros para todos los puntos de entrada, incluyendo emisión, sincronización, correo electrónico y descarga desde internet.

Programas similares a aquellos disponibles en laptops podrían ser desarrollados para permitir a los usuarios cuyos dispositivos se han robado o perdido, para permitirles destruir remotamente la información o hacerla inutilizable para los demás. De tal forma que proteger información importante almacenada en estos dispositivos puede ser crucial.
A pesar de que no se esperan amenazas serias por algún tiempo, se iniciaron actividades para crear software de protección contra virus que residan en estos dispositivos. El entorno de electrónica de consumo será probablemente el primero en ver virus escritos para estas plataformas.

Debido a que las técnicas de comunicación de corto alcance como Bluetooth o conexiones infrarrojas no usan las redes inalámbricas, el software en esos dispositivos llegan a ser un componente importante de la campaña antivirus. Sin tener que enviar los datos a través de un servidor, los usuarios pueden emitir información (y virus) directamente de uno a otro dispositivo.

Con la adquisición de equipos que tengan tecnología de autenticación incluida, los gerentes IT pueden proteger los dispositivos de los trabajadores móviles. Por ejemplo RSA (http://www.rsasecurity.com) es una empresa que esta trabajando en conjunto con los fabricantes de equipos móviles para hacer que estos últimos sean capaces de aceptar firmas digitales.

1.2 Publicaciones locales relacionadas (diario El comercio / Revista de enfoque económico)

A continuación la recopilación de dos notas periodísticas relacionadas al tema que enfocan desde el aspecto empresarial los riesgos existentes.

1.2.1 "Sistemas de redes inalámbricas son vulnerables en Lima"

El Comercio – 14 de Julio 2006

"El 51% de los puntos de acceso en San Isidro y Lima no tienen restricción según Deloitte.
¿Qué tan fácil es acceder a la computadora del Gerente General de una empresa? Quizá no tan complicados como cualquiera se lo imagina. La división de consultoría de Deloitte, a través de área de Riesgos Tecnológicos, se propuso conocer el nivel de seguridad del uso de redes LAN Wireless (inalámbricas) de centros empresariales de Lima.

Para eso se hizo un recorrido por las calles de San Isidro y el centro de Lima con una computadora portátil y el software Kismet para Linux. Al captar las señales en el aire, se detectó 356 puntos de acceso, los cuales permiten la conexión inalámbrica a las redes de una compañía. Los resultados del estudio del mapa de Seguridad Wireless en Lima muestran que el 55% de estos puntos de accesos no utilizan mecanismos de encriptación siendo altamente vulnerables. Un 45% tenía sistemas de seguridad WEP, que se considera inapropiados para una compañía, y solo el 4% contaba con total seguridad.

Si se toma el caso del centro empresarial de San Isidro, donde se ubican las oficinas de las principales transnacionales – incluso empresas tecnológicas – el 49% de los 122 puntos de acceso detectados pueden ser atacados accediendo a información confidencial de las empresas, usurpación de identidades digitales, robo de ancho de banda, etc.

Un porcentaje similar de vulnerabilidad se observa en las calles del centro Financiero de San Isidro (Chinchon, Las Begonias, Paseo de la República y Canaval y Moreyra) . En el caso del centro de Lima, la concentración de puntos de acceso es mucho menor, pero el 85% esta desprotegido.

"Antes un 'Hacker' debía tener muchos conocimientos, pero ahora cualquiera puede bajar las herramientas para vulnerar las redes", dijo Luis Budge, gerente de Enterprise Risk Service de Deloitte.

Según las conclusiones del estudio, si se hace una comparación con el nivel de tecnología de las principales ciudades de Estados Unidos y Europa, el nivel de Lima es el que tenían estas ciudades hace dos años. Esta nota periodística en uno de los diarios mas influyentes del medio es uno de los escasos reportes del año 2006 cuando ya se habían desplegado un número importante de dispositivos Wi-Fi en los distritos mas importantes de Lima, que muestra el poco interés o conocimiento de las vulnerabilidades de esta tecnología.

1.2.2 Redes Inalámbricas (WI-FI) gemelas

Revista Enfoque Económico – 13 de julio de 2007

"De acuerdo con un estudio divulgado por la organización de seguridad informática Systems Security Association, la creación de "redes inalámbricas gemelas" es una de las estrategias cada vez mas utilizadas por los "hackers" o ciberdelicuentes para entrar a computadoras que no les pertenecen y robar información.

En la actualidad tanto en Perú como en otros países las empresas de Telecomunicaciones y proveedores de PC's y equipos informáticos brindan conexión a Internet de manera inalámbrica (Wi-Fi) y lo hacen para tres tipos de ambientes: hogares, empresas y lugares públicos con los que instalan antenas o routers inalámbricos.

Los hackers o ciberdelincuentes crean "redes inalámbricas gemelas" de esta manera simulan se una red inalámbrica instalada previamente. Para esto suelen utilizar un programa que puede ser creado por ellos mismos y un router inalámbrico o tarjeta de red inalámbrica la que configuran poniéndole el mismo nombre de la red que desean suplantar.

Así, cuando un usuario quiera conectarse a Internet de manera inalámbrica verá dos redes con el mismo nombre (SSID) y por equivocación puede llegar a conectarse a la red gemela propiedad de un hacker, con lo cual pone a su alcance la información que tiene almacenada en su computadora, pues esta compartiendo la misma red.

Asimismo existen personas y empresas que revenden acceso a Internet de manera inalámbrica sin contar con permiso del Ministerio de Transportes y Comunicaciones (MTC) y yendo en contra del contrato que firmaron con la empresa de comunicaciones que les proveer el servicio de Internet. Al hacer esto reciben ingresos pero ponen en grandes riesgos a aquellas personas a las que revenden Internet puesto que en muchos casos utilizan antenas fabricadas de manera rústica y no toman medidas de seguridad ante robo de información o contagio de virus informáticos.

Como forma de contingencia para evitar este problema, Telefónica ha señalizado los lugares públicos con servicio Speedy Wi-Fi para que el usuario pueda identificarlos como puntos autorizados. Además, ante la gente inescrupulosa que utiliza señales del vecino para navegar "gratuitamente" utilizando una señal que no le pertenece, Telefónica

configura el MODEM inalámbrico para que solo el titular pueda navegar y no vea afectada su velocidad y la seguridad de información de su PC".

1.3 Perspectivas de las Redes Wi-Fi

Según la consultora Burton Group, especializada en IT y seguridad, el modelo de tecnologías inalámbricas Wi-Fi va a desplazar a Ethernet como sistema de comunicaciones de red de área local (LAN) hasta tal punto que Ethernet desaparezca en aproximadamente tres años. La principal razón expuesta es que la red Wi-Fi puede igualar en velocidades y en condiciones de seguridad las redes LAN, las dos reticencias que los defensores del modelo cableado tenían para argumentar su uso.

Las aplicaciones de las redes inalámbricas son infinitas. De momento van a crear una nueva forma de usar la información, pues ésta estará al alcance de todos a través de Internet en cualquier lugar (en el que haya cobertura) .

En un futuro cercano se reunificarán todo aquellos dispositivos con los que hoy contamos para dar paso a unos nuevos que perfectamente podrían llamarse Terminales Internet en los cuales estarían reunidas las funciones de teléfono móvil, agenda, terminal de vídeo, reproductor multimedia, ordenador portátil, etc.

Se podría dar lugar a una Internet paralela y gratuita la cual estaría basada en las redes que altruistamente cada uno de nosotros pondríamos a disposición de los demás al incorporarnos a las mismas como destino y origen de la información.
En un futuro también cercano la conjunción de las redes Mesh, con las redes inalámbricas y las redes Grid podría llevar a cabo al nacimiento de nuevas formas de computación que permitan realizar cálculos inimaginables hasta ahora debido a las necesidades de hardware de las que eran objeto.

La predicción del fin de IPv4 en 2011 y expansión de IPv6 como estándar de protocolo de comunicación en las redes prometen mejores niveles de seguridad para los dispositivos Wi-fi.

CAPITULO II
FUNDAMENTOS DE WI-FI

Se conoce como "Redes Wi-Fi" a un conjunto de redes de área local (LAN) donde el medio de acceso es inalámbrico. Son sistemas en donde cada computador cuenta con un módem de radio y una antena para poder comunicarse con otros sistemas. El término Wi-Fi proviene del inglés Wireless Fidelity. Las LAN's inalámbricas son hoy comunes en casas y oficinas.

Ampliando un poco mas la introducción, en el momento en que salieron al mercado las computadoras portátiles, surgió una nueva demanda, los usuarios deseaban poder movilizarse libremente con sus dispositivos y permanecer conectados a la red o a Internet. Para satisfacer esta demanda, varios fabricantes empezaron a trabajar en ello. La forma más simple era proveer a las computadoras, de receptores y transmisores de radio de onda corta que les permitan comunicarse, esto dio origen a que varias empresas comercializaran las LAN's inalámbricas (o WLAN). El problema de esta nueva tecnología fue que no había compatibilidad entre ninguna de ellas. Las industrias aceptaron que era necesario crear un estándar para redes inalámbricas. Se encargó al comité IEEE realizar esta tarea. Al nuevo estándar se le llamó 802.11 y en el argot informático adoptó el término Wi-Fi.

2.1 Estándar IEEE 802.11

El primer componente del estándar IEEE 802.11 fue ratificado en 1997 y luego en 1999, cuando también se realizaron las primeras extensiones. La estructura de los estándares de la IEEE es tal que las extensiones se elaboran como modificaciones del estándar original y se nombran agregándole una letra al nombre del estándar. En el caso de 802.11, tenemos extensiones 802.11a, 802.11b, etc. En realidad, el estándar 802.11 es sólo una parte de un conjunto más amplio de estándares de IEEE: el 802. La Figura 1 muestra esquemáticamente la estructura del conjunto de estándares 802, dedicado a las capas más bajas de arquitectura de redes.

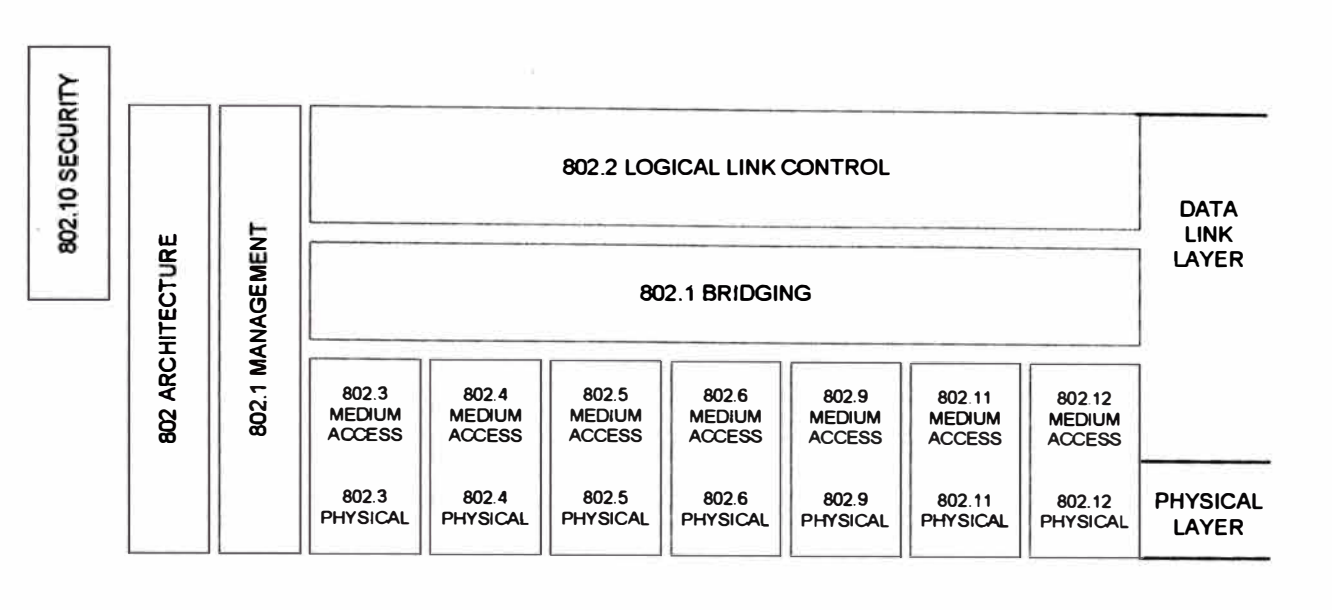

Figura 2.1 Estructura del conjunto de estándares 802

La capa más baja es la fisica, Physical Layer en la Figura 2.1. Esta es la capa lógica encargada de definir los detalles fisicos de la red, como ser potencia transmitida, esquema de modulación, etc. Sobre la capa fisica, se ubica la capa de control de acceso al medio, Media Access Control (MAC Layer) . Esta es la capa que permite la coordinación en el uso del medio de transmisión común entre todas las estaciones que desean comunicarse. Corresponde a una sub-capa inferior del Data Link Layer del modelo OSI de siete capas. Uno de los componentes más conocidos es el estándar 802.3, correspondiente a la especificación de redes de área local (LAN) Ethernet. El éxito de 802.3 hizo que éste se convierta en una de las principales fuentes de las cuales toma el diseño del estándar IEEE 802.11.

El proceso de estandarización tuvo que afrontar cuatro grandes problemas aparte de que debía ser compatible con el estándar 802.3. Primero, en Ethernet, una computadora siempre escucha el medio antes de transmitir. Solo si el medio esta inactivo la computadora puede empezar a transmitir. Con las WLAN's no es lo mismo. El hecho de que un computador no escuche nada en el medio inalámbrico no significa que su transmisión tendrá éxito.

El segundo problema era que los objetos sólidos pueden reflejar las ondas de radio, por lo que la señal se podría recibir múltiples veces, esta interferencia se conoce como desvanecimiento por múltiples trayectorias.

El tercer problema fue del lado de las aplicaciones de software, que no incluyen a la movilidad como variable a considerar en su funcionamiento. Un ejemplo simple seria la lista de impresoras en un entorno, ya no es válida cuando el equipo se cambia de entorno en una WLAN.

El cuarto problema, era que se requería controlar el cambio de un computador de una área de estación base a otra. Se tenía que configurar todas las estaciones base de una red para que se viera desde fuera como una sola red.

2.2 Capa Física

2.2.1 Sub-capa de control de acceso al medio (MAC)

Se puede clasificar a las redes en dos grandes grupos, las de conexión punto a punto y las que usan canales de difusión o broadcast. Es en la sub-capa de control de acceso al medio donde se definen los protocolos que determinan el manejo de las comunicaciones para las redes que pertenecen al grupo que usan canales de difusión.
Esta capa tiene un rol importante en las redes LAN, no así en las redes WAN donde se emplean enlaces punto a punto.

Para dar un ejemplo del uso de canales de difusión, considere una reunión de varias personas donde dos o más de ellas intentan hablar a la vez, esto lleva a una comunicación caótica, por lo que establecen reglas como el que levanta la mano primero, es el que habla primero y el resto escucha, luego contesta el destinatario, termina esta conversación y se establece otra por competencia. A los canales de difusión establecidos en cada conversación se le conoce como canales multiacceso o de acceso aleatorio.

2.3 Protocolo de sub-capa MAC de 802.11

En comparación con el protocolo Ethernet, el estándar 802.11 es muy diferente debido a lo complejo del entorno inalámbrico con respecto al de un sistema cableado. En Ethernet, una estación espera a que el medio este disponible (en silencio) para transmitir y si no recibe interferencia dentro de los primeros 64 bytes puede estar seguro que la trama se envió sin problemas. Esta situación no es la misma para los sistemas inalámbricos. Existen dos problemas que el sistema inalámbrico debe afrontar, el problema de estación

expuesta y el de estación oculta. La figura 2.2 muestra ambos casos. Adicionalmente, la mayoría de radios son semidúplex, es decir no pueden transmitir y escuchar el ruido en una misma frecuencia, por esta razón, 802.11 no usa CSMA/CD como si lo hace Ethernet.

El protocolo 802.11 soporta dos modos de funcionamiento para resolver este problema. Uno llamado DCF (Función de coordinación distribuida) que no usa ningún tipo de control central y otro llamado PCF (Función de coordinación puntual) que usa una estación base para controlar la actividad en su celda. Este último modo es opcional.

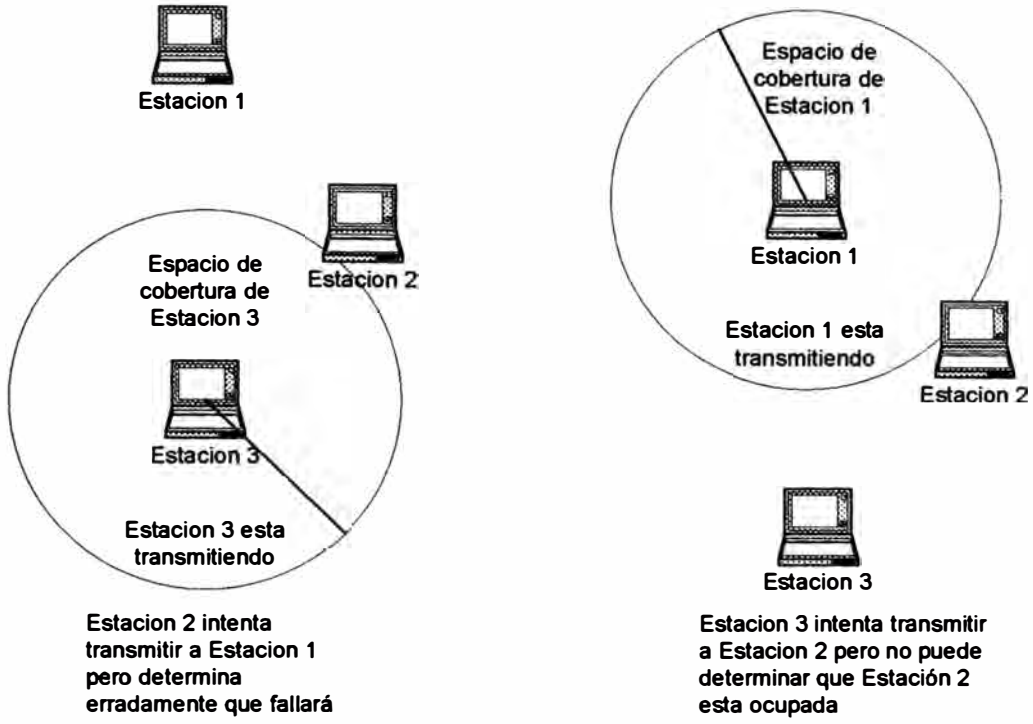

Figura 2.2 Problemas de estación expuesta y estación oculta

Con DCF, 802.11 emplea un protocolo llamado CSMA/CA (CSMA con evitación de colisiones), este protocolo se usa tanto para detección del canal físico como del canal virtual. Para detección del canal físico, cuando una estación desea transmitir, detecta el canal. Si esta inactivo, empieza a transmitir. Mientras transmite no detecta el canal y envía la trama completa, la cual puede ser destruida en el receptor debido a interferencia. Si el canal esta ocupado, el emisor espera hasta que este inactivo para comenzar a transmitir. De ocurrir una colisión, las estaciones involucradas esperan un tiempo aleatorio de acuerdo a un algoritmo de retroceso exponencial binario usado en Ethernet y vuelven a intentar la transmisión.

Para la detección de canal virtual, CSMA/CA usa el protocolo MACAW, este protocolo fija el control sobre la base del envío de una señal RTS de la estación origen "A" hacia una estación destino "B". Si esta última acepta la solicitud, devuelve una señal CTS, entonces "A" empieza a transmitir e inicia su temporizador ACK. Si "B" recibe correctamente la trama, devuelve un ACK hacia "A", terminando satisfactoriamente la transmisión. Si el temporizador ACK de "A" termina antes de recibir confirmación ACK de "B", todo el protocolo se ejecuta de nuevo. Las estaciones vecinas se inhiben al detectar esta operación imponiéndose a si mismas, un estado de canal virtual ocupado indicado por un parámetro NAV (Vector de asignación de Red) . Se debe aclarar que la señal NAV no se transmite, son internos para cada estación.

A diferencia de las redes cableadas, las redes inalámbricas son ruidosas e inestables. Como consecuencia, la probabilidad de que una trama llegue a su destino disminuye con la longitud de la trama. Para resolver esto, 802.11 permite dividir las tramas en fragmentos, cada uno con su propia suma de verificación. Cada fragmento es enumerado de forma individual y no se transmite un fragmento siguiente hasta no recibir confirmación de recepción del fragmento anterior. Una vez adquirido un canal, pueden enviarse múltiples fragmentos en una fila, a esta secuencia se le conoce como ráfaga de fragmentos. Esta forma de operación aumenta la velocidad real de transporte, restringiendo la retransmisión a fragmentos erróneos en lugar de la trama completa. El mecanismo NAV mantiene a las estaciones vecinas en silencio. En DCF no hay control y las estaciones compiten por tiempo / aire tal como la harían en Ethernet.

En el modo PCF, una estación base sondea a las demás estaciones y verifica si tienen tramas que enviar. Como el orden de transmisión es controlado por completo por la estación base, en el modo PCF no ocurren colisiones. Este estándar anula el mecanismo de sondeo pero no la frecuencia de sondeo, el orden de sondeo, ni el hecho de que las demás estaciones necesiten obtener un servicio igual. Este modo consiste en que la estación base difunde una trama de beacon (trama guía o faro) de forma periódica (de 10 a 100 veces por segundo). Esta trama contiene parámetros de sistema como secuencia de salto y tiempos de permanencia, sincronización de reloj, etc. Invita a las nuevas estaciones a suscribirse al servicio de sondeo. Una vez inscrita una estación, se garantiza de manera efectiva cierta fracción de ancho de banda y es posible ofrecer garantías de calidad de servicio.

2.4 Estructura de una trama 802.11

En 802.11 se definen tres clases de tramas: de datos, de control y de administración. Cada una de ellas con cabeceras diferentes dentro de la sub-capa MAC. Adicionalmente algunas cabeceras son empleadas en la capa fisica, asociadas con las técnicas de modulación utilizadas.

Las tramas de administración son similares a las tramas de datos, a excepción que no tienen una de las direcciones de estación base ya que se restringen a una sola celda.
Las tramas de control, mas cortas, tienen una o dos direcciones y no tienen campo de datos ni de secuencia. La información importante en estas tramas esta en el campo de Subtipo, que puede ser: RTS, CTS o ACK.

A continuación, en la figura 2.3 se muestra la estructura de una trama de datos. Primero esta el campo de control de trama. Éste tiene 11 sub-campos. El primero es la versión de protocolo, que permite que 2 versiones del protocolo funcionen al mismo tiempo en la misma celda. Después esta los campos de tipo (de datos, de control o de administración) y subtipo (por ejemplo RTS o CTS). Los bits "A DS" y "De DS" indican que la trama va hacia o viene del sistema de distribución entre celdas (por ejemplo Ethenet). El bit MF indica que siguen mas fragmentos. El bit "Retrans" marca una retransmisión de una trama que se envió anteriormente. El bit de administración de energía es usado por la estación base para poner al receptor en estado de hibernación o sacarlo del mismo. El bit más indica que el emisor tiene tramas adicionales para el receptor. El bit W indica que el cuerpo de la trama se ha codificado usando el algoritmo WEP (Privacidad Inalámbrica Equivalente). Por último, el bit O indica al receptor que una secuencia de tramas que tenga este bit encendido debe procesarse en orden estricto.

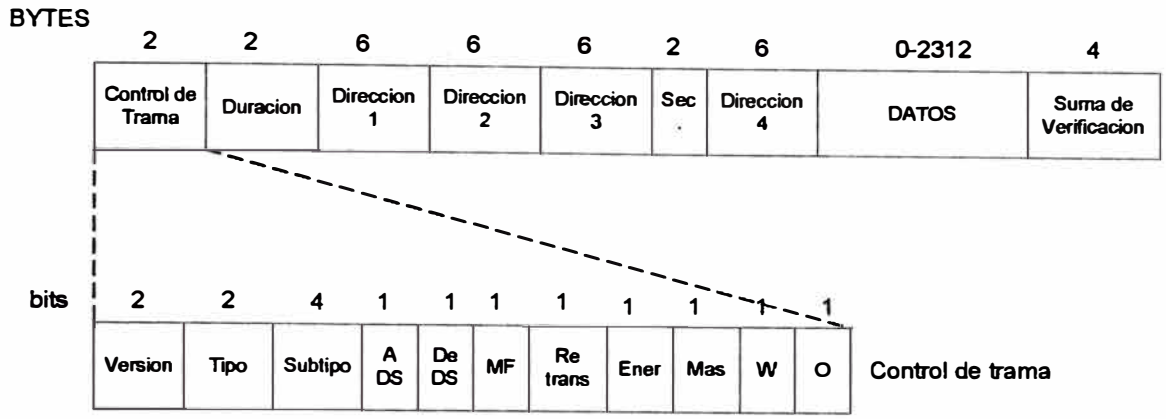

Figura 2.3 Estructura de una de trama de Datos

El segundo campo de la trama de datos es el de duración, indica cuanto tiempo ocuparan el canal la trama y su confirmación de recepción. Este campo también esta presente en las tramas de control y es la forma mediante el cual otras estaciones manejan el mecanismo NAV. La cabecera de la trama contiene cuatro direcciones, todas en formato IEEE 802.2. Dos de ellas corresponden al origen y destino. Las otras dos se emplean para las direcciones de estaciones base origen y destino para el tráfico entre celdas.

El campo de secuencia permite enumerar los fragmentos. De los 16 bits disponibles, 12 identifican la trama y 4 el fragmento. El campo de datos tiene la carga útil, de hasta 2312 bytes, y le sigue el campo de suma de verificación.

2.5 Servicios en el protocolo 802.11

El protocolo 802.11 establece que cada LAN inalámbrica debe proveer 9 servicios. Estos se agrupan en dos categorías. Cinco servicios de distribución y cuatro de estación. Los servicios de distribución están asociados con administración de miembros dentro de una celda y con la interacción con estaciones que están fuera de la celda. Por otro lado los servicios de estación se relacionan con la actividad dentro de una sola celda. Los servicios de distribución son los siguientes:

1. Asociación. Usado por estaciones móviles para conexión a estaciones base, esta última puede aceptar o rechazar a la estación móvil. Si es aceptada, dicha sesión debe autenticarse.

2. Disociación. Es posible que la estación móvil o estación base se disocie para romper la relación. Por ejemplo una estación puede emplear este servicio antes de apagarse o de salir.
3. Reasociación. Mediante este servicio, una estación puede cambiar su base preferida. Es útil para estaciones móviles que se pasan de una celda a otra.
4. Distribución. En este servicio se determina como enrutar tramas enviadas a la estación base. Si el destino es local para la estación base, las tramas se envían directamente a través del aire. De otra forma tendrían que enviarse por la red cableada.
5. Integración. Este servicio maneja la traducción del formato 802.11 al formato requerido por la red destino.

Los siguientes servicios se dan dentro de las celdas. Se emplean luego de que haya ocurrido una asociación, son las siguientes:

1. Autenticación. Una estación debe autenticarse antes que se le permita enviar datos.
2. Desautenticación. Cuando una estación previamente autenticada desea abandonar la red, se desautentica.
3. Privacidad. Permite que la información en una LAN inalámbrica sea confidencial mediante codificación.
4. Entrega de datos. Proporciona una forma de transmitir y recibir datos.

2.5.1 Estándares industriales

Además del estándar IEEE 802.11, existen estándares establecidos por asociaciones de fabricantes. Si bien los estándares de la industria suelen seguir básicamente al IEEE 802.11, muchas veces la industria se adelanta (por cuestiones de mercado) a incorporar mejoras que llevan más tiempo de ser incorporadas a un estándar IEEE. Una de las asociaciones de fabricantes más conocidas es la Wi-Fi Alliance (ver. http://www.wi-fi.org). Algunos de los miembros de esta asociación son Cisco, IBM, Intel Nokia, 3Com, Hewlett Packard, AMD, NEC. Avaya, Apple, Motorota y Microsoft. La importancia de estas compañías da una idea de la relevancia de la asociación.

2.6 Estaciones móviles y redes básicas

En esta sección presentamos algo de la nomenclatura básica en redes de Wi-Fi que será utilizado en adelante. A los equipos conectados a una red inalámbrica los

denominaremos estaciones móviles o simplemente estaciones. La estructura básica de una red inalámbrica es denominada BSS, Basic Service Set. Puede pensarse un BSS como la mínima estructura en la cual se puede organizar un grupo de estaciones móviles que se comunican entre sí. Otra forma de entender una BSS, en una primera aproximación (aunque no exacta, como ya veremos), es como el área de alcance de la transmisión de radiofrecuencia. La Figura 2.4 muestra dos BSSs con dos estaciones móviles cada una. De 802.11 modificado:

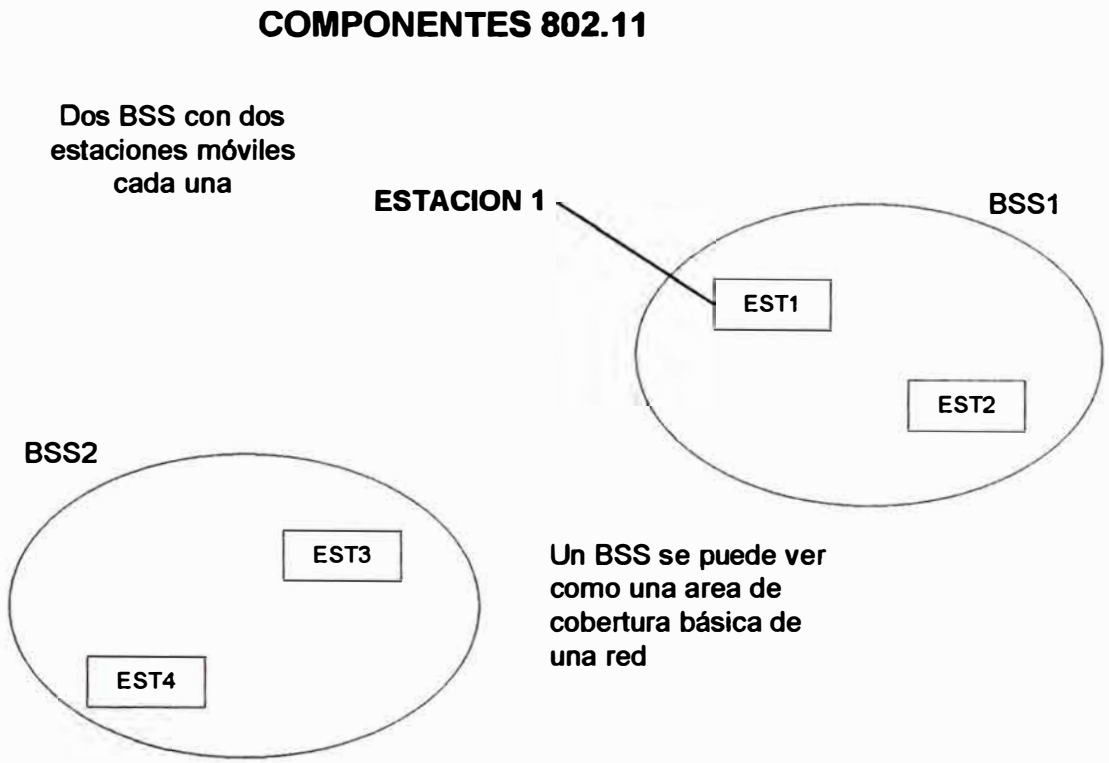

Figura 2.4 Componentes 802.11

2.6 Infraestructura

Existen dos tipos de redes diferentes:

2.6.1 Redes de infraestructura o estación base: En este caso, cada BSS está organizada alrededor de una estación que puede permitir el acceso a una red mayor, por ejemplo, a una LAN cableada. La estación especial recibe, por esto, el nombre de punto de acceso. En inglés es access point, por lo que en muchas oportunidades nos referiremos a él como AP.

2.6.1 Redes independientes o ad hoc: Son redes formadas por un solo BSS, denominado IBSS (Independent BSS), que no se estructuran alrededor de ninguna estación con funciones particulares, sino que distribuyen las tareas de coordinación entre sí.

Los BSSs de redes de infraestructura se pueden agrupar formando una entidad mayor conocida como Extended Service Set (ESS). Un ESS es simplemente una red conformada

por un conjunto de BSSs donde la conectividad entre BSSs está dada gracias a las funciones de puente de los puntos acceso. El medio a través del cual están conectados los puntos de acceso (que puede ser una LAN cableada, como ya se mencionó) se denomina Distribution System (DS). En cambio, el medio común a un BSS se denomina Wireless Distribution System (WDS). La Figura 2.5 representa esquemáticamente estos conceptos.

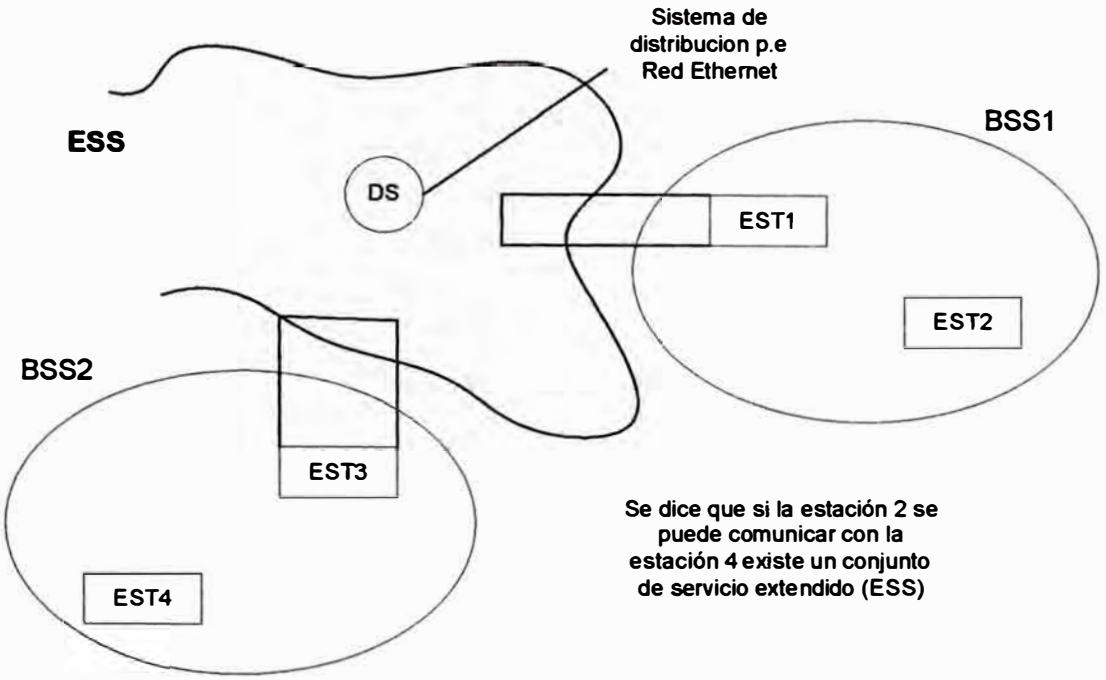

Figura 2.5 Sistemas de Distribución ESS y BSS

2.7 Ventajas de una red Wi-Fi

Las redes, actuando como venas a través de las cuales fluyen los datos, han cambiado. Tradicionalmente, las redes consistían de varios dispositivos conectados entre sí únicamente por cableado, sin embargo, ahora existe una alternativa. Esta alternativa deja fuera el cableado (y sus problemas asociados) y la reemplaza con un método más flexible y de bajo costo para transmisión de datos. Es una tecnología que ha sido usada por muchos años, pero ahora esta siendo utilizada en el mundo de las redes informáticas, particularmente en la implementación de redes de área local (LAN). La migración a este nuevo estilo de redes, aunque con lentitud en el inicio, se efectuó de manera explosiva en estos últimos años. Este medio relativamente nuevo de red es la radio comunicación.

Tradicionalmente las LANs fueron implementadas usando cables, con cada dispositivo conectado a la red mediante una tarjeta de red (NIC), cable y conectores. La

idea detrás de cable fue proveer un medio a través del cual los datos podían viajar en la forma de señales eléctricas discretas. Los datos podían propagarse por el cable (usualmente cable de cobre) por conducción, a tal distancia en que el circuito le permitía propagarse. En este modelo el dato es encerrado y viaja entre dispositivos, a través de los conectores y a lo largo de los cables. Esto provee cierto nivel de protección para los datos encasillando dentro del cable, el blindaje y el plástico.

La configuración típica en una pequeña organización puede consistir de un número de PC's desktop y laptop, impresoras y tal vez un servidor, todos con interfaces de red, cableado y ya sea un switch o un hub, un patch panel, y probablemente un router para conectar a Internet y al mundo exterior. Las interfaces de red de las PC's se conectan a una toma de red en la pared mediante un cable corto, detrás de la toma de red en la pared existe un cable que llega hasta el patch panel, el cual esta conectado a un switch o Hub y este a su vez conectado a un router.

Este tipo de configuración trabaja extremadamente bien, sin embargo, los costos iniciales de cableado pueden ser altos dependiendo del cable utilizado. Adicionalmente algunos edificios pueden ser dificiles de cablear, especialmente los antiguos. Otra desventaja importante es que las redes basadas en cableado pueden ser inflexibles. Si la estructura de la organización debe cambiar y se necesitan mover o añadir nuevas PC's a la red, el cableado viene a ser un problema.

También limita la movilidad de los usuarios, posiblemente impidiendo llevar sus PC's a las reuniones o en otra ubicación del edificio que no tenga el cableado con acceso a la red. Sin embargo, estos problemas se pueden resolver por medio del uso de dispositivos y conexiones inalámbricas. Tan buena como la flexibilidad ofrecida por la Red de Área Local Inalámbrica (WLAN), es que ayudan a mejorar la productividad. Una encuesta sobre 400 empresas Americanas grandes y medianas en el 2003, mostró que las WLAN's dio a los usuarios finales, la posibilidad de estar conectados a la red, un promedio de 3.5 horas mas por día. Esta investigación indica que el personal es un tercio más productivo que cuando trabajaban conectados a una red de cableado.

A continuación algunas ventajas de implementar WLAN's en las organizaciones:

1. Incremento de la productividad

   Como se mencionó anteriormente, dado que los empleados están conectados mas tiempo a la red, obviamente la productividad se incrementará. La WLAN's proveen cobertura en áreas donde las conexiones de red no estaban disponibles o no eran posibles, esto significa que los empleados eran capaces de acceder a Internet, correo y servidores de archivo, independientes de donde estén en el edificio. El tiempo entre las reuniones puede emplearse para ganar productividad y acceso inmediato a información crítica puede proveer inmensos beneficios

2. Mejora de eficiencia en las reuniones

   La información se puede compartir fácilmente en las reuniones, aún con las personas que no son empleados. Los miembros que estén autorizados pueden acceder a información corporativa pertinente en tiempo real y analizar datos para ayudar a acelerar los procesos de toma de decisiones. Los visitantes fácilmente pueden conectarse con acceso limitado a cierta información y servicios mientras están en las instalaciones e involucrarse activamente en la reunión sin ningún problema con el cableado.

3. Facilidad para nuevas instalaciones

   Las WLAN's reducen dramáticamente el tiempo y costo de añadir PC's y LapTop's a una red establecida. Una red WLAN completa se puede instalar en unas cuantas horas, en comparación a unos cuantos días o semanas para una red con cableado equivalente. No hay necesidad de perforar paredes, jalar cables desde el panel central, simplemente conectar un punto de acceso inalámbrico (AP), configurar unos cuantos parámetros básicos y los usuarios con interfaces inalámbricas están listos para conectarse a la red.

4. Conectividad externa

   Una LapTop o un PDA con capacidad WLAN, por ejemplo con una tarjeta inalámbrica instalada, permite a los usuarios móviles ser más productivos cuando están viajando usando "hot spots" (Puntos de acceso público a internet) en los aeropuertos, hoteles y cafés, para acceder a sus correos y más aún a la red corporativa, permitiendo hacer uso de todas las horas perdidas en espera en el aeropuerto o por un vuelo con retraso

5. Redes temporales

Se pueden implementar redes temporales con un mínimo esfuerzo en locales externos para sesiones de capacitación, demostraciones de negocio y reuniones. Se puede transportar todo el equipo hacia el sitio indicado e implementar la red con mínimo esfuerzo. Cualquier visitante que desee conectarse, tal vez para copiar o bajar información de un producto o de la empresa, puede hacerlo en cuestión de minutos y luego fácilmente desconectarse.

6. Reducción de costos de instalación

   Los costos de instalación de cableado pueden variar, especialmente en entornos donde es dificil tender cables, elevando inevitablemente el costo de instalar una red. Las conexiones inalámbricas eliminan completamente el problema del cableado, y facilitan significativamente la implementación de redes, reduciendo consecuentemente los costos. Para conexiones internas, los puentes inalámbricos punto a punto son ideales; rentar enlaces T1/E1 costosos ya no es necesario, estos pueden ser reemplazados con varios puentes (bridges) inalámbricos (uno en cada edificio).

7. Aumento de la flexibilidad

   Probablemente el aspecto más ventajoso de las WLAN's es su flexibilidad. Los usuarios no están atados a sus escritorios por cables y conexiones fisicas, ellos son libres de pasearse por toda la compañía y llevar su PC con ellos. Dentro del rango que la red lo permita, pueden llevar su trabajo hasta el estacionamiento si lo desean. Los administradores de red pueden añadir flexibilidad a su planificación de redes, las WLAN's permiten realizar trabajos que de otra forma serían irrealizables debido a las limitaciones del cableado.

Una WLAN puede integrarse fácilmente en una red de cableado fisico para lograr proveer una red LAN extendida híbrida con cableado e inalámbrica. Las operaciones del usuario en la red son transparentes al cambio y aprovechar muchas ventajas que ofrecen las WLANS.

CAPITULO III
FUNDAMENTOS DE SEGURIDAD WI-FI

Desde el momento en que las redes inalámbricas irrumpieron en la escena, ellas han estado muy relacionadas con la seguridad, o mejor dicho, con la falta de seguridad. Las primeras redes inalámbricas fueron, y con muy buena razón, como dejar un conector sin restricción de acceso a una red en el estacionamiento para uso público.

La seguridad de las redes tradicionales esta enfocada en la asegurar el medio fisico para reducir el riesgo de un ataque a la red, pero la utilidad de las redes inalámbricas se basa precisamente en que el medio no está restringido dentro de unas paredes y puertas. Debe asumir que la capa fisica esta abierta a cualquiera que quiera acceder.

Con un medio de red que ofrece poca seguridad fisica, se debe emplear la criptografia para proteger los procesos de login y el flujo de datos en las conexiones establecidas. La criptografia ayuda a establecer la identidad de usuario, y asegurar que los puntos de acceso sean parte de red que dicen ser. Una vez que un usuario ha sido autenticado, la criptografia asume su mejor rol al hacer que el trafico sea ininteligible para prevenir la intercepción del mismo.

La seguridad de una red esta enlazada a su arquitectura. Las inseguridades fundamentales de las redes 802.11 iniciales condujeron a una arquitectura que impuso barreras fisicas y lógicas entre las redes existentes de cableado fisico y las extensiones inalámbricas.

Informalmente, la seguridad de datos está definida en términos de 3 atributos, los cuales deben mantenerse para garantizar la seguridad.

Integridad: Ampliamente hablando, la integridad esta comprometida cuando los datos son modificados por usuarios no autorizados.

Privacidad: De los tres términos, la privacidad de información es la más fácil de comprender. Todos tenemos secretos y entendemos el efecto de una fuga de información.
Disponibilidad: Los datos solamente son buenos si los puede utilizar. Los ataques de denegación de servicio son las amenazas más comunes para la disponibilidad.

3.1 Encriptación de Datos

En un Sistema de Comunicación de Datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no rechazo de la misma entre otros aspectos. Estas características solo se pueden asegurar utilizando las Técnicas de Firma Digital Encriptada y la Encriptación de Datos.

La Encriptación de datos es el proceso de hacer que la información sea indiscernible para un adversario y la criptografía es el estudio de crear y romper algoritmos de encriptación. Existen dos formas de encriptación ampliamente utilizadas: simétrico y asimétrico. Con la encriptación simétrica, las dos partes comparten una clave secreta que es usada para encriptación y des-encriptación. Con encriptación asimétrica, las dos partes comunicantes, usualmente tienen dos claves, una clave privada para des-encriptación y una clave pública para encriptación. Lo inverso también es cierto. El resultado es esencialmente una firma que puede ser verificada por cualquiera que conozca la clave publica correspondiente.

3.1.1 Métodos de encriptación:

Para poder encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes:
Los algoritmos HASH, los simétricos y los asimétricos.

3.1.1.a Algoritmo HASH:

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC (Código de autenticación de mensaje). Un mismo documento dará siempre un mismo MAC.

3.1.1.b Algoritmos Simétricos:

Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave.

Es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores.

3.1.1.c Algoritmos Asimétricos (RSA):

Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir. El concepto de criptografia de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro.

El usuario, ingresando su PIN genera la clave Publica y Privada necesarias. La clave Publica podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La Privada deberá ser celosamente guardada. Cuando se requiera verificar la autenticidad de un documento enviado por una persona se utiliza la Clave Publica porque él utilizó su Clave Privada.

3.1.2 Firma Digital

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes. Es la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras le dio lugar al concepto. Pero sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas (jurídicas o reales).

Se intenta hacer coincidir el modelo de firma digital con los requerimientos y virtudes que debe tener una firma y así darle validez a esta mecánica. El fin es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado. El papel es el

medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito, etc.). Esta cualidad fisica le da entidad al documento, contiene sus términos, conceptos y sentidos de una manera perdurable, y al ser un elemento fisico cualquier alteración dejará señales identificables.

Pero estas mismas cualidades traen aparejados inconvenientes que el uso de sistemas de computación podría evitar. Ciertamente los papeles ocupan lugar y pesan demasiado, resulta complejo y molesto buscar información en ellos (requiriendo de la acción humana ya sea al archivarlos y/ o al rescatarlos), y el compartir los documentos también resulta inconveniente.

Ventajas Ofrecidas por la Firma Digital

El uso de la firma digital satisface los siguientes aspectos de seguridad:

Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.

No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

3.1.3 Aspectos técnicos

A diferencia de la firma manuscrita, que es un trazo sobre un papel, la firma digital consiste en el agregado de un apéndice al texto original, siendo este apéndice, en definitiva, la firma digital; al conjunto formado por el documento original más la firma digital se lo denominará mensaje. Este apéndice o firma digital es el resultado de un cálculo que se realiza sobre la cadena binaria del texto original.

En este cálculo están involucrados el documento mismo y una clave privada (que, generalmente, pertenece al sistema de clave pública-privada o sistema asimétrico) la cual es conocida sólo por el emisor o autor del mensaje, lo que da como resultado que para cada mensaje se obtenga una firma distinta, es decir, a diferencia de la firma tradicional, la firma digital cambia cada vez con cada mensaje, porque la cadena binaria de cada documento será distinta de acuerdo a su contenido. A través de este sistema podemos garantizar completamente las siguientes propiedades de la firma tradicional: Quien firma reconoce el contenido del documento, que no puede modificarse con posterioridad (integridad). Quien lo recibe verifica con certeza que el documento procede del firmante. No es posible modificar la firma (autenticidad). El documento firmado tiene fuerza legal. Nadie puede desconocer haber firmado un documento ante la evidencia de la firma (no repudio).

Este sistema utiliza dos claves diferentes: una para cifrar y otra para descifrar. Una es la clave pública, que efectivamente se publica y puede ser conocida por cualquier persona; otra, denominada clave privada, se mantiene en absoluto secreto ya que no existe motivo para que nadie más que el autor necesite conocerla y aquí es donde reside la seguridad del sistema.

Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas que algo que es encriptado con la privada, solo puede ser desencriptado por la clave pública.

Resumiendo, la clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma. Si bien no se trata de

un tema estrictamente técnico, es conveniente aclarar que en tiempo de generación de cada par de claves, pública y privada, podría intervenir otra clave que es la de la Autoridad Certificante que provee la garantía de autenticidad del par de claves generadas, así como también, su pertenencia a la persona cuya propiedad se atribuye.

Este esquema se utiliza en intercambios entre entidades cuando se trata de transferencias electrónicas de dinero, órdenes de pago, etc. donde es indispensable que las transacciones cumplan con los requisitos de seguridad enunciados anteriormente (integridad, autenticidad y no repudio del origen), pero no se satisface el concepto de confidencialidad de la información (secreto)

3.2 Protocolo WEP (Wired Equivalent Privacy)

En las redes inalámbricas, la palabra difusión toma un nuevo significado, las redes inalámbricas tienen como base un medio abierto, y el riesgo de acceso no autorizado se incrementa si no se aplica una protección criptográfica en el enlace aéreo. En un medio de red abierto, el tráfico no protegido puede ser visto por cualquiera que tenga el equipo adecuado. En el caso de redes inalámbricas LAN, el equipo correcto es una radio capaz de recibir y decodificar el protocolo 802.11. La protección contra la interceptación de tráfico esta dentro del dominio de los protocolos criptográficos. Dado que las tramas viajan por el aire, se deben proteger contra daño. Existen dos objetivos principales a proteger: la privacidad de los datos y alteración de los mismos. Inicialmente se creó el estándar WEP (Wired Equivalent Privacy) , sin embargo con el tiempo, los expertos lograron demostrar que no es muy seguro, sin embargo es importante conocer WEP porque su modo de operación sirve como base para una nueva tecnología conocida como TKIP.

Para proteger los datos, WEP requiere del cifrado RC4, el cual funciona expandiendo una clave para generar una secuencia de números seudo aleatorios del tamaño del mensaje a transmitir. Esta secuencia de números se unifica con el mensaje mediante una operación XOR (OR exclusivo) para obtener un mensaje cifrado. Para recuperar el mensaje original, el receptor procesa el mensaje cifrado con la misma clave con que fue cifrado mediante una operación XOR. Entonces para recuperar los datos, ambos extremos deben compartir la misma clave y usar el mismo algoritmo para expandir la clave en una secuencia seudo aleatoria.

La seguridad en las comunicaciones tiene tres objetivos principales. Cualquier protocolo que intente asegurar los datos que son transmitidos en una red debe ayudar a los administradores de Redes a cumplir con estos objetivos. Confidencialidad, que es el término para describir que los datos están protegidos de ser interceptados por terceros no autorizados. Integridad que significa que los datos no han sido modificados y Autenticación que es la base de toda estrategia de seguridad porque ofrece la certeza de los datos basados en su origen.

La confidencialidad e integridad son manejadas simultáneamente en el procesamiento WEP. Como se observa en la figura 3.1, antes de la encriptación, la trama es sometida a un algoritmo de chequeo de integridad, que genera un código llamado Valor de Chequeo de integridad (ICV). El ICV protege al contenido contra alteraciones asegurando que la trama no ha cambiado en el tránsito. La trama y el ICV son encriptados luego.

WEP requiere tres datos como entrada:

- La carga útil a ser protegida, la cual proviene de la capa del protocolo superior.
- Una clave secreta, empleada en la trama de encriptación.
- Un vector de inicialización, utilizada por la clave secreta en la transmisión de tramas.

Luego del procesamiento, WEP tiene una sola salida:

- Una trama encriptada, lista para transmitir sobre una red no confiable con suficiente información para que sea desencriptada en extremo remoto.

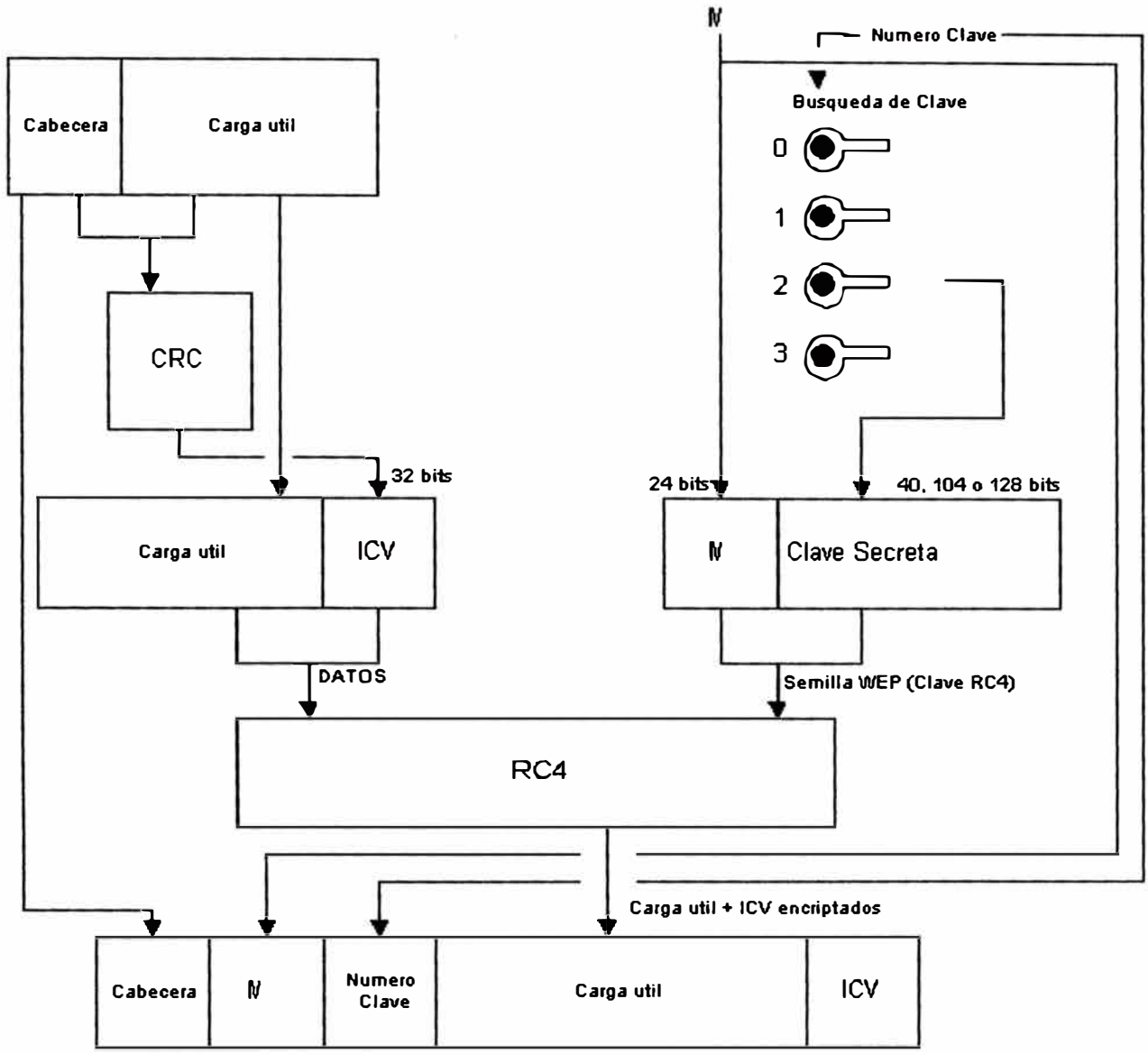

Figura 3.1. Funcionamiento del estándar WEP

3.2.1 Funcionamiento

El funcionamiento es como se describe a continuación:

1. La trama 802.11 es puesta en cola para transmisión. Esta conformada por una cabecera y la carga útil o datos. El estándar WEP solamente protege la carga útil de la capa MAC 802.11 y deja la cabecera así como otras cabeceras de capas nivel inferior intactas.
2. Se calcula un Valor de comprobación de Integridad (ICV) sobre la carga útil de la trama. Este valor ICV empleado por WEP es una Comprobación de Redundancia Cíclica (CRC).

3. Se ensambla la clave de encriptación o semilla WEP. Las claves WEP vienen en dos partes: la clave secreta, y el Vector de Inicialización (IV). La generación del cifrado producirá la misma clave cifrada de una misma clave secreta, entonces se emplea un vector de inicialización para producir diferentes corrientes de cifrado para la transmisión de tramas diferentes. Para reducir la ocurrencia de encriptación con la misma clave cifrada, el transmisor pre-escribe el codigo IV en la clave secreta. El estándar 802.11 no pone ninguna restricción en el algoritmo usado para escoger IV's. Algunos asignan IV's en forma secuencial, mientras que otros utilizan algoritmos seudo aleatorios. La selección de IV tiene implicaciones de seguridad porque la elección de un IV pobre puede comprometer las claves.
4. La clave de encriptación de trama es utilizada como clave RC4 para encriptar la carga útil 802.11 MAC del paso 1 y el ICV del paso 2. El proceso de encriptación es a menudo asistido por chips de la tarjeta Wi-Fi
5. Con la carga útil encriptada en la mano, la estación ensambla la trama final para transmisión. La cabecera 802.11 es retenida en forma intacta. Se inserta una cabecera WEP entre la cabecera MAC 802.11 y la carga útil encriptada. En adición a IV, la cabecera WEP incluye un número clave. WEP permite definir hasta 4 claves, tal que el transmisor pueda identificar que clave se esta utilizando. Una vez que la cabecera final es ensamblada, se puede calcular el valor de Secuencia de Comprobación de trama 802.11 (FCS) sobre toda la trama MAC desde el inicio de la cabecera hasta el final del ICV encriptado.

3.3 Autenticación

El estándar de seguridad WEP tiene dos partes. La primera es la fase de autenticación y la segunda es la fase de encriptación. La idea es la siguiente: cuando un dispositivo móvil desea unirse a un punto de acceso, primero debe probar su identidad. Idealmente, el dispositivo móvil debe pedir al punto de acceso que también pruebe su identidad. Esta fase es conocida como autenticación de la identidad de ambas partes. El propósito de la autenticación es probar que cada uno es quien dice ser.

Los sistemas deben usar la autenticación para proteger los datos apropiadamente. La autorización y control de acceso son implementados en la etapa de autenticación. Antes

de otorgar acceso a los datos, el sistema debe saber quien es el usuario (autenticación) y si la operación de acceso es permitida (autorización).

Como se mencionó anteriormente, el estándar 802.11 usa tres tipos de mensajes: de control, administración y datos. La fase de autenticación usa tramas de administración.
Se pueden utilizar dos métodos de autentificación: mediante Sistema Abierto o mediante Clave Compartida.

En el sistema abierto, el dispositivo móvil envía un mensaje solicitando autenticación y el Punto de Acceso responde con un mensaje de confirmación (exitoso).

En el sistema de Clave Compartida, ocurre un intercambio de 4 mensajes:

1. El dispositivo móvil (o estación cliente) envía una petición de autentificación al Punto de Acceso.
2. El punto de acceso envía de vuelta un texto modelo.
3. El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada, y reenviarlo al Punto de Acceso en otra petición de autentificación.
4. El Punto de Acceso descifra el texto codificado, y lo compara con el texto modelo que había enviado. Dependiendo el éxito de esta comparación, el Punto de Acceso envía una confirmación o una denegación. Después de que la autentificación sea aceptada, ya se puede emplear WEP para cifrar los paquetes de datos.

3.4 WPA (Wi-Fi Protected Access)

WPA (Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas Wi-Fi; creado para corregir las deficiencias del sistema previo WEP. Dado que se han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

WPA fue diseñado para utilizar un servidor de autentificación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo

802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida ([PSK] - Pre-Shared Key) para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits.

WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

Para el uso personal o doméstico: El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

Para el uso en empresarial o de negocios: El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor RADIUS.

Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. La comprobación de redundancia cíclica (CRC - Cyclic Redundancy Check) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar la CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - Message Integrity Code), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más dificil. El algoritmo Michael fue él más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debían funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

3.4.1 WPA2

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i. El estándar 802.11i fue ratificado en Junio de 2004.

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad que la tecnología cumple con estándares de

interoperatividad" declaró Frank Hazlik Managing Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP (ver arriba). AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 será compatible tanto con la versión para la empresa como con la doméstica.

La tecnología SecureEasySetup™ (SES) de Linksys o AirStation OneTouch Secure System™ (AOSS) de Buffalo permite al usuario configurar una red y activar la seguridad de Acceso protegido Wi-Fi (WPA) simplemente pulsando un botón. Una vez activado, SES o AOSS crea una conexión segura entre sus dispositivos inalámbricos, configura automáticamente su red con un Identificador de red inalámbrica (SSID) personalizado y habilita los ajustes de cifrado de la clave dinámico de WPA. No se necesita ningún conocimiento ni experiencia técnica y no es necesario introducir manualmente una contraseña ni clave asociada con una configuración de seguridad tradicional inalámbrica.

3.5 Protocolo de Integridad de Clave Temporal (TKIP)

El primer protocolo nuevo de encriptación de la capa de enlace ampliamente utilizado fue el Protocolo de Integridad de Clave Temporal (TKIP). El motivo principal para el desarrollo de este protocolo fue actualizar la seguridad del Hardware basado en WEP. Típicamente, los circuitos basados en WEP son capaces de soportar encriptación RC4. Con gran parte de la encriptación basada en Hardware, las actualizaciones de Software y Firmware hacen posible el resto. TKIP mantiene el funcionamiento y la arquitectura básica de WEP porque fue diseñado para ser una actualización de software de soluciones basadas en WEP.

Para comprender mejor la necesidad de actualizar los sistemas WEP existentes daremos una vista al interno de los sistemas LAN Wi-Fi. Esencialmente una tarjeta LAN Wi-Fi tiene 4 partes:

- Sección de Radio Frecuencia (RF)
- Sección del MODEM
- Sección de MAC (Control de Acceso al medio)
- Interfase para conectar al computador (PCMCIA o USB por ejemplo)

A grandes rasgos, la sección RF se encarga de la transmisión y recepción de la señal por medio de la antena, el módem extrae los datos de la señal recibida, la sección MAC se encarga del protocolo, incluyendo la encriptación WEP.

Con el avance de la tecnología y la tendencia de miniaturización, estas secciones se han ido integrando en unos cuantos circuitos integrados. La parte que deseamos analizar es la sección MAC de estos circuitos integrados, que es el lugar donde se implementa gran parte del protocolo 802.11. Por un lado (Interfase de computador) recibe desde el computador, paquetes de datos e instrucciones para actividades como "buscar un nuevo punto de acceso (AP)" o "solicitar una conexión para tal AP". También entrega datos recibidos al computador. Por otro lado (la parte del módem) entrega una corriente de bits que contienen varias tramas IEEE 802.11 de control y datos, incluyendo funciones especiales como modos de inactividad, confirmación de datos, retransmisión de datos perdidos, y lo más importante para nosotros, también encripta y desencripta las tramas de datos.

Dado que las operaciones de la sección MAC son más complejas, todas las implementaciones se construyen sobre un pequeño microprocesador incluido en el circuito integrado. El microprocesador es programado para manejar todas las operaciones de formateo y temporización para controlar el protocolo. Sin embargo este procesador no es muy potente y ciertas operaciones son demasiado rápidas para manejar. De ahí que la sección MAC es implementada como una combinación de firmware y hardware.

Existe un bloque llamado Hardware Assist, su funcionamiento se puede comparar como sigue: si uno desea comprar pan en la tienda puede caminar, pero si desea ir a 100Km/h necesita un automóvil, del mismo modo MAC necesita del Hardware Assist. Los

pequeños procesadores incluidos en las tarjetas Wi-Fi fabricadas entre 1997 y 2003 necesitaban ayuda para llegar a la velocidad de 11Mbps, y esta viene en forma de hardware personalizado dentro del circuito integrado.

Si todas las funciones MAC fueran realizadas solamente por el microprocesador, sería posible cambiar la seguridad actualizando solamente el firmware. Sin embargo, dado que la encriptación y desencriptación requieren un poco mas de computación, la implementación de WEP depende casi siempre de las funciones del Hardware Assist. Y, por supuesto, estas funciones no pueden cambiarse después de la fabricación.

Ahora se puede ver porque el TKIP es necesario.

3.5.1 Diferencias entre TKIP y WEP

TKIP añade muchos "cinturones de seguridad" alrededor de los puntos más vulnerables de WEP:

- Jerarquía de Claves y Administración automática de claves

  En lugar de utilizar una sola clave maestra como WEP, TKIP usa claves maestras. Las claves que son usadas para encriptar tramas son derivadas de estas claves maestras. TKIP incluye con operaciones de manejo de claves tal que las claves maestras pueden refrescarse de manera segura.

- Claves por trama

  A pesar de que TKIP mantiene la encriptación de WEP basada en RC4, deriva una única clave RC4 para cada trama (desde la clave maestra) para mitigar ataques contra claves WEP débiles. Este proceso es llamado Mezclado de claves.

- Contador de secuencia

  Numerando cada trama con un número de secuencia, se pueden marcar tramas fuera de orden, mitigando ataques de repetición de tramas, en el cual los atacantes capturan tramas válidas y las retransmiten posteriormente.

- Nuevo chequeo de Integridad de mensaje

  TKIP reemplaza la generación aleatoria lineal de WEP con un algoritmo de chequeo de integridad criptográfico más robusto llamado Michael. Esto permite detectar fácilmente falsas tramas. Adicionalmente, la dirección origen esta dentro de los ítems protegidos por el chequeo de integridad, lo cual hace posible detectar tramas falsificadas que reclaman provenir de algún origen particular.

- Contramedidas sobre fallas de chequeo de integridad de Mensajes
  TKIP fue diseñado para ser implementado sobre hardware existente, y sufre de limitaciones. El algoritmo Michael puede verse comprometido con un ataque activo con relativa facilidad, entonces TKIP incluye contramedidas para limitar el daño desde un ataque activo.

3.5.2 Vector de Inicialización TKIP y uso de Mezclado de Claves

La generación de la semilla WEP a partir del vector de inicialización (IV) y la clave WEP son las que introducen las principales debilidades. Simplemente concatenando el Vector de Inicialización y la clave para generar la semilla, el IV mismo revela una cantidad significativa de la estructura de la clave. Los atacantes pueden reconocer la reutilización del IV y por ende, notar que la corriente clave usada para encriptar la trama es idéntica. Con un IV de 24 bits, el espacio IV alcanza para 24 millones de tramas. En una red congestionada, 16 millones de tramas no es mucho. Para empeorar las cosas, el espacio IV es específico para el entorno de la clave en uso. En una red que utiliza WEP estático, el IV es compartido por todas las estaciones de la red. Finalmente, y esto es lo mas conocido, el IV es los 24 bits iniciales de la clave, y hace que las claves WEP sean fáciles de recuperar con el ataque conocido como Fluher/Mantin/Shamir (FMS).

Para mitigar los ataques contra los Vector de Inicialización, TKIP duplica la longitud de IV de 24 a 48 bits, Esto incrementa el tamaño del espacio del vector de inicialización de 16 a 281 trillones, el cual previene efectivamente agotar el espacio IV durante el limitado tiempo de vida de la clave.

TKIP también realiza un mezclado de claves para contar los ataques contra WEP. El mezclado de claves cambia la clave RC4 usado para encriptar cada trama. Cada trama en TKIP es encriptada con una clave RC4 única. El mezclado de clave extiende el espacio del vector de inicialización. Incorporando la dirección MAC del transmisor en los cálculos del mezclado, dos estaciones pueden usar el mismo IV, aunque se deriven de diferentes claves RC4 para encriptar las tramas. El mezclado de claves permite contar los ataques FMS. Una aplicación exitosa de los principios de un ataque requiere una colección de claves débiles que contengan los mismos bits secretos. Cambiando la clave para cada

trama, TKIP previene que un atacante coleccione suficientes datos para atacar cualquiera de las claves por trama.

3.5.3 Contador de Secuencia TKIP y protección contra reenvío

Adicionalmente a su gran tamaño, el vector de inicialización TKIP sirve como un contador de secuencia. Cuando se instala una nueva clave maestra, el IV / contador de secuencia es puesto en uno. Cada trama transmitida incrementa el contador en uno.

Para defenderse contra ataques de reenvío, TKIP mantiene el número de secuencia mas reciente recibido de cada estación. Cuando se recibe satisfactoriamente una trama, se chequea el contador de secuencia contra el contador de secuencia recientemente recibido. Si es mayor que cualquier valor previamente recibido, la trama es aceptada. Si es menor, la trama es rechazada.

Las tramas unicast 802.11 deben ser reconocidas. Si la trama original o su reconocimiento se pierde, la trama será retransmitida. Como receptor, esto puede resultar en que se reciba el mismo contador de secuencia dos veces. Este duplicado simplemente puede evidenciar un error en el enlace y no necesariamente indica un ataque en progreso.

3.5.4 Chequeo de Integridad MICHAEL y contramedidas

El chequeo de integridad WEP es un valor aleatorio lineal, que es totalmente inadecuado para aplicaciones criptográficas. Uno de los mayores retos enfrentados por TKIP fue reforzar el chequeo de integridad manteniendo un rendimiento razonable. La mayoría de los chips basados en 802.11 existentes en el mercado en el momento en que TKIP fue desarrollado, utilizan un procesador de potencia relativamente baja, entonces no son capaces de realizar operaciones matemáticas lo suficientemente rápidas para efectuar chequeos de integridad a alta velocidad. El algoritmo Michael es implementado íntegramente con operaciones inteligentes a nivel de bit, tales como conmutaciones, intercambios, inclusive con descarte de bits. Como resultado, puede ejecutarse sin afectar el rendimiento, aun en diminutos procesadores halladas en la mayoría de interfaces 802.11.

El corolario para el diseño de Michael es que no provee una garantía total de seguridad. Es significativamente mejor que un chequeo de Redundancia Cíclica, pero no ofrece seguridad contra ataques sostenidos y determinados. TKIP incorpora contramedidas para detectar y responder a un ataque activo, mediante las cuales desactiva la red y refresca las claves en uso.

CAPITULO IV
VULNERABILIDADES

En el pasado, la seguridad de las redes fue desarrollada basada asumiendo que el núcleo de la red no sería físicamente accesible al enemigo. Las personas dentro del edificio eran consideradas amigos, y se espera que estos amigos supervisaran a los visitantes. Se esperaban los ataques solamente desde lugares conocidos como por ejemplo la conexión externa hacia Internet donde se colocaron Firewalls. Las redes Wi-Fi cortaron de raíz esas presunciones. El uso de radio propagación es invitar a cualquiera que este alrededor, amigo o enemigo, a conectarse a la Red. Este nuevo escenario totalmente abierto requiere cambiar el pensamiento acerca de la seguridad en una Red LAN e introduce nuevos retos. Las redes Wi-Fi son vulnerables porque no trabajan de acuerdo a las antiguas reglas.

Otra vulnerabilidad surge del hecho de que la recepción clandestina de la señal puede llevar a descubrir brechas en la red. Uno puede creer que no tiene nada que esconder y que no están haciendo nada secreto. Sin embargo, todos deben cuidarse de la intrusión del enemigo en la red, porque puede borrar información o implantar un virus. Actualmente estas dos amenazas no pueden separarse. Si se permite una escucha pasiva de la señal, se expone a ataques activos.

4.1 Como es el enemigo

Los medios populares de comunicación como la TV, la radio y los periódicos hicieron famoso el término Hacker para señalar a un intruso en la red capaz de dañar o sustraer información.

Desde el punto de vista de seguridad, todo visitante no bienvenido en la Red debe ser clasificado como enemigo potencial sin importar su motivación o habilidad. El enemigo tiene las opciones de donde y cuando atacar. La responsabilidad de las políticas de seguridad es anticipar estas posibilidades y el trabajo de los protocolos de seguridad es

bloquear estos ataques. Anticiparse correctamente a todas las opciones es uno de los retos para un buen nivel de seguridad.

Casi todos los ataques pueden explicarse por una de las siguientes motivaciones:

- Juego: Un hacker apuesta su tiempo y esfuerzo con el fin de lograr un ataque exitoso. Muchos juegos y deportes se basan en motivaciones similares.
- Venganza o Lucro: El atacante desea robar información, dañar un sistema por venganza, o alterar un sistema para adquirir una recompensa tangible.
- Ego: El hacer desea probarse a sí mismo que el mejor en comparación con sus similares.

Comprendiendo la motivación y recursos de los atacantes, se puede establecer una política de defensa. Algunas personas pueden argumentar que su política siempre debe incluir el número máximo de medidas defensivas y nunca comprometer la seguridad. Pero esto es muy simple. Recordemos que la mejor regla de seguridad inalámbrica es no usar una LAN Wi-Fi. Tal como la mejor seguridad en la calle es quedarse en casa. Sin embargo la práctica demuestra que en el uso de redes Wi-Fi existen beneficios reales y una política efectiva balancea el riesgo y la utilidad.

Se definen dos estrategias para el manejo del riesgo de seguridad. Una es tratar a todas las conexiones inalámbricas como si estuvieran fuera del Firewall, esto es completamente no confiables. Esto es un enfoque costoso en términos de equipamiento y rendimiento, pero cabe muy bien dentro de la arquitectura de seguridad existentes. La segunda es tratar a las LAN Wi-Fi como componente confiable. Esto requiere confiabilidad en la integridad del método de seguridad Wi-fi.

4.2 Tipos de Ataque

Los ataques se pueden clasificar en 4 categorías: intrusión, modificación, enmascaramiento y denegación de servicio. Casi todos los ataques empiezan con una intrusión.

4.2.1 Intrusión. Como su nombre lo sugiere, es simplemente acceder a información privada. Esta información puede ser utilizada en provecho propio, tal como obtener secretos de la empresa. Puede utilizarse para asaltos activos como correo indeseable. Se

puede utilizar la encriptación para hacer dificil la intrusión. El atacante requiere saber la clave de encriptación o utilizar alguna técnica avanzada para recuperar la data encriptada.

4.2.2 Modificación. Se puede modificar los datos de varias maneras no obvias. Cuando se piensa acerca de ataques de modificación, la mayoría se imagina a un atacante modificando correo electrónico con contenido malicioso o cambiando los números de una transferencia electrónica de un banco. Mientras que estas modificaciones de alto nivel son complicadas, existen formas más sutiles de modificar datos. Por ejemplo si se intercepta una transmisión inalámbrica y cambia el campo de dirección destino (dirección IP) en un mensaje, puede causar que el mensaje sea enviado a uno a través de Internet en lugar de los destinatarios originales. ¿Porque uno desearía hacer esto? Porque el mensaje en el enlace inalámbrico esta encriptado y no se puede leer el contenido, pero si logra reenviarlo a través de internet, recibirá una versión desencriptada. La cabecera IP es más fácil de atacar porque esta en un formato conocido.

4.2.3 Enmascaramiento. Es el término usado cuando un dispositivo atacante en la red, imita a una dirección válida. Es el enfoque ideal si un atacante quiere pasar inadvertido en la red. Si el dispositivo puede engañar a la red destino validándose como un dispositivo autorizado, el atacante obtiene todos los derechos de acceso que el dispositivo autorizado estableció durante el logon. Mas aún, no habrá advertencias de seguridad. Inclusive un Gerente IT con ojo de águila escudriñando los registros de tráfico, no podrá ver nada a menos que el atacante haga algo anormal como intentar acceder a las áreas del sistema.

4.3 Denegación del Servicio (DoS).

Es bastante diferente de las otras categorías tanto en técnicas como en objetivos. Mientras que las clasificaciones anteriores intentan obtener privilegios extra para el atacante. Un ataque DoS usualmente bloquea todo, inclusive al mismo atacante. El objetivo es causar daño en el destino previniendo la operación de la red. En el 200, el más grande ataque tipo DoS aún publicado ocurrió contra los principales sitios de Comercio Web, este ataque bloqueó el acceso a estos sitios por horas. El ataque se originó desde miles de computadores de todo el mundo controlados remotamente, cuyos propietarios desconocían su participación. Los atacantes emplearon estos computadores Zombis para generar grandes cantidades de tráfico orientado hacia sus víctimas, evitando que puedan atender

peticiones válidas. ¿Porque lo hicieron? Talvez por ganar prestigio entre los demás hackers, esto corresponde la motivación del atacante por Ego.

En principio los ataques tipo DoS podrían montarse por motivos comerciales, tumbarse estos sitios de comercio Web puede infligir daños financieros en una empresa de la competencia, pero es dificil de creer que las grandes empresas hagan uso de estas tácticas. Es más plausible que un ataque de este tipo venga de un ex-empleado con cierto resentimiento hacia la empresa. Los ataques DoS son dificiles de prevenir en Internet y usualmente intentan agotar los recursos de búfer del servidor receptor de tal forma que no pueda aceptar ninguna conexión válida por un periodo de tiempo. Desafortunadamente, los ataques DoS son fáciles de montar en Wi-Fi y casi imposibles de prevenir.

El enemigo puede usar exitosamente alguno de esos ataques sin tener acceso a la clave secreta de la red. Sin embargo en la mayoría de los casos, el daño que puede hacerse sin conocer las claves es bastante limitado. Si el atacante puede descubrir las claves, entonces uno se mueve a una categoría diferente de peligro. Pueden ocurrir modificaciones no autorizadas a los sitios Web y el robo de Base de datos llenas de detalles de tarjetas de crédito debido a que alguien logró descubrir las claves.

4.4 Ataque del falso intermediario

También conocido como ataque del hombre en el medio ("Man in the middle"). Suponga que dos personas están comunicándose, llámense Juan y Pedro. Pedro recibe mensajes de Juan y Juan recibe mensajes de Pedro. Suponga que hay un atacante capaz de interceptar y cortar las comunicaciones. Suponga que este atacante es capaz imitar a Juan mientras se esta enviando mensajes a Pedro e imitar a Pedro mientras se envía mensajes a Juan. En este caso se dice que Juan y Pedro están sujetos a un ataque del hombre en el medio. Tales ataques pueden emplearse para modificar mensajes en transito sin detección.
Existen al menos dos formas de modificar un mensaje: modificarlo en plena transmisión o puede capturar, modificar y reenviar el mensaje, una técnica conocida como almacenar y reenviar. La modificación en plena transmisión es realmente dificil. Necesitaría enviarse un chorro de paquetes de radio transmisión en el momento preciso para ocasionar que el receptor interprete incorrectamente un bit. Debido a la modulación sofisticada usada en las

redes Wi-Fi, los bits son enviados en grupos, codificados, haciendo muy difícil cambiar un bit en el momento de la transmisión.

El método de almacenar y reenviar es llamado el ataque del hombre en el medio. El principio es bastante simple en las redes de cableado: un atacante corta el cable recibe todos los datos, y es cuidadoso de enviarlo de tal modo que los dos dispositivos en los extremos no saben que sus datos están siendo interceptados. Hay, por ejemplo, una posibilidad de ataque del tipo hombre en el medio en cada ruteador de reenvío en Internet, la cual es una razón por la que Internet sea tratado como totalmente inseguro.

En las redes Wi-Fi un ataque del tipo hombre en el medio es un poco más difícil de montar porque no existe un cable que cortar. El enemigo debe detener al receptor de recibir la transmisión inicial, tal que pueda reenviarlo luego de aplicar su malvada intención. El procedimiento puede trabajar como se describe a continuación. Para ser un hombre en el medio entre un dispositivo móvil y un Punto de Acceso el enemigo debe:

1. Escuchar el mensaje del dispositivo móvil hacia el Punto de Acceso
2. Leer en el mensaje el código de comprobación del mismo (Este código es usado por el receptor para detectar errores en los datos)
3. Transmitir un chorro repentino de ruido para corromper el código de comprobación, esto causara que el Punto de Acceso considere el mensaje como inválido y lo descarte, pero el atacante ahora tiene una copia válida del mensaje.
4. Falsificar un mensaje de Reconocimiento con la dirección del Punto de Acceso y enviarlo al dispositivo móvil; Este último piensa que el mensaje ha sido recibido por el Punto de Acceso.
5. Recalcular el código correcto de comprobación y enviar el mensaje capturado al Punto de Acceso; Este último lo tomará como mensaje desde el dispositivo móvil.
6. Esperar por un mensaje de reconocimiento desde el Punto de Acceso y enviar un paquete de ruido al dispositivo móvil tal que este lo ignore y no reciba dos mensajes de reconocimiento por el mismo paquete.

Claramente, este procedimiento no es simple, pero es absolutamente posible y efectivamente podría colocar al atacante en el medio de las comunicaciones. Ni el Punto de

Acceso ni el dispositivo móvil tendrían alguna idea que las comunicaciones han sido intervenidas.

Otro enfoque, y uno que es mucho más posible de que ocurra, es que el enemigo establezca un punto de Acceso falso. Cuando un dispositivo móvil esta buscando conectarse a la Red, encuentra al Punto de Acceso falso y trata de asociarse, este último simplemente copia los mensajes que recibe hacia un Punto de Acceso válido, substituyendo su propia dirección MAC. De manera similar, copia todos los mensajes provenientes del Punto de Acceso válido hacia el dispositivo móvil. Mediante este método no necesita conocer las claves de encriptación porque los campos de dirección MAC que este modifica no están encriptados. Como resultado, todos los datos entre el dispositivo móvil y el Punto de Acceso pasan a través del Punto de Acceso falso.

CAPITULO V
COMPARACIÓN DE MODOS DE SEGURIDAD EN REDES WI-FI

5.1 Seguridad WEP

En redes Wi-Fi, el concepto de la seguridad se extiende más allá de lo que representaba en redes cableadas. El hecho de poder acceder a tráfico de red sensible sin ser necesaria una presencia física, obliga a extremar las medidas de seguridad en entornos corporativos.

Por ello, el primer estándar Wi-Fi (802.11b) incorpora desde su origen un sistema de seguridad denominado WEP (Wired Equivalent Privacy), basado en la encriptación de la información. De todas formas, la popularización de las redes Wi-Fi puso de manifiesto ya en sus inicios que WEP presentaba una serie de vulnerabilidades, debido principalmente al uso de claves estáticas de pocos bits y a un sistema de autenticación débil, que lo hacían poco útil para redes corporativas.

Para contrarrestar estos problemas aparecieron en el mercado soluciones basadas en dos enfoques complementarios:

- Autenticación 802.1x con claves dinámicas más largas.
- Redes privadas virtuales (VPN) entre los clientes inalámbricos y la red local.

5.2 Seguridad WPA

Si bien la utilización de estas alternativas proporcionaba una primera solución al problema de la seguridad en redes inalámbricas, también presentaban una serie de desventajas que las hacían poco viables, como:

- Desarrollos propietarios.
- Nivel de seguridad limitado intrínsecamente por la debilidad de WEP.
- Poca escalabilidad.

Para dar una respuesta final a este problema, el IEEE comenzó en 2002 a desarrollar un nuevo estándar de seguridad para redes Wi-Fi, denominado 802.11i, con el objetivo de que cumpliera todos los requisitos de seguridad necesarios para ser aplicable tanto en entornos corporativos como en entornos PYME y domésticos. Este estándar fue aprobado en el Q1 del 2004.

El hecho de que 802.11i no esté disponible hasta bien entrado el 2004, unido a la presión del mercado, hizo que la Wi-Fi Alliance se adelantara al IEEE promoviendo entre los principales fabricantes un estándar de-facto, el WPA (Wi-Fi Protected Access), que quedó definido a principios de 2003. Este estándar cumple una serie de requisitos básicos:

- Compatible con el futuro 802.11i
- Seguridad fuerte para entornos corporativos y pequeños
- Disponible como actualización software en los equipos existentes

A continuación se presenta un esquema con la comparación entre los tres estándares de seguridad existentes:

	WEP	**WPA**	**802.11i (WPA2)**
Algoritmo de cifrado	RC4	RC4 (TKIP)	Rijndael (AES-CCMP
Clave de encripción	40 bit	128 bit (TKIP)	128 bit (CCMP)
Vector de Inicialización	24 bit	48 bit (TKIP)	48 bit (CCMP)
Clave de Autenticación	Ninguna	64 bit (TKIP)	128 bit (CCMP)
Chequeo de Integración	CRC-32	Michael (TKIP)	CCM
Distribución de Clave	Manual	802.1x (EAP)	802.1x (EAP)
Clave única para:	Red	Paquete, sesión, usuario	Paquete, sesión, usuario
Jerarquía de clave	No	Derivado desde 802.1x	Derivado desde 802.1x
Negociación de cifrado	No	Si	Si

Tabla 5.1 Estándares de seguridad inalámbrica

Como se puede ver, WPA incorpora un nuevo sistema de encriptación (TKIP) y de autenticación y distribución de claves (802.1x). Desde Septiembre de 2003, la mayoría de nuevos equipos Wi-Fi ya soportan este estándar.

5.3 Autenticación de clientes de red

Como hemos comentado, la autenticación en entornos WPA corporativos se basa en 802.1x. Este estándar no define qué autenticación se utilizará, sino cómo se realizará la negociación concreta de una autenticación determinada. Es el protocolo EAP (Extensible Authentication Protocol), incluido en el estándar 802.1x, el que define el procedimiento para realizar esta negociación. Esto permite que la autenticación en entornos WPA soporte varios métodos diferentes, cada uno con sus propias ventajas e inconvenientes. La clave al implantar WPA en una red Wi-Fi consiste en decidir el tipo de autenticación que se utilizará, ya que esto determinará los componentes necesarios para ponerla en marcha.

Existen multitud de métodos EAP especificados (alrededor de 40), siendo los más comunes en la actualidad los siguientes:

- EAP-TLS
- EAP-TTLS
- PEAP

En la siguiente figura se observan las principales diferencias entre los tres:

	EAP TLS (RFC-2716)	**TTLS**	**PEAP**
Software			
Implementaciones Cliente	Cisco, Funk, Meetinghouse, Microsoft, Open Source	Funk, Meetinghouse	Microsoft
Plataformas Cliente soportadas	Linux, Mac OS, Windows NT/2000/XP	Linux, Mac OS, Windows NT/2000/XP	Windows XP
Implementaciones de autenticación en servidor hechas por:	Cisco, Funk, HP, FreeRadius,soft, Open Source	Funk, Meetinghouse	Cisco
Operaciones de Protocolo			
Estructura básica de protocolo	Establece sesión TLS y valida certificados en Cliente y Servidor	Dos fases (1) Establece sesión TLS entre Cliente y	Dos partes (1) Establece sesiones TLS entre el Cliente

		Servidor (2) Intercambia valores de atributos pares entre Cliente y Servidor	y servidor EAP (2) Ejecuta intercambio EAP sobre túnel TLS
Reconexión rápida de sesión	No	Si	Si
Integración WEP	El servidor puede proporcionar clave WEP mediante protocolo externo (por ejemplo RADIUS)		
Procesamiento de Certificados			
Certificado de Servidor	Requerido	Requerido	Requerido
Certificado de cliente	Requerido	Opcional	Opcional
Autenticación de usuario y Cliente			
Dirección de autenticación	Mutuo: usa Certificados digitales en ambos sentidos	Mutuo: Certificado para autentificación de Servidor, y método de Túnel para Cliente	Mutuo: Certificado para Servidor, y método de protección EAP para Cliente
Protección de intercambio de identidad de usuario	No	Si, protegido por TLS	Si, protegido por TLS

Tabla 5.2 Esquemas de autenticación más comunes

Para redes pequeñas y / o domésticas, el estándar WPA también contempla un modo de funcionamiento especial (WPA-PSK) que permite evitar la utilización de un servidor RADIUS y el protocolo 802.1x-EAP correspondiente. Este modo utiliza claves preasignadas (pre-shared keys) localmente en los puntos de acceso y en los clientes de red para realizar la autenticación. Una vez realizada ésta, la encriptación y el cambio dinámico

de claves se efectúan de la misma manera que ya se ha comentado (vía TKIP), lo que permite un nivel de seguridad muy superior al conseguido vía WEP a la vez que la dificultad en la implantación resulta mínima.

5.4 Protección de una Red existente

Las redes inalámbricas WI-FI, son altamente inseguras y ofrecen muchas facilidades a los intrusos potenciales. Temas como el de los Puntos de Acceso Hostiles y las Conexiones WI-FI Incontrolables son un buen ejemplo de ello. En la actualidad la tecnología que existe, como los Switches WLAN / Controladores WI-FI no es perfecta y, además es muy cara y no está al alcance de la mayoría de los usuarios. Como es sabido, la seguridad informática, y mucho más la seguridad WI-FI, no se logra sólo con tecnología. Las políticas y la capacitación de los usuarios desempeñan un papel fundamental en el logro de los objetivos.

El NIST (National Institute of Standards and Technology), ha publicado un muy completo documento sobre la implementación de redes inalámbricas WI-FI en las dependencias del gobierno de USA y entre sus recomendaciones principales está la de desarrollar políticas de seguridad para redes inalámbricas antes de comprar los equipos. Esta recomendación es precisamente la que nadie cumple. La mayoría de las empresas primero se dedican a comprar tecnología Wi-Fi y luego, cuando ven los problemas, se dan cuenta que necesitan establecer políticas que regulen y controlen la utilización de las redes inalámbricas WI-FI .

En otro interesante documento publicado por la oficina del contralor de USA (GAO - Government Accountability Office) se estipula que "Hay que reconocer que el desarrollo de políticas es esencial para reducir de una manera económica el riesgo a la información debido al uso de las redes inalámbricas Wi-Fi"

Las políticas que hay que establecer para la utilización de las redes inalámbricas Wi-Fi, se refieren a:

1. Viajeros frecuentes de la organización: Se debe estipular la manera correcta de utilizar los recursos Wi-Fi cuando se está por fuera de la organización.

2. Visitantes: Son muchos los temas a decidir. ¿Pueden utilizar su máquina en nuestra red Wi-Fi? A qué servicios pueden acceder?, etc.
3. Vigilancia: ¿Se pueden ingresar Access Points a la empresa sin autorización?
4. Temas laborales: ¿Pueden los empleados traer Puntos de Acceso Inalámbricos sin autorización? ¿Pueden utilizar sus equipos Wi-Fi (notebooks, PDAs, etc.) particulares?

5.5 Políticas de Seguridad y Gestión en Redes Inalámbricas WI-FI

A continuación se detallan, brevemente, algunas políticas relevantes que se aconseja establecer en las empresas e instituciones.

- Verificar que los usuarios están debidamente entrenados en el uso de la tecnología WI-FI y conocen los riesgos asociados con su utilización
- Cambiar el SSID por defecto
- Desactivar la difusión del SSID
- Verificar que el SSID no contenga datos de la organización
- Política de instalación de parches en el Punto de Acceso y clientes WI-FI
- Auditar periódicamente que los Puntos de Acceso no hayan sido reseteados
- Política de contraseñas para Puntos de Acceso y clientes
- Política de configuración de los Punto de Acceso
- Cómo configurar los suplicantes y proteger la configuración con contraseña, si es posible
- Auditorias periódicas de la red inalámbrica Wi-Fi

El diseño de Arquitecturas de seguridad no es un trabajo fácil. Demanda mucho cuidado, experiencia y conocimiento, al margen del cambio de tecnologías, se puede definir tres principios clave para las arquitecturas de seguridad:

1. Aislar tráfico potencialmente hostil del tráfico sensitivo
2. Canalizar tráfico potencialmente hostil a través de un pequeño conjunto de puntos de entrada fijos estén bien protegidos y monitoreados.
3. Utilizar defensas por capas siempre que sea posible.

Se puede reconocer a estos principios como directrices que se aplican a conexiones a Internet. El Firewall es una implementación de estos principios. Aísla y canaliza tráfico a través de un punto fijo, y puede aplicar capas adicionales de seguridad a través del uso de redes privadas virtuales o mecanismos adicionales de autenticación.

Sin embargo, las redes inalámbricas son más dificiles de proteger que una conexión a Internet. Mientras que una conexión a Internet ingresa a la empresa a través de unos cuantos puntos fijos, los puntos de acceso inalámbricos deben instalarse a lo largo de toda la empresa para proveer áreas de cobertura razonables.

Podríamos pensar en cada punto de acceso como un Firewall, ciertamente se cumplirían nuestros objetivos, pero introduciría horrendos problemas de administración en la empresa y no puede ser la mejor solución en todas las situaciones. Sin embargo, para escenarios SOHO (Pequeña Oficina / Oficina en el hogar), puede tener cierto sentido porque solamente existe un punto de acceso.

Una buena arquitectura de seguridad debe balancear las amenazas, el valor de la información y los costos (económicos y administrativos) en el diseño de la arquitectura. Mientras que la solución de convertir cada Punto de Acceso en un Firewall cumple los criterios de diseño, introduce serios problemas de administración. Como resultado se debe seleccionar cuidadosamente el equipamiento. Puede obtener ventaja trabajando en conjunto con el vendedor o distribuidor con valor añadido en la selección del equipamiento. No se debe aceptar a ciegas las afirmaciones del vendedor o sus integradores de que los equipos son seguros. Se debe ser diligente con el vendedor, especialmente si ofrece soluciones propietarias. Pregunte quien ha revisado la solución, y solicite detalles de la misma para que sea revisada por personal de su empresa. En estos días hay pocas razones para utilizar soluciones propietarias porque WPA y RSN ofrecen protección suficientemente robusta para casi todas las organizaciones. Y si se desea extremar medidas, se puede añadir seguridad usando protección a nivel de capas superiores, tal como VPN.

Si ya cuenta con una Red inalámbrica desplegada en la empresa, necesita seguir varios pasos para asegurarse que este protegida. Primero aplicar los principios de diseño

mencionados anteriormente: aislar y canalizar el tráfico. Segundo, actualizar el firmware del equipo a WPA.

5.5.1 Aislar y Canalizar tráfico

Aislar el tráfico de los puntos de acceso puede ser el aspecto más difícil de intentar reforzar la seguridad en la red a menos que los puntos de acceso se encuentren en el mismo segmento LAN.

Esencialmente se tiene dos opciones. La primera es instalar un nuevo cableado entre los puntos de acceso para colocarlos en el mismo segmento LAN sin tráfico adicional de la empresa. La segunda es usar los switches actuales para crear una LAN Virtual (VLAN / IEEE 802.10) para aislar los equipos inalámbricos. La primera opción no es óptima en términos de tiempo y costos, dado que requiere trabajo adicional e inversión. La segunda opción es relativamente menos penosa si el equipamiento soporta VLAN's. Si no cuenta con estos últimos, se debe decidir entre comprar nuevos switches o el tendido de nuevo cableado. Una VLAN ofrece un grado moderado de aislamiento. Sin embargo el aislamiento no es completo si los switches son atacados con una emulación ARP u otros medios. Pero la protección que provee una VLAN es mejor que permitir que el tráfico de los puntos de acceso conviva con el tráfico del resto de la organización.

Una vez aislado el tráfico, es fácil de canalizarlo. Y dependiendo del modelo de amenaza, puede emplearse un equipo de conversión de direcciones de red, un router o un Firewall en uno o múltiples puntos de entrada hacia la red de la organización.

5.5.2 Actualizar el Firmware de los equipos a WPA

Por suerte, hoy en día, la base instalada de puntos de acceso y las tarjetas Wi-Fi de los clientes puede ser actualizadas a WPA simplemente re-grabando el Firmware en cada dispositivo y realizando pequeños cambios de configuración. Si este es el caso, debe realizar la actualización para que soporten WPA tan pronto como sea posible. Una vez actualizados a WPA, puede emplearse en dos modos: Clave pre-compartida (PSK) o infraestructura basada en un servidor. En el modo PSK, ingresa una contraseña en cada cliente y en cada punto de acceso y eso es todo. Esta modalidad es una solución adecuada

para hogares y pequeñas oficinas, pero no es escalable para una empresa. En estos casos, se requiere desplegar un servidor de autenticación.

5.5.3 Que hacer si no puede implementar nada de lo anterior

Los pasos descritos anteriormente involucran un gran despliegue de trabajo e inversión económica para mejorar las cosas. Que ocurre si no puede efectuar ninguna de estas sugerencias. Entonces debe evaluar la situación contestando las siguientes interrogantes: ¿Cuál es la utilidad de emplear un sistema inalámbrico versus no emplearlo?. ¿Añade valor a su negocio?. Adicionalmente debe considerar el valor de la información en la red. Que podría hacer o conseguir un intruso en la red. Finalmente considerar la amenaza contra la red. ¿Existe alguna razón para que alguien intente irrumpir en la red?.

Si luego de este análisis, se decide continuar utilizando una red inalámbrica, estas son unas recomendaciones a seguir para disminuir los riesgos de la red:

1. Utilice todas las medidas de seguridad disponibles en sus equipos. Esto quiere decir usar WEP, filtrado de direcciones MAC, y autenticación de clave compartida. Si, todas estas medidas pueden ser quebradas, pero no por todos. Entonces se reduce la amenaza. Pero aun se permanece vulnerable
2. Cambie la clave WEP tan frecuente como sea posible
3. Apague los dispositivos inalámbricos cuando no se utilicen. Esto probablemente sea práctico en hogares y pequeñas oficinas, pero el punto es reducir el riesgo lo mas que se pueda
4. Actualice sus equipos al menos a WPA, o mejor aún, a RSN tan pronto como sea posible.

El objetivo de estas recomendaciones es ayudar a proteger lo mejor posible. Se debe recordar sin embargo que la red y toda la información continuaran siendo vulnerables, y la mejor recomendación es invertir en tiempo y equipamiento actualizado para estar mejor protegido en lugar de basarse solamente en estos consejos. El objetivo principal es lograr que irrumpir en la red sea lo más dificil posible.

CAPITULO VI
RECOMENDACIONES PARA ACCESOS PUBLICOS, EMPRESAS Y HOGARES

Con el desarrollo de la tecnología inalámbrica LAN, al mismo tiempo se expandía el uso de acceso a Internet, no es dificil concluir que estas dos tendencias han estado ligadas. Hoy existe un número creciente de lugares donde puede encender su LapTop con adaptador inalámbrico y conectarse a Internet. Es una forma de continuar con su trabajo fuera de oficina.

Un Acceso público (en inglés **hotspot** o 'punto caliente') es una zona de cobertura Wi-Fi, en el que uno o varios puntos de acceso (access point) proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico (WISP). Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, etcétera. Este servicio permite mantenerse conectado a Internet en lugares públicos. Este servicio puede brindarse de manera gratuita o pagando una suma que depende del proveedor.

Los dispositivos compatibles con Wi-Fi van aumentando día a día, haciendo que las PDAs, los ordenadores y los teléfonos móviles se conecten mediante este sistema.

6.1 Acceso público inalámbrico

Algunos países como el Reino Unido regulan el uso de IEEE 802.11 ofrecido como servicio público. Esto ha causado controversia sobre lo que se considera como público. Por ejemplo si una empresa permite a sus visitantes el acceso a Internet por una LAN IEEE 802.11, ¿esta proveyendo un servicio público?

En el sentido de difusión, el acceso inalámbrico público simplemente significa que cualquier persona que ha comprado una laptop o dispositivo con capacidad IEEE 802.11 pueda conectarse legítimamente a un punto de acceso y obtener servicio de una zona

abierta como un café por ejemplo. La única restricción es que quienes pueden conectarse son aquellos que han pagado un derecho por el acceso a menos que el servicio sea gratuito. Si existen suficientes puntos de acceso instalados en áreas públicas, IEEE 802.11 podría eventualmente proveer acceso de banda ancha inalámbrica universal en las ciudades. En principio esto significa que podría competir con la infraestructura existente de telefonía celular en el futuro, un prospecto que remece a las grandes operadoras de telecomunicaciones y excita con atracción a los capitales aventureros.

6.1.1 Problemas de seguridad en HotSpots públicos

Los problemas de seguridad en las LAN's Wi-Fi públicas son diferentes de aquellos en las LAN's Wi-Fi corporativas. Los objetivos son los mismos: privacidad, integridad, etc. Pero dada la naturaleza pública de la red, existen algunas amenazas reales adicionales. Una de las suposiciones base de las LAN Corporativas es que existen solamente dos grupos de usuarios: los confiables y no confiables. A nivel local, muchas de las empresas nunca previenen a un usuario confiable de atacar a otro, suponiendo que son empleados son buenos ciudadanos y trabajaran correctamente en la red. Puede tener contraseñas separadas para acceso a archivos y otras políticas, pero nunca se espera que un usuario suplante a otro, o que este último acceda ilegalmente al disco del primero. Si esto ocurre, probablemente la empresa despedirá a la parte ofensora, quien pasara a ser parte del grupo no confiable.

La situación es un poco diferente en un HotSpot público. Existen también dos grupos, los que se pueden conectar a la red y los que no. Pero el criterio de acceso no tiene nada que ver con la confianza; solamente depende si pago su suscripción. A diferencia del caso corporativo, en este caso tiene que asumir que un miembro conectado puede atacar a otro.

Otra diferencia entre la seguridad corporativa y un HotSpot es la motivación de los participantes en la red. Generalmente en una red Corporativa, el empleador y los empleados comparten los objetivos similares. El empleador busca proteger a los empleados de un ataque y los empleados velan por los intereses de la empresa. Este no es el caso de un HotSpot inalámbrico. El proveedor de servicio solamente busca obtener rentabilidad y no le preocupa si sufre un ataque, a excepción de sí esto causa mala publicidad para el negocio. La motivación del proveedor del servicio es prevenir el fraude. La motivación de

los usuarios es protegerse a sí mismos y no se preocupan si un error de seguridad les permite dar acceso a sus amigos usando la misma cuenta.

La tercera diferencia y más critica entre el acceso corporativo y público es que la infraestructura detrás de la red Wi-Fi no es segura. En un entorno corporativo, la red Wi-Fi actúa como gateway entre el mundo inalámbrico inseguro y el mundo seguro de la red de cableado fisico.

6.2 Organización de un Acceso Público (HotSpot)

A pesar de que los detalles pueden variar entre diferentes instalaciones, todos los hotspots tienen esencialmente la misma arquitectura. Los componentes son:

- Subscriptores
- Puntos de acceso para proveer cobertura inalámbrica
- Controladores HotSpot para proveer control de acceso
- Servidor de autentificación para verificar usuarios legítimos
- Servicios Intranet de contenido local
- Servicios públicos de internet

La figura 6 muestra la relación de estos componentes entre uno y otro.

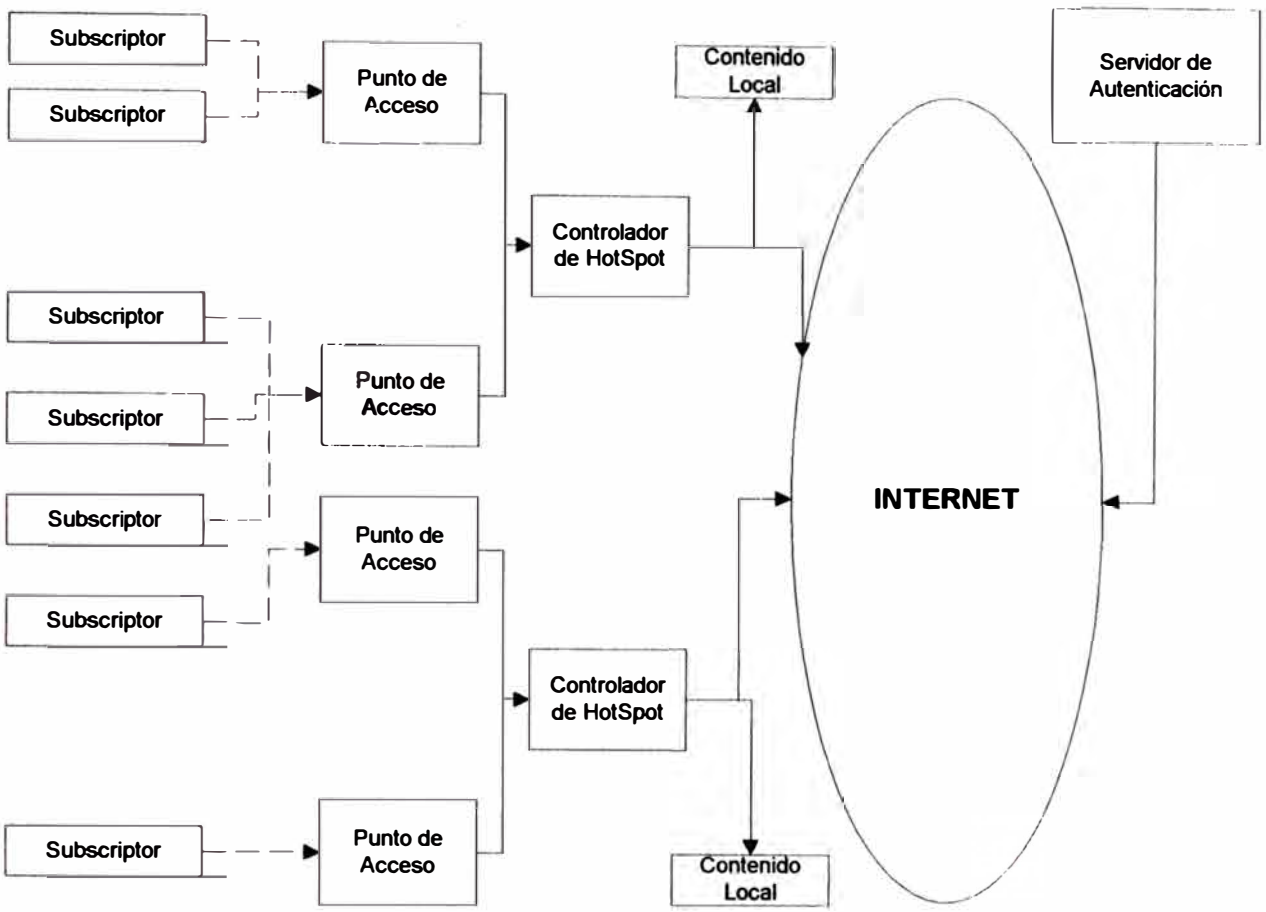

Figura 6.1 Organización de un HotSpot

6.2.1 Subscriptores

El equipamiento del subscriptor y del punto de acceso es a menudo componente completamente estandarizados IEEE 802.11, del mismo tipo que compraría para la oficina o el hogar. El uso de componentes estándar es especialmente útil desde el punto de vista del subscriptor. Idealmente no debe requerirse que el cliente tenga que instalar nuevo hardware o software en su laptop para conectarse. Deben poder subscribirse a varios servicios y también acceder por la red Wi-Fi de la oficina sin necesidad de efectuar ningún cambio en su equipo.

Requerir hardware o software especial en la laptop del usuario bloquea el impulso del efecto de compra. Se debe brindar un servicio de conectividad transparente para el usuario independiente de su movilidad, tal como lo brinda un servicio de telefonía celular, por ejemplo. Por el contrario, muchos Hotspots requieren que el usuario ingrese por medio

de un login mediante un navegador Web, lo cual no es dificil hasta que olvida la contraseña.

6.2.2 Puntos de Acceso

En casi todas partes, los puntos de acceso usados en HotSpots inalámbricos tienen las mismas características que los utilizados en el hogar u oficina. Típicamente, no se emplea la encripción WEP y la autenticación es responsabilidad de un controlador HotSpot. Mientras los equipos convencionales para puntos de acceso pueden utilizarse apenas desembalados, los vendedores han empezado a introducir puntos de acceso especialmente diseñados para Hotspots. El diseño mecánico necesita ser más robusto y a prueba de alteraciones si va a estar ubicado en un área pública. Muchos sitios resuelven el problema instalándolos en un closet o caja cerrada.

Los puntos de acceso deben conectarse al controlador HotSpot. Usualmente esto se hace mediante cableado Ethernet. Si existen múltiples puntos de acceso, estos se conectarían a la red usando un concentrador (hub). Estas conexiones de cableado son origen de una de una debilidad desde el punto de vista de seguridad. Un atacante podría conectarse fácilmente a la red de cableado e interceptar flujos de datos para después analizar la información capturada.

6.2.3 Controladores de Hotspot

El controlador de HotSpot es el componente clave que hace posible una instalación de HotSpot. Este componente realiza muchas funciones, que incluyen:

- Autenticación de usuario
- Colección de información de facturación
- Control de utilización de tiempo donde la suscripción es limitada por tiempo
- Proveer direcciones locales IP
- Filtrar peticiones para permitir acceso libre a ciertos servidores y sitios Web
- Emular servidores de correo para permitir reenvío de correo
- Emular resolución de nombres DNS.

Los puntos de acceso están operando en modo abierto sin encripción WEP o autenticación. Por ende, cualquiera con una tarjeta inalámbrica adecuada puede conectarse

a la red del Hotspot. El controlador le dará a cualquier dispositivo conectado una dirección IP, después del cual el nuevo dispositivo puede enviar paquetes a Internet. Sin embargo todos los paquetes pasan a través del controlador, y no lo reenviará al verdadero Internet hasta que no haya cumplido con un proceso de login válido.

El uso de login vía Web permite establecer algunos niveles de seguridad en el navegador como por ejemplo habilitar un puerto seguro (https://) en la dirección URL y ofrece cierta garantía de que el HotSpot es legítimo y no una falsa representación.

En muchos casos el controlador del Hotspot permite el acceso a ciertas páginas Web de manera libre. Estos son conocidos como sitios de lista Blanca, como por ejemplo, en un aeropuerto se puede permitir acceso a las páginas Web de las aerolíneas o un supermercado puede permitir acceso a sus páginas publicitarias.

En algunas circunstancias, el login por medio de un navegador puede ser problemático. Si esta moviéndose de un HotSpot a otro, puede ser forzado a registrarse cada vez por que tiene un controlador separado. Peor aún si su Laptop esta configurada para usar red privada virtual (VPN), porque el nuevo controlador no podría decodificar sus requerimientos, tras lo cual tendrían finalizar su sesión VPN, registrarse nuevamente y volver a habilitar VPN antes de proceder. Existen varios esquemas propietarios que permiten que el proceso de autenticación sea automático, evitando los tediosos pasos mencionados anteriormente.

6.2.4 Servidor de Autenticación

Las credenciales de cada subscriptor tienen que ser almacenadas en una base de datos centralizada para verificación. Como se mencionó anteriormente, EAP e IEEE 802.1x permiten al subscriptor negociar su acceso directamente con el servidor central de autenticación. Sin embargo en la mayoría de los HotSpots primero se colectan las credenciales en los controladores y luego verificados en una transacción separada entre el controlador y el servidor de autenticación. Desde el punto de vista de arquitectura, aquellos HotSpots que requieren a los subscriptores a registrarse con un usuario y contraseña válidos se asemejan a una agrupación de conexión dial-up vía módem. Cuando uno se conecta a Internet vía módem dial-up, el computador transfiere su usuario y contraseña al controlador del pool de módems, los cuales usan RADIUS para verificar los

derechos de acceso. Es natural entonces que un HotSpot utilice RADIUS de la misma forma, en realidad esta es una ventaja, el mismo servidor puede soportar ambos tipos de acceso, HotSpot y dial-up.

6.3 Protección del Usuario móvil

No hay duda de que el usuario de un HotSpot es vulnerable a muchos tipos de ataque. Como mínimo, sus datos pueden ser interceptados y leídos. En el peor escenario, un intruso puede entrar en su computador y copiar, borrar o modificar archivos o inclusive instalar un virus. El tráfico inalámbrico en un HotSpot generalmente no esta encriptado. Sin embargo, aún si lo fuere, el enlace entre el punto de acceso y el controlador esta desprotegido y los datos probablemente van a Internet público de todas maneras.

El peligro más grande proviene de los archivos compartidos. Muchos sistemas operativos populares permiten que los archivos se muestren como carpetas compartidas para otras computadoras en la red. Esto puede ser observado e investigado por un extraño. Se puede ganar un nivel de protección protegiendo con una contraseña las carpetas compartidas. Pero un atacante motivado probablemente rompería esta barrera.

Un segundo peligro proviene de los virus Troyanos. Como el mítico caballo de Troya, un virus troyano es introducido en su computador por medio de un archivo infectado, una vez dentro, inadvertidamente enviara mensajes mientras esta conectado en la red, avisando al enemigo donde esta y abriendo un portal para que ellos puedan conectarse a su computador. Se debe utilizar una buena protección antivirus para evitar estas situaciones.

6.3.1 Software Firewall personal

Si necesita una protección real, se recomienda instalar un software de Firewall personal. Este no proveerá privacidad para sus datos pero lo protegerá contra ataques. El software monitorea todos los datos entrantes o salientes de su computador. Bloquea cualquier intento sospechoso de acceder a su computador. Por ejemplo cuando desea acceder a un sitio Web o Servidor de correo, el computador establece una conexión con el servidor y luego envía y recibe datos. Una vez establecida la conexión, los datos pasan en ambos sentidos. El objetivo es lograr que el firewall permita todas las conexiones que inicie y

rechace conexiones que provengan de otro lugar. Esto impide a otros usuarios conectarse a su computador.

Desafortunadamente, si bloquea todas las conexiones entrantes, algunos servicios dejan de funcionar. Un buen software de Firewall tiene la habilidad de permitir ciertas conexiones entrantes basadas en el conocimiento de lo que esta intentando hacer. Algunas aplicaciones usan paquetes UDP en lugar de TCP. El uso de tales aplicaciones será limitado si esta activa la protección de un FireWall. Tales aplicaciones como Video Conferencia o Voz sobre IP son usualmente más especializadas. Para estas aplicaciones debe considerar una protección más avanzada como la red privada virtual (VPN).

6.3.2 Red privada Virtual (VPN)

VPN es un termino muy utilizado y poco comprendido. Tiende a ser empleado para describir alguna suerte de sistema de seguridad general operando en la capa TCP/IP. El concepto de VPN es superponer una red privada sobre una red pública tal que pueda conseguir las ventajas de una red dedicada y el bajo costo de una red compartida. La seguridad es el componente clave de implementar una VPN. La mayoría de los VPN's crean conexiones punto a punto entre dos usuarios o entre un usuario y un servidor. Esta técnica crea un túnel a través del medio de una red compartida de tal modo que solamente las partes en los extremos del túnel pueden leer los mensajes enviados desde el otro extremo. Se emplean varias técnicas de seguridad para envolver los datos enviados por la red para que sean impenetrables por cualquiera en el medio. Estos túneles son como conexiones virtuales, de aquí el nombre de VPN. Un uso típico de VPN es la conexión de un empleado a la Intranet de la empresa. Este tipo de conexión es particularmente útil cuando el empleado esta fuera de la empresa y conectado a Internet..

Al margen de la seguridad ofrecida por los HotSpots, VPN es la forma más segura de operar en un HotSpot inalámbrico. VPN elimina todos los problemas de seguridad mencionados anteriormente, incluyendo la debilidad del cableado de la planta para los puntos de acceso y el peligro de compartir la red con otros usuarios.

Si no cuenta con acceso a un servidor VPN, ciertamente debe considerar la instalación de un Firewall personal.

CONCLUSIONES

La seguridad en las redes inalámbricas es un tema crítico para el área de Tecnologías de Información de una organización, que no debe descuidarse. Dado a que las transmisiones viajan por un medio no seguro, requieren mecanismos que aseguren la confidencialidad, integridad y autenticidad de los datos.

No existe una solución definitiva para implementar un ambiente totalmente seguro, la solución es en sí, un camino de cambios constantes y anticipados, una carrera contra las debilidades y amenazas que afronta constantemente una red inalámbrica en contra de las ventajas que ofrece, el objetivo es minimizar los riesgos de seguridad. Recuerde que los hackers y los virus también están en constante evolución.

Los avances en Tecnología Inalámbrica ofrecen cada vez dispositivos mejorados en cuanto a seguridad, sin embargo es recomendable adoptar las soluciones estandarizadas en lugar de soluciones propietarias, así el soporte y búsqueda de nuevas soluciones en común son más provechosos, este es el fin por el que se han formado alianzas y grupos de trabajo.

Empresas del Sector financiero, Industrial y organismos del sector público y militar en conjunto con los proveedores de servicios de comunicación ya están adoptando políticas de seguridad entorno a esta tecnología que ya es parte de la infraestructura cotidiana en las redes de información.

BIBLIOGRAFÍA

1. Jon Edney – William A. Arbaugh "Real 802.11 Security Wi-Fi protected Access and 802.11i"
   Editorial Addison – Wesley – USA 2007

2. Matthew S. Gast "802.11 Wireless Networks The definitive guide" 2nd. edition
   Editorial O'Reilly – USA 2005

3. Natalia Olifer – Victor Olifer "Computer Networks – Principles, Technologies and Protocols for Network Design"
   University of Petrograd, UK Education and Research Networking Association
   Editorial Jon Wiley & Sons – UK 2006

4. Andrew S. Tanenbaum "Redes de Computadoras"
   Editorial Prentice Hall – USA 2003

OTRAS FUENTES DE INFORMACION

CONFERENCIAS

IV Cátedra de Telecomunicaciones – Redes inalámbricas

Centrum La Católica en convenio con la Universidad Politécnica de Catalunya

Expositor: Jordi Casademont

Lima - Julio 2007

INTERNET

Wi-Fi Alliance (http://www.wi-fi.org)

IEEE Wireless zone (http://standards.ieee.org/wireless)