UNIVERSIDAD DE SOTAVENTO, A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INFORMATICA

"SEGURIDAD PARA REDES INALAMBRICAS"

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

PRESENTA:

MORALES ENRIQUEZ JOSÉ ALFREDO

ASESOR DE TESIS:

Lic. JUAN JOSÉ GUTIÉRREZ QUIROZ.

COATZACOALCOS, VERACRUZ. AGOSTO DE 2005

AGRADECIMIENTOS

SABIENDO QUE JAMÁS EXISTIRÁ UNA
FORMA DE AGRADECER EN ESTA VIDA DE
LUCHA Y SUPERACIÓN CONSTANTE, DESEO EXPRESAR
QUE MIS IDEAS, ESFUERZOS, LOGROS Y TRIUNFOS, HAN SIDO TAMBIÉN SUYOS Y
CONSTITUYE EL LEGADO MAS GRANDE
QUE PUDIERA RECIBIR CON CARIÑO, ADMIRACIÓN Y RESPETO.
POR ESO Y MUCHO MAS AGRADEZCO A DIOS Y JESUS CRISTO, QUE SIN ELLOS NO
SOY NADA, Y POR SUPUESTO A MIS PADRES, FAMILIARES Y AMIGOS.

INDICE GENERAL

INTRODUCCION

La integración de los dispositivos móviles, Internet y la conectividad inalámbrica nos ofrece una oportunidad extraordinaria para que las empresas puedan extender su información y servicios hasta los profesionales móviles. La combinación de estos tres factores puede aumentar la productividad, reducir los costos operativos e incrementar la satisfacción de los usuarios. La conectividad inalámbrica es un nuevo concepto que se está extendiendo vertiginosamente.

Por lo que resulta hablar de redes inalámbricas (Wireless LAN) ser muy abstracto y ambiguo, aparte de ser muy controvertido tema, más si se hace especial hincapié en el momento de construir su seguridad. Tema a tratar en la presente Tesis. Tomando como apoyo de estudio y ejemplo, un Router inalámbrico SMC modelo **SMC2804WBRP-G, DE 54Mbps.**

Debido a que en los múltiples medios de comunicación e información de hoy en día le dan una definición un poco menos distinta una de otra, partiremos de la definición tomada de un diccionario para redes informáticas. Inseguras por naturaleza, las redes sin cables son más vulnerables que las tradicionales, dado que utilizan ondas electromagnéticas como medio de transmisión, en vez de cable. Pero potencialmente productivas y seguras si se toman las medidas de protección adecuadas para integrar su seguridad. Y es que pueden llegar a ser potencialmente tan seguras como las redes de cables. Al respecto, revisaremos conceptos como el rango y limites de operación de una red sin cables, el uso combinado de una red tradicional y un segmento inalámbrico, la conexión a Internet con la misma cuenta, la conexión de un router, los diversos riesgos que están expuestos los usuarios y los datos de la red y los recursos de protección o seguridad.

Este proyecto de investigación se encuentra enmarcado en un enfoque hacia la seguridad para una red sin cables, realizando una propuesta que busca demostrar la eficiencia de una red inalámbrica protegida, ¿como? Haciendo uso

de su entorno físico y lógico que las rodea. Las redes inalámbricas han tenido una notoria aceptación en el mercado como solución para **La libertad de movilidad.** Las Wireless LAN. Sin olvidar integrar una protección adecuada.

El mercado ha evolucionado muy lentamente, sin obedecer a las expectativas generadas en los últimos años, que hablan de importantes crecimientos de negocios. Esto se ha debido, entre otros motivos, a los propios problemas que siempre con lleva el nacimiento de una tecnología; los precios normalmente elevados y la ausencia de normas.

Sin embargo, parece que ahora el panorama podría cambiar realmente, se financiaron los trabajos relativos a la norma IEEE 802.11 para redes locales inalámbricas.

Gracias a los esfuerzos de los organismos normativos y los líderes del sector, las palabras "seguridad WLAN" han dejado de ser contradictorias. Las WLAN pueden implementarse y utilizarse actualmente con un gran nivel de confianza en su seguridad.

CAPITULO I
ENTORNO INALAMBRICO

I.1 DEFINICIÓN

Wireless (inalámbrico): perteneciente o relativo a, o característico de, las comunicaciones que tienen lugar sin utilizar cables o hilos de interconexión, como por ejemplo, las comunicaciones de radio, microonda o luz infrarroja.

Ahora bien, entonces una red de área local por radio-frecuencia o WLAN (Wireless Red de Área Local) puede decirse que es como una red local que utiliza tecnología de radio-frecuencia para enlazar los equipos conectados a la red, en lugar de los cables, UTP (Unshielded Twisted-Pair, Cable de Par Trenzado), coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas, o simplemente definirla de esta manera: cuando los medios de unión entre sus terminales no son los cables, sino un medio inalámbrico, como los infrarrojos o el láser, estamos hablando de redes sin cables. Este tipo de redes se diferencia de las convencionales, principalmente, en la capa física y en la capa de enlace de datos, según el modelo de referencia OSI (Open Systems Interconnection, Interconexión de Sistemas Abiertos). La capa Física (PHY, Physical, fisica) indica cómo son enviados los bits de una estación a otra. La capa de Enlace de Datos MAC (Control de Acceso al Medio). Se encarga de describir cómo se empaquetan y verifican los bits de manera que no tengan errores. Las demás capas se encargan de los protocolos, de los puentes, encaminadores o puertas de enlace que se utilizan para conectarse.

Los dos métodos que se emplean para reemplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la luz infrarroja.

I.2 ANTECEDENTES Y ORIGEN.

Veinticinco años de historia avalan a esta prometedora tecnología (WLAN), su origen se remonta a la publicación hecha en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistió en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los proceeding del IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), son considerados como el punto de partida en la línea evolutiva de esta tecnología.

Para las telecomunicaciones desde un principio tres han sido las opciones principales para llevar a cabo una comunicación:

a) Transmisión por medios guiados (Cables de cobre).
b) Transmisión por el vacío o espacio (**Radiofrecuencia**).
c) Transmisión por medios ópticos (Fibra óptica o de vidrio).

b) **Radiofrecuencia**: Vibración que viaja a través del vacío o espacio por medio de ondas. Abreviatura RF, es un termino que se refiere a la corriente alterna (AC) ésta alimenta una antena que a su vez genera un campo electromagnético adecuado para la transmisión de datos de modo inalámbrico, estas frecuencias cubren un rango significativo del espectro de radiación electromagnética.

Las redes de tipo inalámbrico son potencialmente vulnerables y eso las tiene hasta ahora hecha más promesa que realidad, las redes locales inalámbricas no han sido o podido conquistar el mercado. Aunque con gran nivel de aplicabilidad a distintos escenarios donde el cable resulta inadecuado o imposible de colocar, la falta de estándares y sus reducidas prestaciones en cuanto a velocidad han limitado el interés de la industria como de los usuarios. La aparición de la norma IEEE 802.11 podría suponer una reactivación del mercado.

Las investigaciones han seguido adelante tanto como para radio frecuencias, infrarrojos como con microondas donde se utilizaba el esquema del "spread-spectrum" (frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, la FCC (Comisión Federal de Comunicaciones), y la Agencia del Gobierno de Estados Unidos encargadas de regular y administrar en materia de telecomunicaciones, asigna un conjunto de estrechas bandas de frecuencia IMS (Industria Medica y Científica) para libre uso de las bandas de los 2,4 y 5,7 Gigahercios, a las redes inalámbricas basadas en "spread-spectrum". IMS es una banda para uso comercial sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda. La asignación de esta banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya mas en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN. Las redes de estos rangos de frecuencia son claras: no requieren licencias, permisos ni necesidad de comunicación para su despliegue y pueden ser implantadas en cualquier ubicación. Pero como contrapartida surge una serie de importantes inconvenientes: invasores, interferencias impredecibles con redes próximas por selección de frecuencias iguales o parcialmente solapada, espectro empleado por otras aplicaciones (redes BLUETOOTH, usos domésticos como

teléfonos inalámbricos, emisiones de video, mandos de control remoto, etc.), potencia de emisión muy limitada que restringe mucho la cobertura y una banda de uso muy estrecha que permite delimitar muy pocos canales no interferentes. Y entre otros intrusos en la red.

I.3 NORMALIZACIÓN

Resulta mejor ponerse de acuerdo en este aspecto ya que es por ley, que se debe de tener bajo Normas de regularización a este tipo de servicio tecnológico, para evitar que los fabricantes del hardware y software se enfrasquen en un inútil y costosa guerra de estándares, donde cada uno trata de hacer que sus productos sean aceptados como los mejores para resolver determinado problema, en el mundo de las computadoras existen organismos que regulan una amplia variedad de aspectos, tanto físicos como lógicos, en la manera de operación de estos equipos. Por mencionar uno, JEDEC (Joint Electronic Devices Engineering Council, Consejo de Ingeniería de Dispositivos Electrónicos) que regula el encapsulado de circuitos integrados.

En nuestro caso especifico de la conectividad en computadoras, el organismo regulador es el Instituto de Ingenieros Eléctricos y Electrónicos, mejor conocido por sus siglas IEEE. Aunque este nombre era conocido por un numero relativamente pequeño de usuarios de computadoras, la situación ha cambiado debido a la aparición de algunos estándares que influyen directamente en la forma en que el usuario interactúa con su maquina o con su grupo de trabajo. Una vez que estamos familiarizados con el ámbito de las redes de computadoras, será común encontrarnos con estas reglas. Las redes informáticas, que trabajan o usan el estándar Ethernet, se ajustan a las reglas del estándar IEEE-802; siendo así un campo muy amplio abarcado por este estándar y es tan amplio que se ha decidido dividir dicho estándar en varios sub-estándares; mencionare unos de los mas importantes. Que en realidad son muchos pero son necesarios.

ESTÁNDARES IEEE 802.X

<table>
<tr>
<td>IEEE-802.1

Es la primera especificación que aparece. En ella se fijan las reglas generadas que controlan todas las comunicaciones entre los equipos de una red; por ejemplo, se determina como estará dividido un archivo, para enviarlo a través de la red; que información debe cada “paquete”; de que manera pueden ser identificados el emisor y el receptor; como hay que evitar que un paquete que va hacia “X” llegue a “Y”; que se hace en caso de que ocurra un conflicto en la red; cuales son las medidas de seguridad internas, etc.</td>
<td>IEEE-802.8

Reglamenta las redes basadas en fibra óptica. Se trata de redes locales de muy alta velocidad, que por lo general solo se utilizan en las grandes corporaciones.</td>
</tr>
<tr>
<td>IEEE-802.2

Estándar general que rige la capa de enlace de datos en modelo de referencia OSI (interconexión de sistemas abiertos). Aquí se establecen los protocolos de comunicación que permiten que incluso maquinas con distintos sistemas operativos, idiomas, programas, etc., se intercomuniquen sin ningún problema.

IEEE-802.3

Puede decirse, que este estándar es el que define propiamente los protocolos de una red Ethernet. Originalmente, estas reglas se aplican a las redes de tipo bus; pero ahora se usan también en nuevas formas de comunicación, que son más rápidas y efectivas. Los principales estándares cubiertos por esta regla, son los siguientes:

° 10base-2: es la especificación original para una red tipo bus. Utiliza un cable coaxial, como medio de transmisión. En la actualidad, ya casi no se usa. Su velocidad de transmisión es de 10Mbps.

° 10base-T: tipo de red que utiliza cable UTP (pares trenzados). Tiene un límite de velocidad de 10Mbps.

° 100base-T: es el estándar que más se emplea en nuestros días. Aunque sigue utilizando cables de pares trenzados, ha aumentado el volumen de datos hasta 100Mbps.

° 1000base-T: nuevo estándar, que poco a poco sea introducido en el mundo de las redes empresariales. Como su nombre lo indica, puede</td>
<td>IEEE-802.9

Estándar que especifica las reglas para la integración de voz y datos en una red local. Si se apega a este estándar y aprovecha el cableado de su red local, una empresa puede intercambiar tanto información como conversaciones de tipo telefónica. Últimamente, ha sido reemplazado por el estándar VoIP.

IEEE-802.10

Estándar específicamente dedicado a la seguridad de las redes locales. Paradójicamente, esta reglamentación también ha sido abandonada.</td>
</tr>
</table>

manejar hasta 1Gbps de datos; por eso es ideal para el intercambio de grandes volúmenes de información.	
IEEE-802.4 Especificaciones para redes tipo token-bus. Es un estándar que casi ha desaparecido, pero que se utilizo ampliamente en los principios de la computación.	**IEEE-802.11** Estándar que reglamenta las redes locales inalámbricas. Tal como se ha mencionado a lo largo de esta tesis, existen varios sub-estándares; y los que mas se emplean son el 802.11b (2.4Ghz, 11mbps) y el 802.11G(2.4Ghz, 54Mbps). El estándar 802.11 fija las especificaciones que regulan a las redes inalámbricas, como su frecuencia, beneficios, rangos y tecnologías, y un sin numero mas de requerimientos que son necesarios para armar una red de este tipo, desde su protección, que se apoya en la criptografía hasta su implementación e instalación.
IEEE-802.5 Estándar que regula las redes tipo token-ring. Las redes de esta clase, son muy sólidas. Casi nunca tienen conflictos que puedan ocasionar el bloqueo general de la red; pero como requieren de componentes especiales de hardware y de software, generalmente son un tanto costosas. Se usan, sobre todo, en empresas grandes.	IEEE-802.15 Estándar para las redes de área personal (PAN). El estándar Bluetooth, forma parte de este conjunto de reglas.
IEEE-802.6 Estándar para las redes de área metropolitana (MAN). Es aplicable, cuando varios sitios de una zona geográfica específica necesitan intercambiar datos, ya sea mediante enlaces de tipo telefónico o radial. Ya no se utiliza.	IEEE-802.16 Estándar que controla las redes de área metropolitanas de tipo inalámbrico.
IEEE-802.7 Especificación que cubre las redes locales de banda ancha. En la actualidad, ya no se utilizan.	

- Resumiendo, en el año de 1990, en el seno de IEEE-802, se forma el comité IEEE-802.11, que empieza a trabajar para tratar de generar una norma para las WLAN. Pero no es hasta 1994 cuando aparece el primer borrador.
- En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Sistema personal de comunicaciones). En ese mismo año, la ETSI(Instituto de Estándares Europeo de Telecomunicaciones), a través del comité ETSI-RES 10, inicia actuaciones para crear una norma a la que denominarían

HiperLAN (High Performance LAN) para, que en 1993, se asignaran las bandas de 5.2 y 17.1 Ghz, para el uso de las Wireless.

- En 1993 también se constituye la IRDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos.
- En 1996, finalmente, un grupo de empresas del sector de Informática Móvil (Mobile Computing) y de servicios forman el Wireless LAN Interoperability Forum(WLI Forum) para así potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Entre los miembros fundadores de WLI Forum se encuentran empresas como ALPS Electronic, AMP, Data General, Control, Seiko y Zenith Data Systems.

I.4 LA FAMILIA DEL ESTÁNDAR IEEE-802.11

El primer estándar que surge de esta familia es el **802.11** (1997), el cual sienta las bases tecnológicas para el resto de la familia. No tuvo mucha relevancia por su baja velocidad binaria alcanzada, cerca de 2Mbps, y la carencia de mecanismos de seguridad de comunicaciones, no hizo de ella un gran uso. Muy poco después en 1999, se publica el **802.11b**, el cual es recibido con un gran éxito comercial. Opera en la banda de los 2.4 GHz y permite alcanzar velocidades binarias teóricas de 11Mbps mediante el empleo de mecanismos de modulación de canal y protección frente a errores bastante robustos, aunque en la practica es difícil superar un ancho de banda efectivo de 7Mbps. Cuando el canal de transmisión es ruidoso, posee un mecanismo de negociación que reduce la velocidad binaria en escalones predefinidos, aumentando paralelamente la robustez de los mecanismos de protección frente a errores. Para complementar

su operatividad, incorporan un protocolo de seguridad de las comunicaciones, el WEP o Wired Equivalent Privacy (Privacidad Equivalente a la de las redes cableadas), habida cuenta de imposibilidad de confinar las emisiones en un medio mas protegido como es el cable en el caso de las redes fijas. Desafortunadamente, la WEP utilizaba claves estáticas como parte de su metodología de encriptación, que en cierta forma facilitaban la interpretación de paquetes suficientes para discernir la clave y por lo tanto descifrar el tráfico codificado. Una vez que los hackers descubrieron este fallo, desarrollaron programas automatizados de penetración maliciosa que pronto atacaron La Internet dando incluso a los hackers inexpertos las herramientas necesarias para descifrar casi cualquier LAN inalámbrica basada en la WEP (WLAN). Aun peor, es posible que un atacante modifique los paquetes, comprometiendo la integridad de la información.

El siguiente estándar fue el **802.11ª**, el cual tiene la particularidad de operar a un mayor capacidad binaria (teóricamente hasta 54Mbps) mediante unos esquemas de codificación de canal mas sofisticados y sobre bandas en los 5GHz, cuyo uso acaba de ser permitido en nuestro país. Su empleo no esta tan extendido como el 11b por el menor rango de cobertura debido ala mayor atención de las frecuencias empleadas en algunos casos y la necesidad de mecanismos de control de potencia todavía no incluidos, aunque pronto se equiparara.

Muy recientemente, el 12 de junio 2003, ha sido aprobado el **802.11g**, que mejora ostentosamente en varios frentes: mantiene el rango de los 2.4GHz pero amplia el bitrate hasta los 54Mbps teóricos (en la practica se obtiene una tasa efectiva menor que la mitad), mantiene la conectividad con el 11b y propone un protocolo de seguridad mas robusto denominado WPA (Wi-FI protected Acces, Wireless-Fidelity. Fidelidad Inalambrica Acceso Protegido) Dichas mejoras realizadas, han hecho ganar mas la confianza del mercado de esta tecnología y como consecuencia de ello las implementaciones y venta de productos.

Los tres estándares (b, g y a) presentan unos parámetros de operación muy similares: para el nivel máximo de potencia permitido la cobertura en áreas abiertas en general no supera los 300 metros, mientras que en interiores se obtendrán 100 metros en el mejor de los casos. Es necesario visibilidad directa entre los equipos emisores si hay obstáculos entre medias disminuye su rendimiento.

La familia no termina ahí: un conjunto de nuevos estándares serán aprobados en breve. El 802.11i es realmente la formalización del WPA, el cual fue prematuramente lanzado con funcionalidades restringidas debido a la presión de mercado por encontrar una solución al grave problema de seguridad puesto de relevancia con el antiguo WEP. Otro estándar importante será el 802.11e, el cual definirá los mecanismos para proporcionar calidades de servicio bajo las WLAN. Esto dará entrada a aplicaciones que permitan ofrecer servicio de garantía por priorización de tráfico, necesario para usos como militares, video conferencias o transacciones de carácter Bancarias y así, ampliando el potencial de la tecnología.

Un nuevo estándar es el 802.11h: que permitirá incluir las nuevas condiciones de utilización que muchos países, entre ellos España, Japón y Francia exigen para el uso de los rangos de frecuencias en torno a los 5Ghz para redes inalámbricas, como son el control automático de la potencia emitida, el análisis continuo del espectro para evitar el empleo de canales ya ocupados. Con ello se pretende solventar el problema de posibles interferencias de estas redes con las emisiones de satélite y militares que también las emplean y que son prioritarias. Una de las claves del éxito comercial ha sido la buena interoperabilidad existente entre equipos de diferentes fabricantes, labor que ha llevado a cabo la Wi-Fi Alliance.

Solo nos queda la buena noticia de que la familia no termina ahí, ya antes he mencionado que se esta trabajando en una nueva norma (la 802.11i) para proporcionar una seguridad consistente, aunque no se espera que sea ratificada

hasta fines de este año, por parte, la alianza Wi-Fi, una Asociación Inalámbrica Internacional sin ánimo de lucro.

La norma WPA tiene como objetivo solucionar todas la deficiencias de la WEP; combinando la autentificación de usuario (que la WEP no suministro) con un elemento de encriptación mas fuerte que el de la futura norma 802.11i denominado Protocolo de Integridad Clave Temporal (TKIP), la cual incluye el Control de Integridad de Mensajes (MIC), que protege de falsificaciones y de los denominados ataques repetidos (replan).

Como lo ha descrito eWEEK.com [(1)] *"El transmisor de un paquete agrega aproximadamente 30 bits (el MIC) al paquete antes de cifrarlo y transmitirlo. El receptor lo descifra y verifica el MIC (con base en un valor derivado de la función MIC) antes de aceptar el paquete. Si el MIC no concuerda, se abandona el paquete. Con el MIC se garantiza que se abandonaran los paquetes modificados y que los atacantes no podrán falsificar mensajes para persuadir a los dispositivos de red de que los autentiquen".*

Aunque la WPA impulsa la seguridad WLAN, muchos la consideran una solución temporal por que el equipo futuro de 802.11 posiblemente utilizara un modelo de encriptación más potente.

I.5 BREVE EXPLICACION DE LAS 7 CAPAS DEL MODELO OSI.

MODELO OSI.

La necesidad de intercambiar información entre sistemas heterogéneos, entre sistemas cuyas tecnologías son muy diferentes entre si, llevo a las ISO (Internacional Standard Organization, Organización Internacional de Estandarización) a buscar la manera de regular dicho intercambio de información. El modelo de referencia OSI (Open Systems Interconnection, Interconexión de Sistemas Abiertos) surge en el año de 1983 y es el resultado del trabajo de la ISO para la estandarización internacional de los protocolos de comunicación. Este protocolo está basado en la arquitectura de redes

estratificada, en ésta arquitectura el proceso de comunicación se divide en etapas y a cada etapa le corresponde un protocolo diferente, algunas etapas son implementadas en hardware y otras en software y otras en una combinación de las dos.

El modelo OSI es un estándar basado en 7 niveles o capas y cada capa como está dicho anteriormente tiene definido un protocolo; el protocolo para comunicaciones TCP/IP (Protocolo de Control de Transmisión/ Protocolo de Internet) es el que mas se apega a este modelo el OSI, éstos protocolos están basados en el supuesto de que una Terminal se organiza de tal forma que la comunicación fluye por cada una de las siguientes capas:

La capa **física** se encuentra en el nivel 1,
La capa de **enlace de datos** en el nivel 2,
La capa de **red** nivel 3,
La capa de **transporte** en el nivel 4,
La de **sesión** en el 5,
La de **presentación** en el 6
Y la de **aplicación** en el 7.

Las capas inferiores están orientadas al hardware y las capas superiores al software del usuario de OSI. OSI es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red. **Ver Figura 1.10**

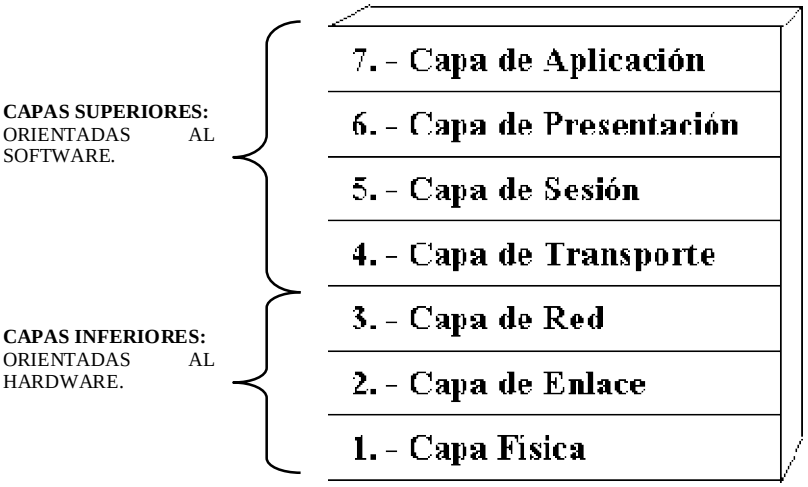


Fig. 1.10

Como se muestra en la Figura, las capas de OSI están numeradas de abajo hacia arriba. Las funciones más básicas, como el poner los bits de datos en el cable de la red están en la parte de abajo, mientras las funciones que atienden los detalles de las aplicaciones del usuario están arriba.

El modelo OSI tiene un propósito en cada capa y es proveer los servicios para la siguiente capa superior, resguardando la capa de los detalles de como los servicios son implementados realmente. Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra computadora, cuando realmente cada capa se comunica sólo con las capas adyacentes de la misma computadora. **Ver Figura 1.11.**

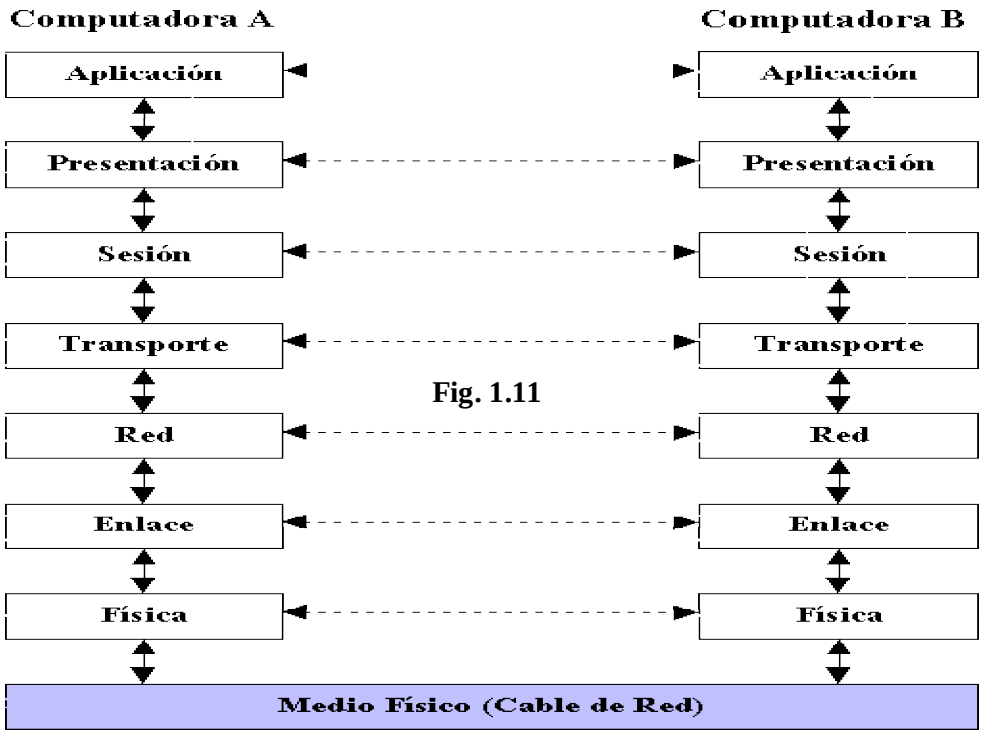


Fig. 1.11

Con esta última figura sobre el modelo OSI, se puede apreciar que a excepción de la capa más baja del modelo OSI, ninguna capa puede pasar información directamente a su contraparte en la otra computadora. La información que envía una computadora debe de pasar por todas las capas inferiores. La información entonces se mueve a través del medio físico de transmisión de la red hacia la computadora que recibe y hacia arriba a través de las capas de esta misma computadora hasta que llega al mismo nivel de la capa que envió la información.

Por ejemplo, si la capa de red envía información desde la computadora A, esta información se mueve hacia abajo a través de las capas de Enlace y Física del lado que envía, pasa por el cable de red, y sube por las capas de Física y Enlace del lado de el receptor hasta llegar a la capa de red de la computadora B.

La interacción entre las diferentes capas adyacentes se llama interface. La interface define que servicios de la capa inferior ofrece a su capa superior y como esos servicios son accesados. Además, cada capa en una computadora actúa como si estuviera comunicándose directamente con la misma capa de la otra computadora. La serie de las reglas que se usan para la comunicación entre las capas se llama protocolo.

Toda la comunicación se da desde 2 puntos de vista (transmisor y receptor) el punto de vista del transmisor, la información parte de la capa de aplicación de aquí hacia la de presentación, y luego a la de sesión, transporte, red, enlace de datos y finalmente la física. Siempre en ese orden y no es posible que una capa omita alguna capa durante el proceso.

Desde el punto de vista del receptor la información fluye en sentido contrario, desde la capa física hasta la de presentación, respetando el orden de las capas y de igual forma no se podrá omitir alguna de ellas.

NOTA: El modelo OSI sólo indica qué debe hacerse en cada una de las capas, pero no indica cómo, esto es cuestión de la tecnología que se vaya a usar a la hora de instalar una red ya sea cableada o inalámbrica.

I.5.1 CARACTERÍSTICAS GENERALES DE LAS CAPAS DEL MODELO OSI.

- cada una de las capas desempeña funciones bien definidas.
- los servicios proporcionados por cada nivel son utilizados por el nivel superior.
- existe una comunicación virtual entre 2 mismas capas, de manera horizontal.

- existe una comunicación vertical entre una capa de nivel N y la capa de nivel N+1.
- la comunicación física se lleva a cabo entre las capas de nivel 1.

I.5.2 FUNCIONAMIENTO GENERAL DE CADA UNA DE LAS CAPAS DEL MODELO OSI.

Física: Capa del nivel más bajo, su protocolo consiste en transmitir la información a través del medio según las especificaciones del hardware que tenga la red a la que pertenece el nodo. Aquí nos encontramos con los cables, concentradores de cableado, hubs y los repetidores. Este nivel también se ocupa de la codificación y decodificación de las tramas binarias en señales analógicas. En definitiva se definen las características mecánicas y eléctricas del medio de transmisión.

Enlace de datos: En el nivel de conexión de datos se controlan que las tramas de información lleguen correctamente a su destino, así como se asegura el control de acceso al medio para la compartición simultánea del mismo.

En este nivel aparecen los puentes (bridges) y se definen los métodos de acceso utilizados por la red, tales como Ethernet (CSMA/CD, Carrier Sense Multiple Access with Collision Detection (Acceso Múltiple por Detección de Portadora con Detección de Colisiones), Token-Ring, Apple Talk. En las redes locales, este segundo nivel se divide en dos: el nivel MAC (Media Acces Control) y el nivel LLC (Logical Link Control, Control del Enlace Lógico).

Con dos funciones primordiales:

a. le corresponde identificar de forma inequívoca a las terminales a las que se dirige un paquete en particular, así como las terminales en donde se origina éste paquete.
b. También se encarga de asegurar que la información dirigida a capas superiores esté libre de errores.

Red: realiza una función muy similar a la capa de enlace de datos, es decir se asegura que un paquete llegue ala terminal destino, la capa de red utiliza un paquete conocido como datagrama, este paquete que sólo tiene significado para la capa de red contiene información a cerca de la red y del número de terminal en esa red, tanto de la terminal origen como la terminal destino. La capa de red se encarga de que las tramas de información se organicen adecuadamente en paquetes. En este nivel los protocolos red aseguran la elección del camino más eficaz para ir de un punto a otro de la red. Conmutar los paquetes a medida que avanzan en la red y encontrar un camino alternativo si el habitual no estuviera libre.

Transporte: La información del usuario comúnmente tiene que ser acondicionada para que pueda viajar por la red, en particular cuando el usuario desea manejar la información en una cantidad mayor a la que la red puede manejar. Una red que maneja paquetes de Kbytes cuando recibe información de un usuario que excede la longitud del paquete entonces éste debe seccionarse en partes, cada una con kbytes de longitud; a cada una de estas partes se les denomina UDP (Unit Data Package) y cada UDP es ruteado por separado hacia la terminal destino. En la terminal destino la capa de transporte se encarga de anexar cada UDP en el orden requerido hasta formar el paquete dirigido a la placa de aplicación; por lo tanto este es el trabajo que realiza la capa de transporte a demás de otros como controlar los errores que se generan cuando un UDP se pierde, control de flujo (que la terminal transmisora no sobrecargue a la receptora), etc. Este nivel solo gestiona el control de flujos mediante protocolos de comunicación.

Sesión: en el nivel de sesión se permite establecer, mantener y terminar una conversación entre dos elementos de la red mediante los protocolos de sesión.

Hay dos tipos de red desde el punto de vista de la capa de sesión:

* Redes Orientadas a conexión.

* Redes No orientadas a conexión.

* Una red orientada a conexión envía todos los UDPs de la capa de transporte exactamente por la misma ruta que conecta la terminal origen con la terminal destino; la ruta es decidida por la capa de red y ésta se decide previo a la transmisión.

* Redes No orientadas a conexión. En este tipo de redes cada paquete es ruteado por separado hacia la terminal destino, esto indica que pueden llegar en desorden y es tarea de la capa de transporte ordenarlos para que formen el paquete original.

Para asegurar la comunicación entre dos terminales se requiere de un proceso conocido como "hand shaking" (saludo de mano) mediante el cual ambas terminales llevan a cabo un proceso de reconocimiento de acceder a comunicación, términos de comunicación, inicio y finalización de la transmisión.

Presentación: se encarga de formatear la información de usuario para que pueda ser manipulada por la red de la mejor forma, esto significa que la información que viene de la capa de aplicación debe comprimirse, encriptarse o simplemente traducirlo a otro formato para facilitar el proceso de transmisión. Esta capa estructura los datos en un formato y a un lenguaje tal que los dos elementos de la red puedan comprenderse.

Aplicación: Hace disponible al usuario o a otras aplicaciones los servicios que la red le ofrece, cada servicio se asocia a un puerto que no es otra cosa que un número que lo referencia. Esta capa define la manera en que las aplicaciones accesan a al red.

Entre otros servicios que la capa de aplicación ofrece a usuario se encuentran los siguientes: correo electrónico, servicios de archivos (ftp), servicios de directorios, terminal emulada, etc.

I.6 OSI EL MODELO MAS ADHERIDO A EL PROTOCOLO TCP/IP.

Éste protocolo (TCP/IP) fue diseñado a finales de los 60's como el fundamento de la red ARPANET (Advanced Research Projects Agency, Red de la Agencia del Ministerio de Defensa de Estados Unidos) que conectaba las computadoras de sus oficinas gubernamentales y universitarias. Fue desarrollado por el Departamento de Defensa de Estados Unidos. Funciona bajo el concepto de cliente servidor, lo que significa que alguna computadora pide los servicios de otra computadora; la primera es el cliente y la segunda el servidor.

ARPANET evolucionó para lo que ahora se conoce como INTERNET (red de redes) y con ello también evolucionó el protocolo TCP/IP. Sin embargo la organización básica del protocolo sigue siendo la misma, se organiza en sólo tres niveles: el de red, transporte y aplicación.

La capa de red de TCP/IP equivale a la capa de red de OSI. La capa de transporte de TCP/IP equivale a la capa de transporte de OSI y la capa de aplicación de TCP/IP equivale a las capas de sesión, presentación y aplicación todas en conjunto del modelo OSI.

El protocolo TCP/IP no especifica nada a cerca del hardware de red por lo que las capas de enlace de datos y físicas no existen.

Capa de Red de TCP/IP.

Se encargan de ruteo de información a través de una red de área amplia. Existen dos protocolos en este nivel, uno de ellos conocido como IP (Internet Protocol) que es probablemente el protocolo de ruteo más utilizado y trabaja bajo el principio de direcciones enmascaradas; también existe una versión más simplificada de IP conocida como ICMP (Internet Control Message Protocol, Protocolo de Mensaje de Control Internet) que se encarga de rutear paquetes sin ningún esquema de seguridad pero a mayor velocidad, se utiliza en particular para transmisión de e-mails.

Capa de Transporte de TCP/IP.

La capa de Transporte de TCP/IP ofrece dos protocolos: TCP para redes orientadas a conexiones y UDP para redes no orientadas a conexión. La red orientada a conexión y las no orientadas a conexión, fueron explicadas en el tema funcionamiento general de cada una de las capas del modelo OSI, específicamente en la capa de sesión, ya que para TCP/IP la capa de sesión de OSI equivale a la capa de aplicación. Un complementario a cerca de las capas de transporte TCP y UDP es que a diferencia de OSI pueden trabajar a nivel local sin necesidad de enrutamientos ni partición o segmentación de paquetes.

Capa de Aplicación para TCP/IP.

Los servicios de aplicación de TCP/IP son idénticos a los de OSI pero incorporan características que en el modelo de OSI corresponden a las capas de presentación y de sesión. Entre ellos se encuentran los siguientes:

1. Telnet: protocolo y programa que da servicio de terminal remota para permitir a un usuario remoto acceder a los servicios de un servidor como si tuviera conexión directa.
2. FTP (File Transfer Protocol): protocolo para transferencia de archivos y servicios de directorio entre terminales remotas.
3. SMTP (Simple Mail Transfer Protocol): protocolo para correo electrónico.
4. Kerberos: protocolo que ofrece servicios de encriptación y codificación de información y otros esquemas de seguridad para aplicaciones de usuario.
5. TNS: este protocolo permite mapear las direcciones lógicas de una terminal a un nombre simbólico más fácilmente identificable por los usuarios de la red. Ese servicio a su vez es utilizado por otros servicios como el de correo electrónico y FTP.

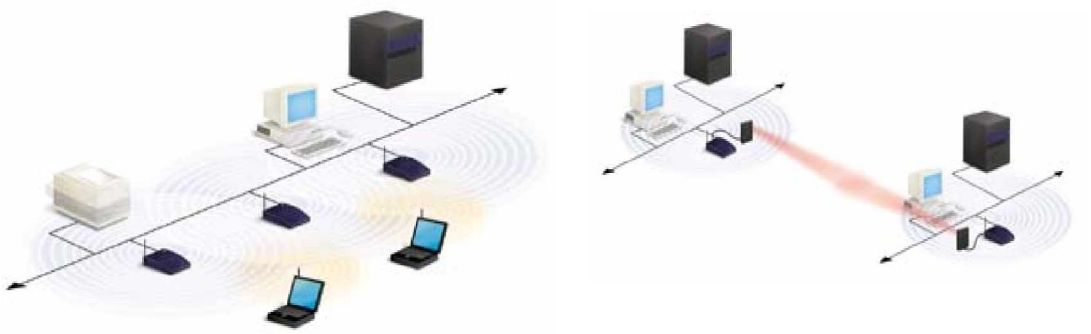
Todos estos servicios están basados en TCP a nivel capa de transporte y aunque son más simples de usar no son tan seguros, entre ellos están:

a. RCP: éste protocolo se utiliza para que los programas de usuario estén accesibles a otros usuarios en la red ofreciendo a estos últimos una interfaz con el primero.
b. TFTP (Trivial File Transfer Protocol, Protocolo Trivial de Transferencia de Archivo): idéntico a ftp pero sin verificación de errores.

Con esta breve pero clara explicación del modelo OSI (1983) y la explicación del protocolo TCP/IP (1960), pretendo mostrar que son los 2 estándares mas utilizados en las comunicaciones sin importar la tecnología que usan (inalámbrica o alámbrica), ambos siempre son y serán instalados, configurados y usados en donde quiera que se arme una red sea cual sea su modalidad, inalámbrica o alámbrica. Ahora bien, hecha esta explicación que aparentemente no tiene que ver con el tema, pero en realidad, si tiene mucho que ver con la gestión de todo este entorno, iniciemos pues de lleno con el tema en cuestión.

1.7 PRINCIPALES VENTAJAS Y DESVENTAJAS DE UNA RED TIPO INALAMBRICA.

Las redes locales inalámbricas se han vuelto bien populares hoy en día, éstas pueden proveer acceso a Internet por ejemplo a estudiantes alrededor de un campus universitario utilizando una computadora portátil provista con una tarjeta con acceso inalámbrico. Esto permite al usuario viajar a distintas ubicaciones salas de reuniones, pasillos, vestíbulos, cafeterías, salas de clases, etc. Y aún tener acceso a los datos en red. Sin un acceso inalámbrico, el usuario tendría que llevar molestos cables y encontrar un punto de red para conectarse.



Más allá del campo corporativo, el acceso a Internet y hasta los sitios corporativos podría estar disponible a través de puntos de redes inalámbricas en lugares públicos. Aeropuertos, restaurantes, estaciones de ferrocarril y áreas comunes en una ciudad pueden contar con este servicio. Tan es así que la aparición en el mercado de los laptops y los PDA (Personal Digital Assisteant), y en general de sistemas y equipos de informática portátiles es lo que ha generado realmente la necesidad de una red que los pueda acoger, tal es el caso de las WLAN. De esta manera, la WLAN hace posible que los usuarios de ordenadores portátiles puedan estar en continuo movimiento, al mismo tiempo que están en contacto con los servidores y con los otros ordenadores de la red, la WLAN permite movilidad y acceso simultaneo a la red. **Ver Figura (collage) 1.12**

Fig. 1.12

En una LAN convencional, cableada, si una aplicaron necesitara información de una base de datos central tiene que conectarse a la red mediante una estación de acogida o “docking station”, pero no puede estar en movimiento continuo y libre. La WLAN puede ser auto contenida o bien puede actuar como una extensión de la red de cable Ethernet o token-ring. Veamos pues sus ventajas y desventajas en comparación con sus homónimas las cableadas.

Ventajas:

1. Facilidad de Instalación:
La administración e la instalación de los equipos y de las tarjetas también son muy sencillas. Lo que agiliza la rapidez de su implementación, puesto que el tiempo que más consume la instalación de una red inalámbrica es la instalación de los puntos de acceso con la red local de la empresa, el cual puede durar días. Sin embargo la implementación en redes fijas puede durar semanas.

2. **Movilidad:**
Las redes tienen un rango de aproximadamente 20mts. (Este rango varia) alrededor de donde esta ubicado el punto de acceso. Sin embargo, las paredes disminuyen la intensidad de la señal. Las redes inalámbricas pueden proveer a sus usuarios el acceso a la información en tiempo real en cualquier lugar o punto de conexión. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red alámbrica. Posiblemente esta es la ventaja más fuerte frente a las cableadas, tanto a nivel empresarial como en un hogar debido al gran auge de los portátiles.

3. Facilidad de configuración para el usuario:
La persona que se va a conectar a la red solo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red esta abierta no es necesario configurar nada, pues la tarjeta detecta la red automáticamente. Una red inalámbrica puede ser tan rápida y fácil de instalar y además se puede eliminar la posibilidad de tirar cable a través de paredes y techos.

4. Las conexiones inalámbricas pueden ampliar o reemplazar una infraestructura cableada en situaciones en donde es costoso o está prohibido tender cables.

5. Flexibilidad en la instalación:
La tecnología inalámbrica permite a la red ir donde la alámbrica no puede ir. Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán

comunicar y no estarán atados a un cable para poder estar comunicados con el entorno que les rodea.

6. Escalabilidad:

Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

7. Poca planificación:

Haciendo una comparación con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas o la trayectoria que llevar el cableado estructurado, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.

8. Diseño:

Algunos receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.

9. Robustez:

En la vida nos pasan o suceden eventos inesperados que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa, hasta un pequeño terremoto o algo similar lo arruine todo. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede aguantar bastante mejor este tipo de percances inesperados. Aun que las redes basadas en cableado estructurado son por lo general más robustas frente a interferencias y condiciones adversas que las inalámbricas. Ahí ciertos entornos como en fábricas con elevada humedad, agentes químicos agresivos, calor, etc. las instalaciones cableadas pueden sufrir una rápida degradación o ser inviables.

10. Economía:
El precio para instalación de una Wlan depende de los requisitos y de las características de la implementación, cuyo coste puede rondar los 100 EUROS (€), sin embargo en una red cableada el coste se puede triplicar por los problemas físicos del cableado.

11. Estética:
En una red de cableado se necesitan metros de cables los cuales se introducen en canaletas y rosetas, sin embargo esto desaparece en una red Wireless. Este es un pequeño ejemplo que en ocasiones se convierte en fundamental.

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

Desventajas:

1. Interferencias:
Se pueden ocasionar por teléfonos inalámbricos que operen a la misma frecuencia, por redes inalámbricas cercanas o incluso por otros equipos conectados inalámbrica mente a la misma red o algún otro tipo de factor externo, el ruido.

2. Velocidad y límites de operatividad:
Las redes cableadas alcanzan la velocidad de 100 Mbps mientras que las redes inalámbricas alcanzan cuando mucho 54 Mbps. Su rango de operatividad es relativamente pequeño, su alcance oscila entre 100 y 300 metros respectivamente.

3. Seguridad:
En una red cableada es necesario tener acceso al medio que transmite la información (cable) mientras que en la red inalámbrica el medio de transmisión es el aire. Por una parte seguridad e integridad de la información que se transmite. Este campo está bastante criticado en casi todos los estándares

actuales, que, según dicen no se deben utilizar en entornos críticos cuyos en los cuales un “robo” de datos pueda ser peligroso.

Por otra parte este tipo de comunicación podría interferir con otras redes de comunicación (policía, bomberos, hospitales, etc.) y esto hay que tenerlo en cuenta en el diseño debido a que su comunicación es 100% hecha a través del aire.

Su seguridad no solo se ve manchada por los ladrones informáticos si no también por las interferencias entre diferentes dispositivos como de dispositivos independientes que generen campos electromagnéticos, por ejemplo, microondas o control remoto.

4. En un principio la ausencia de Estándares: se ha trabajando duramente en estos, apareciendo nuevos estándares como el 802.11h, g, i. entre otros que son el perfeccionamiento de cada uno de su antecesor.

5. Calidad de servicio:

Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps teóricamente llegan a 54 Mbps, frente a los 100 que puede alcanzar una red normal y corriente. Por otra parte hay que tener en cuenta también la tasa de error debida a las interferencias. Esta se puede situar alrededor de 10-4 frente a las 10-10 de las redes cableadas. Esto significa que hasta 6 errores de diferencia y eso es mucho. Estamos hablando de 1 bit erróneo cada 10.000 bits o lo que es lo mismo, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo. Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad. Puntos grises en el área de cobertura.

6. Coste:

Aunque cada vez se está abaratando bastante esta tecnología aún sale bastante más caro su costo inicial. Podríamos pensar que aún no merece la pena debido a la poca calidad de servicio, falta de estandarización y coste.

I.8 ¿QUE ES UN PAQUETE?

PAQUETE: La información transmitida en una red no se envía toda de una vez, sino que se divide en unas unidades de menor tamaño, denominadas paquetes, que son unidades de información agrupados de forma lógica. Estos paquetes incluyen, además de la información, otros elementos necesarios para que la comunicación se produzca verdaderamente y de forma fiable. En los paquetes se incluyen también las direcciones de origen y de destino de los datos. Esta agrupación lógica de los datos, permite que los envíos se reensamblen en su destino de forma que la información llegue completa.

La Agrupación lógica de información siempre debe de incluir un encabezado que contiene la información de control y (generalmente) los datos del usuario. El término "paquete" se usa con mayor frecuencia para referirse a las unidades de datos de la capa de red. **Ver Figura 1.13** Los términos datagrama, trama y mensaje también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI.

TRAMA: Agrupación lógica de información enviada como unidad de capa de enlace de datos en un medio de transmisión. Generalmente se refiere al encabezado y a la información final, utilizados para la sincronización y el control de errores, que rodean los datos de usuario contenidos en la unidad. En el protocolo TCP/IP, al paquete de datos se le denomina datagrama IP.

DATAGRAMA: un paquete o unidad de información junto con su información de entrega correspondiente, como, por ejemplo, la dirección de destino, y que se envía a través de una red de comunicación de paquetes.

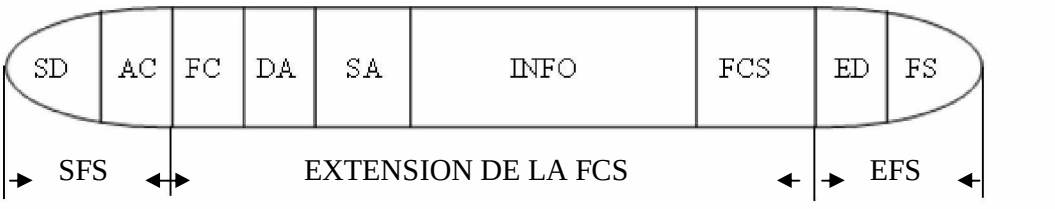


Fig.1.13
Esquema de un paquete

Donde:

SFS = secuencia de comienzo de trama

SD = delimitador de comienzo (1 octeto)

AC = control de acceso (1 octeto)

FC = control de trama (1 octeto)

DA = dirección destino (2 o 6 octetos)

SA = dirección origen (2 o 6 octetos)

INFO = información (0 o mas octetos)

FCS = secuencia de comienzo de trama (4 octetos)

EFS = secuencia de fin de trama

ED = delimitador de fin (1 octeto)

FS = estado de trama (1octeto)

CAPITULO II
SEGURIDAD INFORMATICA Y TOPOLOGIAS INALAMBRICAS.

II.1 SEGURIDAD INFORMATICA.

Seguridad Informática: Son las tecnologías utilizadas para hacer que un servicio sea resistente a los accesos no autorizados, así como los datos que el servicio contiene o de los cuales se es responsable. Uno de los objetivos principales de la seguridad informática, esta dirigido especialmente ha aquellos sistemas a los que acceden muchas personas o a los que se accede a través de líneas de comunicaciones, es la prevención de posibles accesos al sistema por parte de personas no autorizadas.

Es lo mismo que ha pasado para toda la humanidad, desde su inicio, usa de una u otra forma, la aplicación de ciertas medidas de seguridad para mantener a salvo su casa, oficina o nuestra vida misma; poniendo fuertes cerraduras a la puerta principal, poniendo barrotes a las ventanas, algún tipo de alarma o seguro, etc. Y Si nosotros retiramos todas estas protecciones, ya sabemos lo que podría pasar: algún extraño podría introducirse con la intención de llevarse todo lo posible o de hacer daño.

En un ambiente informático, una red bien protegida y resguardada con todas las medidas precautorias necesarias de seguridad, equivale a una casa u oficina debidamente protegida. Y una red instalada sin las menores medidas de seguridad, es blanco propicio de toda clase de ataques informáticos, tanto a través de Internet como por medios mas directos; esto es especialmente delicado en el caso de las redes inalámbricas, que son potencialmente vulnerables sin necesidad de conectarse físicamente a ella; solo bastaría con que este dentro del área de influencia del invasor, para que este pueda acceder a los recursos de la red, a la cuenta de Internet, a los archivos compartidos de los equipos conectados, etc.

Ahora pienso que decir no a los intrusos es una filosofía que debe de estar por siempre presente en nuestro que hacer como ensambladores de redes. En algunos casos los usuarios configuran de manera muy superficial su sistema y de inmediato comenzar a aprovechar los recursos de la red; pero no se dan cuenta de que es insegura. Y tampoco saben que los fabricantes de equipo inalámbrico suelen vender sus dispositivos con las medidas de seguridad intencionalmente apagadas, para que el usuario o administrador de la red tome las decisiones respectivas de seguridad.

II.2 ACCESOS NO AUTORIZADOS

Conforme al tema anterior Seguridad Informática es clave y básico que tengamos cuidado con el acceso no autorizado, por que es Obvio que la seguridad de las redes inalámbricas no se garantiza solo con normas. Por eso nosotros como responsables profesionales de la seguridad de la información lucharemos arduamente en contra de estos factores como es un acceso no autorizado, o alguna especie de ataques que se pueden lanzar contra las WLAN, como por ejemplo la intercepción del tráfico, ataques con semillas de virus, negación de servicio y secuestro de una sesión, por nombrar unos cuantos.

También es sabido que el auge de la interconexión inalámbrica puede tomar por sorpresa a muchos departamentos o empresas en general, debido a que muchos

equipos inalámbricos pueden ser introducidos a las empresas por medio de los empleados y grupos de trabajo y no a través del departamento de Sistemas o Informática u otros canales adecuados. Debido a este "acceso no autorizado", el equipo inalámbrico no fue sometido al proceso normal de comprender sus capacidades y limitaciones antes de implementarlo. Por consiguiente, los esfuerzos que se hicieron por proteger los dispositivos y en general la red inalámbrica no fueron oportunos o no fueron lo suficientemente rigurosos.

Afortunadamente, muchos riesgos se pueden mitigar siguiendo prácticas básicas de seguridad inalámbrica con tecnologías de protección a clientes y a nivel empresarial. Vamos a ver algunos de los aspectos que implica la protección y creación de una red inalámbrica segura.

Para proteger una WLAN de los accesos no autorizados y de **ataques.** Las empresas deben actualizar sus mejores medidas de seguridad, las cuales pondrían incluir lo siguiente:

1. Controlar el área de transmisión y cierre todos los puntos de acceso:
Muchos puntos de acceso inalámbrico permiten ajustar el poder de la señal. Coloquemos los puntos de acceso tan lejos como sea posible de las paredes y ventanas exteriores. Probemos el poder de la señal para que usted únicamente pueda conectarse a estos sitios. Luego, aseguremos cambiar la contraseña predeterminada en todos los puntos de acceso. Utilice una contraseña fuerte para proteger todos los puntos de acceso.

2. Para tener compatibilidad, compre hardware siempre del mismo distribuidor:
Mientras la norma IEEE tiene compatibilidad entre los dispositivos inalámbricos de diferentes fabricantes, las interpretaciones de las normas y las extensiones de propiedad exclusiva pueden impedir la integración total entre dispositivos de diferentes fabricantes.

3. Use el SSID (Identificador de Servicio del Equipo) inteligentemente:
Compre puntos de acceso que le permitan deshabilitar la transmisión de los SSID (Identificador de Servicio del Equipo) para evitar que los puntos de acceso

transmitan el nombre de la red y se asocie con clientes que no están configurados con su SSID. También cambie inmediatamente un SSID predeterminado para el punto de acceso. (Y al mismo tiempo, cambie también la contraseña del administrador y el nombre de usuario predeterminado).

4. Usar autenticación de direcciones MAC (Control de Acceso a Medios de transmisión):

Si contamos con un número administrable de usuarios inalámbricos y pocos puntos de acceso, la dirección MAC nos permite restringir las conexiones a sus puntos de acceso al especificar la única dirección de hardware de cada dispositivo autorizado en una lista de control de acceso y al permitir únicamente aquellos dispositivos específicos que se conectan a la red inalámbrica.

5. Activar el mayor nivel de seguridad que soporta su hardware:

Incluso si se tiene un equipo de un modelo anterior que soporta únicamente WEP, asegúrese de activarlo. En lo posible, utilice por lo menos una WEP con un mínimo de encriptación de 128 bits.

6. Instalar tecnologías de protección de clase empresarial (Instale firewalls personales y protección antivirus en todos los dispositivos móviles).

Implica emplear un firewall de Capa 7 en la zona inalámbrica y clientes firewalls en todos los equipos de escritorio; así como emplear también, sistemas de detección de intrusos; software antivirus en los servidores y equipos de escritorio; para hacer evaluaciones periódicas de vulnerabilidades de la red WLAN.

II.3 DEFINICION DE ATAQUE, TIPOS DE ATAQUES Y DEFINICION DE SISTEMAS DE DETECCION DE INTRUSOS.

Antes de continuar es preferible saber la definición de lo que es un ataque y los tipos de ataque mas comunes utilizados para penetrara la red, así como mencionar que es un sistema para la detección de intrusos.

Un **ataque** no es más que la realización de una **amenaza**. Y por **amenaza** de vemos entender que es el entorno riesgoso que rodea un ambiente informático, ya

sea un sistema o red (persona, maquina, suceso o idea) y es así como se puede dar lugar a que se produzca una violación de la seguridad, ya se de carácter de confidencialidad, integridad o de uso ilegitimo. Esto se puede contrarrestar con el uso de mecanismos de seguridad.

II.3.1 TIPOS DE ATAQUES:

Ataque externo: una forma de ataque informático en la que el intruso informático se introduce en el sistema sin disponer de conocimiento ni acceso previo al sistema. El intruso usara normalmente una combinación de técnicas y herramientas de detección para obtener información acerca de la red que quiere atacar. Seda de Internet hacia la Intranet.

Ataque interno: es un ataque contra una red o sistema llevado a cabo por una persona que tiene algún tipo de relación con el sistema atacado. Los atacantes internos son normalmente obra de empleados o ex empleados de una empresa u organización que conocen las contraseñas y vulnerabilidades de la red.

Existen asi mismo otros 2 tipos de ataques:

Ataques **Pasivos** y ataques **activos**.

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Ø Obtención del origen y destino de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Ø Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de la actividad o inactividad inusual de la red.

- Ø Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los periodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de información.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en tres categorías:

Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".

Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes basura. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc

II.3.2 FORMAS DE ATAQUES:

Los métodos de ataque descritos a continuación están divididos en categorías generales que pueden estar relacionadas entre si, ya que el uso de un método en una categoría permite el uso de otros métodos entre otras. Por ejemplo: después de pasar un password, un intruso realiza una sesión como usuario legitimo para

navegar entre los archivos y explorar vulnerabilidades del sistema. También el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema entes de huir.

1.- EAVESDROPPING Y PACKET SNIFFING

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de la red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están diseccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a la red o en un gatewey, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Este método es muy utilizado para capturar logias, ip¨s y passwords de usuarios que generalmente viajan sin encriptación alguna, ala hora de ingresar a algún sistema remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mailes entrantes y salientes.

2.- TAMPERING O DATA DIDDLING

Esta categoría se refiere a la modificación desautorizada a los datos, o al software en un sistema, incluyendo borrado de archivos. Este tipo de ataque es particularmente serio cuando el que lo realiza ha obtenido derechos de administrador, con la capacidad de disparar cualquier comando y poder alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada

3- DIFUSION DE VIRUS

Es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo, un diskette o a través de la red (e-mails u otros medios) sin intervención directa del atacante. Dado que el virus tiene como característica propia su auto reproducción no necesita de mucha ayuda para propagarse a través de una red rápidamente, si es que no se esta instalado una protección antivirus.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc.) pero los que causan mas problemas en estos tiempos son los macro-virus, que están ocultos en simples documentos, aplicaciones que utiliza cualquier usuario de una computadora, y cuya difusión se potencia con la posibilidad de su transmisión de un continente otro a través de cualquier red o Internet.

4.-CABALLOS DE TROYA

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecute no conoce, para que dicho programa actué de una forma diferente a como estaba previsto, por ejemplo formatear el disco duro, modificar un fichero, sacar un mensaje, etc.

5.- BOMBAS LOGICAS

Este es el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificar la información o provocara el bloqueo del sistema.

6.- SNOOPING Y DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un dowloading de esa información a su propia computadora.

El snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo y la difusión ilegal de reportes oficiales.

7.- SPOOFING

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tempering. Una forma común de spoofing es conseguir el nombre y password de un usuario legitimo para una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envió de falsos e-mails.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utilizar este para entrar en otro, y en otro. Este proceso, es llamado looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante.

8.- JAMMING O FLOODING

Este tipo de ataques desactiva o satura los recursos del sistema. Por ejemplo un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Muchos proveedores de Internet han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP o sea que este ataque involucra también spoofing. El sistema responde al mensaje, pero como no recibe respuesta, acumula la información de las conexiones abiertas, no dejando lugar a las conexiones legitimas.

9.- OBTENCION DE PASSWORDS, CODIGOS Y CLAVES. (cracking).

Este método (usualmente denominado cracking), comprende la obtención por fuerza bruta de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchos password de acceso son obtenidos fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca lo cambian. En este caso el ataque se simplifica e involucra algún tipo de prueba y error. Es muy frecuente crackear un password explorando agujeros en los algoritmos de encriptación utilizados, o en la administración de claves por parte de la empresa.

II.4 SISTEMAS DETECTORES DE INTRUSOS:

Existen numerosas medidas de seguridad para proteger los recursos informáticos de cualquier organización, pero aunque se sigan todas las recomendaciones, no estaremos libres de posibles ataques con éxito. Esto se debe a que conseguir un sistema invulnerable es sumamente costoso, además de que las medidas de control de protección darían mayor lentitud en nuestra red notablemente.

Dentro de las soluciones tecnológicas que en la actualidad están disponibles para reforzar la seguridad de una red, los firewalls son muy populares. Un firewall es un sistema encargado del cumplimiento de las políticas de control de acceso a la red. Un firewall actúa como guardia de su contorno o exterior de una red, es decir protege una red de ataques que provengan del exterior de ésta. Pero esto se puede complicar, ¿Qué pasaría si un atacante pudiera lograr pasar el firewall? Dejaría a su merced la red, un firewall no protege contra ataques desde adentro, el solo protege los accesos no autorizados hacia la red interna.
Realmente cuando sucede este caso solo nos queda detectar el ataque o el intrusión lo antes posible para que cause el menor daño en el sistema.

Antes de continuar vamos a definir qué se entiende normalmente por intrusión. Normalmente un intruso intenta:

1. Acceder a una determinada información.
2. Manipular cierta información.
3. Hacer que el sistema no funcione de forma segura o inutilizarlo.

Entonces una intrusión es un conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático. Los intrusos pueden utilizar debilidades y brechas en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para entrar normalmente como un usuario autentico.

La detección de intrusos se puede hacer a partir de notar alguna anómala del comportamiento y del uso que se hacen de los recursos del sistema. Este tipo de detección pretende cuantificar el comportamiento normal de un usuario.

Ya que tenemos definido lo que es una intrusión, así como lo que es un intruso, nos toca hablar de los SDI (Sistemas de Detección de Intrusos) o en ingles IDS (Intrusión Detection System). Hoy en día existen en el mercado una buena cantidad de productos conocidos como IDS. Se empezó a desarrollar en el año de 1980.

Un IDS es una herramienta mas de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red en busca de intentos de comprometer la seguridad de dicho sistema, entonces un IDS basa su funcionamiento en la recolección y análisis de información de diferentes fuentes, que luego utilizan para determinar la posible existencia de un ataque o penetración de intrusos.
En caso de que exista la suficiente certeza de la detección de un incidente, el SDI tiene como función principal alertar al administrador o personal de seguridad, para que tome acciones al respecto. Otras implementaciones más complejas son capaces de ir más allá de la notificación de un posible ataque, es decir pueden ejecutar acciones automáticas que impidan el desarrollo de éste. Los IDS buscan específicamente patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host. En definitiva un IDS aporta a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa, aunque no están diseñados para detener un ataque, pueden generar ciertos tipos de respuestas ante estos, pudiendo detectar las primeras fases de cualquier ataque.

Clasificación de los SDI:
Los SDI pueden clasificarse en base a varios aspectos: método de detección, tipo de monitoreo y forma de recolección y análisis de la información.

Según el tipo de detección, la mayoría de este tipo de software consiste en observar cualquier proceso que intente explotar los puntos débiles de un sistema en específico. Las diferentes acciones, que integran el mencionado proceso, comúnmente se denominan patrones o firmas del ataque.
Estas firmas pueden ser simples, como cadenas de caracteres, estructuras de memoria o bits, pero también pueden ser más complejas como vectores ó expresiones matemáticas. Una ventaja de este método es que permite centralizar las labores de detección en el conjunto de firmas que posee el SDI, minimizando así, la carga de procesamiento del sistema. Muchos productos comerciales utilizan este enfoque e inclusive periódicamente proporcionan actualizaciones de éstas firmas.

II.4.1 TIPOS DE IDS:

1. HIDS (Host IDS)

Protege contra un unico servidor, PC o host. Monitorizando gran cantidad de eventos, analizando actividades con gran precision, determinado de esata manera que procesos y usuarios se involucran en una determinada accion. Recaban información del sistema como archivos, logs, recursos, etc, para su posterior anales en busca de posibles incidentes. Todo ello en modo local, dentro del propio sistema. Fueron los primeros IDS en desarrollarse por la industria del la seguridad informatica.

2. NIDS (Net IDS)

Protegen un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red. Es decir, son snuffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algun tipo de ataque.

Por su tipo de respuesta se clasifican en:

Pasivos: Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea, alerta, etc. Pero no actúan sobre el ataque o atacante.

Activos: Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predeterminada en nuestra configuración.

Características deseables de un SDI

1. Debe ejecutarse continuamente sin intervención o supervisión de un operador humano.
2. Debe ser confiable, lo suficiente como para ejecutarse en background, pero no debe ser una caja negra, es decir, que su funcionamiento interno pueda ser examinado.
3. Debe ser capaz de tolerar fallas, en el sentido de que pueda sobrevivir a una caída del sistema, sin tener que reconstruir su base de datos de conocimientos al reiniciarse.
4. El sistema debe estar en capacidad de automonitorearse para asegurar su correcto funcionamiento.
5. Debe ser ligero, es decir su ejecución no debe cargar al sistema de una manera tal que le impida ejecutar otras tareas con relativa normalidad
6. Debe observar desviaciones del comportamiento estándar.
7. Debe poder adaptarse al comportamiento cambiante del sistema, es decir, si la configuración del sistema cambia, el SDI se adaptará.
8. Debe ser difícil de engañar.

Un IDS puede ser instalado en cada host o en cada tramo de red. Esto seria lo mas lógico cuando se trata de grandes redes y para redes pequeñas lo lógico seria instalar un IDS en un dispositivo por donde pase todo el trafico de red que nos interese, en el servidor Proxy. Es un verdadero problema cuando se desea implementar un IDS en redes conmutadas ya que no hay segmento de red por donde pase todo el tráfico.

Si llegáramos a instalar un IDS antes del corta fuegos, en una red que no fuera conmutada, capturaríamos todo el trafico de entrada y salida de nuestra red. La posibilidad de falsas alarmas es grande. Para algunos administradores de sistemas colocan dos IDS, uno adelante y otro detrás del cortafuegos para obtener información exacta de los tipos de ataques que recibe nuestra red. Y para ambientes domésticos se puede colocar el IDS en la misma maquina que el corta fuegos. En este caso actúa en paralelo, es decir, el firewall detecta los paquetes y el IDS los analiza.

Para ejemplificar y citar el nombre de un IDS usare el software para detección de intrusos uno específicamente, llamado snort ya que en mi plan de investigación de este tema fue el software que mayor mente se propuso para este tipo de seguridad.

Snort es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real.

Snort funciona bajo plataformas Windows. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas.

Inconvenientes de un IDS:

1. Pueden generarse falsas alarmas si el ambiente cambiara repentinamente, por ejemplo cambio en el horario de trabajo.
2. Un atacante puede ir cambiando lentamente su comportamiento para asi engañar al sistema.

Los inconvenientes antes mencionados pueden ser controlados mediante una implementación robusta y minuciosa, Según el tipo de IDS.

II.5 MECANISMOS DE SEGURIDAD

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN desde la calle.

Existe el término llamado “wardriving”, que se refiere a la acción de recorrer una ciudad para buscar la existencia de redes inalámbricas y ganar acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes.

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

La seguridad WLAN abarca **dos** elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquéllos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Estos “hoyos” en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red alámbrica a la cual se conecta. La tabla siguiente contiene los mecanismos de seguridad usados en redes WLAN, así como una pequeña descripción de cada uno de ellos.

Mecanismos de seguridad para redes WLAN

Mecanismo de seguridad	*Descripción*
Especificación original 802.11	Utiliza tres mecanismos para proteger las redes WLAN: - SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para accesar a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía (beacon). - Filtrado con dirección MAC (Control de Acceso al Medio): restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico. - WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.
802.1X	Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autenticación remota de usuarios entrantes (RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes).
	Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de Llaves Integras Seguras Temporales). TKIP fue construido tomando como base el estándar WEP, para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación. Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden

WPA **(Wi-Fi Protected Access)**	ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi. Esta especificación proporciona una mayor encriptación de datos para corregir las vulnerabilidades de seguridad WEP, además de añadir autenticación de usuarios que no se habían contemplado.

II.6 ¿QUE ES EL ESPECTRO EXTENDIDO (SPREAD SPECTRUM)?

Tecnologías.

Existen varias tecnologías de frecuencias utilizadas en redes inalámbricas. El empleo de cada una de ellas depende mucho de la aplicación. Cada tecnología tiene sus ventajas y desventajas. A continuación se listan las más importantes en este género.

- **Infrarrojo** (Infrared)
- **Banda Angosta** (Narrowband)
- **Espectro Extendido** (Spread Spectrum) o radiofrecuencia.

INFRARROJO.

Los sistemas de comunicación por infrarrojo utilizan muy altas frecuencias, justo abajo del espectro de la luz visible para transportar datos. Como la luz, el infrarrojo no puede penetrar objetos opacos, ya sea directamente (línea de vista) o indirectamente (tecnología difundida/reflectiva). El alto desempeño del infrarrojo directo es impráctico para usuarios móviles pero su uso es prácticamente para conectar dos redes fijas. La tecnología reflectiva no requiere línea de vista pero está limitada a cuartos individuales en zonas relativamente cercanas.

BANDA ANGOSTA.

Un sistema de radio de banda angosta transmite y recibe información en una radio frecuencia específica. La banda mantiene la frecuencia de la señal de radio tan angostamente posible para pasar la información. El cruzamiento no deseado entre canales es evitado al coordinar cuidadosamente diferentes usuarios en diferente canal de frecuencia. En un sistema de radio la privacidad y la no-interferencia se incrementan por el uso de frecuencias separadas de radio. El radio receptor filtra todas aquellas frecuencias que no son de su competencia. La

desventaja de esta tecnología es el uso amplio de frecuencias, uno para cada usuario, lo cual es impráctico si se tienen muchos.

ESPECTRO EXTENDIDO ¿Qué es?

La gran mayoría de los sistemas inalámbricos emplean la tecnología de Espectro Extendido (Spread Spectrum), una tecnología de banda amplia desarrollada para proveer comunicaciones seguras y confiables. La tecnología de Espectro Extendido está diseñada para intercambiar eficiencia en ancho de banda por confiabilidad, integridad y seguridad. Es decir, más ancho de banda es consumida con respecto al caso de la transmisión en banda angosta, pero el 'trueque' [ancho de banda/potencia] produce una señal que es en efecto más fuerte y así más fácil de detectar por el receptor que conoce los parámetros de la señal de espectro extendido que está siendo difundida. Si el receptor no está sintonizado a la frecuencia correcta, una señal de espectro extendido se miraría como ruido en el fondo. Otra característica del espectro disperso es la reducción de interferencia entre la señal procesada y otras señales no esenciales o ajenas al sistema de comunicación.

Es de suma importancia mencionar y aclarar lo que no es un espectro extendido, nos resultaría conveniente tener presente que existen equipos que utilizan estas mismas frecuencias y que producen una energía de radiofrecuencia, pero que no transmiten información. Estos equipos tienen aplicaciones Industriales, Científicas y Médicas (ICM) y en particular dichos equipos operan en otras bandas de frecuencia [902-908 MHz; 2,400-2,500 MHz y 5,525-5,875 MHz]. Ejemplos de estos equipos son: limpiadores domésticos de joyería, humidificadores ultrasónicos, calefacción industrial, hornos de microondas, etc.

Existen dos tipos de señales de Espectro Extendido: Salto en Frecuencia (Frecuency Hopping, FH) y Secuencia Directa (Direct Sequence, DS).

II.6.1 Espectro extendido con salto en frecuencia (FHSS):

FHSS utiliza una portadora de banda angosta que cambia la frecuencia en un patrón conocido tanto por el transmisor como por el receptor. Tanto transmisor

como receptor están debidamente sincronizados comunicándose por un canal que está cambiado a cada momento en frecuencia. FHSS es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto, donde se tienen una cantidad de receptores diseminados en un área relativamente cercana al punto de acceso.

II.6.2 Espectro extendido en secuencia directa (DSSS):

DSSS genera un patrón de bits redundante para cada bit que sea transmitido. Este patrón de bit es llamado código chip. Entre más grande sea este chip, es más grande la probabilidad de que los datos originales puedan ser recuperados (pero, por supuesto se requerirá más ancho de banda). Más sin embargo si uno o mas bits son dañados durante la transmisión, técnicas estadísticas embebidas dentro del radio transmisor podrán recuperar la señal original sin necesidad de retransmisión. DSSS se utilizará comúnmente en aplicaciones punto a punto.

Son ya muchas Organizaciones que promueven la competencia y avances tecnológicos, algunas de ella son alianzas, consorcios y forums, lo cual significa mejores soluciones para los usuarios de redes inalámbricas e incremento del crecimiento de la industria. La demanda del mercado decidirá el valor de cada organización y algunas de estas organizaciones son:

- Bluetooth SIG: basado en la especificación *Bluetooth*^{TM} especificación que utiliza la tecnología de radio para proveer conectividad a Internet a bajo costo a computadoras portátiles, teléfonos móviles o otros dispositivos portátiles.
- HiperLAN1, HiperLAN Alliance e HiperLAN2 Global Forum: organizaciones Europeas que utilizan enlaces de radio de alto desempeño a frecuencias en el rango de 5 GHz.
- HomeRF: Basada en una especificación para comunicaciones inalámbricas en hogares conocida por sus siglas en inglés SWAP (shared wireless access protocol). El HRFWG (homeRF Working Group) fue fundado para proveer los cimientos para un amplio rango de dispositivos al establecer una especificación

abierta a la industria para comunicaciones digitales inalámbricas entre PCs y dispositivos domésticos alrededor de los hogares.

- OFDM: Esta organización está basada básicamente en una tecnología patentada conocida como W-OFDM (Wide-band orthogonal frecuency división multiplexing)
- WLI forum: WLIF estableció un estándar interoperable en 1996 conocido como OpenAir, el estándar está disponible a cualquier compañía que se une al Forum. OpenAir es una tecnología de espectro extendio con salto en frecuencia a 2.4 GHz
- WECA: La misión de la WECA (Wireless Ethernet Compatibillity Alliance) es certificar la interoperatibilidad del estándar conocido como Wi-Fi™ que es una versión de alta velocidad del estándar 802.11b de la IEEE.

Bluetooth es una tecnología inalámbrica Europea desarrollada por Ericsson que, en 1994 comenzara unos estudios sobre la posibilidad de implementar pequeñas redes inalámbricas. Ericsson quería convertir Bluetooth en un estándar mundial, para ello inició contactos con diversas empresas. En primavera de 1998, cinco compañías (Ericsson, Intel, IBM, Nokia y Toshiba) forma el Bluetooth Consortium. Por lo tanto, no es un estándar apoyado por organismos de estandarización, pero que se prevé que se convierta en un estándar normalizado. Bluetooth permite la ínterconectividad de dispositivos inalámbricos con otras redes e Internet. Bluetooth es una Especificación abierta de una tecnología inalámbrica para redes basadas en radiofrecuencia, de bajo coste. Bluetooth al igual que 802.15 y HomeRF trabajan en la banda de frecuencias de espectro esparcido de 2.4 GHz . Bluetooth es capaz de transferir información entre un dispositivo a otro a velocidades de hasta 1 Mbps, permitiendo el intercambio de video, voz y datos de manera inalámbrica.

HomeRF también es una especificación que permite la interconexión de dispositivos inalámbricos en un área pequeña. Con cualquiera de estas últimas dos tecnologías se podrá accesar a la red de tu casa u oficina y podrer controlar dispositivos o consultar a distancia los datos importantes para tu beneficio y

accesar Internet con sólo conectarte a tu red en el caso de tener una red casera u oficina conectada a Internet.

II.7 ESTRATEGIA DE INSTALACION Y UTILIZACION DE UNA RED INALAMBRICA:

Ahora bien, el primer paso en la creación de una WLAN segura, es establecer una estrategia empresarial para su instalación y utilización. La estrategia debe abarcar las siguientes áreas:

- Determinar las necesidades de la empresa: ¿Cuáles son las motivaciones y necesidades de su empresa? Identificar claramente los objetivos y asegurarse de que los beneficios superan los riesgos.
- Integrar las políticas inalámbricas a las actuales políticas del departamento de Sistemas. (Recordemos que las soluciones inalámbricas son una extensión de la red alámbrica).
- Proteger la infraestructura existente: es importante no poner los dispositivos inalámbricos directamente en la red interna, sino suministrar una WLAN separada con gateways muy controlados a la red principal.
- Capacitar a los usuarios sobre las políticas inalámbricas: incluye instruir a los empleados en la configuración de sus dispositivos para que tengan acceso de manera segura a la red.

Si llegamos a cumplir al pie de la letra estas prácticas de seguridad y en conjunto con las estrategias de instalación, aplicando todo esto estaríamos cada vez más cerca de la integración y solides de una WLAN en un 86.99% segura de no tener algún tipo de ataque, accesos no autorizados o alguna otra especie de atentado, ya que no ahí una red 100% Segura, Cumplamos con esto. Para proteger una WLAN de todos los ataques e inseguridad que las rodea, a un ha esto es importante que las empresas actualicen sus medidas de seguridad.

II.8 TOPOLOGÍAS DE LAS REDES INALAMBRICAS.

Hay dos modos de operación o topologías para esta tecnología, uno ad-hoc, en el que las estaciones se comunican entre sí directamente, y otro de Infraestructura,

en el que las estaciones acceden a la red a través de uno o varios puntos de acceso (administradas y no administradas). Se podría decir que esta es su topología. **Ver Figura 1.14**

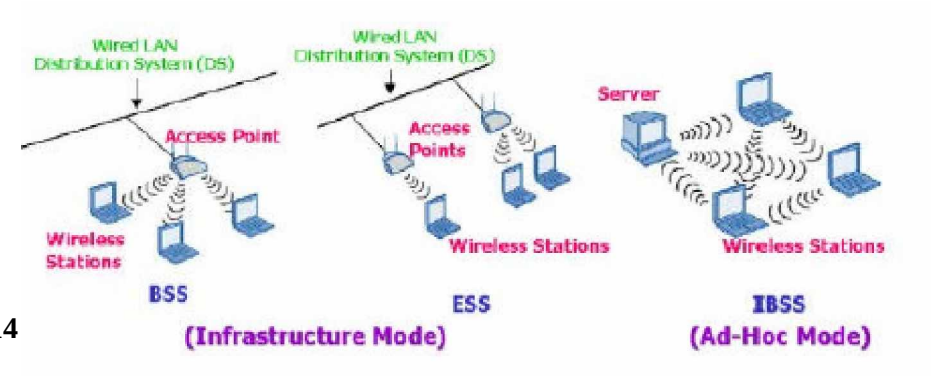


Fig. 1.14

II.9 DEFINICIÓN DE MODO AD-HOC Y MODO INFRAESTRUCTURA:

Modo Infrastucture: Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño. Es decir en este modo, cada cliente envía toda su comunicación a una estación central o punto de acceso (Access Point – AP). Este AP actúa como un bridge(puente) ethernet y reenvía las comunicaciones a la red apropiada, ya sea una red cableada u otra red inalámbrica.

Modo ad-hoc: En una topología ad hoc es solo un poco distinto, aquí los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los

demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas. En el modo ad-hoc, los clientes siempre se comunicaran directamente entre ellos generando una red de clientes únicamente. Como lo muestra la **Figura 1.14** Este modo fue diseñado de tal manera que solamente los clientes dentro de un rango de transmisión definido pueden comunicarse entre ellos. Si el cliente en una red ad-hoc desease comunicarse fuera de ese perímetro definido (también llamado celda), un miembro de esa celda debe actuar como si fuera un gateway y encaminar el tráfico fuera del perímetro hacia la otra celda.

Descripción general del funcionamiento de la modalidad de infraestructura.

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo. La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación. La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. Observemos que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir" e incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.
El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permita a la estación asociarse a un punto de acceso diferente para así proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

Descripción general del funcionamiento de la modalidad ad hoc.

Después de explicar el funcionamiento básico de la modalidad de infraestructura, del modo ad hoc se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

II.10 LIMITACIONES OPERATIVAS (RANGO) DE LAS REDES INALÁMBRICAS Y LÍMITES DE VELOCIDAD.

Si alguna vez nosotros hemos montado una red inalámbrica, seguramente siempre nos tendremos que responder esta pregunta: ¿hasta donde llega la señal del nuestro punto de acceso? ¿Alcanzara a cubrir todas las áreas del lugar donde se implementara?

En los manuales y especificaciones técnicas de los fabricantes de esta tecnología, es indicado que es casi imposible que no se cubra un área de trabajo “normal” con una red de este tipo. A un a esto los fabricantes también agregan que sus dispositivos inalámbricos (especialmente, sus puntos de acceso), tienen un rango que va desde los 45 metros (para el caso de las interiores) y hasta los 90 metros (en el caso de que la comunicación se realice en exteriores). Sin embargo, son estimaciones demasiado optimistas; y que no nos sea sorpresivo que no mencionen que la presencia de cierto tipo de muebles; paredes, estructuras metálicas, etc., pueden reducir considerablemente este rango de influencia. Para encontrar un parámetro mucho más realista de 30 metros de alcance en interiores, y 60 metros en exteriores, de la cobertura de una red WI-FI, restemos simplemente un tercera parte de las distancias “teóricas”. Esto deberá de ser mas que suficiente para cubrir con creces el área de una red WI-FI o inalámbrica. No olvidemos que hay que tomar en cuenta factores externos tales como el ruido electromagnético presente en la zona, el numerote de paredes entre el WAP y el adaptador, la velocidad de transmisión de los datos, etc., también es posible que

dentro de dicho rango, nos encontremos con puntos “grises”, donde la comunicación inalámbrica si es posible, pero es irregular o demasiado lenta. **Ver Figura 1.15**

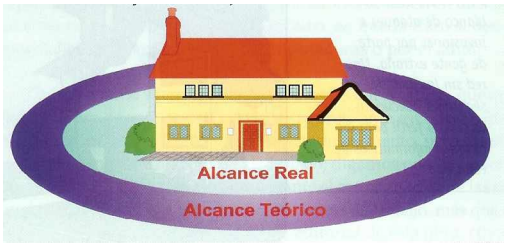


Fig. 1.15

Como ya lo mencione, antes, que unas de las principales desventajas de las redes inalámbricas, es que su desempeño puede ser afectado por diversos factores externos; entre ellos, la distancia entre el emisor y el receptor, la cantidad de ruido electromagnético que existe en la zona, el material y numero de las paredes que tiene que atravesar la señal para alcanzar su objetivo, entre otros, esto se complementaria si el punto de acceso inalámbrico (WAP) emitiera la señal con mayor potencia; o si de alguna manera pudiéramos aumentar la capacidad de recepción de nuestros adaptadores inalámbricos. Sorpresa esto ya puede ser posible veamos como. **Ver Figura 1.16**

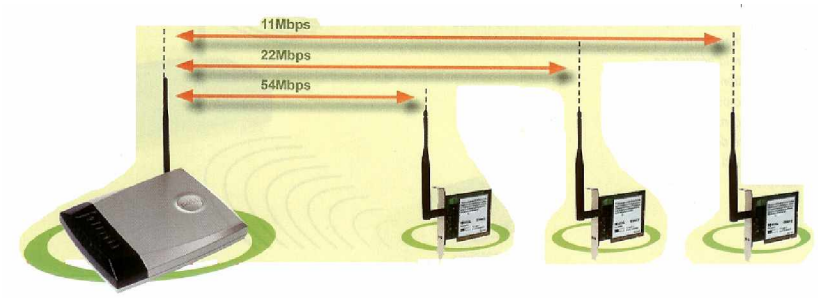


Fig.1.16

Pareciera que la integración de las redes inalámbricas esta rodeada de muchos factores enemigos que diríamos no es conveniente una red de este tipo, pero no es así, los problemas de **atenuación de la señal** es otro factor interesante en ellas.

En primer lugar, recordemos que la señal de radio de una red inalámbrica es una emisión electromagnética, que se rige por el teorema del cuadrado inverso.

Entonces, mientras mayor sea la distancia entre el emisor y el receptor, mayores dificultades habrá para conseguir un enlace adecuado.

Para dar solución a este problema en las redes inalámbricas, se puede reducir la cantidad de datos que se envían en un momento dado. Un intercambio de datos de muy alta frecuencia, fácilmente puede ser interferido, y si la señal es débil, pueden perderse porciones considerables de información. Así, reduciendo el flujo de datos, se reduce la probabilidad de interferencia y se mejora la posibilidad de recibir los datos completos y sin ningún problema. De manera de que si se monta una red con el estándar 802.11G (de 54Mbps), mientras mayor sea la distancia entre el emisor y el receptor, este flujo de datos se reducirá a 22 Mbps e incluso a 5Mbps. **Ver Figura 1.17**

Una de las formas en que las redes inalámbricas compensan la perdida de señal ocasional por la distancia o por interferencias externas, consiste en reducir la cantidad de datos que interpretan el emisor y el receptor.

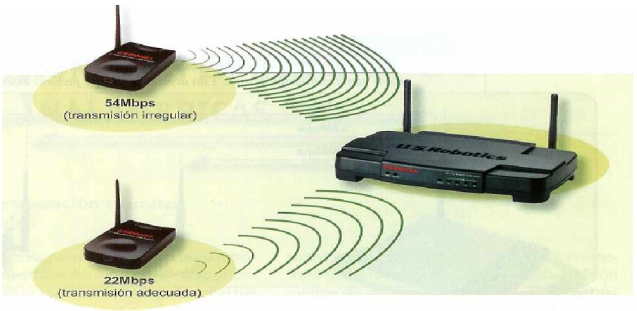


Fig.1.17

Para evitar tal efecto, se pueden aplicar dos métodos recomendados por los fabricantes de equipo inalámbrico. Uno de ellos, consiste en colocar antenas de alta ganancia, tanto en el emisor como en el receptor. La otra opción es colocar algunas “estaciones repetidoras”, cuyo objetivo es precisamente tomar la señal del emisor y reenviarla amplificada para que alcance con mayor facilidad al receptor. Este tipo de hardware no es muy costoso, y su instalación, es sumamente sencilla. Así que para evitar disminuciones de desempeño en ciertos puntos de nuestra red, coloquemos las antenas o los repetidores adecuados; con esto toda el área de trabajo puede quedar cubierta con condiciones de recepción-emisión óptimas. **Ver figura 1.18**

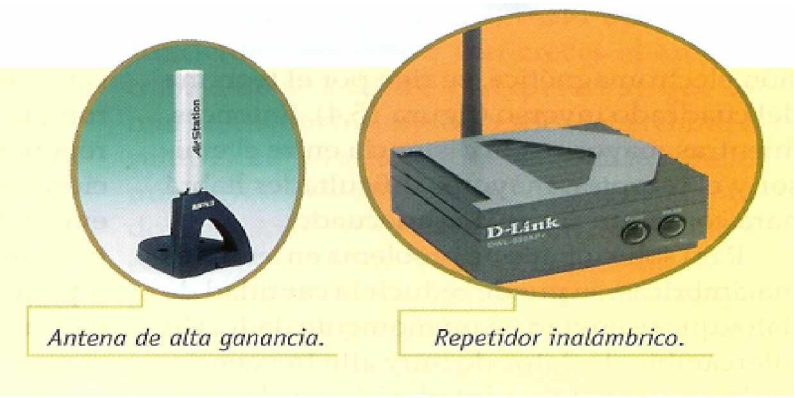


Fig. 1.18

Existe una ley y es, La “Ley de los cuadrados inversos”, dice que si se mide una emisión electromagnética puntual a una distancia “X”, en el momento de medirla a una distancia “2X”, tendremos apenas una cuarta parte de la potencia en X; y que al medirla a una distancia 3X, tendremos una novena parte de la potencia. Esto significa que el nivel de una señal radial disminuye rápidamente, conforme nos vamos alejando de su fuente. Y tal es el problema que se divide en varios. Atenuación de la señal, perdida de señal y puntos grises.

II.11 USO COMBINADO DE UNA RED TRADICIONAL CON UNA RED INALÁMBRICA.

Este es un punto muy inquietante e interesante de esta tecnología, si nos llegáramos a en contara con un cliente que ya posee una red alambrada, y ahora desea contar con una red inalámbrica para aprovechar al máximo algunas de sus maquinas portátiles o algún otro dispositivo inalámbrico, nosotros como diseñadores de soluciones para redes, le tenemos que hacer ver que una red de computadoras no tienen que ser totalmente alambradas o totalmente inalámbrica; que sepa que ambos estándares pueden coexistir perfectamente, sin ningún problema. Y que en efecto, una red inalámbrica puede “fundirse” con una red alámbrica tradicional, sin que esto implique problema alguno en el desempeño de una, de otra o de ambas. **Ver figura 1.19**

Fig.1.19

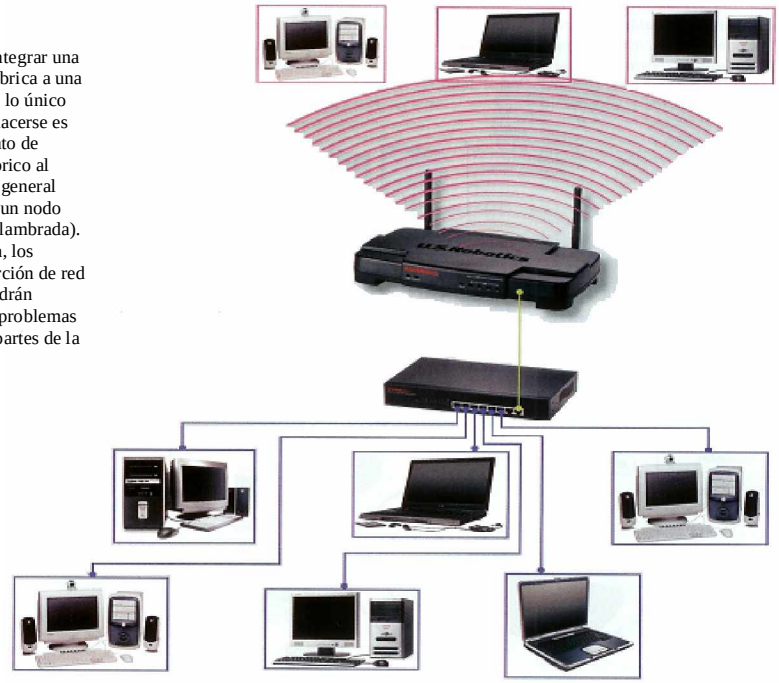
La mayoría de los usuarios piensan que las redes tienen que ser totalmente alambradas (A) o totalmente inalámbricas (B). Pero en realidad, ambos tipos de red pueden coexistir sin el menor problema; es decir, puede haber segmentos inalámbricos integrados en una red alámbrica o viceversa.

Podría parecer un choque de dos mundos, por ser tecnologías aparentemente distintas, para que nosotros configuremos un punto de acceso inalámbrico (WAP) es necesario conectarlo a una computadora; al menos en un principio, esto debe hacerse por medio de un cable RJ45 normal. **Ver Figura 1.20.**

Fig.1.20

Una vez realizada la configuración, este cable puede retirarse, para utilizarse de ahí en adelante solo enlaces radicales. Sin embargo, no es forzoso retirar el cable del WAP; puede dejarse conectado y utilizarse después para una red alambrada. **Ver Figura 1.21**, donde el WAP solo se ha colocado como un nodo mas de la red tradicional; y a partir de este punto, la señal inalámbrica puede “repartirse” a todas las computadoras que posean dicha capacidad. El hecho de tener una red

combinada, en donde se aprovecha la flexibilidad de la red inalámbrica y la velocidad y robustez de la red alambrada, es una de las situaciones mas comunes en el ámbito empresarial, donde existen varios sistemas de escritorio (que difícilmente son cambiados de lugar) y donde también se dispone de maquinas portátiles.



Con el fin de integrar una porción inalámbrica a una red tradicional, lo único que tiene que hacerse es conectar el punto de acceso inalámbrico al switch central general (como si fuera un nodo mas de la red alambrada). De esta manera, los usuarios de porción de red inalámbrica podrán interactuar sin problemas con sus contrapartes de la red normal.

Fig.1.21

II.11.1 CONECTANDO UNA RED INALÁMBRICA A INTERNET.

Si en una casa, oficina o empresa se trabaja con varias computadoras de escritorio que compartan una conexiona Internet, este recurso puede ser aprovechado por las maquinas portátiles que forman la red inalámbrica. Y para lograrlo, hay que configurarlas adecuadamente en el servidor Proxy o el router general; a un que la mayoría de las veces, solo es necesario conectar el punto de acceso en el conmutador central; y con esto, el acceso a la red también quedara disponible para dichos sistemas. **Ver Figura 1.22.**

Fig.1.22.

Si la red ya posee un acceso compartido a Internet por medio de un enrutador, se puede colocar, como un nodo más, un punto de acceso inalámbrico. Y entonces, de manera automática, el acceso a la red mundial también será distribuido entre todos los usuarios de la porción de red inalámbrica.

Si, se nos pidieran, el caso de que instalemos una red combinada desde abajo o desde cero, nosotros tendremos cierta libertad para elegir los componentes fundamentales de la red a construir. En este caso y tomando una suposición que el proveedor de acceso a Internet de nuestro cliente no pueda proporcionar directamente una combinación de MODEM DSL (**D**igital **S**ubscriber **L**ine, Línea Digital de Abonado)-router-WAP (que es la opción ideal para satisfacer todas las necesidades de una vez), quedándonos como responsabilidad de establecer el acceso inalámbrico y de distribuir la señal de Internet entre todos los sistemas del conjunto. Podríamos preocuparnos, pero esta conexión se simplifica mucho con la ayuda de un solo equipo. **Ver figura 1.23.**

Algunos proveedores de acceso a Internet, le dan a su cliente la opción de adquirir una combinación de MODEM DSL-router-WAP. Este hardware es ideal para armar rápidamente una red mixta.

Fig. 1.23

Otra buena opción es instalar un ROUTER inalámbrico, (**Ver figura 1.24**) pero también tiene sus ventajas y desventajas, en el mercado informático actual, se ofrece una amplia variedad de Routers inalámbricos. Tal como su nombre nos lo indica, estos componentes pueden hacer funciones de un enrutamiento normal y de un punto de acceso inalámbrico, ya no tendríamos que adquirir por separado el encaminador ni el WAP.

Una de las formas más sencillas y seguras de integrar una porción inalámbrica a una red tradicional que ya tiene acceso compartido a Internet, es reemplazar el Router normal por un Router que también pueda funcionar como punto de acceso inalámbrico (WAP). Esto evita la necesidad de hacer otra configuración, y el riesgo de que los componentes de un tipo de red entren en conflicto con los de la otra.

Fig. 1.24

La gran ventaja de esta solución, es que minimiza la cantidad de elementos necesarios para que funcione la red (entre menos piezas tenga un mecanismo, menos posibilidades habrá de que falle). Además, simplifica considerablemente la tarea de configuración de la red en general; y es que un solo dispositivo, se encarga del protocolo NAT **(**Net Addresses Translation o Traducción de Direcciones de Red) de todas las maquinas de la red (tanto las alambradas, como las de enlace radial) y esto naturalmente, evita que entren en conflicto. La única desventaja de este arreglo, es que si el Router inalámbrico sufre algún daño, se desconectara tanto la red inalámbrica como la red tradicional. **Ver Figura 1.25.**

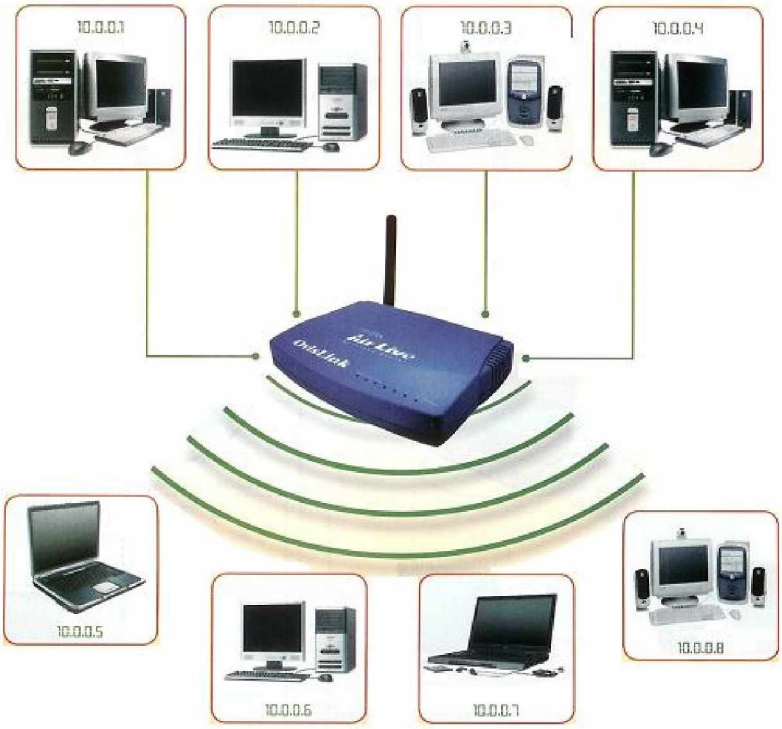


Fig.1.25

La gran ventaja de usar un router inalámbrico es que este dispositivo puede repartir las direcciones IP de todas las maquinas de la red. Así se evitaran conflictos entre ellas y se agiliza su interacción con la red mundial.

Ejemplo de cómo hacer la conexión de un Router inalámbrico:

Para conectar este componente ejecutemos los siguientes pasos, estos pueden variar de acuerdo a la marca:

Paso 1

Por medio de un cable RJ45 normal, conectemos el MODEM de banda ancha en la entrada **WAN** del Router inalámbrico.

Paso 2

En una de las salidas RJ45 del Router, conectemos la porción alambrada de la red; si esta consta de menos de cuatro computadoras fijas, conectémoslas directamente al dispositivo, **Ver Figura 1.26** muy detenidamente caso **A** Y **B**; si tenemos mas de cuatro maquinas, utilicemos nuevamente un cable RJ45 para conectar el conmutador central en una de las salidas del Router inalámbrico. Con esto quedaría lista la porción cableada de la red, muy importante, no olvidemos configurar adecuadamente el acceso a Internet.

Paso 3

Para configurar los accesos inalámbricos, entremos a la utilería de configuración del Router. Activemos su característica inalámbrica y configuremos las medidas de seguridad de la red (esto será explicado mas adelante y detalladamente).

Paso 4

En cada uno de los demás equipos que tengan adaptador inalámbrico, se repiten los tres pasos anteriores.

Paso 5

Por ultimo, comprobaremos la conexión entre todos ellos.

Comentario: la gran mayoría de los Routers inalámbricos, se pueden conectar directamente hasta cuatro computadoras con alambrado directo. Y en el caso de que tengan más de cuatro maquinas para conexión alambrada, una de las salidas del Router deberá enlazarse con el Switch general.

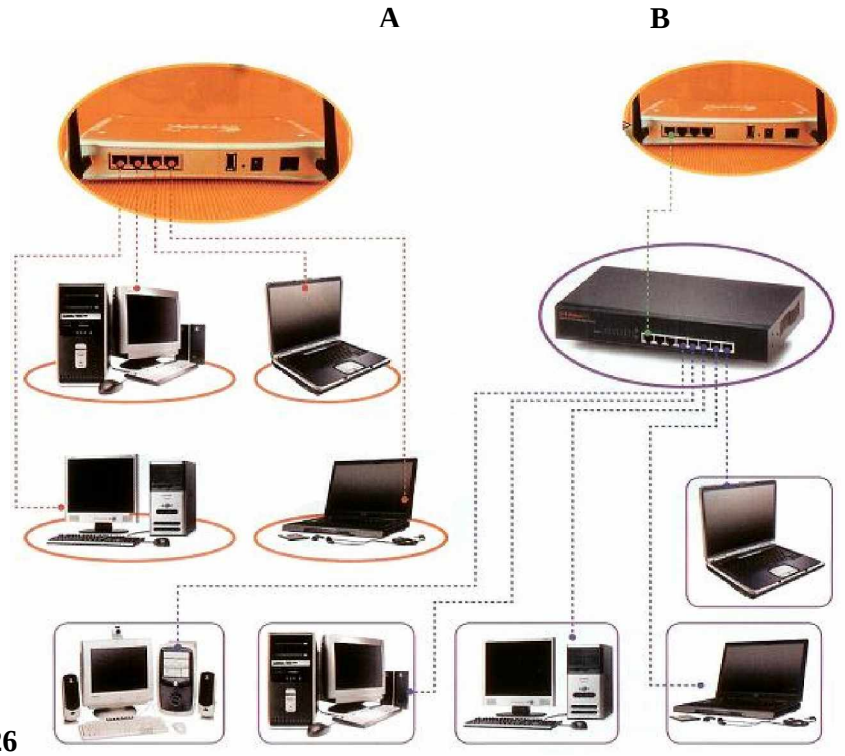


Fig.1.26

Y con esto, se termina el armado de la red combinada.

CAPITULO III
PROBLEMÁTICA DE UNA RED INALAMBRICA, CONFIGURACION DE PROTOCOLOS Y ENCRIPTACION.

III.1 ASEGURANDO LA RED

Llego por fin al tema específico, donde realizare mi propuesta, sin duda alguna el tema que ha sido más descuidado por muchos técnicos y profesionistas que montan o tejen redes inalámbricas, afectando más en el montaje a los usuarios residenciales u hogareños. Por que no solo podrían invadir nuestro territorio si no algo mas que eso, protejámoslo con seguridad nuestros recursos informáticos.

No es exagerado, cuando hablamos e insistimos en las medidas de protección para el sistema. Cuando una red inalámbrica es "invalida", el intruso puede hacer prácticamente todo lo que quiera; y como el sabe que las consecuencias de sus acciones no recaerán en él, sino en el titular de la red en cuestión. Por tal motivo es muy importante extremar las precauciones en el momento de instalar una red sin cables. Esto es el hincapié que propongo, un poco mas adelante.

Un problema de seguridad en las redes inalámbricas, puede ser evitado, en el tema "rango de operación y limites de velocidad, menciones que el alcance practico de una red inalámbrica es de aproximadamente 30 metros en interiores. Esto no parece mucho; pero si tuviéramos en nuestras manos los planos típicos de una casa, edificio o de un departamento y dibujáramos en ellos ese radio de alcance, nos daríamos cuenta que la señal de la red sin cables rebasa con facilitad los limites.
Es decir, que cualquier persona que se coloque dentro del rango de influencia de la red inalámbrica, puede en lazar su sistema portátil (que cuente con un adaptador inalámbrico) e invadiera la privacidad del propietario de la red, sin que los usuarios autorizados puedan hacer algo por evitarlo; por ejemplo, no podemos evitar que un vecino aproveche los recursos de nuestra red, puesto que no esta invadiendo físicamente nuestro hogar u oficina; de hecho, él se encontraría trabajando desde su casa y solo está aprovechando los "huecos" de seguridad que tiene la red. **Ver Figura 1.27.**

Fig. 1.27

Esta situación, es un ejemplo de los grandes riesgos que implica el montaje de una red inalámbrica de computadoras. Como se usan ondas radiales para establecer comunicación entre los distintos equipos del grupo de trabajo, siempre existiría el riesgo de que alguna persona ajena espié o aproveche los recursos de la red. Esto es especialmente delicado en caso de la conexión a Internet.

III.1.1 PROPUESTA:

Todo consiste en hacer un proceso de configuración, cosa que la mayoría de los integradores y tejedores de redes inalámbricas no lo hacen, tal vez por desconocimiento o su falta de interés por dotar de seguridad a este activo tan valioso de la oficina u organización, solo es un acto de conciencia que debemos hacer en nosotros mismos como profesionistas y especiales en la rama, por que cambian tanto y tan rápido las tecnologías informáticas de esta gran dinastía de comunicaciones, cosa que me da amplia seguridad y me hace sentirme seguro de especializarme en un determinada rama o segmento de la informática, en su seguridad, claro, pero sin perder de vista la amplia gama de posibilidades que se presentan en el mercado de trabajo; digamos que hay que pararse junto a un árbol pero sin dejar de mirar el bosque. Y para ello, no solo es importante el conocimiento de las diferentes tecnologías involucradas en nuestro quehacer, sino también el disponer de lógicas de trabajo, mas que rutinas cabalmente estructuradas. Y es por eso que con el afán de poner mí empeño y espirito enfocado a la seguridad de las redes de esta tecnología inalámbrica.

Mi propuesta es tan simple, solo ahí que hacer simple una rutina, como una receta de la elaboración de algún tipo de postre, talvez la de un rico pastel, sino ponemos el ingrediente y el porcentaje adecuado de harina o azúcar, simplemente no tendrá consistencia o un sabor agradable, lo mismo dijo de ellas las redes inalámbricas si no le ponemos esa pizca de sal, en la integración de su seguridad, no tendremos la plena tranquilidad y satisfacción de construir una red segura, y si no queremos tener una red inalámbrica inconsistente y de un desagradable trago a margo para nosotros como ensambladores de ellas, propongo que siempre y adonde quiera que se lleve o de, la comunicación de este tipo, ya sea en la parte mas remota de nuestro bello planeta, ahí este siempre como punto primordial y política de la organización, implementar su seguridad.

Y es por esa razón y motivo, es que propongo que en cada lugar, en cada sitio o área que se arme una red inalámbrica tener siempre primero que nada presente estas reglas de ORO que propongo que se incluyan el los manuales de procedimientos de la organización y planeación de la construcción de esta telaraña invisible a la vista, y dijo reglas de oro en sentido figurado, por que, eso es realmente lo que procesamos desde el envió de un pequeño mail hasta el mandar un relación financiera de números confidenciales de algunos clientes, información valiosa como el oro mismo, por que de ser robada, extraviada y duplicada no solo pone en riesgo el prestigio de la institución si no también puede provocar daños a las personas que ahí laboren, por que no solo la información es valiosa sino también la persona que la analiza, procesa y usa, que somos nosotros. Por eso a donde quiera que haya y en cualquier lugar que se monte esta tecnología propongo las siguientes reglas doradas que en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos.

REGLAS DE ORO
1. Cambia la contraseña por defecto.
2. Usar encriptación WEP/WPA.
3. Cambia el SSID por defecto.
4. Desactiva el broadcasting SSID.
5. Activa el filtrado de direcciones MAC.
6. Establece el nº máximo de dispositivos que pueden conectarse.
7. Desactiva DHCP.

8. Desconecta el AP cuando no se vaya ha usar.
9. Cambia las claves WEP/WPA regularmente.

III.1.1.1 DETALLES DE CADA UNA DE LAS REGLAS DE ORO:

Nota 1: Antes de ejecutar las reglas recomiendo siempre, **consulta el manual** del Punto de Acceso y del accesorio o dispositivo Wi-Fi para ganar información detallada.

Nota 2: En las siguientes reglas aparece un personaje, él observador o intruso, como la persona de la que queremos proteger nuestra red.

Asegurar el Punto de Acceso:
1. Cambia la contraseña por defecto.

Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso. Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que el observador la conozca.

Evitemos las contraseñas como la fecha de nacimiento, el nombre de la pareja, etc. Intentemos intercalar letras con números.

Aumentar la seguridad de los datos transmitidos:
2. Usar encriptación WEP/WPA.

Activar en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits cuanto mayor sea el número de bits mejor.
Los Puntos de Acceso más recientes permiten escribir una frase a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercalemos mayúsculas con minúsculas y números, evitemos utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").
También tendremos que establecer en la configuración WEP la clave que se utilizará de las cuatro generadas (Key 1, Key 2, Key 3 o Key 4).

Después de configurar el AP tendremos que configurar los accesorios o dispositivos Wi-Fi de la red. En éstos tendremos que marcar la misma clave WEP (posiblemente podremos utilizar la frase anterior) que hemos establecido para el AP y la misma clave a utilizar (Key 1, Key 2, Key 3 o Key 4).
Es sabido que con algunos programas y el suficiente tiempo pueden obtenerse estas claves. En cualquier caso si el observador encuentra una red sin encriptación y otra con encriptación, preferirá "investigar" la primera en vez de la segunda.

Algunos Puntos de Acceso más recientes soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.

Si activamos WPA en el Punto de Acceso, tanto los accesorios y dispositivos WLAN de la red como el sistema operativo deben soportarlo o actualizar.

Ocultar la red Wi-Fi:
3. Cambiar el SSID por defecto:

Este nombre la mayoría de las veces suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID", en vez de "MiAP", "APAlfredo" o el nombre de la empresa, es preferible escoger algo menos atractivo para el observador, como puede ser "Descompuesto", "Abajo" o "Desconectado".
Si no llamamos la atención de él observador hay menos posibilidades de que éste intente entrar en nuestra red.

Desactiva el broadcasting SSID.
4. El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual.

Al desactivarlo tendremos que introducir manualmente el SSID en la configuración de cada nuevo equipo que se quiera conectar.

Si el observador conoce nuestro SSID (por ejemplo si está publicado en alguna web de acceso libre) no conseguiremos nada con este punto.

Evitar que se conecten:
5. Activa el filtrado de direcciones MAC.

Activar en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tenga funcionando. Al activar el filtrado MAC dejaremos que sólo los dispositivos con las direcciones MAC especificadas se conecten a la red Wi-Fi.

Por un lado es posible conocer las direcciones MAC de los equipos que se conectan a la red con tan sólo "escuchar" con el programa adecuado, ya que las direcciones MAC se transmiten "en abierto", sin encriptar, entre el Punto de Acceso y el equipo. Aunque en teoría las direcciones MAC son únicas a cada dispositivo de red y no pueden modificarse, la MAC puede ser escuchada.

Establece el número máximo de dispositivos que pueden conectarse.
6. Establecer el nº máximo de dispositivos que pueden conectarse.

Si el AP lo permite, establece el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

Desactiva DHCP.
7. Desactiva DHCP.

Desactivar DHCP en el router y en el AP. En la configuración de los dispositivos/accesorios Wi-Fi tendremos que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario.
Si el observador conoce "el formato" y el rango de IPs que usamos en nuestra red, no habremos conseguido nada con este punto.

Para los más cautelosos:
8. Desconecta el AP cuando no lo uses:

Desconecta el Punto de Acceso de la alimentación cuando no se esté usando o no vaya a hacerlo durante una temporada. El AP almacena la configuración y no necesitarás introducirla de nuevo cada vez que lo conectes.

Cambia las claves WEP regularmente:
9. Cambia las claves WEP/WPA regularmente.

Por ejemplo semanalmente o cada 2 ó 3 semanas.
Antes decíamos que existen aplicaciones capaces de obtener la clave WEP de nuestra red Wi-Fi analizando los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 Gb de datos para romper una clave WEP, dependiendo de la complejidad de las claves.

Cuando lleguemos a este caudal de información transmitida es recomendable cambiar las claves.

Recordar que tenemos que poner la misma clave WEP en el Punto de Acceso y en los dispositivos que se vayan a conectar a éste.

Tomemos pues estas nueve reglas como parte de un hábito de cultura en nuestro que hacer como ensambladores de esta tecnología, enfocándonos a uno de los recursos más preciados de la informática y desde luego de la organización, la seguridad de sus datos e información. Ahora puedo afirmar con estas consideraciones no será fácil para los observadores escuchar nuestra red, aun que no ahí sistema seguro, con estas consideraciones bastara para no tener intrusos o fugas de información confidencial.

III.2 SIGNIFICADO DE Broadcast

Un **Broadcast** es un método de comunicación donde un dispositivo envía un único paquete de datos direccionado a cada uno de los dispositivos en una red, de comunicación de uno a todos.

En Ethernet, existen inherentemente al menos 2 tipos de comunicaciones, unicast y broadcast. Unicast es una forma de comunicación uno a uno.

En otros protocolos, puede haber un tercer tipo de modo de comunicación llamado Multicast. Multicast es una forma de comunicación de uno a muchos, y es ligeramente más complejo.

Una Tormenta de Broadcast (Broadcast Storm) es una condición donde los dispositivos en una red están generando principalmente tráfico Broadcast (los cuales a su vez pueden causar que se genere más tráfico) tal que dicho tráfico cause que el rendimiento de la red se degrade drásticamente, llegando en ocasiones a la perdida total de la operatividad de la red, debido a la magnitud de la Tormenta de Broadcast.

III.3 CONSECUENCIAS DE MANTENER "ABIERTA" UNA RED INALÁMBRICA.

Para muchos usuarios que hemos trabajado en redes alambradas, estamos acostumbrados a conectarnos y usarlas sin fijarnos en ningún aspecto de seguridad. Por esta razón, pensamos que en una red inalámbrica tampoco hay que preocuparse por nada; pero existe mucha diferencia en la forma de usar un tipo de red y otro. Si una persona extraña quisiera invadir una red alambrada, tendría que colocar un cable entre el conmutador general (Switch) y su, maquina; es algo muy complicado, desde cualquier punto de vista; el eventual intruso, tendría que introducirse a la casa u oficina sin ser descubierto; luego, tendría que conectar y tender su cable de conexión, de modo que nadie lo encontrara; tendría que llevarlo hasta el exterior del inmueble, y finalmente conectarlo en su sistema. Obviamente, no podría hacerlo todo esto sin que nadie lo viera, es decir, las redes alambradas son, por definición, casi completamente seguras. **Ver Figura 1.28.**

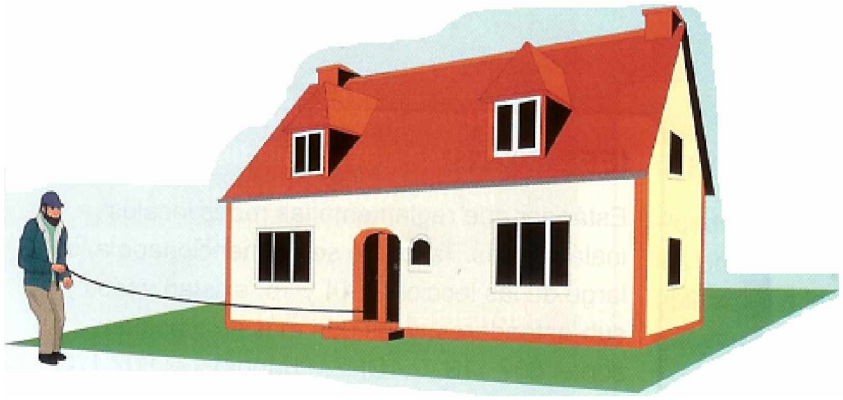


Fig. 1.28

En cambio, una red inalámbrica utiliza un medio inmaterial para hacer el intercambio de información; se trata de las ondas radiales. Esto significa que no hay un enlace físico entre el emisor y el receptor; basta con que el invasor se coloque en un sitio suficientemente cercano al punto de acceso inalámbrico (WAP), para que pueda recibir la señal que este elemento emite. **Ver Figura 1.29.**

Fig.1.29

Particularmente esta situación, ha dado origen a un fenómeno muy interesante y peligroso: el **war-driving**. Aunque en América Latina este problema todavía no es muy conocido, seguramente será el "dolor de cabeza" de muchos usuarios, cuando el uso de las redes inalámbricas sea tan común como el de las redes tradicionales.

III.4 EL FENÓMENO "WAR-DRIVING" Y SUS POSIBLES CONSECUENCIAS.

El termino "War-driving", se usa para hacer referencia a una practica común de los hackers y crackers en los países avanzados, donde las redes inalámbricas se

están generalizando rápidamente. Un War-driving es una persona (obviamente no autorizada), que se sube a su automóvil con una computadora portátil con un adaptador inalámbrico y comienza a recorrer las zonas de clase media y alta, para localizar puntos en que existen redes inalámbricas no protegidas. Cuando localizan una red con intensidad de señal adecuada, simplemente estacionan el automóvil en un sitio cercano (dentro del área de cobertura de la red) y comienza a explotar los archivos del usuario, su información confidencial, etc.; o bien aprovecha su acceso a Internet para recibir o enviar mensajes. **Ver Figura 1.30.**

Fig. 1.30

Un ejemplo, supongamos que un cracker utiliza el método de War-driving para acceder de forma ilegal a la red de determinado usuario, para desde ahí difundir un virus muy peligroso. Cuando las autoridades locales comiencen a investigar y localicen el acceso a Internet desde el cual se inicio la proliferación del virus, finalmente llegaran hasta la red de dicho usuario; pero él no tendrá manera de probar que en realidad el problema lo genero una persona ajena. Lo mismo puede suceder con el envió de spam, con el intercambio de pornografía infantil, con el envió de mensajes terroristas, con transacciones de dinero ilegales, etc.

Una vez logrado su objetivo, el cracker que tuvo acceso a una red ajena simplemente apagara su equipo, encenderá su automóvil y se alejara; y las consecuencias de sus actos recaerán en el titular de la misma.

¿Cómo se puede evitar todo esto? Aplicando ciertas medidas de seguridad, estaríamos indefensos si no hiciéramos esto, por que la información es el todo

para una organización, empresa u oficina. Protejamos pues nuestros intereses. Razón de ser de mi propuesta.

III.5 LA PROTECCIÓN WEP

WEP, son las siglas en ingles de “protección equivalente a alambrado”; pero algunas autoridades, lo interpretan como “protocolo de encriptación inalámbrico” (Wireless Encoding Protocol). Esto significa que en el momento de activar el protocolo, todas las comunicaciones entre un punto de acceso inalámbrico (WAP) y alguna de las maquinas “cliente”, se harán de forma encriptada; esto impide que los usuarios no autorizados tengan acceso a los recursos de la red. **Ver figura 1.31.** Existen dos niveles de protección WEP: la de 64 bits, que es la mas común y la de 128 bits, que es mucho mas segura pero consume mayores recursos de la red es conveniente hacer una aclaración: cuando un fabricante de equipo inalámbrico señala que su dispositivo puede manejar hasta 54 Mbts, quiere decir que dicha razón de transferencia se aplica en señales abiertas sin encriptación. De esta manera, si al momento de activar el protocolo WEP, de inmediato se nota una notoria caída de el flujo máximo de datos, es que una porción de este ancho de banda se utilaza, precisamente, en labores de encriptación; la reducción es mas notoria, cuando se usa un WEP de 128 Bits. Por tal razón, la gran mayoría de los usuarios preferimos mantenerse en un nivel de 64 Bits; aunque es un poco menos seguro, es más rapito.

Fig. 1.31

Para activar el protocolo WEP, simplemente entremos a la configuración de su punto de acceso o Router inalámbrico e ir al apartado de seguridad. Como ejemplo principal que tome para tratar de explicar como se gestiona esto se muestra en la imagen de abajo, de un, Router inalámbrico ***SMC modelo SMC2804WBRP-G, de 54Mbps,*** es uno de los que con mas facilidad se puede conseguir en México y América Latina, la imagen nos muestra como es físicamente el Router ***SMC2804WBRP-G.*** **Ver Figura 1.32.**

Fig. 1.32

La siguiente imagen nos mostrara la pantalla de configuración de este enrutador; se explica detalladamente el significado de cada punto, y la forma de configurarlos para tener una red segura. **Ver Figura 1.33**. Existen otros puntos que no están relacionados con la protección WEP, pero que ayudan a incrementar la seguridad de una red inalámbrica; se configura en el apartado "Wireless". Ver imagen respectiva, que explica el significado de cada punto, y la forma correcta de configurarlos. **Ver Figura 1.34.**

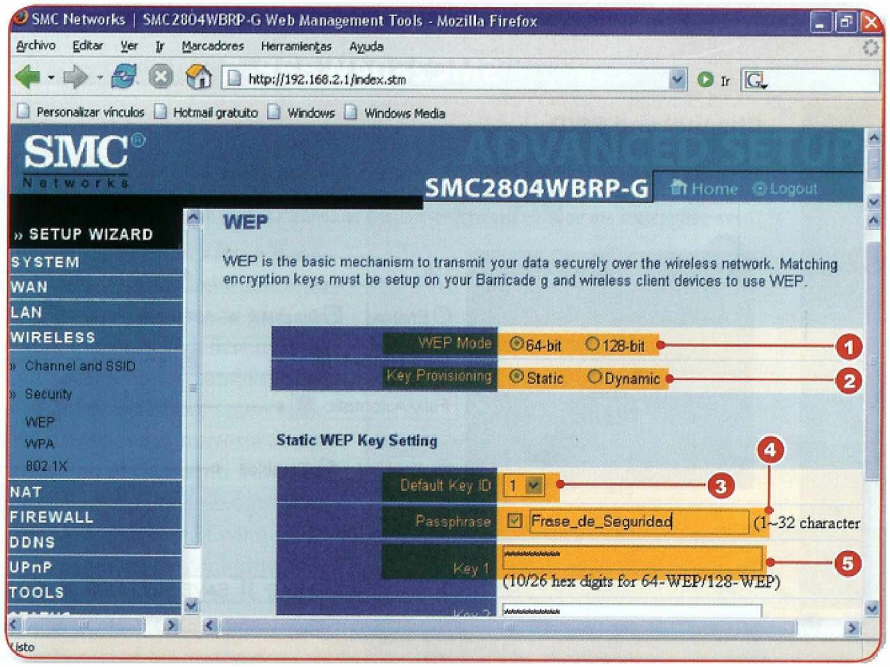


Fig.1.33

1. **Modo WEP**: aquí se fija la cantidad de bits que se utilizan para encriptar la señal inalámbrica. Podemos elegir entre 64 bits y 128 bits. En México y América Latina, en general, una codificación de 64 bits suele ser suficiente, además, así no se resta velocidad de intercambio de datos a la red.
2. **Tipo de clave empleada:** podemos elegir una clave fija y una variable. En realidad, es mas fácil configurar una red con clave fija, las de clave variante, en ocasiones suelen presentar algunos problemas, sobre todo al momento de añadir nuevos equipos.
3. **Identificador de clave predeterminada:** en este punto, podemos elegir el número del conjunto de claves generadas que se usaran para la codificación de las comunicaciones en esta red. Es mejor dejarla en "1", por que no todos los adaptadores inalámbricos tienen esta capacidad.
4. **Frase de seguridad:** aquí debemos escribir una frase de hasta 32 caracteres, la cual servirá para generar las claves encriptadas que se usaran para el intercambio de datos entre sistemas. Procuremos que sea lo mas larga posible y que combinemos letras mayúsculas, minúsculas y números, para mayor seguridad. Pero no lo olvidemos.
5. **Clave 1,2, etc.:** a partir de la frase elegida, se generaran diversas claves, mismas que pueden ser escogidas por el usuario, si este es el caso. Aseguremos de elegir exactamente el mismo número de clave en todos sus elementos inalámbricos, para garantizar la comunicación entre ellos.

III.5.1 OTROS PUNTOS QUE ESTÁN RELACIONADOS CON LA PROTECCIÓN WEP, QUE AYUDAN A INCREMENTAR LA SEGURIDAD DE UNA RED INALÁMBRICA.

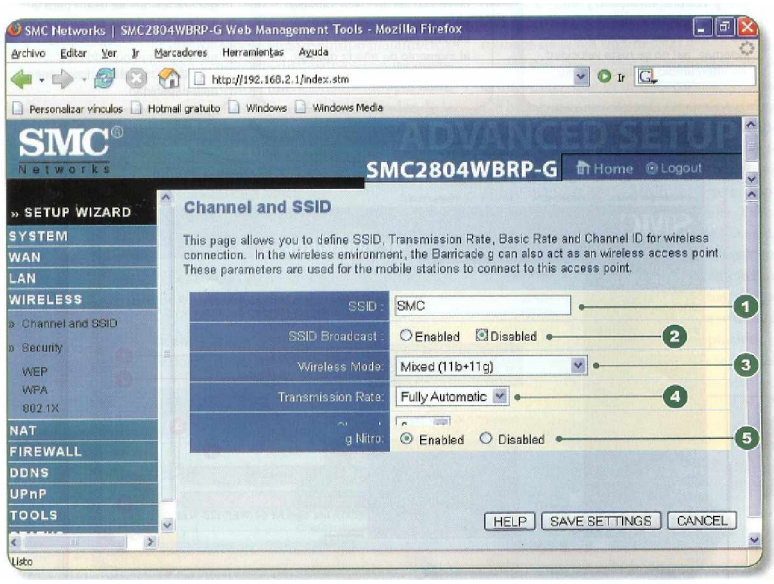


Fig. 1.34

1. SSID (identificador de servicio del equipo):

Aquí debemos colocar el nombre que se dará a la porción inalámbrica de la red. Nunca dejemos el nombre que el fabricante incluye de fábrica, ya que los crackers los conocen y esto facilitara el ataque a la red inalámbrica.

2. Transmisión del SSID:

Se puede habilitar o deshabilitar. Si está habilitada la red transmitirá continuamente un mensaje diciendo algo así como “soy una red inalámbrica y me llamo OFICINA”. De esta manera un cracker podrá conocer el nombre de la red. Es mejor dejarla deshabilitada.

3. Modo inalámbrico:

Podemos elegir entre una red de tipo G (54Mbps), una tipo B (11Mbps) o una combinada. Si todos sus dispositivos cumplen con el estándar G, es mejor configurarla así, si no estamos seguros, mejor déjelo como una red combinada.

4. Velocidad de transmisión:
Aquí podemos elegir entre "automático", "54Mbps", "22Mbps", "11Mbps" y "5Mbps" (las opciones varían de marca en marca). Lo mejor es dejarlo en automático, para que el transmisor fije la velocidad óptima para la comunicación.

5. Canal inalámbrico empleado:
Fijemos el número de canal que utilizamos para enlazar los equipos. Este mismo canal deberá se configurado en todos los dispositivos inalámbricos de la red.

III.6 PUNTOS FUERTES Y DÉBILES DEL PROTOCOLO WEP.

La protección WEP, es el primer intento realizado para dar mayor seguridad a las redes inalámbricas; pero como fue creada hace varios años, sus limitaciones y deficiencias se han hecho evidentes ante los cambios ocurridos en las redes de este tipo; sobre todo, si tomamos en cuenta que la mayoría de los ensambladores actuales, en el momento de configurar su punto de acceso inalámbrico, no se toman la molestia de cambiar la contraseña de entrada a las plantillas de configuración; siguen o seguimos usando la clave proporcionada por le propio fabricantes del WAP. **Ver Figura 1.35.**

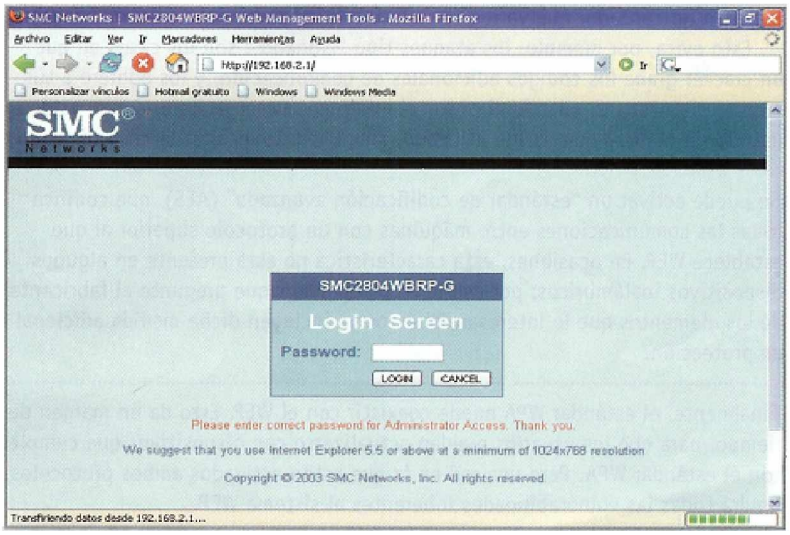


Fig. 1.35

Y para nuestra mala suerte, los crackers conocen perfectamente todas estas contraseñas; de manera que si nosotros no cambiamos la del WAP con que estamos trabajando, "facilitamos" el trabajo de estos nefastos personajes. Otro problema que se presenta, y que esta relacionado directamente con la protección

WEP, es que al activarla se solicita al usuario que introduzca una “frase de seguridad” (passphrase) de hasta 32 caracteres. A un así, desgraciadamente elegimos una palabra que es fácil de recordar para él (el nombre de la esposa, fecha de nacimiento, etc.) y es sumamente fácil de adivinar para cualquier persona que quiera invadir nuestra red. Para evitar este problema, debemos elegir una frase de seguridad que tenga la mayor cantidad posible de caracteres; y se es necesario, integrémosla con letras mayúsculas, minúsculas y números, para dificultar todavía mas la “labor de adivinación” de cualquier persona extraña. **Ver Figura 1.36.**

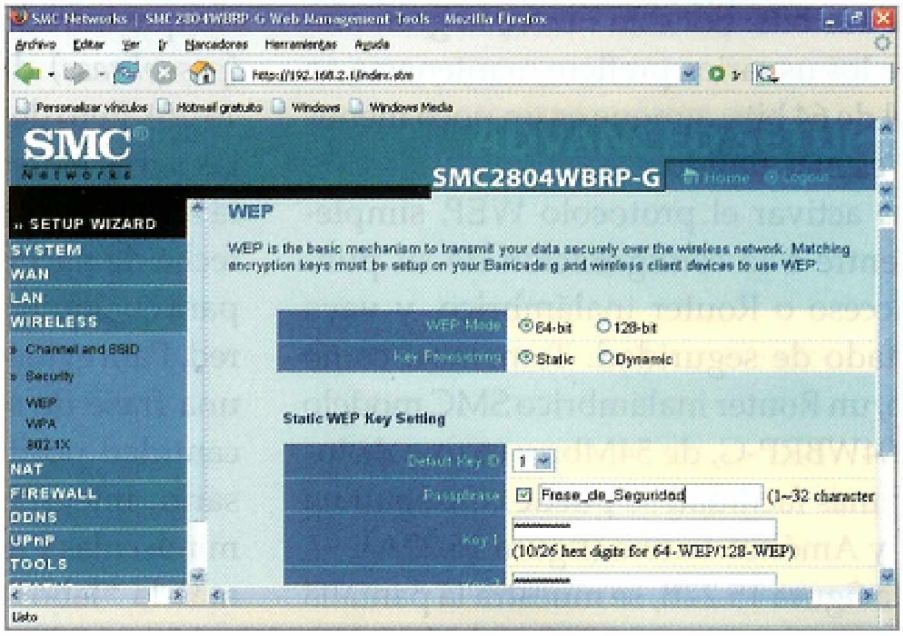


Fig.1.36

III.7 LA LLEGADA DE UN NUEVO ESTÁNDAR: EL PROTOCOLO WPA.

Aunque el protocolo WEP suele ser suficiente para desalentar las intenciones de los crackers promedio, a veces estos personajes, por “cuestión de honor”, insisten en introducirse en determinada red; y hacen acopio de todos los recursos a su alcance (entre ellos la paciencia), para conseguir su objetivo; y casi siempre, encuentran algún “hueco” por el que se introducen a la red; es decir, la protección WEP no es la clave de acceso (por ejemplo, mediante un ataque de

"fuerza bruta"), podría disponer de todos los recursos compartidos de la red, incluyendo el acceso a Internet.

Para complicarles la existencia a los crackers y mejorar en gran medida la protección de las redes inalámbricas, recientemente fue aprobado por IEEE una nueva especificación que contempla medidas de seguridad mucho más estrictas. A estas reglas se les conoce generalmente como "protección **WPA**".WPA (no confundir con WAP) son las siglas en ingles de "Acceso Protegido a WiFi". Es un nuevo estándar de seguridad, inicialmente planteado por varias compañías del área de las redes informáticas, que mas tarde recibiría el aval del IEEE. En la tabla siguiente de abajo se especifican tales disposiciones.

El estándar WPA representa un gran avance en el campo de la seguridad de las redes inalámbricas. En lo posible, construyámosla solamente con los elementos que cumplan tales especificaciones.

TABLA DE CARACTERÍSTICAS DE WPA
° En el estándar de seguridad WPA, se exige que todas las comunicaciones realicen un protocolo de autenticación que cumpla con el estándar 802.1x. En el estándar WEP, este procedimiento era opcional.
° En todas las computadoras y dispositivos inalámbricos que utilicen este nuevo estándar, deberá usarse una "contraseña común" formada hasta por 64 caracteres.
° Una vez elegida esta contraseña común, los dispositivos WPA la tomaran como base; y periódicamente, van generando nuevas claves dinámicas (protocolo TKIP: protocolo de integridad con clave temporal). De manera que si algún cracker logra averiguar la contraseña común de una red instalada, ni siquiera con ella podrá acceder a los recursos de la misma.
° El cambio de contraseñas se hace de manera simultanea en todas las maquinas de la red. Y el punto de acceso inalámbrico, se encarga de avisar del movimiento a todos sus "clientes".
° Incluye un nuevo protocolo, llamado Michael, que sirve para llevar un control muy preciso de las comunicaciones entre los clientes y el punto de acceso. Para el efecto, a cada comunicación se añade una serie de códigos de seguridad que incluyen un contador que va registrando todas las comunicaciones realizadas. Esto evita, por ejemplo, los ataques tipo "clonado" que son los casos en que un cracker graba los códigos adicionales de comunicación, y los adhiere a sus mensajes. Entonces, cuando el protocolo detecta que en el contador se esta usando un numero que ya fue utilizado, simplemente rechaza la comunicación.
° Se puede activar un estándar de codificación avanzado (AES), que codifica todas las comunicaciones entre maquinas con un protocolo superior al que establece WEP. En ocasiones, esta característica no esta presente en algunos dispositivos inalámbricos; por eso se recomienda que preguntemos al fabricante de los elementos que le interesan, si estos ya incluyen dicha medida adicional de protección.
° Finalmente, el estándar WPA puede coexistir con el WEP. Esto da un margen de tiempo, para que los usuarios puedan actualizarse con dispositivos que cumplan con el estándar WPA. Pero una red en la que estén activados ambos protocolos, tendrá todas las vulnerabilidades inherentes al WEP.

III.7.1 CONFIGURACION DEL PROTOCOLO WPA.

¿Como se configura la protección WPA en una red inalámbrica? Para este efecto, nos serviría de base el ruteador SMC que he venido utilizando en explicaciones anteriores. Bueno, una vez que se haya conectado este elemento y que se haya

puesto la configuración de la conexión a Internet, ejecutemos los siguientes pasos:

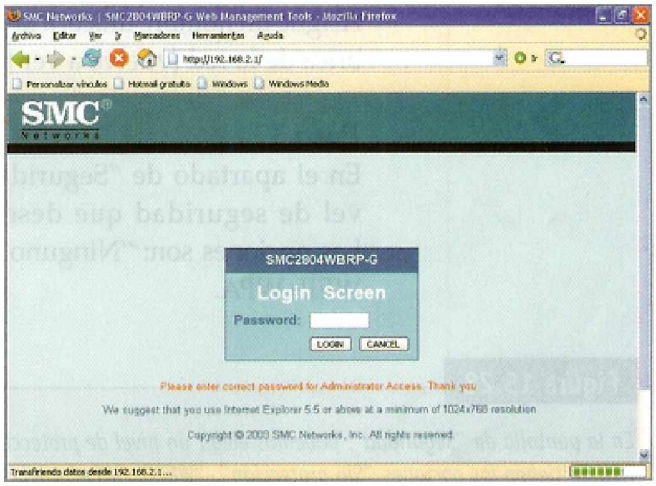
Paso 1

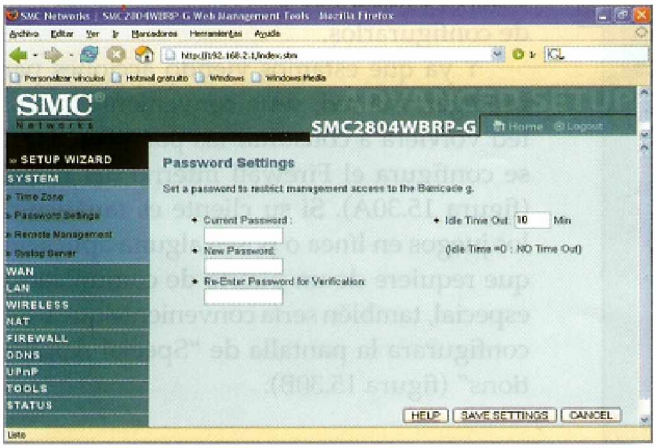
Acceder a la utilería de configuración de nuestro ruteador, mediante el navegador de Internet (Explorer, opera, mozilla o firefox).

Paso 2

Introduzcamos en la barra de direcciones, la combinación de números que le indique el fabricante (en el caso de SMC, la dirección a escribir es http:// 192.168.2.1). En ese momento, aparecerá una ventana en donde se nos pide que escriba la contraseña adecuada ver la ilustración de esta ventana mas abajo. Busquemos en el manual del equipo; y luego de encontrar, procuremos cambiarla de inmediato a un valor que solo nosotros o el administrador de la red conozca. Esto evitara que cualquier persona extraña, entre y modifique la configuración. **Ver Figura 1.37.**

Fig.1.37





Todos los componentes de una red inalámbrica, incluyen una contraseña de seguridad que normalmente viene predeterminada desde fábrica. Cambiémosla lo más pronto posible

Paso 3

Ya que se tenga esta configuración básica, es recomendable que desactivemos la opción "administración remota". Si no lo hacemos, dejaremos abierta la posibilidad de que algún usuario, malicioso acceda a estas pantallas de configuración y de que, por lo tanto haga cambios en la red, **ver figura 1.38.**

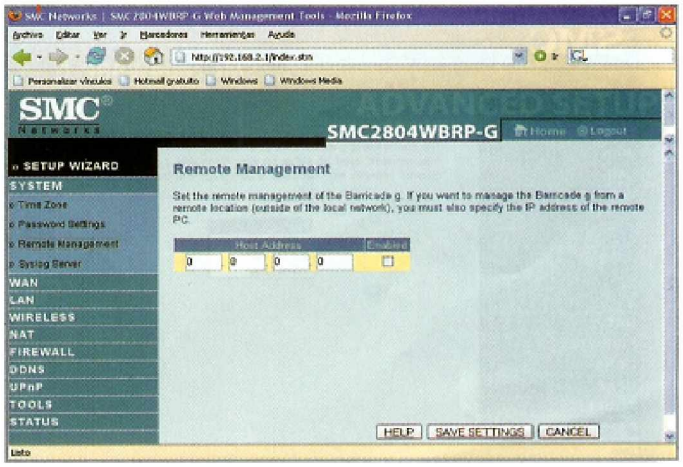


Fig. 1.38

Aunque hay otros puntos que se pueden configurar, la mayoría de ellos corresponden a la función de Router del dispositivo. Después de esto dirijámonos al menú "Wireless" (inalámbrico) para ver como se gestiona la configuración de la protección de la red local.

III.8 PROCESO INICIAL DE CONFIGURACIÓN PARA LA PROTECCIÓN INALÁMBRICA WAP:

Para llevar acabo este proceso para de configuración de la protección de este tipo de redes, ejecutemos los siguientes pasos:

Paso 1

Lo primero que debe de hacerse, es indicar al equipo que va a trabajar como un punto de acceso inalámbrico (WAP). Para el efecto, habilitemos el modulo respectivo.

Paso 2

Asignemos un nombre único, a la porción inalámbrica de la red volver a ver la **Ver figura 1.34**

Paso 3

Ya en el apartado de "seguridad", elijamos el nivel de seguridad que deseemos para la red. Las opciones son: "Ninguno", WEP, WPA Y WEP+WPA.

Dado que el nivel de seguridad que ofrece el estándar WPA es mucho mayor que el de WEP, conviene que solo deje habilitada la opción WPA. Pero esto tiene un pequeño detalle: como algunos equipos no tan modernos son incapaces de soportar el nivel WPA (ya sea por limitaciones de hardware o de sistema operativo), no podrían ser integrados a una red que tuviese activada dicha característica.

NOTA: el sistema operativo también importa para WPA. Debido a que la especificación de seguridad de WPA es de muy reciente aparición, no todos los sistemas operativos están acondicionados, de manera predeterminada, para trabajar con ella; carecen de las rutinas necesarias para integración lógica. De hecho, en el mundo de las computadoras personales con ambiente Windows, tan solo la versión Windows XP puede manejar el nivel de seguridad WPA; pero para esto, debe contar con un pequeño parche adicional que puede descargarse desde el sitio de Microsoft; y si nosotros estamos utilizando otra versión de Windows, tendremos que recurrir a programas expertos para poder activar la protección WPA; por ejemplo, el programa Odyssey, de la compañía Funk software (http://www.funf.com/), o el programa Aegis, de Meeting House (http://www.mtghouse.com/). Con esto reafirmo que más vale invertir lo que sea necesario en la compra de estas aplicaciones comerciales, que dejar la red inalámbrica expuesta a serios ataques extremos.

Es por esta razón, que en la actualidad se prefiere dejar el nivel de protección como una combinación de WEP+WPA; así, los usuarios que ya cuentan con un equipo moderno obtienen un mayor nivel de protección; y los que carecen de dicha capacidad, tendrán que conformarse con una seguridad tipo WEP. **Ver Figura 1.39.**

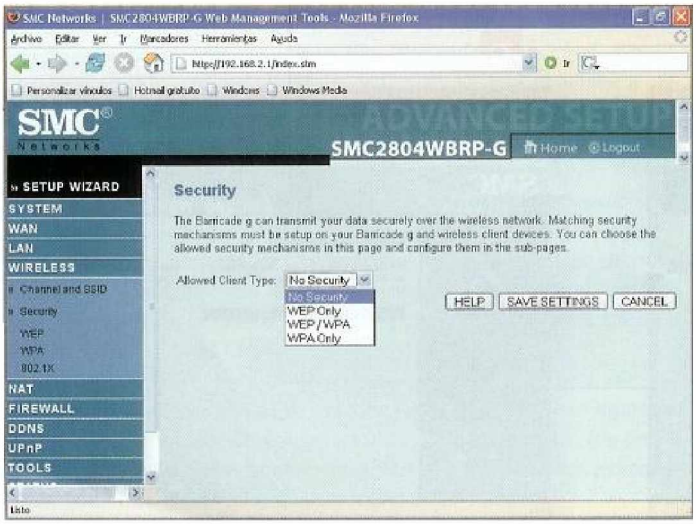


Fig.1.39

Bueno ya fue explicado como se configura una protección para una WEP o WPA, dependiendo de la tecnología que use esa red, menciones los 3 pasos iniciales de configuración que son a groso modo 1.indicar al equipo que va a trabajar con un punto de acceso inalámbrico, 2. La asignación de un nombre único y 3.la elección del nivel de seguridad, la cuestión no termina ahí. Ahora pasare a explicar los pasos complementarios de la configuración para una WPA o WEP.

Ahora bien, antes de pasar a los pasos complementarios de la esta configuración, **Ver Figura 1.40.** Algo a un también importante ya que estamos viendo las acciones para proteger una red, es conveniente que usemos y hagamos la configuración del Firewall interno del Router y el uso de aplicaciones especiales. Esto es específicamente si nos llegáramos a encontrar un cliente que fuese fanático de los juegos en línea o que posea alguna aplicación que requiere de un puerto de comunicación especial.

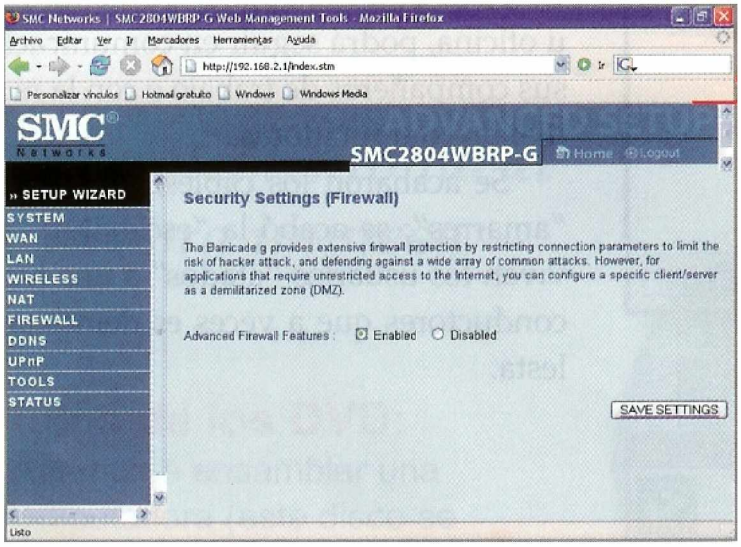
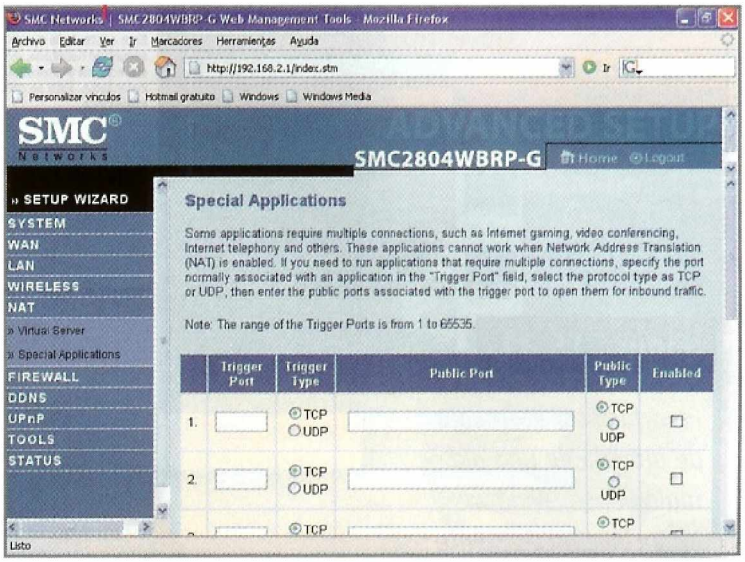


Fig. 1.40



Vale la pena activar otros factores de protección, tales como el Firewall interno del Router. Y si es necesario, también activar la lista de excepciones, de esta manera, ciertos programas podrán comunicarse con la red mundial.

Pasos complementarios para la configuración, se ilustrara primero con la **Figura 1.41.**

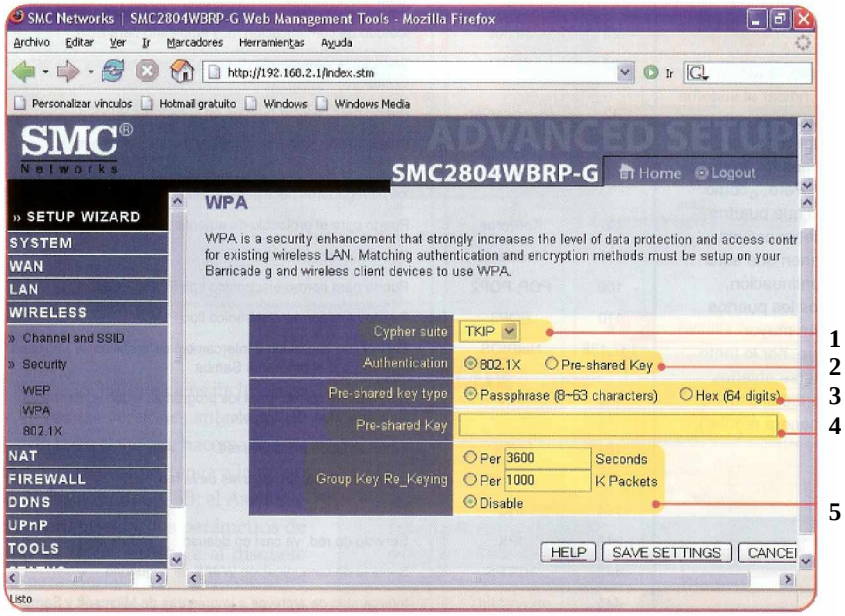


Fig.1.41

Paso1 SUITE DE CIFRADO:

Tiene como opción predeterminada TKIP (protocolo de integridad por clave temporal). Implica el uso de una clave de acceso dinámica (no fija); esto significa que incluso si un cracker llegara a determinar la clave correcta en un momento dado, al cabo de unos momentos, como cambia la clave, perdería nuevamente el acceso a la red.

Paso 2 AUTENTICACIÓN:

Tiene dos opciones: 802.1x y clave pre-compartida; aquí debemos definir si la protección WPA cumplirá con los estándares de la especificación 802.1x (que es extremadamente segura), o simplemente se definirá una clave compartida común para todos los dispositivos inalámbricos. La primera es más segura, la segunda es más rápida y fácil de configurar.

Paso 3 FRASE DE CONTRASEÑA:

Aquí elegiremos si se escribirá una frase alfanumérica (de hasta 64 caracteres; puede incluir símbolos), o si se fijara una contraseña en modo hexadecimal. Por facilidad, se prefiere la primera.

Paso 4 CAMPO PARA ESCRIBIR LA FRASE-CONTRASEÑA:

Procure que tenga la mayor cantidad de caracteres posibles y, de preferencia, mezcle letras mayúsculas, minúsculas, números y símbolos, para hacer mas difícil la tarea de "forzar" dicha clave.

Paso 5 TIEMPO PARA EL CAMBIO DE UNA NUEVA CLAVE:

Este ultimo campo se define cada cuanto tiempo calcular una nueva clave de seguridad; se puede fijar un tiempo determinado (en segundos), una cierta cantidad de paquetes de información intercambiados o bien deshabilitarlo.

Una vez hechas estas selecciones, guardémoslas en el sistema. Entonces, el ruteador inalámbrico quedara listo para comenzara distribuir la señal de Internet entre todas las maquinas de la red, y para comunicarse con aquellas que incluyan un adaptador inalámbrico. Sin embargo, para que se pueda establecer la comunicación, todavía hay que configurar estos adaptadores de manera individual.

Para configurar el adaptador de acceso a la red inalámbrica, ahí que especificarle que usuarios pueden interactuar con la red inalámbrica, es necesario ir a cada equipo y configurar su respectivo adaptador, esto implica la introducción del nombre del grupo inalámbrico, del canal de comunicaciones, etc. Para ejemplificar este caso, usare un adaptador inalámbrico tipo USB. **Ver figura 1.42.** Observemos su pantalla de configuración en la **figura 1.42** (si deseamos modificar los parámetros predeterminados, solo presione el botón "change" y haga los cambios necesarios).

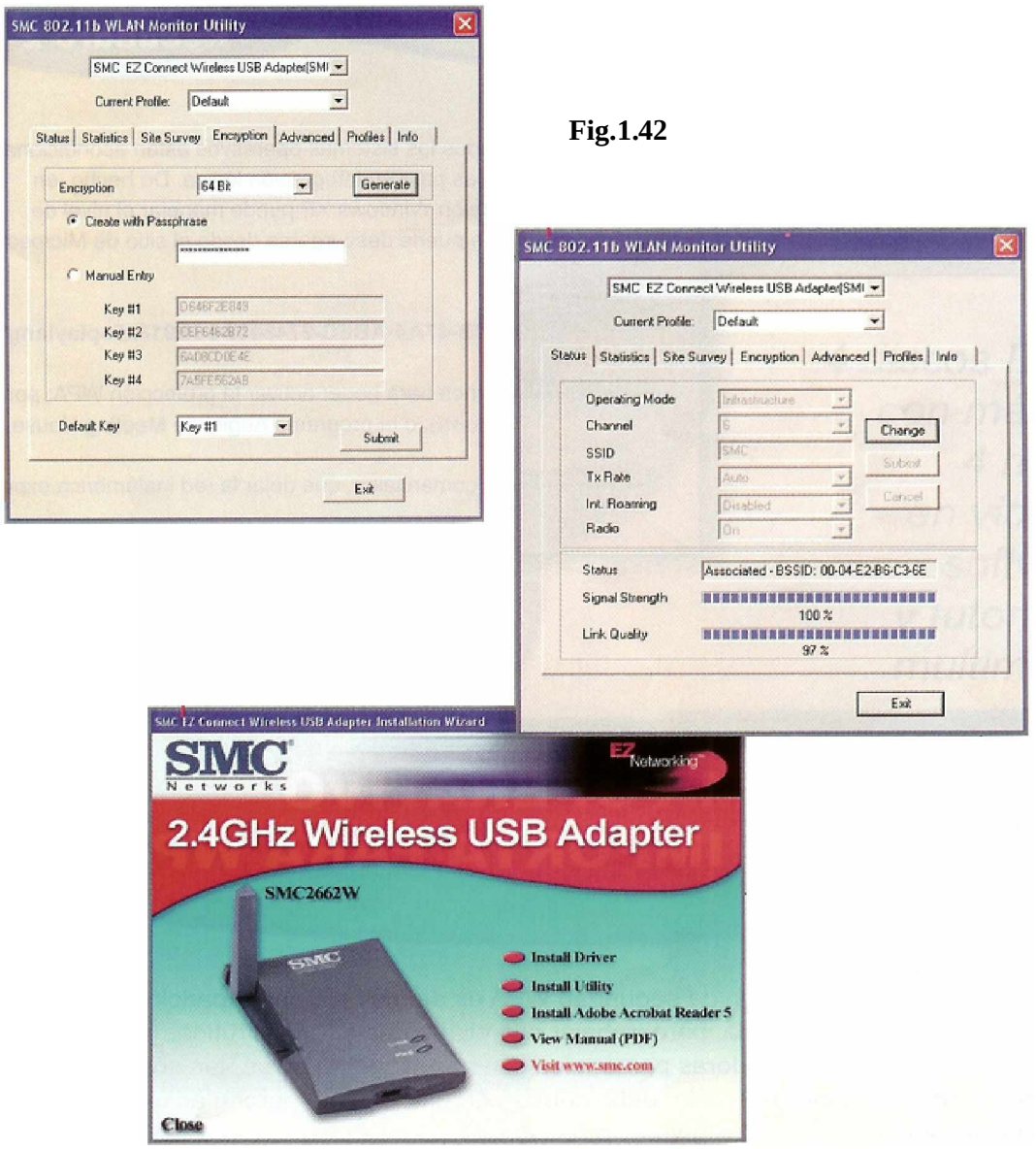


Fig.1.42

Para que el adaptador inalámbrico pueda comunicarse con el punto de acceso, deberemos configurar adecuadamente las protecciones WEP y WPA**.** La configuración de los equipos se hace con mayor facilidad usando el asistente de conexión a redes inalámbricas. **Ver Figura 1.43**; que viene incluido en Windows XP (en las versiones anteriores de Windows, esta tarea tiene que hacerse de forma manual). Y si es posible, tener a al mano una memoria flash de tipo USB; el asistente la solicitara, para guardar los parámetros de cada equipo, es decir, sustituye al disquete que se usa para ciertas tareas del asistente de conexión a

redes locales. El precio de estos dispositivos ha disminuido en los últimos meses, así que su adquisición no implicara un gasto extraordinario.

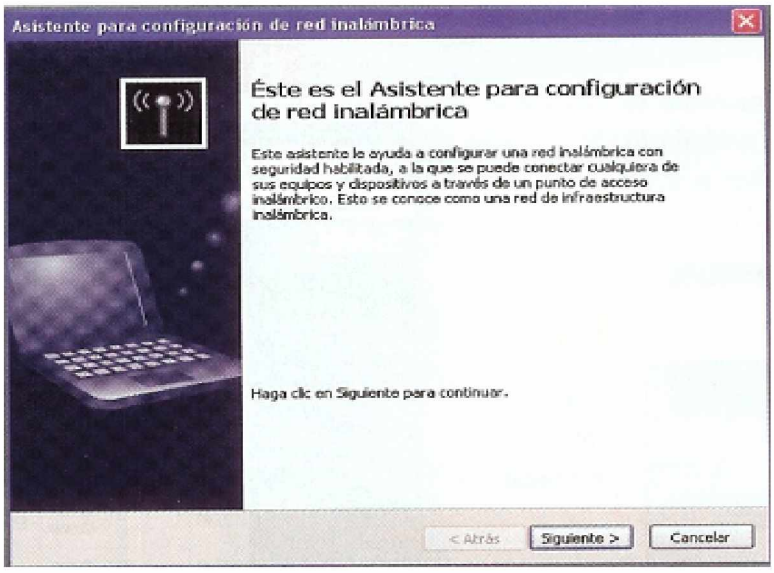
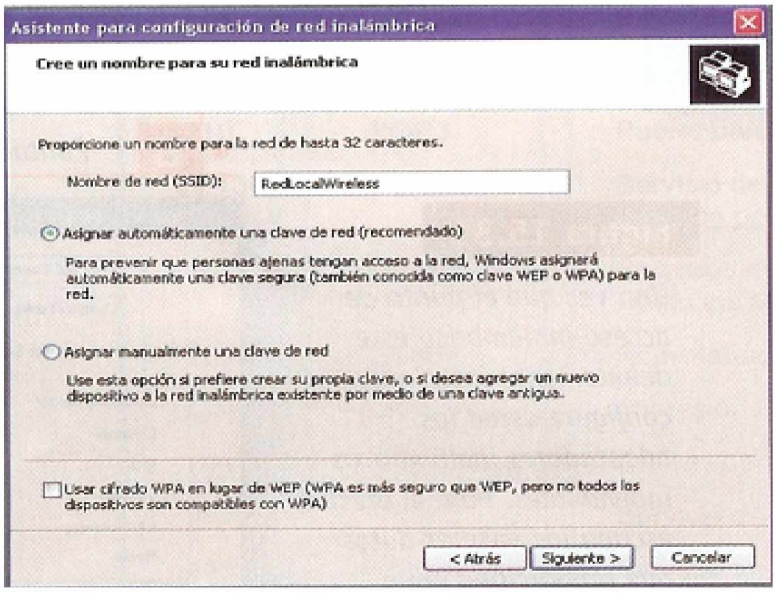


Fig.1.43



Una vez que hayamos configurado adecuadamente cada punto de la red inalámbrica, tenderemos como principal satisfacción de a ver instalado una red inalámbrica con los mas altos niveles de SEGURIDAD y desde luego dejando

satisfecho a nuestro cliente si ese fuera el caso. Aplicando estas medidas de seguridad, fomentando la cultura de que no ahí que escatimar en la protección de uno de los tesoros mas preciados de una oficina, empresa, organización y hogar, en su defecto, la información. Con esto tendremos solamente como tarea disfrutar de ella, con absoluta libertad y sobretodo gocemos nosotros una plena seguridad desde cualquier punto de donde se origine la comunicación.

III.9 PUERTOS USADOS CON MAYOR FRECUENCIA EN LAS COMUNICACIONES DE LA PLATAFORMA PC.

Este punto es muy importante, puesto que si queremos tener el control total de seguridad, también tenemos que tener el control sobre los puertos de comunicación abiertos de una computadora, sobre todo, cuando se encuentra conectada a la red mundial. Y es precisamente, la función de un Firewall que es indicar al sistema que puertos de comunicación pueden permanecer abiertos, y que aplicaciones tendrán acceso a ellos. Pero, ¿Cómo sabremos que puertos deben de permanecer activos y que puertos tienen que estar cerrados? He aquí una tabla mas de los puertos que se usan con mayor frecuencia y que, por lo tanto, deben mantenerse abiertos (siempre y cuando el usuario los utilice de manera regular).

N°. de puerto	Servicio que lo utiliza	Descripción
20	ftp-data	Intercambio de datos a través del estándar FTP.
21	ftp	Intercambio de datos a través del estándar FTP.
23	Telnet	Método de comunicación muy empleado para BBS.
25	SMTP	Servicio de intercambio de correo, con servicios tipo sendmall, postfix y exchange.
42	Nameserver	Puerto para replicar puertos en servidores WINS de Microsoft.
53	Domain	Puerto usado para intercambiar Dominios de Internet.
80	HTTP	Puerto principal para la comunicación a través del estándar WWW. Todos los navegadores necesitan de este puerto, para acceder a Internet.
88	Kerberos	Puerto para el protocolo de autenticación Kerberos.
101	Hostname	Puerto usado por los NICs.
109	POP,POP2	Puerto para correo elctronico tipo pop y pop2
110	POP3	Puerto para correo electronico tipo pop3
137,138y139	NetBIOS	Servicio de impresión e intercambio de archivos de Microsoft. También es utilizado por el programa Samba.
143	IMAP	Servicios de correo, para los programas Outlook, Exchange,

		Netscape mail, Eudora, etc.
161	SNMP	Administración simple de red.
170	printsrv	Impresión Postcript, a treves de la red.
194	IRC	Chateo por Internet.
213	IPX	Servicio de red, ya casi en desuso.
443	HTTPS	Servicio de comunicación WWW de seguridad.
445	microsfotds	Intercambio de archivos e impresoras de Microsoft y samba.
464	Kpass	Intercambio de contraseñas de Kerberos.
532	Netnews	Servicio de noticias por Internet.

III.10 LA SEGURIDAD DE LA INFORMACION Y CRIPTOGRAFIA.

Seguridad de la Información.

El concepto de seguridad en la información es mucho más amplio que la simple protección de los datos a nivel lógico. Para proporcionar una seguridad real hemos de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar habrá que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podemos hacer la siguiente subdivisión:

1. Sistemas aislados. Son los que no están conectados a ningún tipo de red. De unos años a esta arte se han convertido en minoría, debido al auge que ha experimentado Internet.

2. Sistemas interconectados. Hoy por hoy casi cualquier ordenador pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes sean cada día más complejas y supongan un peligro potencial que no puede en ningún momento ser ignorado.

En cuanto a las cuestiones de seguridad las podemos clasificarlas de la siguiente forma:

1. **Seguridad física**. Englobaremos dentro de esta categoría a todos los asuntos relacionados con la salvaguarda de los soportes físicos de la

información, más que de la información propiamente dicha. En este nivel están, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de backup, etc. También se suelen tener en cuenta dentro de este punto aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.

2. Seguridad de la información. En este apartado prestaremos atención a la preservación de la información frente a observadores no autorizados. Para ello podemos emplear tanto **criptografía simétrica** como **asimétrica**, estando la primera únicamente indicada en sistemas aislados, ya que si la empleáramos en redes, al tener que transmitir la clave por el canal de comunicación, estaríamos asumiendo un riesgo excesivo.

3. Seguridad del canal de comunicación. Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.

4. Problemas de autentificación. Debido a los problemas del canal de comunicación, es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente creemos que viene. Para esto se suele emplear criptografía asimétrica.

5. Problemas de suplantación. En las redes tenemos el problema añadido de que cualquier usuario autorizado puede acceder al sistema desde fuera, por lo que hemos de confiar en sistemas fiables para garantizar que los usuarios no están siendo suplantados por intrusos. Normalmente se emplean mecanismos basados en password para conseguir esto.

III.10.1 CRIPTOGRAFÍA

El ser humano siempre ha tenido secretos de muy diversa índole, y ha buscado mecanismos para mantenerlos fuera del alcance de miradas indiscretas. Julio César empleaba un sencillo algoritmo para evitar que sus comunicaciones militares fueran incerceptadas. Leonardo Da Vinci escribía las anotaciones sobre sus trabajos de derecha a izquierda y con la mano zurda. Otros personajes, como Sir Francis Bacon o Edgar Allan Poe eran conocidos por su afición a los códigos criptográficos, que en muchas ocasiones constituían un apasionante divertimento y un reto para el ingenio.

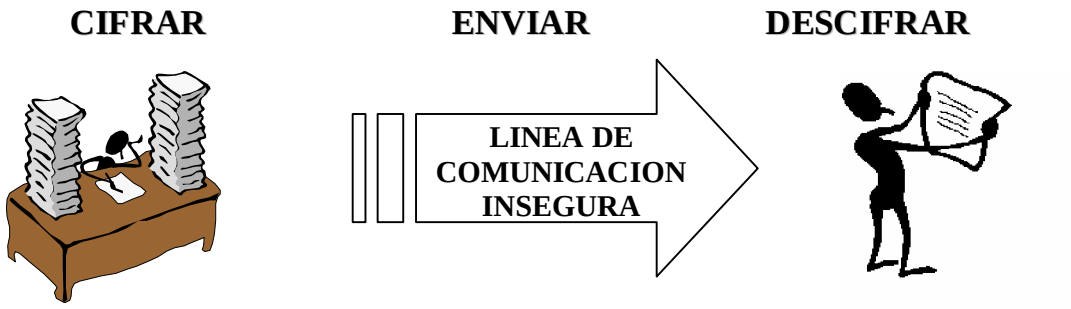
Los mecanismos criptográficos considerados clásico son todos los sistemas de cifrado anteriores a la II Guerra Mundial, o lo que es lo mismo, al nacimiento de las computadoras. Estas técnicas tienen en común que pueden ser empleadas usando simplemente lápiz y papel, y que pueden ser criptoanalizadas casi de la misma forma. De hecho, con la ayuda de las computadoras, los mensajes cifrados empleando estos códigos son fácilmente descifrables, por lo que cayeron rápidamente en desuso.
La transición desde la Criptografía clásica a la moderna se da precisamente durante la II Guerra Mundial, cuando el Servicio de Inteligencia aliado rompe la máquina de cifrado del ejército alemán, llamada ENIGMA.
Todos los algoritmos criptográficos clásicos son simétricos, ya que hasta mediados de los años setenta no nació la Criptografía asimétrica.

Según el Diccionario de la Real Academia, la palabra Criptografía proviene del griego *kryptos*, que significa oculto, y *gráphein*, que significa escritura, y su definición es: Arte de escribir con clave secreta o de un modo enigmático. Obviamente la Criptografía hace años que dejó de ser un arte para convertirse en una técnica, o más bien un conglomerado de técnicas, que tratan sobre la protección ocultamiento frente a observadores no autorizados de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la

Teoría de Números o Matemática Discreta, que estudia las propiedades de los números enteros, y la Complejidad Algorítmica.

La palabra Criptografía solo se refiere al uso de códigos, por lo que no engloba a las técnicas que se usan para romper dichos códigos (Criptoanálisis). El término Criptología, aunque no está recogido aún en el Diccionario, se emplea habitualmente para agrupar estas dos disciplinas.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje "escondido" (lo llamamos descifrar o descencriptar).



Criptosistema

Definiremos un criptosistema como una quíntupla (M; C; K; E; D), donde:

- **M** representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto plano, o plaintext) que pueden ser enviados.
- **C** representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- **K** representa el conjunto de claves que se pueden emplear en el criptosistema.
- **E** es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente.

- **Ek** para cada valor posible de la clave k.
- **D** es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

Dk (Ek (m)) = m

Es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

Criptoanálisis.

El criptoanálisis consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación. No se considera criptoanálisis el descubrimiento de un algoritmo secreto de cifrado; hemos de suponer por el contrario que los algoritmos siempre son conocidos.

Existen dos tipos fundamentales de criptosistemas:

Criptografía simétricas o de clave privada. La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar. Este tipo de criptografía se conoce también como criptografía de clave privada o criptografía de llave privada.

Existe una clasificación de este tipo de criptografía en tres familias, la criptografía simétrica de bloques (block cipher), la criptografía simétrica de lluvia (stream cipher) y la criptografia simétrica de resumen (hash functions).

Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas, sin embargo es importante verlas por separado dado que se usan en diferentes aplicaciones.

La criptografía simétrica ha sido la más usada en toda la historia, ésta ha podido ser implementada en diferentes dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

La criptografía simétrica es aquella que emplean la misma clave K tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave K debe estar tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitir la clave de forma segura.

Criptografia asimétricos o de llave pública. La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada.

Dependiendo de la aplicación que le demos al algoritmo, la clave pública será la de cifrado o viceversa. Para que estos criptosistemas sean seguros también ha de cumplirse que a partir de una de las claves resulte extremadamente difícil calcular la otra.

Los algoritmos de llave pública, o algoritmos asimétricos, han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet). Introducidos por Whitfield Diffiey Martin Hellman a mediados de los años 70, su novedad fundamental con respecto a la criptografía simétrica es que las claves no son únicas, sino que forman pares. Hasta la fecha han aparecido multitud de algoritmos asimétricos, la mayoría de los cuales son inseguros.

Otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que el mensaje original, bien sea porque la longitud de la clave es enorme. Se basan en general en plantear al atacante problemas matemáticos difíciles de resolver. En la práctica muy pocos algoritmos son realmente útiles. El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable. Otros algoritmos son los de El Gamal y Rabin.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos se recomiendan claves de al menos 1024 bits. Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado por bloques.

En la práctica los métodos asimétricos se emplean únicamente para codificar la clave Secreta (simétrica) de cada mensaje.

El método asimétrico emplea una doble clave (kp; kP). kp se conoce como clave privada y kP se conoce como clave pública. Una de ellas sirve para la transformación E de cifrado y la otra para la transformación D de descifrado.

En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp.

En la práctica se emplea una combinación de estos dos tipos de criptografía, puesto que los segundos presentan el inconveniente de ser computacionalmente mucho más costosos que los primeros. En el mundo real se codifican los mensajes (largos) mediante algoritmos simétricos, que suelen ser muy eficientes, y luego se hace uso de la criptografía asimétrica para codificar las claves simétricas (cortas).

Para poder entender un poco de la criptografía, es tiempo de plantear que tipo de problemas resuelve ésta. Los principales problemas de seguridad que resuelve la criptografía son: la privacidad, la integridad, la autenticación y el no rechazo.

La privacidad, se refiere a que la información sólo pueda ser leída por personas autorizadas.

Ejemplos: en la comunicación por teléfono, que alguien intercepte la comunicación y escucha la conversación quiere decir que no existe privacidad. Si mandamos una carta y por alguna razón alguien rompe el sobre para leer la carta, ha violado la privacidad.
En la comunicación por Internet es muy difícil estar seguros que la comunicación es privada, ya que no se tiene control de la línea de comunicación. Por lo tanto al cifrar (esconder) la información cualquier intercepción no autorizada no podrá entender la información. Esto es posible si se usan técnicas criptográficas, en particular la privacidad se logra si se cifra el mensaje con un método simétrico.

La integridad, se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.

Ejemplos: En Internet las compra se puede hacer desde dos ciudades muy distantes, la información tiene necesariamente que viajar por una línea de transmisión de la cual no se tiene control, si no existe integridad podrían cambiarse por ejemplo el número de una tarjeta de crédito, los datos del pedido en fin información que causaría problemas a cualquier comercio y cliente.

La integridad también se puede solucionar con técnicas criptográficas particularmente con procesos simétricos o asimétricos.

La autenticidad, se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.

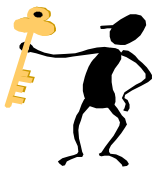
Ejemplo: cuando se quiere cobrar un cheque a nombre de alguien, quien lo cobra debe de someterse a un proceso de verificación de identidad para comprobar que en efecto es la persona quien dice ser, esto en general se lleva a cabo con una credencial que acredita la identidad de la persona que la porta. La verificación se lleva a cabo comparando la persona con una foto o con la comparación de una firma convencional.

Por Internet es muy fácil engañar a una persona con quien se tiene comunicación respecto a la identidad, resolver este problema es por lo tanto muy importante para efectuar comunicación confiable.

Las técnicas necesarias para poder verificar la autenticidad tanto de personas como de mensajes usan quizá la más conocida aplicación de la criptografía asimétrica que es la firma digital, de algún modo ésta reemplaza a la firma autógrafa que se usa comúnmente. Para autenticar mensajes se usa criptografía simétrica.

El no rechazo, se refiere a que no se pueda negar la autoría de un mensaje enviado.

Información Segura Autorizada



Persona

Cuando se diseña un sistema de seguridad, una gran cantidad de problemas puedes ser evitados si se puede comprobar autenticidad, garantizar privacidad, asegurar integridad y evitar el no-rechazo.

La criptografía simétrica y asimétrica conjuntamente con otras técnicas, como el buen manejo de las claves y la legislación adecuada resuelven satisfactoriamente los anteriormente problemas planteados.

III.11 CRIPTOGRAFÍA SIMÉTRICA vs CRIPTOGRAFÍA ASIMÉTRICA.

La **Criptografía Simétrica**, es claramente insuficiente para llevar a cabo comunicaciones seguras a través de canales inseguros, debido a que los dos interlocutores necesitan compartir una clave secreta. Dicha clave debe ser transmitida en algún momento desde un extremo a otro del canal de comunicación de forma segura, ya que de ella depende la protección de toda la información que se transmita a lo largo de esa sesión en particular. Necesitamos, pues, un canal seguro para poder crear otro canal seguro.

La **Criptografía Asimétrica** ofrece una salida al problema, proporcionando ese canal seguro de comunicación que va a permitir a los participantes intercambiar las claves de sesión (como se mencionaba anteriormente). Y ésa no es la única ventaja, ya que los algoritmos asimétricos ofrecen mecanismos fiables para que ambos interlocutores se puedan identificar frente al otro de manera segura. La razón por la que no se emplean algoritmos asimétricos todo el tiempo es porque, entre otras ventajas, los criptosistemas simétricos resultan mucho más eficaces y rápidos. Ver las siguientes imágenes de cómo es el funcionamiento y el proceso de encriptado y descecriptamiento, usando el algoritmo de cifrado RC4.

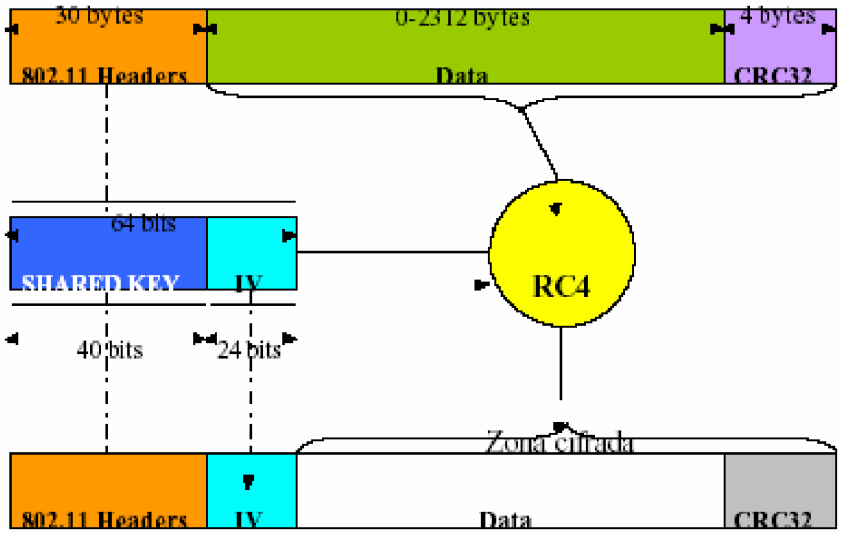
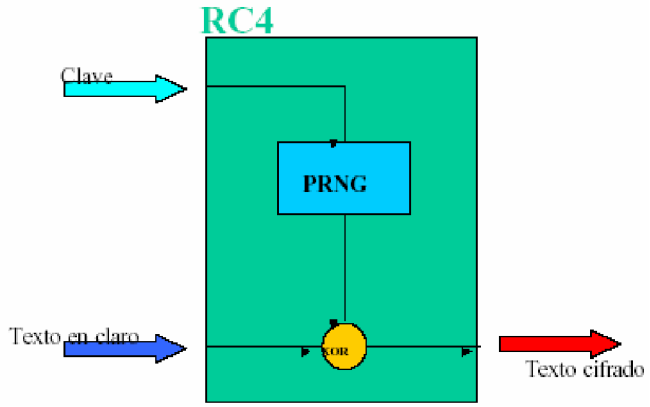
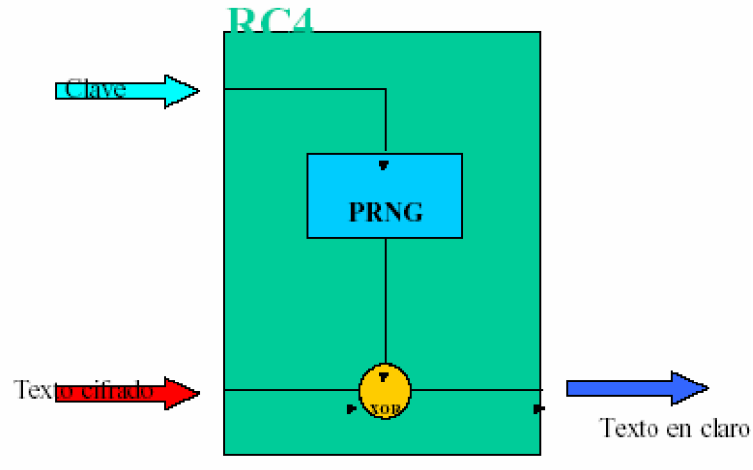


DIAGRAMA DEL PROCESO DE ENCRIPTADO Y VICEVERSA.





RC4 creado en 1987 por Ronald Rivest, secretario comercial de RSA Data Security, por eso la R de RSA. RC4 usa claves a partir de 1 a 256 bytes (8 a 1024 bits) donde cada paquete cifrado, contiene un IV sin cifrar y el bloque de datos cifrado, el cual a su vez contiene un CRC32 (cifrado) para comprobar la integridad. Inicializando una tabla de estados, esta tabla se usa para generar una lista de bytes pseudos-aleatorios, que a su vez estos bytes se combinan mediante la función XOR con el texto en claro, y el resultado es el texto cifrado. La clave se introduce de forma manual, no hay un sistema automático seguro de distribución de claves y normalmente todas las estaciones que comparten un Access Point utilizan la misma clave. Si se requiere cambiar la clave se aria en forma manual.

CRC32: Es un sistema pensado para solucionar errores producidos de forma involuntaria en el sistema de transmisión. No sirve para evitar modificaciones maliciosas ya que al ser lineales permiten la reconstrucción de los códigos. Cambiando ciertos bits de los datos, es posible calcular los cambios necesarios en el CRC32 para mantenerlo coherente, antes de encriptar se realiza un CRC32 del paquete, los paquetes cuyo CRC32 sea incorrecto, simplemente son rechazados. Algunos algoritmos de cifrado son:

- DES: Data Encryption Standard, llave de 56-bits.
- IDEA: Internacional Data Encryption Algorithm, llave de 128bits.
- RC2, RC4, RC5: Ronald Rivest RSA, llave de long variable.
- RIJNDAEL: (AES) Advanced Encryption Standard, adoptado en 2001.

III.12 EL FUTURO DE LAS REDES INALÁMBRICAS *(proyección).*

Los fabricantes de WLANs migraron de la banda de 900 MHz a la banda de 2.4 GHz para mejorar la velocidad de información. Este patrón continua al abrirse el estándar IEEE 802.11a en la banda de 5.7 GHz operando con una velocidad de datos de hasta 54 Mbps, actualmente en desarrollo. Esta banda de 5.7 GHz promete otras mejoras en velocidad permitiendo quizá algún día romper la barrera de los 100 Mbps; esperemos.

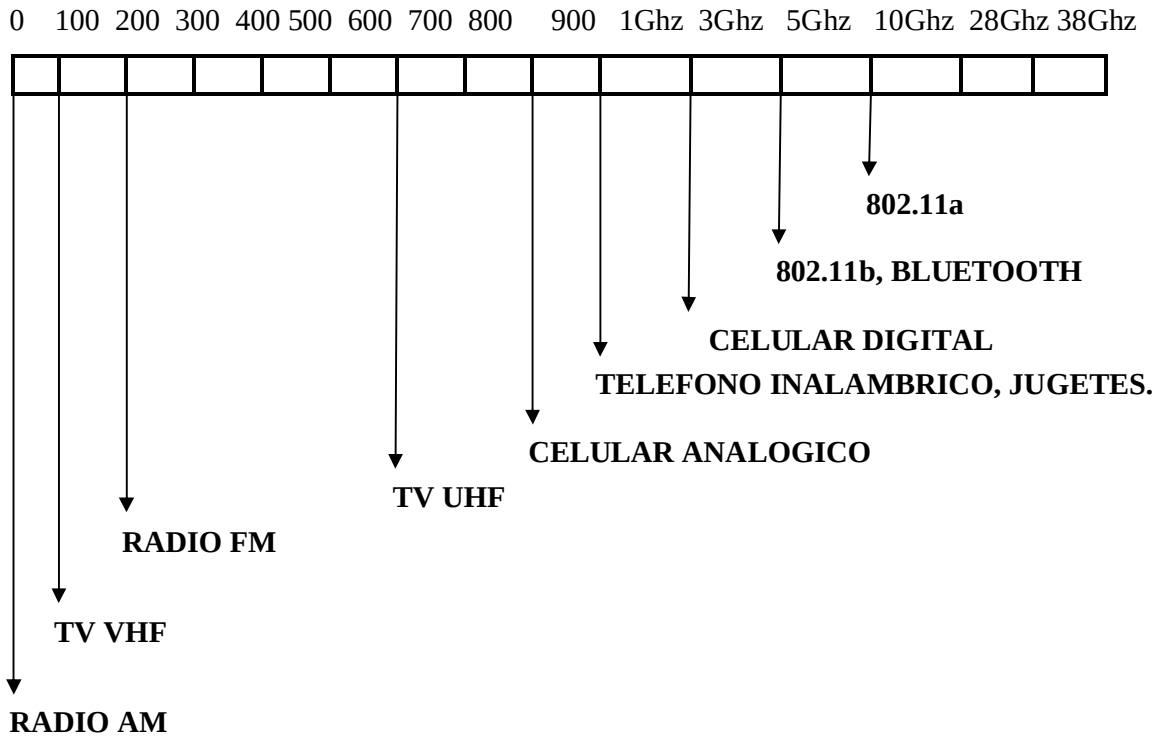
Otras tecnologías para redes inalámbricas también han emergido paralelamente a las definidas por la IEEE 802.11x, tales como Bluetooth, HomeRF, LMDS (Local Multipoint Distribution Service), WLL (Wireless Local Loop), también la entrada de nuevos protocolos, lenguajes y esquemas de seguridad ha sido de gran importancia en el avance de las redes inalámbricas tales como WAP (Wireless Application Protocol), WML (Wireless Markup Language), WEP (Wired Equivalent Privacy), entre otros.

Hoy en día las WLANs han redefinido lo que significa estar conectado. Han extendido los límites de las LANs. Hacen infraestructuras tan dinámicas de acuerdo a las necesidades. Con los estándares y productos inalámbricos interoperables.

Con relación al costo los equipos de WLANs han abierto nuevos mercados. Para esta tecnología, la demanda continua incrementándose, la reducción del costo en la ingeniería y eficiencia en la fabricación permitirán la reducción mas de los costos, hasta que llegue un día en que un adaptador de un cliente inalámbrico cueste lo mismo que un adaptador alámbrico. Si tomamos en cuenta el cableado y el costo de mano de obra que involucra instalar una red alámbrica, esta diferencia será muy poca entre ambas tecnologías.

TABLA DE FRECUENCIAS INALAMBRICAS

WIRELESS



GLOSARIO

ANALOGICO: Relativo o referente a un dispositivo o señal que esta variando continuamente en intensidad o magnitud, como, por ejemplo, una tensión o un sonido, en lugar de estar basado en unidades discretas, como son los dígitos binarios 1 y 0. Un atenuador de luz, de los que pueden encontrarse en algunas casas, es un dispositivo analógico porque (a diferencia de los interruptores tradicionales) no dispone de un conjunto limitado de posiciones absolutas.

ANCHO DE BANDA: 1. La diferencia entre la frecuencia mas alta y la mas baja que un sistemas de comunicaciones analógico puede dejar pasar, medidas en hercios (Hz) o ciclos por segundo. Por ejemplo, un teléfono tiene un ancho de banda de 3.000 Hz: la diferencia entre la frecuencia mas baja (300Hz) y la mas alta (3.300Hz) que puede transportar. **2**. la capacidad de transferencia de datos o velocidad de transmisión de un sistema de comunicaciones digitales medida en bits por segundo (bps).

APPLE TALK: Una red de área local de bajo coste desarrollada por apple computer, inc; para computadoras Macintosh y que puede ser usada por computadoras tanto apple como no apple para comunicarse y compartir recursos, como, por ejemplo, impresoras y servidores de archivos. Los equipos no apple deben incluir hardware apple talk y el correspondiente software. La red utiliza un conjunto de niveles de protocolo similar al modelo de referencia ISO/OSI y transfiere la información en forma de paquetes denominados tramas. Apple talk soporta conexiones a otras redes apple talk a través de dispositivos que se conocen con el nombre de puentes y soporta conexiones con redes de otros tipos a través de dispositivos denominados pasarelas.

ARPANET: una gran red de área extensa (WAN) creada en la década de 1960 por la ARPA (Advanced Reserch Projects Agency, una agencia del ministro de Defensa de Estados Unidos que paso a denominarse DARPA en la década de 1970) para libre intercambio de información entre universidades y organismos de investigación, aunque el ejercito americano utilizo también esta red para sus comunicaciones. En la década de 1980 se desgajo de ARPANET una red separada, MILNET, para su uso por el ejército. ARPANET fue la red a partir de la cual evoluciono Internet.

BEACON: Beacon es un pequeño programa en Java. Al ser activado, Beacon pasa a enviar y recibir datos de un grupo *multicast* específico, al cual otros Beacons también estarán vinculados. Todos los Beacons pasan a intercambiar informaciones entre sí y a calcular parámetros como pérdida, retraso (delay) y nervioso (jitter). Estos datos son enviados a una estación central, el Beacon Server, donde son consolidados. La matriz de parámetros resultante es presentada en formato HTML, permitiendo que los usuarios puedan evaluar cómo está la conectividad del propio Beacon con los demás.

BINARIO: es un programa cliente FTP, es el comando que ordena al servidor FTP que transmita o reciba los archivos en forma de datos binarios.

BIT: abreviatura de binardigit (digito binario). La unidad más pequeña de información que puede ser manejada por un equipo informático. Un bit expresa un numero binario, 1 o 0, una condición lógica, verdadera o falsa, y esta representado físicamente por un elemento como, por ejemplo, un nivel de tensión alto o bajo en un determinado punto de circuito o un pequeño punto de un disco magnetizado en un sentido o en otro. Un solo bit contiene poca información que un humano pudiera considerar significativa. Un grupo de 8 bits, sin embargo, forman un byte, que puede ser usado para representar muchos tipos de información, como una letra del alfabeto, un digito decimal u otro carácter.

BITRANTE: BINARI

CRIPTOGRAFÍA: (encriptación) es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.

DHCP: Protocolo de Configuración Dinamica de Host, un protocolo de servicio TCP/IP que permite la concesión dinámica de direcciones IP de host y distribuye otros parámetros de configuración a los correspondientes clientes de red. DHCP ofrece una configuración de red TCP/IP segura, fiable y simple, impide que existan conflictos con las direcciones, y ayuda a ahorra el numero de direcciones IP cliente en la red. DHCP usa un modelo cliente/servidor donde el servidor DHCP lleva a cabo la gestión centralizada de las direcciones IP que se utilizan en la red. Los clientes compatibles con DHCP podrán solicitar y obtener la concesión de una dirección IP de un servidor DHCP como parte de su proceso de arranque de la red.

DNS: Domain Name Service (Servicio de Nombres de Dominio). La utilidad Internet que implementa el sistema de nombres de dominio. Los servidores DNS, también denominados servidores de nombres, mantienen bases de datos que contienen las direcciones y a las que se accede de forma completamente transparente para el usuario.

DSL: Digital Subscriber Line (línea digital de abonado), una tecnología digital de telecomunicaciones recientemente desarrollada (a fines de la década de 1990) que puede proporcionar transmisiones a alta velocidad sobre cables telefónicos estándar de cobre. A menudo se hace referencia a DSL mediante las siglas Xdsl, donde la x hace referencia a uno o dos caracteres que definen diversas variantes de la tecnología DSL básica. Actualmente, ADSL (DSL asimétrica) es la forma que mas normalmente se implanta, pero incluso esta por el momento disponible solo para grupos limitados de abonados.

EAP: Protocolo de Autenticación Extensible.

MASCARA: Un número que, comparado por la computadora con un número de dirección de red, bloqueará toda la información excepto la que sea necesaria. Así, por ejemplo, en una red que utilice XXX.XXX.XXX.YYY y donde todas las computadoras de le red utilicen los primeros números de dirección iguales, las máscara bloqueará XXX.XXX.XXX y usará sólo los números significativos de la dirección, es decir, YYY.

ETHERNET (CSMA/CD): El estándar IEEE-802.3 para redes basadas en contienda. Ethernet utiliza una topología basada en bus o en estrella y emplea una forma de acceso denominada CSMA/CD (Carrier Sense Multiple Access with Collision Detection, acceso múltiple por detección de portadora con detección de colisiones) para regular el trafico en la línea de comunicaciones. Los nodos de red están enlazados mediante cable coaxial, cable de fibra óptica o cable par trenzado. Los datos se transmiten en tramas de longitud variable que contienen información de entrega y de control y hasta 1500 bytes de datos. El estándar Ethernet permite la transmisión en banda base a 10 megabits (10 millones de bits) por segundo y esta disponible en distintas variantes, incluyendo las de 10Base5, 10Base-F y Gigabit Ethernet, opera a una velocidad diez veces superior, a 100Mbps.

FDDI: Acrónimo de Fiber Distributed Data Interface (interfaz de datos distribuidos por fibra). Un estándar desarrollado por ANSI (American Nacional Standards Institute, Instituto Nacional de Estándares de Estados Unidos) para redes de área local (LAN) de alta velocidad con cables de fibra óptica. FDDI proporciona especificaciones para velocidades de transmisión de 100 megabits (100 millones de bits) por segundo en redes basadas en el estándar token ring.

FIREWALL: (Corta fuegos) Sistema de seguridad que trata de proteger la red de una organización contra amenazas externas procedentes de otra red, como piratas informáticos que intenten acceder desde Internet. Usualmente, es una combinación de hardware y software que evita que los equipos informáticos de la red de la organización se comuniquen de forma directa con otros equipos extraños a la red y viceversa. En lugar de ello, todas las comunicaciones se encaminan a través de un servidor Proxy situado fuera de le red de la organización, y el servidor Proxy decide se resulta seguro permitir que un mensaje o archivo concreto pase a su través hacia la red de la organización.

GATEWAYS: Del inglés, pasarela. Aplicación que permite la transmisión de datos de un servidor en red a otro. Red o sub red.

GHZ: abreviado de Gigahertz, es un múltiplo de la unidad de medida de frecuencia hercio, equivale a 10^9 hercios. Se utiliza fundamentalmente en informática para referirse a la velocidad de procesamiento de un microprocesador. Un Gigahertz, bien sea una unidad de corriente alterna, o de frecuencia electromagnética, que es igual a mil millones de herzios (1.000.000.000 herzios). El Gigahertz es usado como unidad de medida para frecuencia de señales

HAND SHAKING: Saludo de mano.

HETEROGENO: Conformado por partes de distintas naturalezas o tecnologías. Conjunto de elementos de diferentes especies.

HOST: Cualquier dispositivo de una red TCP/IP que tiene una dirección IP. Algunos de estos hosts son los servidores, las estaciones de trabajo, los dispositivos de impresión con interfaz de red y los encaminadotes. Algunas veces se utiliza este término para hacer referencia a un equipo específico de la red que ejecute un servicio utilizado por los clientes de la red o los clientes remotos.

ISO: Abreviatura de Internacional Organization for Standardization (a menudo, las siglas ISO se identifican incorrectamente como acrónimo de Internacional Standards Organization). Una asociación internacional de 130 países, cada uno de los cuales esta representado por su principal organización de definición de estándares. ISO trabaja para establecer estándares globales para las comunicaciones y el intercambio de información.

KERBEROS: Un protocolo de autenticación de red desarrollado por el MIT. Kerberos autentica la identidad de los usuarios que intentan iniciar una sesión en una red y cifra sus comunicaciones utilizando mecanismos criptográficos de clave secreta. El MIT distribuye una implementación gratuita de kerberos, aunque kerberos también esta disponible en muchos productos comerciales.

KILOBYTE: Unidad de medida de la capacidad de transmisión de una línea de telecomunicación equivalente a mil bytes aunque actualmente es usado como 1024 (dos elevado a la 10) bytes.

LLAVE: Un objeto metálico utilizado con una cerradura física para desactivar un sistema informático.

LLC: acrónimo de Logical Link Control (control de enlace lógico). En las especificaciones IEEE-802.x, es el mas alto de los dos subniveles que forman el nivel de enlace de datos ISO/OSI. El subnivel LLC es responsable de gestionar los enlaces de comunicaciones y procesar el tráfico de tramas.

MAC: Acrónimo de Media Accesso Control (control de acceso al medio). En las especificaciones IEEE-802.x, es el mas bajo de los dos niveles que forman el nivel de enlace de datos ISO/OSI. El subnivel MAC gestiona el acceso a la red física, delimita las tramas y se encarga del control de errores.

MODEM-DSL: Equipo que combina las funciones de tres distintos dispositivos: un MODEM DSL para el manejo de Internet de banda ancha, la capacidad de "repartir" la señal de Internet entre varios usuarios y el manejo directo de elementos inalámbricos. Ver DSL.

NAT: Net Addresses Translation o traducción de direcciones de red, proceso por medio del cual, un ruteador puede distribuir la señal de Internet sin que haya conflictos entre los distintos miembros de una red. Consiste en asignar a cada uno de ellos una dirección IP interna, desde la que recibe y a la que envía todo el flujo de Internet que sea necesario, a al vez que absorbe la dirección IP asignada por el proveedor de acceso a la red mundial.

OCTETO: Término utilizado para referirse a los ocho bits que conforman un byte.

OSI: Interconexión de Sistemas abiertos.

PICONET: El término piconet concretamente se refiere a redes de área local con pequeña cobertura y sin infraestructura.

PROTOCOLO: descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes**.**

PUENTE (BRIDGE): 1. Dispositivo que conecta redes que utilizan los mismos protocolos de comunicaciones, de modo que la información pueda pasar de una red a otra. **2.** Dispositivo que conecta dos redes de área local que pueden utilizar o no los mismos protocolos y que permite que la información fluya entre ellas. El puente opera en el nivel de enlace de datos de ISO/OSI.

PUNTO GRIS: En una red inalámbrica, se conoce así a los equipos que aun encontrándose dentro del área de cobertura de un punto de acceso, no tienen una comunicación adecuada con el resto de las computadoras de la red (conexión irregular o inexistente, extrema lentitud, etc.).

ROBUSTO: Fuerte, vigoroso, de fuertes miembros y firme salud. Resistente y fortaleza.

ROUTER: Es un equipo similar pero mas complejo que los switches. A diferencia de estos últimos, los cuales filtran el trafico en base a la dirección MAC (dirección física integrada de cada tarjeta de red), los ruteadores filtran el trafico en base a al IP (dirección lógica). Tiene además, información sobre cual debe ser la ruta a seguir por cada paquete (en base a parámetros como velocidad y trafico) y la habilidad de aprender estas direcciones. Permite el punto de interconexión entre diferentes redes y son, generalmente, el punto de entrada y salida de estas. Un router extiende el tamaño de la red con la ventaja de unir redes diferentes, proporcionan un servicio de interconexión a un mas inteligente, eligen una vía mas rapita.

SEGURIDAD: se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos. El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

SERVIDOR PROXY: Un componente corta fuegos que gestiona el trafico Internet entrante y saliente de una red y que puede proporcionar otras funciones, tales como las de almacenamiento en cache de documentos y el control de acceso. Los servidores Proxy pueden mejorar las prestaciones del sistema al encargarse de suministrar su propia copia local de los datos ,as frecuentes suministrados, como, por ejemplo, las paginas Web mas populares y pueden filtrar y descartar las solicitudes que el propietario no considere adecuadas, como por ejemplo las peticiones para obtener acceso no autorizado a archivos confidenciales.

SINCRONIZACION: Hacer que coincidan en tiempo dos o mas movimientos o fenómenos.

SNIFFER: Un sniffer es un programa que absorbe o captura datos de la red. Todo lo que pasa por delante de sus narices lo absorbe y lo almacena para su análisis posterior. De esta forma, sin poseer acceso a ningún sistema de la red, se puede obtener información, claves de acceso o incluso mensajes de correo electrónico en el que se envían estas claves.
La forma más habitual de sniffing, probablemente porque está al alcance de cualquiera, es la que podríamos llamar sniffing por software, utilizando un programa que captura la información de la red.

SPAM: Correo basura. Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico.

SWITCHES: Desde el punto de vista puramente funcional, no son muy diferentes a los Bridges. En efecto permiten segmentar las redes con los mismos criterios y los mismos modos, incorporan funciones, potencial y prestaciones muy superiores a estos. Los switches son netamente superiores a los puentes que están rápidamente desapareciendo del mercado. Entre las ventajas de los switches recordemos el numero elevado de puertos (y por lo tanto de los segmentos que se pueden conectar contemporáneamente al switch) y la posibilidad de trabajar con velocidades diferentes en cada puerto. Un switch resuelve problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelera la salida de los paquetes, reduce el tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI.

TCP/IP: Protocolo de control de transmisión/protocolo Internet. Un conjunto de protocolos desarrollados por el Departamento de Defensa de Estados Unidos para comunicaciones a través de redes interconectadas y posiblemente heterogéneas. Forma parte del sistema operativo UNIX y se ha convertido en el estándar de facto para la transmisión de datos a través de todo tipo de redes, incluyendo Internet.

TKIP: Protocolo de Integridad Clave Temporal. ISO 802.11i.

TOKEN RING: Una red de área local con topología en anillo que utiliza el paso de testigo como modo de regular el trafico en la línea. En una red token ring, se pasa de una estación a otra un testigo (token) que gobierna el derecho a transmitir, describiendo un círculo físico. Si una estación tiene información para transmitir, retiene el testigo, lo marca para indicar que esta en uso e inserta la información. El testigo de ocupado, junto con el mensaje, pasa entonces alrededor del círculo, siendo el mensaje copiado cuando llega a su destino y terminando por volver al emisor. El emisor elimina entonces el mensaje asociado y pasa el testigo libre a la siguiente estación de línea. Las redes token ring se definen en los estándares IEEE-802.5.

UDP: Paquete de Unidad de Datos.

VECTOR: Un vector es todo, segmento de recta dirigido en el espacio. Cada vector posee unas características que son: Origen, Modulo, Dirección y Sentido.

VoIP: Voice over IP. Voz sobre IP el uso del protocolo IP (Internet Protocol) para transmitir comunicaciones de voz. VoIP se utiliza para suministrar audio digitalizado en forma de paquetes y puede emplearse para transmitir a través de Internet y de redes intranet y extranet. Es esencialmente, una alternativa de bajo coste a las comunicaciones telefónicas tradicionales a través de la red telefónica general de conmutación. voIP cubre comunicaciones entre computadoras y entre teléfonos.

VoWLAN: Voz por una red inalámbrica.

VPN: Nodos de una red publica, como Internet, que pueden comunicarse entre si utilizando tecnología de cifrado, de modo que sus mensajes estén protegidos frente a posibles intercepciones y no pueden ser entendidos por los no autorizados, como si los nodos estuvieran conectados mediante líneas privadas,

WAP: Punto de Acceso Inalámbrico.

WEP: Privacidad Equivalente Alámbrica (WEP) la WEP utilizaba claves estáticas. Es también comúnmente llamado Protocolo de Encriptación Inalámbrico, utilizado desde un principio en redes inalámbricas. Permite asegurar un cierto grado de privacidad en las comunicaciones entre equipos de un mismo grupo de trabajo.

Wi-Fi: Wireless Fidelity. Fidelidad inalambrica.

WPA: Wi-Fi Acceso Protegido o también llamado, protocolo de acceso protegido.

CONCLUSIÓN

En el recién terminado siglo XX, ocurrieron acontecimientos que revolucionaron el desarrollo humano. Una de sus consecuencias es la llamada era de la información, Hoy la necesidad de comunicación y el conocimiento es un factor clave, tanto para el avance de la ciencia y la innovación tecnológica como para la vida en general.

Los avances tecnológicos actuales, resultantes en gran medida de la evolución de los medios de comunicación y electrónicos, han generado nuevas tendencias en la comunicación. El nacimiento de nuevas tecnologías. Así grandes volúmenes de información circulan por todo el mundo. Internet, el símbolo más significativo de esta nueva etapa del desarrollo humano, facilita a millones de personas obtener información desde cualquier parte del mundo, enlazada a la red. La globalización en la informática se asocia a la concentración de la información, a las tecnologías de avanzada. Valor más sagrado: la vida humana y su entorno. Debe, por lo tanto, potenciarse los conocimientos y la inteligencia empapándonos de los nuevos conocimientos, para no ser simplemente espectadores si no participadotes de esta nueva era digital. Enfoquémonos a solo una pequeñísima parte de ese mundo y su era digital, las redes inalámbricas y su seguridad.

Tenemos la herencia del siglo pasado que fue el inició para desarrollar una gran variedad de redes para las comunicaciones, entre ellas las inalámbricas. Hoy ellas rodean el globo terráqueo. La radio, la televisión y el teléfono permiten que millones de personas estén en permanente contacto y que salten distancias de miles de kilómetros, aunque son muchísimos los que carecen de acceso a ellas.

Entonces ahora puedo, con una total seguridad concluir que la tecnología inalámbrica llego para quedarse y ayudarnos a hacer mas prácticos, mas libres y productivos. Hoy en día los porcentajes de tener una red de este tipo son muy altos, ya es un hecho y es posible usarla con plena satisfacción de que nadie nos escuche y no es por que no veamos las ondas de su frecuencia, si no básicamente en el apoyo que nos brindan las medidas de seguridad propuestas. A un que no ahí sistema seguro en su totalidad. Creo y con amplia seguridad que la tendencia

general, es pensar que la comunicación inalámbrica es segura, como ya comenté en el transcurso de esta tesis seguridad para redes inalámbricas.

Espero que esta seguridad se implemente en donde quiera que haya una red de este tipo, nos hagamos tan solo un acto de conciencia de la necesidad de poner en marcha una serie de estrategias de seguridad para blindar nuestra red.

Poner en práctica las nueve reglas de oro o sólo algunas de ellas, será suficientemente para estar seguros, el poner en marcha tan solo únicamente una de ellas, ya estaremos asegurando nuestra red inalámbrica un punto más que antes. Wi-fi ha sido, sin lugar a dudas una de las tecnologías de grana apoyo para la consecución del dote de seguridad.

Wi-fi pilar fundamental en la formalización de esta tecnología, Wi-fi no solo significa conectividad y seguridad a toda hora en cualquier lugar, cafeterías, hoteles, edificios antiguos, aeropuertos, universidades, hospitales, campos militares, el hogar, oficinas o lugares temporales donde las redes se empacan y se guardan, como si fueran una simple maleta y cualquier otro sitio donde se implementen, no es solo eso, tiene una verdadera razón de ser, razón que las convirtieron en mucho mas atractivas para los ojos de los gerentes de tecnologías de información o sistemas, fue su flexibilidad, su facilidad de instalación y sobre todo el aumento de productividad que generan. Cortando cables para aumentar la productividad.

Sólo hace falta, entonces, tomar tijeras, cortas las redes y dar movimiento a la productividad de las empresas, dotarlas de seguridad y listo. Con estos antecedentes no cabe duda de la consolidación de Wi-Fi. La evidencia está a la vista. El momento de las redes sin ataduras ha llegado.

La red inalámbrica es una tecnología innovadora que apenas está surgiendo como una solución alternativa para las implementaciones empresariales, públicas y residenciales. Para dar soporte a estas implementaciones, se deben superar varios retos importantes. Aun que data desde ya casi mas de un cuarto de siglo apenas estamos viviendo un poco de lo mucho que nos podrán dar.

BIBLIOGRAFÍA:

SÁNCHEZ GONZÁLEZ, Carmelo. Microsoft Diccionario de Internet y Redes. Editorial Mc Graw Hill; España, 2003.

Manual del Club de Informática de la Universidad Autónoma de Nuevo León. Redes LAN Básico. Editorial Departamento de conectividad; México 2002.

BTcino de México. Manual de Sistemas de Cableado Estructurado. Editorial BTcino de México, S.A. de C.V. 2004.

SMC NETWORKS, Inc. Guía de usuario para el Router SMC2804WBRP-G, de 54 Mbps. Editorial SMC NETWORKS; U.S. 2003.

http://www.maxitrucos.com/articulos/montse/wireless_la_conexion_sin_cables.htm
http://www.microsoft.com/latam/technet/seguridad/guidance/lan/peap_int.mspx
http://www.maxitrucos.com/articulos/montse/wireless_la_conexion_sin_cables_2.htm
http://electronica.cicese.mx/exgallardo(innov).htm
http://www.gerencia.cl/articulo.mv?sec=3&num=89&mag=1&wmag=34
http://www.microsoft.com/latam/prensa/2001/ene/Davos_LAN.asp
http://www.ieee.org/portal/site/mainsite/menuitem.818c0c39e85ef176fb2275875bac26c8/index.jsp?&pName=corp_level1&path=about/whatis&file=index.xml&xsl=generic.xsl
http://standards.ieee.org/wireless/
http://www.microsoft.com/latam/technet/articulos/windowsxp/2008/default.asp
http://www.arturosoria.com/eprofecias/art/wireless.asp
http://www.microsoft.com/latam/technet/seguridad/guidance/lan/peap_int.mspx#EFAA
http://www.monografias.com/especiales/comunicamov/index.shtml
http://www.monografias.com/especiales/comunicamov/index2.shtml
http://www.monografias.com/trabajos12/redes/redes.shtml#redes
http://www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/solutions.asp
http://www.wirelessmundi.com/Dealer_01_2.shtml
http://www.wirelessmundi.com/Dealer_01.shtml
http://www.google.com.mx/search?hl=es&lr=&oi=defmore&q=define:Wi-Fi
http://www.red.es/glosario/glosariog.html
http://www.red.es/glosario/glosariok.html
http://www.hackxcrack.com/phpBB2/viewtopic.php?t=21310
http://www.tec-mex.com.mx/promos/bit/bit0302.htm