ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

SEGURIDAD EN REDES WIRELESS

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN INFORMÁTICA CON MENCIÓN EN REDES DE INFORMACIÓN

LOURDES MARGARITA BARRIONUEVO CELA
ROMEL ANÍBAL PAZMIÑO MOLINA

DIRECTOR: ING. MYRIAM HERNÁNDEZ

Quito, Octubre del 2004

DECLARACIÓN

Nosotros, LOURDES MARGARITA BARRIONUEVO CELA y ROMEL ANÍBAL PAZMIÑO MOLINA, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Lourdes Margarita Barrionuevo Cela Romel Aníbal Pazmiño Molina

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por LOURDES MARGARITA BARRIONUEVO CELA y ROMEL ANÍBAL PAZMIÑO MOLINA, bajo mi supervisión.

ING. MYRIAM HERNÁNDEZ
DIRECTORA DE PROYECTO

AGRADECIMIENTO

Agradecemos a Dios por sus bendiciones, a nuestros Padres y Hermanos que con su esfuerzo y dedicación supieron apoyarnos para lograr culminar con nuestra carrera universitaria

Agradecemos a la Ing. Myriam Hernández por toda la ayuda que nos ha dado y por su acertada dirección durante la elaboración de este proyecto de titulación.

DEDICATORIA

Este proyecto de titilación lo dedicamos a todas las personas que nos apoyaron durante nuestra preparación académica, a nuestros Padres y Hermanos.

CONTENIDO

CAPITULO I

INTRODUCCIÓN

CAPITULO II

SEGURIDAD EN REDES INALÁMBRICAS

CAPITULO III

ANÁLISIS Y DISEÑO DE UN PROTOTIPO BÁSICO DE RED INALÁMBRICA

CAPITULO IV

IMPLEMENTACIÓN Y PRUEBAS

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITULO I

INTRODUCCIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

Las Redes Inalámbricas de Área Local (WLAN) son la solución ideal para ejecutivos de empresas y profesionales de sistemas que desean tener una mayor libertad de movimiento, más allá de las tradicionales redes conectadas por cables o que necesitan una mayor flexibilidad para adaptarse a los cambios frecuentes. Asimismo, las redes inalámbricas de área local le dan una mayor capacidad a sus trabajadores, permitiéndoles mantenerse en contacto y dándoles un fácil acceso a la información en tiempo real.

Lugares como los aeropuertos, hoteles y restaurantes pueden instalar redes inalámbricas de área local para obtener dos soluciones en una: usar redes privadas para aumentar su productividad y redes públicas para mejorar la atención a los clientes ofreciéndoles un acceso más cómodo a servicios de correo electrónico e Internet.

Las redes inalámbricas proporcionan a las empresas una tecnología eficaz y flexible, pero con un costo de implementación y mantenimiento menor en comparación con las tradicionales redes cableadas. Al mismo tiempo las redes inalámbricas permiten a los usuarios desplazarse dentro del radio de cobertura que ofrece la instalación de la red inalámbrica sin perder la conectividad.

Hoy en día las actuales tecnologías sobre las que se sustentan las redes inalámbricas permiten la vulnerabilidad en aspectos básicos relativos a la seguridad de las mismas, esta situación además se ve agravada si las redes inalámbricas están conectadas a Internet, por lo que cualquier infraestructura

inalámbrica debe considerar paliar estas deficiencias con la incorporación de soluciones específicas que garanticen a todos los niveles una seguridad óptima.

1.2 JUSTIFICACIÓN DEL PROYECTO

En una red inalámbrica (WLAN o WWAN) autentificar usuarios y mantener confidencial las comunicaciones es más difícil que en una red conectada con cableado.

Las implicaciones en seguridad son obvias. En una red inalámbrica se puede producir fácilmente una violación de políticas de autentificación, pues cuando un usuario tiene los permisos necesarios para acceder a un sistema no está basado en una localidad física como en una LAN en una instalación segura. Igualmente puede violarse otra política fundamental de seguridad que es la confidencialidad debido a la circunstancia de que los datos se transmiten usando frecuencias de radio que viajan fuera del control de la organización: a través de paredes y techos y aún en la calle. La información que atraviesa la red inalámbrica es muy susceptible al acceso de intrusos.

El proyecto propuesto estudiará las ventajas y desventajas de la tecnología inalámbrica y analizará medidas de seguridad que eviten los problemas planteados en el párrafo anterior.

1.3 OBJETIVOS

Objetivo general:

Estudiar las ventajas y desventajas de la tecnología inalámbrica de redes. Presentar estándares y arquitecturas que se pueden usar para mejorar la seguridad en este ambiente.

Objetivos específicos:

Estudiar las bases de redes inalámbricas
Estudiar la seguridad en estas redes por niveles:

- Implementación y políticas
- Control de acceso
- Perímetros de seguridad
- Seguridad de aplicaciones

Presentar algunos diseños de redes inalámbricas usando estos principios.

1.4 ALCANCE

- Realizar un acercamiento por niveles del problema de seguridad con puntos centralizados de acceso, implementando dispositivos de seguridad en distintos niveles y gobernando el acceso interno con políticas de niveles de firewall.
- Presentar una lista de prácticas óptimas en el diseño de redes inalámbricas.
- Aplicar estos principios en algunos diseños de redes inalámbricas con distintas especificaciones.
- Presentación de un prototipo básico para análisis.

1.5 RESUMEN DE CADA CAPÍTULO

El contenido de este proyecto se encuentra estructurado de la siguiente forma:

CAPÍTULO I.-

Se realiza una introducción a lo que es seguridad en redes inalámbricas, se hace un planteamiento del problema, se establecen los objetivos y el alcance que tendrá este proyecto.

CAPÍTULO II.-

Se realiza un estudio general de las redes inalámbricas, además se hace un estudio de las políticas y perímetros de seguridad, los riesgos inherentes con que cuentan estas redes, las soluciones y los beneficios que se pueden tener.

CAPÍTULO III.-

Se muestran los detalles de la implementación de un prototipo básico para lo cual se hace un análisis de la tecnología que se utilizará.

CAPÍTULO IV.-

Se presenta toda la configuración y características de los dispositivos que se utilizaran para la implementación del prototipo básico, y se recoge todas las pruebas relacionadas con el prototipo.

CAPÍTULO V.-

Se tienen las conclusiones que se ha recopilado a través del desarrollo del proyecto.

CAPITULO II

SEGURIDAD EN REDES INALÁMBRICAS

2.1 INTRODUCCIÓN

2.1.1 RED DE ÁREA LOCAL INALÁMBRICA (WLAN) [1]

Una red de área local inalámbrica (WLAN) es un sistema flexible de comunicación de datos implementado como una extensión o como una alternativa para, una LAN alambrada. WLANs transmite y recibe los datos sobre vía aérea con tecnología de RF, minimizando la necesidad de cualquier conexión alambrada, y a su vez, combina conectividad de datos con movilidad de usuario. WLANs provee toda funcionalidad de WLANs sin la coacción física, y los rangos de configuración van desde la simple topología punto a punto a redes complejas ofreciendo conectividad de datos distribuidos y roaming. Además de ofrecer movilidad del usuario final con un ambiente conectado a una red de computadoras, WLANs habilita la portabilidad de la red física, permitiendo a las LANs moverse entre los usuarios que hacen uso de ellas.

El intercambio de flexibilidad y movilidad es una amenaza de hackers usando dispositivos portátiles de computación o escáner para interceptar datos o ganar acceso a la LAN. Las LANs inalámbricas son más susceptibles de ataques por las fuerzas externas vía Internet que las LANs alambradas. Un hacker puede romper una red desde la conveniencia de su automóvil estacionado cerca de la WLAN. La norma IEEE 802.11, de WLAN, proporciona traslado confiable de datos inalámbricos pero es vulnerable a hacking o eavesdropping (Escuchar secretamente por medio de dispositivos electrónicos).

---

[1] Red de Area Local Inalámbrica (WLAN), Wireless Security, Randall K. Nichols, Panos C. Lekkas, 2003

Las WLANs eliminan el laso físico de la red, permitiendo a los usuarios conectarse directamente a un sistema de distribución sin interconexión de cables. La red principal está oculta entre paredes y pisos y no necesita estar anclada a una localización física particular.

Decir que las WLANs son completamente sin alambres no sería estrictamente correcto. Una parte del quipo es alimentado con baterías, hay una conexión con cable de poder, y la configuración típica tiene uno o más puntos de acceso fijos que son conectados a la LAN, a través de un cable de datos tradicional. Los puntos de acceso transmiten información de clientes inalámbricos que están dentro del rango de transmisión. Bajo circunstancias ideales, asumen un ambiente con pocas obstrucciones, la área cubierta para un solo punto de acceso pueden alcanzar varios cientos de pies y cubrir a un grupo pequeño de usuarios sin introducir mucha degradación.

En su forma más simple, una WLAN comprende un solo Transmisor – Receptor, llamado punto de acceso (AP), que está conectada a una red alambrada por medio de un cable Ethernet. Los puntos de acceso existen en localizaciones fijas a través de la organización y sirven como guía de comunicación. Los clientes de la red con un adaptador de red inalámbrico instalado son hábiles para facilitar transferencia de datos de clientes a los puntos de acceso y de los clientes al servidor. Introduciendo más puntos de acceso cerca de los límites previamente desplegados por las unidades de transmisión pueden extender el rango a una red inalámbrica. Funcionando de manera similar a los teléfonos celulares, las WLANs se comunican entre células. Las células recubren a los perímetros, habilita a los administradores de red a extenderse en áreas cubiertas. Los clientes "vagan" alrededor de la oficina, ellos se mueven de célula a célula, manteniendo una conexión en todo momento.

[2] Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de

---

[2] Redes Inalámbricas, http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de solo 10 Mbps.

Existen dos categorías de Redes Inalámbricas:

a.- De Larga Distancia.-

Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps. Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares.

b.- De Corta Distancia.-

Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

2.1.1.1 Transmisión Inalámbrica media [3]

Las LANs inalámbricas emplean radio frecuencia (RF) y vías aéreas electromagnéticas infrarrojas (IR) para transferir datos de punto a punto. La Comisión Federal de Comunicaciones (FCC) y un acuerdo mundial general ponen a un lado las frecuencias de radio que están disponibles para el uso comercial ilícito. Esas bandas Industrial Científica y Médica (ISM) incluyen los 900-MHz, 2.4-GHz, y 5-GHz que son usadas por muchos dispositivos de comunicación inalámbricos comerciales. La mayoría de los elementos que salen de la WLAN son diseñados para operar en la banda de los 2.4 GHz debido la disponibilidad global y reducida interferencia.

Varios medios de la transmisión son capaces de transferir los datos por las ondas hertzianas. Como la mayoría de las tecnologías, cada una de ellas tiene su propio beneficio y limitación. Los sistemas infrarrojos y sistemas de radio de banda estrecha son las tecnologías principales siendo usadas por la industria inalámbrica.

2.1.1.2 Los Sistemas Infrarrojos

Mientras la capacidad, infrarrojo (IR) los sistemas no constituyen una práctica solución para las empresas WLAN y por consiguiente no son ampliamente empleadas, IR es capas de transferir los datos tomando ventaja de esas frecuencias localizadas en la proximidad, pero cerca de la luz visible en el espectro electromagnético. Esas bandas altas muestran las mismas limitaciones de la luz visible que no pueden penetrar los objetos no transparentes como las paredes, pisos y techos. Como resultado, se restringen WLANs que transmiten vía IR a operar dentro del mismo cuarto, y podría limitarse más allá a un pequeño rango de línea de vista de corto alcance.

---

[3] Red de Area Local Inalámbrica (WLAN), Wireless Security, Randall K. Nichols, Panos C. Lekkas, 2003

2.1.1.3 Sistemas de Radio de Banda Estrecha

El sistema de radio de banda estrecha transmite y recibe los datos en un radio específico de frecuencia. Diferentes usuarios se comunican en frecuencias alternativas o canales para asegurar algunos niveles de privacidad y evitar la interferencia. Los radios receptores son construidos para escuchar únicamente sus frecuencias designadas y filtran las demás. La limitación natural de este sistema debe estar clara: Si otro transmisor está operando a la misma frecuencia y en el mismo rango, se producirá interferencia e indudablemente se perderán los datos o se dañaran. Por otro lado la implementación de la tecnología de banda estrecha es que, al menos en los Estados Unidos, una licencia debe ser obtenida de la FCC para cada sitio dónde es implementada.

2.1.1.4 Sistemas de Banda Ancha: Espectro Extendido

En lugar de usar una sola frecuencia, la tecnología de Espectro - Extendido, como su nombre sugiere, cambia la banda de frecuencia a una banda de frecuencia confiable para transmitir datos, Originalmente empleada por los militares, el Espectro – Extendido distribuye la señal sobre un amplio rango de frecuencia uniformemente, consumiendo más ancho de banda a cambio de la fiabilidad, integridad, y seguridad de comunicaciones. Esto, llamado uso de banda ancha permite evitar interferencias y otras señales de ruido en un modo no posible con las transmisiones de la banda estrecha. Los beneficios vienen con un precio. Por su naturaleza, las comunicaciones en banda ancha son más ruidosas y por consiguiente más fáciles para detectar. Por suerte, para una sintonía inapropiada de un receptor una señal de Espectro – Extendido aparece nada mas como un ruido de fondo.

El Espectro - Extendido viene en dos formas: Frequecy–Hopping Spread Spectrum (FHSS) y Direct-Sequence Spread Spectrum (DSSS). De los dos, la frecuencia hopping es menos costosa para desplegar.

Sin embargo, direct-sequence tiene potencial para un uso más amplio. Esto puede atribuirse a las proporciones de los datos más altos, rango mayor, y las capacidades de corrección de errores incorporados de DSSS.

2.1.1.4.1 Frequency Hopping Spread Spectrum (FHSS)

FHSS exitosamente mitiga los efectos de interferencia atando la señal de datos de transporte a la señal portadora. Esta señal portadora modula literalmente saltos, como una función del tiempo, de la frecuencia a la próxima a través de la banda. Cada transmisor-receptor esta programado con un código hopping que define el rango de frecuencias usadas. Para una comunicación apropiada, cada dispositivo debe ser configurado con el mismo código hopping, para asegurar que las señales son enviadas y recibidas en el tiempo correcto y en la frecuencia apropiada. Como resultado, transmisores-receptores sincronizados crean un canal de comunicaciones lógico con rangos de datos que alcanzan los 3 Mbps y un rango de 1000 pies sin instalaciones repetidoras.

Para interferencias a ocurrir, la señal conflictiva de banda estrecha necesitaría ser difundida a la misma frecuencia y al mismo tiempo como el signo hopping. Podrían ocurrir errores en la transmisión de una frecuencia, la señal será re-difundida en una frecuencia diferente hacia el siguiente salto. Para los receptores que no son programados con el código hopping apropiado, las transmisiones de FHSS parecen ser impulsos de ruido de corta duración. Distintos códigos hopping pueden ser implementados en la misma WLAN para prevenir que la WLAN interfiera con otras. FHSS basado en WLAN son mejores para soportar un alto número de clientes.

2.1.1.4.2 Direct-Sequence Spread Spectrum (DSSS)

DSSS es un patrón de bit redundante en cada bit que esta siendo transferido. Los bits insertados son referidos como un chip o un código chipping.

Por la inclusión del chip, un receptor esta habilitado para tener rutinas de recuperación de datos en señales basadas en análisis estáticos. Un gran número de bits en el código chipping resulta en una señal que es menos probable a ser negativamente afectada por la interferencia. Como eso incrementa el tamaño de la señal, DSSS requiere más ancho de banda para operar, generalmente usando tres frecuencias no-solapadas, para comunicarse. La capacidad de corrección de errores previene al DSSS de la necesidad de retransmitir datos que pueden haber sido dañados mientras se enrutan.

Retomando que la interferencia contada por los sistemas FHSS por tratar de evitar colisiones de señales a través de un movimiento constante, atendiendo esencialmente a los conflictos fuera-paso. Mientras esto es un método exitoso, se limita, el traspaso de los datos a paquetes relativamente pequeños porque la técnica de modulación tiene consecuencias adversas en los rangos de datos largos. Para compensar, los sistemas DSSS incluyen bits de corrección de errores, quitando la necesidad de saltar las frecuencias y para retransmitir en caso de un error. Como resultado los rangos de datos superiores a 11 Mbps y rangos superiores a miles puede ser almacenados con DSSS.

2.1.2 REDES PÚBLICAS DE RADIO. [4]

Las redes públicas tienen dos protagonistas principales: "*ARDIS*" (una asociación de Motorola e IBM) y "Ram Mobile Data" (desarrollado por Ericcson AB, denominado *MOBITEX*). Este último es el más utilizado en Europa. Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia. La compañía proporciona la infraestructura de la red, se incluye controladores de áreas y Estaciones Base, sistemas de cómputo

---

[4] Redes Inalámbricas, http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

tolerantes a fallas, estos sistemas soportan el estándar de conmutación de paquetes X.25, así como su propia estructura de paquetes. Estas redes se encuentran de acuerdo al modelo de referencia OSI. ARDIS especifica las tres primeras capas de la red y proporciona flexibilidad en las capas de aplicación, permitiendo al cliente desarrollar aplicaciones de software.

Estas redes operan en un rango de 800 a 900 Mhz. ARDIS ofrece una velocidad de transmisión de 4.8 Kbps. Motorola Introdujo una versión de red pública en Estados Unidos que opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta). Las redes públicas de radio como *ARDIS* y *MOBITEX* jugaran un papel significativo en el mercado de redes de área local (LAN´s) especialmente para corporaciones de gran tamaño. Por ejemplo, elevadores OTIS utiliza *ARDIS* para su organización de servicios.

2.1.3. REDES DE ÁREA LOCAL (LAN).

Las redes inalámbricas se diferencian de las convencionales principalmente en la "Capa Física" y la "Capa de Enlace de Datos", según el modelo de referencia OSI. La capa física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos (denominada MAC), se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, ruteadores o compuertas para conectarse. Los dos métodos para remplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

2.1.4 REDES INFRARROJAS.

2.1.4.1 Ondas Infrarrojas

Las ondas infrarrojas se usan mucho para la comunicación de corto alcance. Por ejemplo los controles remotos de los equipos utilizan comunicación infrarroja.

Estos controles son direccionales, tienen el inconveniente de no atravesar los objetos sólidos.

El hecho de que las ondas infrarrojas no atraviesen los sólidos es una ventaja. Por lo que un sistema infrarrojo no interferirá un sistema similar en un lado adyacente. Además la seguridad de estos sistemas contra espionaje es mejor que la de los sistemas de radio.

Este sistema no necesita de licencia del gobierno para operar en contraste con los sistemas de radio. Esta propiedad a hecho del infrarrojo un candidato interesante para las LAN inalámbricas en interiores.

2.1.4.2 Modos de Radiación Infrarrojos

Las estaciones con tecnología infrarroja pueden usar tres modos diferentes de radiación para intercambiar la energía Óptica entre transmisores-receptores: punto-a-punto cuasi-difuso y difuso (Fig.1, 2, 3).

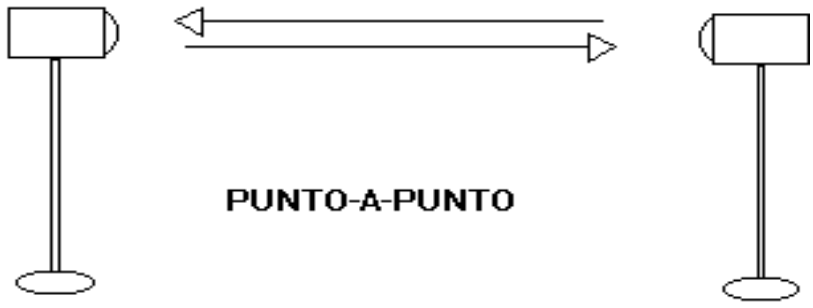


Fig. 1 Radiación Punto a Punto http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

En el modo punto-a-punto los patrones de radiación del emisor y del receptor deben de estar lo más cerca posible, para que su alineación sea correcta. Como resultado, el modo punto-a-punto requiere una línea-de-vista entre las dos estaciones a comunicarse. Este modo es usado para la implementación de redes

Inalámbricas Infrarrojas Token-Ring. El "Ring" físico es construido por el enlace inalámbrico individual punto-a-punto conectado a cada estación.

A diferencia del modo punto-a-punto, el modo cuasi-difuso y difuso son de emisión radial, o sea que cuando una estación emite una señal Óptica, ésta puede ser recibida por todas las estaciones al mismo tiempo en la célula.

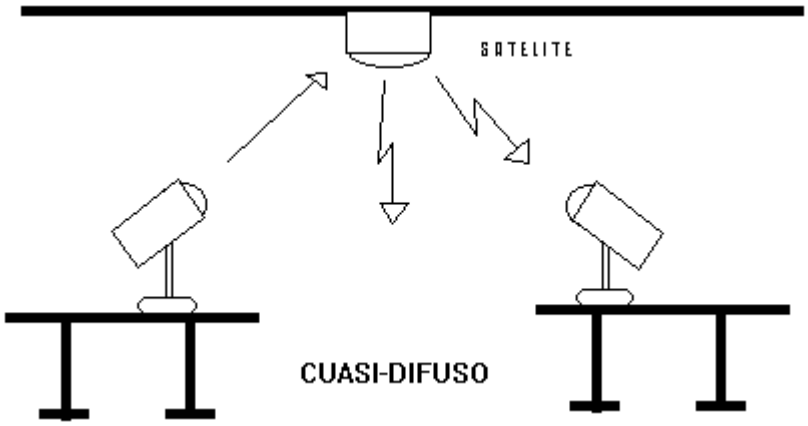


Fig. 2 Radiación Cuasi-Difusa http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

En el modo cuasi–difuso las estaciones se comunican entre si, por medio de superficies reflejantes. No es necesaria la línea-de-vista entre dos estaciones, pero si deben de estarlo con la superficie de reflexión. Además es recomendable que las estaciones estén cerca de la superficie de reflexión, esta puede ser pasiva ó activa. En las células basadas en reflexión pasiva, el reflector debe de tener altas propiedades reflectivas y dispersivas, mientras que en las basadas en reflexión activa se requiere de un dispositivo de salida reflexivo, conocido como satélite, que amplifica la señal óptica. La reflexión pasiva requiere más energía, por parte de las estaciones, pero es más flexible de usar.

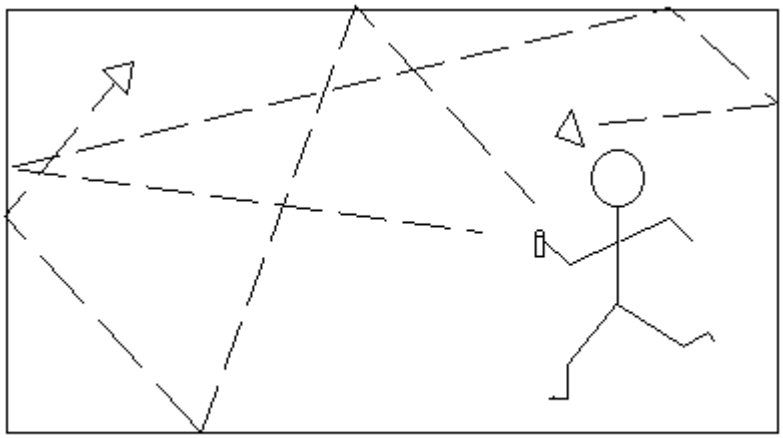


Fig. 3 Radiación Difusa http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

En el modo difuso, el poder de salida de la señal óptica de una estación, debe ser suficiente para llenar completamente el total del cuarto, mediante múltiples reflexiones, en paredes y obstáculos del cuarto. Por lo tanto la línea-de-vista no es necesaria y la estación se puede orientar hacia cualquier lado. El modo difuso es el más flexible, en términos de localización y posición de la estación, sin embargo esta flexibilidad esta a costa de excesivas emisiones ópticas.

Por otro lado la transmisión punto-a-punto es el que menor poder óptico consume, pero no debe de haber obstáculos entre las dos estaciones. En la topología de Ethernet se puede usar el enlace punto-a-punto, pero el retardo producido por el acceso al punto óptico de cada estación es muy representativo en el rendimiento de la red. Es más recomendable y más fácil de implementar el modo de radiación cuasi-difuso. La tecnología infrarroja esta disponible para soportar el ancho de banda de Ethernet, ambas reflexiones son soportadas (por satélites y reflexiones pasivas)

2.1.4.3 Redes conectadas con rayos Infrarrojos

Los investigadores de redes infrarrojas se han puesto como meta usar haces de luz infrarroja que se reflejen en todas las superficies de una habitación para crear redes de información de alta velocidad. A pesar de que las redes locales que usan

ondas de radio, como el sistema AirPort de Apple, han acaparado la atención, los científicos que trabajan en infrarrojo dicen que la luz puede ser, a largo plazo, una alternativa más rápida y mejor.

Toda persona que haya usado un control remoto para cambiar de canal ha visto el infrarrojo en acción. Esa tecnología también se utiliza en notebooks y computadoras de mano para la comunicación inalámbrica en distancias cortas. Pero estos enlaces trabajan mejor cuando el transmisor apunta al receptor, cuestión nada práctica cuando se trata de enlazar toda una oficina.

Una forma de encarar el problema es hacer rebotar amplios haces infrarrojos, por ejemplo, en el cielo raso, difundiendo las reflexiones en la habitación. Esto permite que los receptores puedan apuntar en cualquier dirección. A pesar de que algunos productos de redes ya usan este método los rayos dispersados crean una suerte de eco, lo que provocaba pérdida de datos y limita la velocidad de la red.

Proporcionar la banda ancha necesaria para actividades como videoconferencias es un campo donde el infrarrojo resulta ventajoso. El espectro de la radio se regula de forma muy estrecha, tanto es así que sólo algunas frecuencias son aptas para la transmisión de datos. Los fabricantes pueden presionar llegando a frecuencias más altas en búsqueda de espacio libre pero, por otro lado, los componentes que necesitan son cada vez más caros.

El infrarrojo, en cambio, no tiene estos problemas porque las frecuencias que usa, que son apenas por debajo de la luz visible en el espectro electromagnético, no están reguladas. Y como los rayos infrarrojos no traspasan las paredes, no da cabida a las interferencias ni a las superposiciones con ambientes vecinos. Esto también constituye una ventaja en seguridad; las redes de radiofrecuencia abren la posibilidad a las escuchas secretas.

Pero la incapacidad del infrarrojo de atravesar las paredes u otros objetos también puede significar su ruina. La tecnología necesita al menos un receptor y un transmisor en cada habitación que se conecten a una red cableada. Esto la

convierte en una opción poco probable para alguien que quiera permanecer en línea sin cable, mientras se traslada con la portátil de habitación en habitación. Y ni pensar en estar en línea en el parque vía infrarroja: los rayos necesitan superficies, en particular cielos rasos para rebotar.

Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso, algunas compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores / emisores en las ventanas de los edificios. Las transmisiones de radio frecuencia tienen una desventaja: que los países están tratando de ponerse de acuerdo en cuanto a las bandas que cada uno puede utilizar.

La transmisión Infrarroja no tiene este inconveniente por lo tanto es actualmente una alternativa para las Redes Inalámbricas. El principio de la comunicación de datos es una tecnología que se ha estudiado desde los 70´s, Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar.

El mismo principio se usa para la comunicación de Redes, se utiliza un "*transreceptor*" que envía un haz de Luz Infrarroja, hacia otro que la recibe. La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente. Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un "Transreceptor Infrarrojo". Las primeros transreceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transreceptor recibía la señal. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transreceptor. La Fig. 4 muestra un transreceptor. En la actualidad Photonics a desarrollado una versión AppleTalk/LocalTalk del transreceptor que opera a 230 Kbps. El sistema tiene un rango de 200 mts. Además la tecnología se ha mejorado utilizando un transreceptor que difunde el haz en todo el cuarto y es

recogido mediante otros transreceptores. El grupo de trabajo de Red Inalámbrica IEEE 802.11 está trabajando en una capa estándar MAC para Redes Infrarrojas.

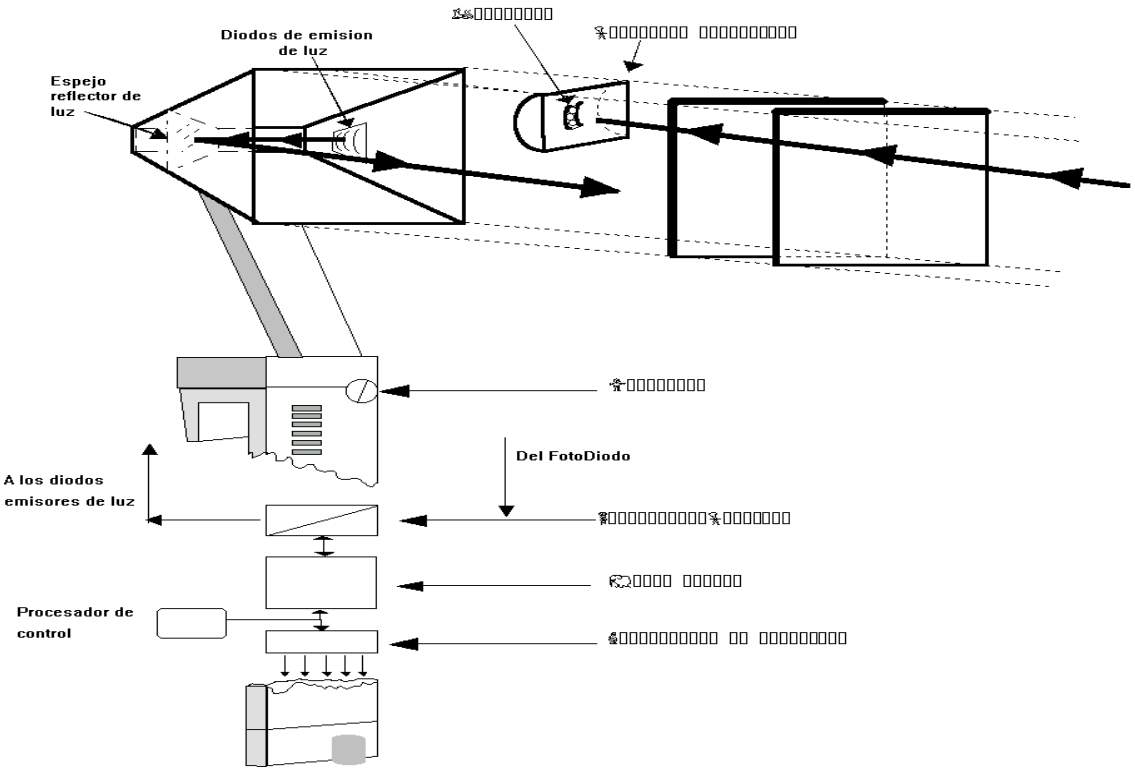


Fig. 4 Transreceptor. http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

2.1.5 REDES DE RADIO FRECUENCIA

Por el otro lado para las Redes Inalámbricas de Radio Frecuencia, la FCC permitió la operación sin licencia de dispositivos que utilizan 1 Watt de energía o menos, en tres bandas de frecuencia: 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 Mhz. Estas bandas de frecuencia, llamadas bandas ISM, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales. Esta banda, a diferencia de la ARDIS y MOBITEX, está abierta para cualquiera. Para minimizar la interferencia, las regulaciones de FCC estipulan que una técnica de señal de transmisión llamada *spread - spectrum modulation*, la cual tiene potencia de transmisión máxima de 1 Watt deberá ser utilizada en la banda ISM. Esta técnica a sido utilizada en aplicaciones militares. La idea es tomar una señal de

banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia. Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente:

2.1.5.1 La secuencia directa

En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada.

2.1.5.2 El salto de frecuencia

Este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 Mhz que son utilizadas por hornos de Microondas.

2.1.6 BLUETOOTH [5]

Bluetooth es un enlace de bajo costo, baja potencia, de onda corta para conexión inalámbrica entre dos dispositivos móviles y redes de área inalámbrica y redes de área local (WAN/LAN) de puntos de acceso. Eso incluye una especificación de hardware y arquitectura de software. Bluetooth opera en la banda sin licencia ISM de 2.4GHz. Pero porque otros numerosos dispositivos inalámbricos y productos también operan en esta banda, Bluetooth ha sido plagado por problemas de interferencia. Para resolverlos, los diseñadores de Bluetooth se han inclinado a la solución de frecuencia – hooping donde ellos encontraran otros problemas. Algunos países tienen una banda ISM más angosta que otros y los dispositivos desarrollados para operar en estos países son incompatibles con dispositivos Bluetooth en cualquier otra parte.

A pesar de estos problemas, las propuestas Bluetooth continúan vertiginosas con las numerosas posibilidades que Bluetooth ofrece para las aplicaciones móviles. Pero Bluetooth esta fuera de un comienzo con irregularidades con una incompleta interoperabilidad, altos costos y ciclos de desarrollo lentos. Eso significa que tenemos todavía que ver la envergadura de la implementación que probara medidas de seguridad basadas en especificaciones, arquitecturas y extrapolaciones de tecnologías de comunicaciones inalámbricas con similares provisiones.

Bluetooth tiene tres modos de seguridad, el más bajo tiene mecanismos de seguridad, y los más altos exigen autentificación, autorización y la encriptación al nivel de enlace. El nivel intermedio refuerza la autentificación y encriptación selectiva a través de mecanismos conocidos como manejo de seguridad.

---

[5] Bluetooth, Wireless Security, Randall K. Nichols, Panos C. Lekkas, 2003

2.1.6.1 Especificaciones básicas de Bluetooth

Bluetooth soporta las comunicaciones de voz y datos y las transmisiones punto a punto o multipunto. Las especificaciones son ambiciosas. Lo describe un pequeño rastro tecnológico que optimiza el uso del modelo de todos los dispositivos móviles y provistos para:

- Uso global
- Manejo de voz y datos
- La habilidad para establecer conexiones ad hoc y redes
- La habilidad para soportar la interferencia de otras fuentes de banda abierta
- Consumo de potencia insignificante en comparación a otros dispositivos de uso similar
- Un estándar de interfase abierta
- Competitividad de bajo costo de toda las unidades, comparadas a la que no son Bluetooth

2.1.6.2 Tecnología Bluetooth

El radio Bluetooth esta construido en un pequeño micro chip que opera en la banda de los 2.4 GHz. EL chip tiene dos niveles de potencia: un nivel bajo que cubre el área personal entre un cuarto de tamaño razonable y un nivel alto que puede cubrir un rango medio de espacio en una casa o tienda. El software controla e identifica al código construido en cada microchip que son usados para limitar la comunicación estrictamente a aquellas unidades preseteadas por sus dueños. El microchip puede ser incluido en cantidad de productos. El SIG Bluetooth actualmente propone cinco modelos de uso:

- **Un teléfono tres en uno** El teléfono celular actúa como un teléfono portátil en casa, un teléfono móvil cuando este viajando, un walkie-talkie cuando este en el rango de otro teléfono habilitado Bluetooth.

- **Un puente de Internet** La computadora móvil puede navegar por Internet donde sea, más aún cuando el usuario esta conectado a través de un moden o línea de tierra.
- **Una plataforma para conferencias interactivas** Cambio electrónico de documentos con participantes seleccionados sin alguna conexión inalámbrica.
- **El último heatset** Conecta su set de cabeza inalámbrico a su teléfono móvil, computadora móvil o cualquier conexión inalámbrica para mantener sus manos libres para cosas más importantes cuando este en la oficina o en el carro.
- **Un sincronizador automático** Una sincronización automática de datos entre computadoras de escritorio, laptos, teléfonos celulares y PDAs. El usuario puede cambiar el calendario o contactar información en cualquier dispositivo y todos los dispositivos que se fecharán automáticamente.

2.1.6.3 Desarrollo de las especificaciones Bluetooth

El grupo de interés especial (SIG) de Bluetooth sirve como cuerpo específico del gobierno, el cual esta compuesto de los lideres de comunicaciones de la industria y muchos otros campos técnicos. Ericsson, Intel, Nokia y toshiba originalmente formaron el SIG en 1998. Actualmente, hay más de 2000 miembros del SIG. En 1999 el SIG sacó la versión 1.0 de las especificaciones Bluetooth y con expectativas para sacar la versión 2.0 de las especificaciones Bluetooth a finales del 2001. El progreso del intercambio de información ha sido:

Punto a punto ---- LAN ---- Internet ---- Conectividad Ubicua

Bluetooth es una de muchas tecnologías que prometen conectividad ubicua. Una vez descrita como una tecnología de conexión sin cables con su reciente diseño de misión (1.0A y 1.0B), Bluetooth ha visto su utilidad expandida. Ahora esta posicionada como un contendor en la red personal (PAN), entre los pesos pesados como la HOME RF y 802.11b (también conocida como Wi-Fi). Los

estándares inalámbricos LAN (WLAN) están apuntando en diferentes mercados y tienen diferentes objetivos de seguridad.

Con velocidades que alcanzan los 10Mbps, Bluetooth esta disponible para señales de video y multimedia. Las especificaciones Bluetooth que salieron a finales de los noventas se enfocaron principalmente en la transmisión de datos y voz por siempre en aplicaciones digitales. Esta omisión le permitió a Bluetooth SIG, organizar comités para construir archivos de aplicaciones varios para la siguiente versión para ayudar a los dispositivos Bluetooth a comunicarse con otros y coexistir con otros protocolos inalámbricos.

2.1.6.4 Decisiones de Diseño

Una de las ventajas de Bluetooth es su bajo costo. Si se va a trabajar como una tecnología de reemplazo al cable, no puede ser mucho más caro que el cable a ser reemplazado. La solución del sistema de bajo costo Bluetooth consiste en el hardware, software y los requerimientos de interoperabilidad, implementados en pequeños, no caros, transreceptores de rango corto en los dispositivos móviles disponibles actualmente, envueltos directamente en las tarjetas de componentes existentes o añadidos en un dispositivo adaptador (tal como una tarjeta de PC insertada en una computadora de bolsillo).

La decisión de operar Bluetooth sobre la banda ISM fue hecha para dejar a un lado cualquier necesidad para obtener una licencia de espectros de cada país y para permitir a Bluetooth habilitar dispositivos para operar globalmente. Sin embargo, este objetivo no ha sido completamente alcanzado. Algunos países han puesto limitaciones en el rango de frecuencia de la banda ISM y han negado su libre licencia de acceso a toda la banda. Los dispositivos Bluetooth deben ser hechos ahora con una variedad de especificaciones de frecuencia. El SIG Bluetooth ha sido perseguido activamente por los gobiernos en países rebeldes para organizar el uso de la banda ISM e incompatibilidades embarazosas entre dispositivos.

2.1.6.5 Piconets

La red básica Bluetooth es llamada un piconet. Los Piconets son colecciones arbitrarias de los dispositivos habilitados Bluetooth físicamente cercanos para habilitar la comunicación y el intercambio de información. La tecnología Bluetooth habilita muchos tipos de dispositivos inalámbricos para comunicarse con otros, tanto como los de una red alambrada.

Un ejemplo del uso Bluetooth podría ser la transmisión de la información de un Asistente Personal Digital (PDA) a un teléfono celular. Bluetooth hace esto posible por el uso de las ondas de radio en el espacio de los 2.4Ghz para transmitir los datos. Usar ondas de radio le permite a Bluetooth enviar y recibir ambas transmisiones de voz y de datos en tiempo real. Está frecuencia no es regulada ampliamente, lo cual es particularmente ventajoso a la nueva tecnología. Las comunicaciones Bluetooth pueden ser conducidas individualmente (punto a punto) o en masa (punto a multipunto). Una transmisión multipunto usando esta tecnología esta limitada a ocho dispositivos, los cuales, como grupo son llamados piconet.

1.1.6.6 Arquitectura de la seguridad Bluetooth

La arquitectura de la seguridad Bluetooth, como especificaciones de su SIG, incluye provisiones para autentificación y encriptación. Todas las funciones de seguridad son presentadas al nivel de enlace. Cuatro ítems son necesarios para establecer las transmisiones Bluetooth:

1. Un dispositivo de dirección único de 48 bits
2. Una clave pseudo-random privada de 128 bits usada para la autentificación
3. Una clave privada para la encriptación de 8-128 bites, y
4. Un número pseudo-random de 128 bits generado por el dispositivo.

La especificación Bluetooth también detalla tres modos de seguridad en que el protocolo puede operar:

Modo 1 – No seguro
La no seguridad esta fortalecida por el protocolo.

Modo 2 – Servicio – nivel de seguridad fortalecido
La seguridad esta fortalecida después del seseo del canal.

Modo 3 – Nivel de enlace fortalecido de seguridad
La seguridad esta reforzada antes del seteo del canal.

Note que un dispositivo Bluetooth puede operar únicamente en un modo de seguridad a la vez. Un dispositivo que opera en Modo 3 no autentificará con otros dispositivos en una base selectiva pero autentificará todos los dispositivos que intenten comunicarse con él.

En adición a los tres modos de seguridad, Bluetooth permite dos niveles de confianza confiado y no confiado y tres niveles de servicio de seguridad. Dispositivos no confiables no mantiene una relación permanente o son etiquetados como no confiables, resultando en acceso de servicio restringidos.

La debilidad en la arquitectura de seguridad Bluetooth afecta la confidencialidad, autentificación, disponibilidad, no repudiación de la transmisión. La confidencialidad es siempre concerniente con las transmisiones de aire-abiertas y Bluetooth no requiere encriptación de todas las transmisiones. En muchos casos esto se deja a la capa de aplicación.

Esta falta de encriptación requerida potencialmente deja a usuarios de transmisiones en el aire. Una debilidad publicada de Bluetooth describe una situación donde un atacante podría obtener la clave de encriptación entre dos dispositivos. Y una vez que la clave es comprometida, el atacante podría espiar

las transmisiones, enmascararla como uno de los usuarios o insertar comunicaciones falsas en el flujo de datos.

La autentificación es un problema con Bluetooth porque los dispositivos son autentificados, no los usuarios.

El Hecho de que Bluetooth opere en un espacio aéreo sin regulación podría llegar a ser una debilidad disponible. Bluetooth y los dispositivos 802.11b pueden causar del uno al otro degradación de las características, cuando operan en las cercanías. Las pruebas hechas por Symbol Tecnology Inc y la Toshiba Corporation confirmaron que mientras las dos puedan coexistir en una locación, la perdida de características se incrementa si las dos están entre dos o tres metros el uno del otro. Si Bluetooth y la 802.11b están entre medio metro, el efecto puede ser significativo. El conflicto es el resultado de ambas tecnologías operando entre el espectro de 2.4GHz. Bluetooth usa el salto – frecuencia a una velocidad de 1600 hops/seg para reducir la interferencia en los dispositivos Bluetooth, pero no lo elimina.

Finalmente, la privacidad de las transmisiones es un problema para los usuarios Bluetooth. Cada dispositivo Bluetooth tiene un identificador único. Cuando un dispositivo interactúa con, o se mueve en el rango de una red Bluetooth, ese identificador puede ser logeado. Si esa base de datos log fuera perdida una grabación de los movimientos del dispositivo puede ser creada. Si alguien cambiara esa base de datos con la garantía de grabado para los dispositivos, la grabación de los movimientos del dueño podrían ser logeados.

2.1.6.7 Scatternets

Cuando los dispositivos establecen un enlace Bluetoorh, el uno actúa como MASTER y el otro como ESCLAVO. El master no tiene privilegios especiales o autoridad; en su lugar se determina el patrón salto-frecuencia para la comunicación entre dispositivos. Un master puede comunicarse con múltiples

esclavos, tanto como 7 esclavos activos y sobre los 255 esclavos pasivos. (Los componentes Bluetooth operan en cuatro modos: activos, sniff, sostenido y pasivo. Cada uno opera a diferente nivel de actividad y consumo de potencia, con el modo pasivo siendo el nivel más bajo de ellos.)

La comunicación de esclavos con un master particular constituye el piconet en el medio. El adhesivo que une piconets es que todos sus dispositivos están sincronizados. Más allá de dispositivos adicionales están la cercanía piconet, ellos deben estar comunicándose con un master para llegar a ser parte de el.

Si múltiples piconets cubren la misma área una unidad puede participar en dos o más aplicando la múltiplexación de tiempo, tanto como canales son guardados, separados y las fases son calibradas. Una unidad Bluetooth puede actuar como un esclavo en muchos piconets, pero como un master en un único piconet.

Un set de piconets Bluetooth es llamado scatternets, el cual tiene el interés propio de estar habilitado para formar sin alguna integración de los piconets involucrados

2.1.6.8 El stack Bluetooth

La unicidad de Bluetooth proviene de su arquitectura. A pesar de que Bluetooth no une exactamente el modelo de Sistema de Interconexión Abierto (OSI), comparando a las dos ayuda ágilmente a la división de responsabilidad en el stack de Bluetooth.

Capa Física

Responsable de la interferencia eléctrica a las comunicaciones media, incluyendo modulación y codificación de canales. Bluetooth lo lleva fuera de esta función a través de su radio y protocolos de banda – base.

Capa de Enlace de Datos

Provee transmisión y control de errores sobre un enlace particular. En Bluetooth esta función es manejada por un protocolo controlador de enlace, en le cual cubre la etiqueta y el control final de la banda base, incluyendo un chequeo de error y corrección.

Capa de Red

Controla la transferencia de datos a través de la red, independientemente de la media y topología de la red. Bajo el protocolo de Bluetooth, el límite superior de la red del controlador de enlace y parte del manejador de enlace (LM) maneja esas responsabilidades poniéndolos arriba y manteniendo enlaces múltiples.

Capa de Transporte

Controla la múltiplexación de datos transferidos a través de la red a los niveles provistos por la aplicación, y de ahí superpone con el límite superior de la LM y el controlador de interfase huésped (HCI), el cual provee los actuales mecanismos de transporte.

Capa de Sesión

Provee manejo y control de servicios en el flujo de datos, los cuales son cubiertos por el Control de Enlace Lógico y el Protocolo de Aplicación (L2CAP) y el límite inferior de RFCOMM / SDP.

Capa de Presentación

Provee una representación común para la capa de aplicación de datos de la unidad, la cual es la principal etiqueta de la FCOMM / SDP.

Capa de Aplicación

Responsable del manejo de la comunicación entre las aplicaciones invitadas.

2.1.7 CARACTERÍSTICAS DE BLUETOOTH [6]

Bluetooth es una norma abierta para una tecnología de punta que posibilita la conexión inalámbrica de corto alcance de voz y datos entre computadoras de escritorio y portátiles, agendas digitales personales, teléfonos móviles, impresoras, escáneres, cámaras digitales e incluso dispositivos de casa, a través de una banda disponible a nivel, global (2,4 GHz) y mundialmente compatible. En otras palabras, Bluetooth desenchufa los periféricos digitales y convierte a la atadura de los cables en cosa del pasado.

Es la norma que define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son:

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

La tecnología Bluetooth comprende hardware, software y requerimientos de interoperatibilidad, por lo que para su desarrollo ha sido necesaria la participación de los principales fabricantes de los sectores de las telecomunicaciones y la informática, tales como: Ericsson, Nokia, Toshiba, IBM, Intel y otros. Posteriormente se han ido incorporando muchas más compañías, y se prevé que próximamente los hagan también empresas de sectores tan variados como:

[6] Que es Bluetooth, http://www.zonabluetooth.com/que_es_bluetooth.htm

Automatización industrial, maquinaria, ocio y entretenimiento, fabricantes de juguetes, electrodomésticos, etc., con lo que en poco tiempo se nos presentará un panorama de total conectividad de nuestros aparatos tanto en casa como en el trabajo.

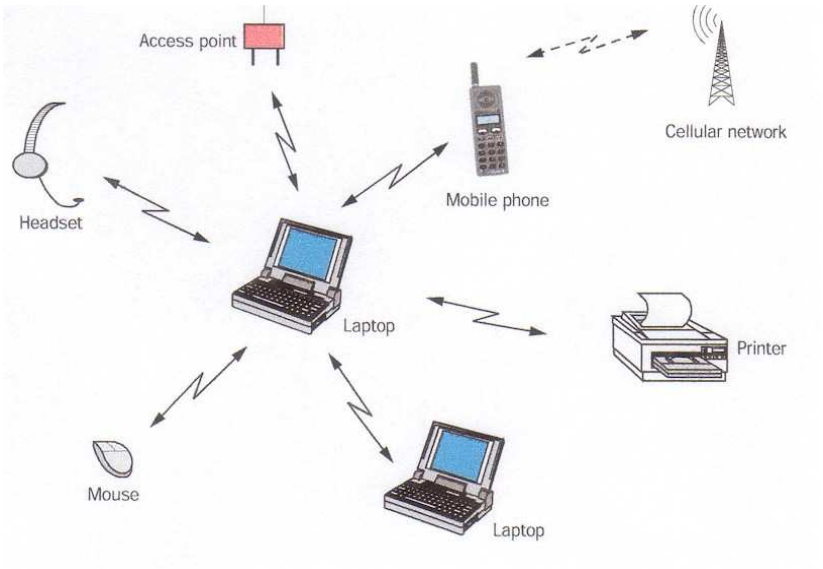


Fig. 5 Bluetooth. http://www.zonabluetooth.com/que_es_bluetooth.htm

2.1.7.1 Antecedentes

En 1994 Ericsson inició un estudio para investigar la viabilidad de una interfase vía radio, de bajo coste y bajo consumo, para la interconexión entre teléfonos móviles y otros accesorios con la intención de eliminar cables entre aparatos. El estudio partía de un largo proyecto que investigaba sobre unos multicomunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance, llamado *MC link.* Conforme éste proyecto avanzaba se fue viendo claro que éste tipo de enlace podía ser utilizado ampliamente en un gran número de aplicaciones, ya que tenia como principal virtud el que se basaba en un chip de radio relativamente económico.

2.1.7.2 El Sig

A comienzos de 1997, según avanzaba el proyecto MC link, Ericsson fue despertando el interés de otros fabricantes de equipos portátiles. En seguida se vio claramente que para que el sistema tuviera éxito, un gran número de equipos debían estar equipados con ésta tecnología. Esto fue lo que originó a principios de 1998, la creación de un grupo de interés especial (SIG), formado por 5 promotores que fueron: Ericsson, Nokia, IBM, Toshiba e Intel. La idea era lograr un conjunto adecuado de áreas de negocio, dos líderes del mercado de las telecomunicaciones, dos líderes del mercado de los PCS portátiles y un líder de la fabricación de chips. El propósito principal del consorcio fue y es, el establecer un estándar para la interfase aérea junto con su software de control, con el fin de asegurar la interoperatibilidad de los equipos entre los diversos fabricantes.

2.1.7.3 Definición de Canal

Bluetooth utiliza un sistema FH/TDD (salto de frecuencia / división de tiempo duplex), en el que el canal queda dividido en intervalos de 625 µs, llamados slots, donde cada salto de frecuencia es ocupado por un slot. Esto da lugar a una frecuencia de salto de 1600 veces por segundo, en la que un paquete de datos ocupa un slot para la emisión y otro para la recepción y que pueden ser usados alternativamente, dando lugar a un esquema de tipo TDD.

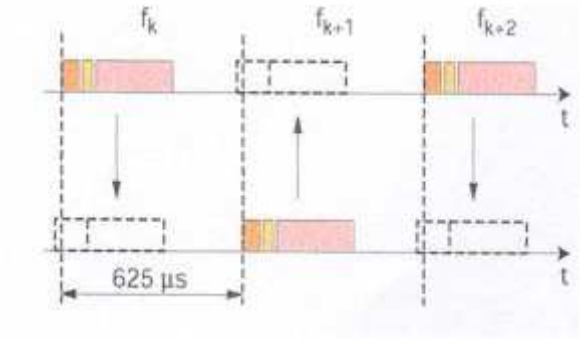


Fig. 6 Canal Bluetooth**,** http://www.zonabluetooth.com/que_es_bluetooth.htm

Dos o más unidades Bluetooth pueden compartir el mismo canal dentro de una piconet , donde una unidad actúa como maestra, controlando el tráfico de datos en la piconet que se genera entre las demás unidades, donde estas actúan como esclavas, enviando y recibiendo señales hacia el maestro. El salto de frecuencia del canal está determinado por la secuencia de la señal, es decir, el orden en que llegan los saltos y por la fase de ésta secuencia. En Bluetooth, la secuencia queda fijada por la identidad de la unidad maestra de la piconet (un código único para cada equipo), y por su frecuencia de reloj. Por lo que, para que una unidad esclava pueda sincronizarse con una unidad maestra, ésta primera debe añadir un ajuste a su propio reloj nativo y así poder compartir la misma portadora de salto.

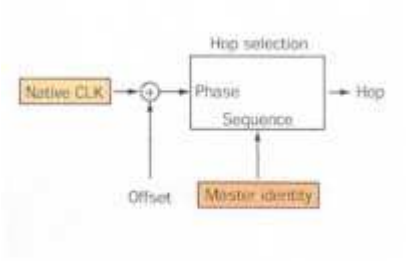


Fig. 7 Secuencia de Reloj**,** http://www.zonabluetooth.com/que_es_bluetooth.htm

En países donde la banda está abierta a 80 canales o más, espaciados todos ellos a 1 Mhz., se han definido 79 saltos de portadora, y en aquellos donde la banda es más estrecha se han definido 23 saltos.

2.1.7.4 Definición de Paquete

La información que se intercambia entre dos unidades Bluetooth se realiza mediante un conjunto de slots que forman un paquete de datos. Cada paquete comienza con un código de acceso de 72 bits, que se deriva de la identidad maestra, seguido de un paquete de datos de cabecera de 54 bits. Éste contiene importante información de control, como tres bits de acceso de dirección, tipo de paquete, bits de control de flujo, bits para la retransmisión automática de la pregunta, y chequeo de errores de campos de cabeza. Finalmente, el paquete

que contiene la información, que puede seguir al de cabeza, tiene una longitud de 0 a 2745 bits. En cualquier caso, cada paquete que se intercambia en el canal está precedido por el código de acceso.

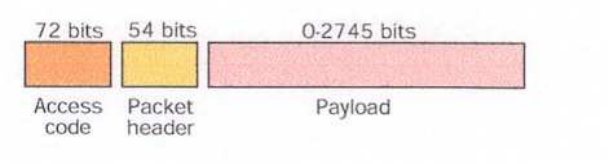


Fig. 8 Paquete**,** http://www.zonabluetooth.com/que_es_bluetooth.htm

Los receptores de la piconet comparan las señales que reciben con el código de acceso, si éstas no coinciden, el paquete recibido no es considerado como válido en el canal y el resto de su contenido es ignorado.

2.1.7.5 Definición de Enlace Físico

En la especificación Bluetooth se han definido dos tipos de enlace que permitan soportar incluso aplicaciones multimedia:

- Enlace de sincronización de conexión orientada (SCO)
- Enlace asíncrono de baja conexión (ACL)

Los enlaces SCO soportan conexiones asimétricas, punto a punto, usadas normalmente en conexiones de voz, estos enlaces están definidos en el canal, reservándose dos slots consecutivos (envío y retorno) en intervalos fijos. Los enlaces ACL soportan conmutaciones punto a punto simétrico o asimétrico, típicamente usadas en la transmisión de datos.

Un conjunto de paquetes se han definido para cada tipo de enlace físico:

- Para los enlaces SCO, existen tres tipos de slot simple, cada uno con una portadora a una velocidad de 64 kbit/s. La transmisión de voz se realiza sin ningún mecanismo de protección, pero si el intervalo de las señales en el

enlace SCO disminuye, se puede seleccionar una velocidad de corrección de envio de 1/3 o 2/3.

- Para los enlaces ACL, se han definido el slot-1, slot-3, slot-5. Cualquiera de los datos pueden ser enviados protegidos o sin proteger con una velocidad de corrección de 2/3. La máxima velocidad de envío es de 721 kbit/s en una dirección y 57.6 kbit/s en la otra.

2.1.7.6 Beneficios

Bluetooth permitirá que los usuarios se conecten a una amplia gama de aparatos de computación y telecomunicaciones - fácil- y rápidamente - sin la necesidad de usar cables.

Los usuarios podrán acceder, entre otros, a horarios de vuelos y de clases, mapas locales, ofertas especiales en áreas públicas tales como escuelas, aeropuertos, centros comerciales y salas de exhibición.

La tecnología inalámbrica Bluetooth permitirá que los empleados sean más efectivos. Después de alguna reunión, los usuarios no tienen que regresar a sus escritorios para sincronizar sus dispositivos de mano, revisar sus mensajes o su email. Los usuarios pueden tomar mejores decisiones porque tienen acceso a la información más reciente, utilizando sus aparatos clientes de la tecnología Bluetooth.

Debido a que el Bluetooth se enfoca en aparatos 'personales', no tomará mucho tiempo en que la tecnología se convierta en una parte integral de nuestro cotidiano vivir.

2.1.8 WIRELESS FIDELITY (WI-FI)

2.1.8.1 Introducción

Las redes Wireless son un estándar desarrollado por la IEEE (Institute of Electrical and Electronic Engineers) que permite conectar dispositivos mediante una frecuencia de 2,4 Ghz, con drivers que permiten comunicarse a través de los protocolos actuales de comunicación (TCP / IP), disponiendo cada dispositivo de una dirección única a nivel de Hardware (MAC address), y con una potencia de transmisión que va desde los 10-20 mW a los 100 mW (según la FCC / CEPT o la legislación de cada país).

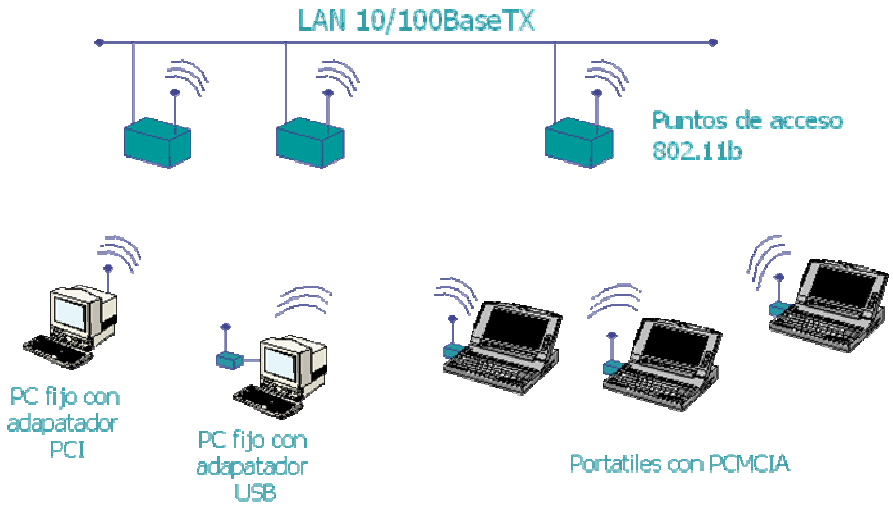


Fig. 15 Introducción a lasWLAN, José Manuel Huidobro

Dentro de cada estándar hay variaciones según la tecnología va cambiando. En el caso del 802.11 se fueron creando subgrupos, que se han ido identificando mediante letras. Es por eso que se comenzó a hablar de la 802.11b, siendo su fecha de aprobación en 1999. Y esta fue la que casi todos los fabricantes aceptaron como la más estándar y la más completa. Al aceptarla los fabricantes se agruparon en otra asociación que simplemente certifica que los productos son compatibles entre sí dentro de la norma 802.11. Este grupo se denominó Wi-Fi (Wireless Fidelity).

Comparación de tres protocolos que actualmente se comercializan dentro del estándar 802.11. Estos son el 802.11b, 802.11a y 802.11g en orden de aprobación por el IEEE:

Estándares Wireless			
Estándar	**802.11b**	**802.11a**	**802.11g**
Aprobado IEEE	Julio 1999	Julio 1999	Junio del 2003
Popularidad	Adoptado masivamente	Nueva tecnología, crecimiento bajo	Nueva tecnología, con un rápido crecimiento
Velocidad	Hasta 11 Mbps	Hasta 54 Mbps	
Costo	Barato	Relativamente caro	Relativamente barato
Frecuencia	2.4 - 2.497 Ghz	5.15 - 5.35 Ghz 5.425 - 5.675 Ghz 5.725 - 5.875 Ghz	2.4 - 2.497 Ghz
Cobertura	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos	Cobertura baja, unos 150 metros, con mala conectividad con obstáculos	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos

Acceso Público	El número de Hotspots crece exponencialmente	Ninguno en este momento.	Compatible con los HotSpots actuales de 802.11b. El paso a 802.11g no es traumático para los usuarios
Compatibilidad	Compatible con 802.11g, no es compatible con 802.11a	Incompatible con 802.11b y con 802.11g	Compatible con 802.11b, no es compatible con 802.11a
Modos de datos	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Modulación	CCK	OFDM	OFDM y CCK

Como se ha comprobado la frecuencia más usada es la de 2.4Ghz. Dicha frecuencia es libre en prácticamente todos los países del mundo, ya que se trata de una frecuencia reservada para la investigación, educación o sanidad.

En la tabla adjunta se puede ver la relación entre los canales y la frecuencia.

Relación entre canal y frecuencia	
Canal	**Frecuencia**
1	2.412 Ghz
2	2.417 Ghz
3	2.422 Ghz
4	2.427 Ghz
5	2.432 Ghz
6	2.437 Ghz
7	2.442 Ghz
8	2.447 Ghz
9	2.452 Ghz
10	2.457 Ghz
11	2.462 Ghz
12	2.467 Ghz
13	2.472 Ghz
14	2.484 Ghz

En la siguiente tabla podemos ver los canales disponibles, dependiendo de cada país:

Países y Canales	
Países	**Canales**
Europa (ETSI)	1 – 13
USA (FCC)	1 – 11
Francia	10 – 13
Japón	1 – 14

2.1.9 SEGURIDAD

Para asegurar la protección de la información se ha definido un nivel básico de encriptación, que se ha incluido en el diseño del chip de radio para proveer de seguridad en equipos que carezcan de capacidad de procesamiento, las principales medidas de seguridad son:

- Una rutina de pregunta-respuesta, para autentificación
- Una corriente cifrada de datos, para encriptación
- Generación de una clave de sesión (que puede ser cambiada durante la conexión)

Tres entidades son utilizadas en los algoritmos de seguridad: la dirección de la unidad Bluetooth, que es una entidad pública; una clave de usuario privada, como una entidad secreta; y un número aleatorio, que es diferente por cada nueva transacción.

Como se ha descrito anteriormente, la dirección Bluetooth se puede obtener a través de un procedimiento de consulta. La clave privada se deriva durante la

iniciación y no es revelada posteriormente. El número aleatorio se genera en un proceso pseudo-aleatorio en cada unidad Bluetooth.

2.1.10 SOLUCIONES CON REDES INALÁMBRICAS. [7]

A continuación algunos ejemplos de cuándo una red inalámbrica podría ser su solución ideal.

• Para oficinas temporales
• Cuando los cables no son prácticos ni posibles
• Soporte de usuarios móviles en localidades externas
• Expansión de una red de cables
• Redes temporales
• Oficinas en el hogar

2.1.10.1 Para oficinas temporales

Si opera en un espacio de una oficina temporal, debe utilizar una solución inalámbrica para evitar costos de instalación de los cables de una red. Además, cuando se mude, usted podrá llevarse consigo la red inalámbrica e instalarla fácilmente en sus nuevas oficinas.

Cuando una red tradicional, el dinero que se gasta en el cableado de una oficina temporal, se pierde cuando se va. Además necesitará construir una nueva infraestructura en su nueva oficina. Si piensa que las instalaciones existentes le quedarán pequeñas, una red inalámbrica puede ser una inversión muy astuta.

---

[7] Redes Inalámbricas, http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

2.1.10.2 Cuando los cables no son prácticos ni posibles

A veces los dueños de las propiedades no permiten la instalación de cables en el piso, las paredes o los techos. Algunas veces los cables pueden ser viejos o las paredes sólidas, o podría haber asbestos en las paredes o el techo. Algunas veces no se pueden instalar cables a través de un pasillo para acceder otra de las oficinas; o tal vez usted cuente con algún espacio, frecuentado por varios empleados, donde el cableado causaría desorden y congestionamiento. En cualquier caso en el que los cables sean imprácticos, imposibles o muy costosos, instale una red inalámbrica.

2.1.10.3 Soporte de usuarios móviles en localidades externas

Una red inalámbrica representa una estrategia excelente para ofrecerles conectividad a la red cuando visiten las instalaciones. Una vez que las computadoras portátiles estén equipadas para comunicarse en forma inalámbrica con la red, se hará automáticamente cuando estén en el área de alcance de su punto de acceso inalámbrico. No se puede sobrecargar a su personal técnico con la instalación de conexiones y se evita el tener cables dispersos que no se utilizan, la mayoría de las veces para el uso exclusivo de los usuarios remotos. Además se usará el espacio de oficina más eficientemente porque ya no se necesita mantener espacios disponibles para aquellos empleados que están presentes de forma esporádica.

2.1.10.4 Expansión de una red de cables

Utilizar una red inalámbrica para extender cualquier red existente, evitando los costos y la complejidad de los cables. Conecta a nuevos usuarios en cuestión de minutos, en vez de horas. Provee conectividad a la red en las salas de conferencia, cafetería o vestíbulo sin problemas de cables. Se puede expandir la red fuera del edificio, permitiendo que los empleados se mantengan conectados

cuando se encuentren fuera, accediendo a la red sin esfuerzo ni interrupciones, como cualquier persona que se conecta con cables.

2.1.10.5 Redes temporales

Si necesita crear redes temporales de computación, como por ejemplo en obras de trabajo, centros de conferencia o cuartos de hotel, las soluciones inalámbricas son simples, rápidas y económicas. Desde prácticamente cualquier lugar en alguna localidad o instalación, los empleados podrán compartir archivos y recursos para gozar de una mayor productividad. Las tarjetas PC cards inalámbricas se comunican directamente entre sí y sin la necesidad de un punto de acceso inalámbrico.

2.1.10.6 Oficinas en el hogar

Utilizar una solución inalámbrica para crear una red en la oficina de su casa, evitando los desagradables cables dispersos en su sitio de trabajo. Además, se puede enlazar a la familia, permitiendo que todos compartan impresoras, escáners y si usa un router de acceso, o un módem de cable o DSL el Internet. Conéctese a la red desde cualquier cuarto o hasta el patio.

2.1.11 REQUERIMIENTOS PARA CREAR UNA RED INALÁMBRICA.

- Puntos de acceso
- PC Cards

Las redes inalámbricas están formadas por dos componentes: puntos de acceso y PC cards. Los componentes se comunican entre sí, a través de transmisiones de frecuencia de radio, que eliminan la necesidad de cables.

2.1.11.1 Puntos de acceso

Una red inalámbrica se crea con uno o más puntos de acceso que actúan como hubs, enviando y recibiendo señales de radio desde o hacia computadoras personales equipadas con PC cards inalámbricas para clientes. El punto de acceso puede ser un aparato en sí que forma parte de la base de la red o la conecta por medio de cables a una red de área local (LAN) convencional. Los usuarios pueden enlazar múltiples puntos de acceso a una LAN, creando segmentos inalámbricos en todas sus instalaciones.

2.1.11.2 PC cards

Para comunicarse con el punto de acceso, cada computadora portátil o de escritorio necesita una tarjeta especial para redes inalámbricas. Al igual que las tarjetas de interfaz para redes (NICs) de las redes tradicionales, estas tarjetas permiten que los aparatos se comuniquen con el punto de acceso. Se instalan fácilmente en las ranuras PC de las computadoras portátiles, las ranuras PCI de los dispositivos de escritorio, o se enlazan a puertos USB. Una característica exclusiva que presenta la PC card inalámbrica de uno de los fabricantes líder, es una pequeña antena que se retrae cuando no se encuentra en uso. Esto resulta muy beneficioso, dado el nivel de movilidad de las computadoras portátiles. Además, un usuario puede conectar cualquier otro dispositivo que no tenga una ranura para Tarjetas PC o PCI a su red inalámbrica, al usar un Ethernet Client Bridge que funciona con cualquier dispositivo que cuente con Ethernet o puerto serial, impresoras, escáners, etc.

Una vez que se conecta el punto de acceso a una toma de poder y los aparatos en red están debidamente equipados con tarjetas inalámbricas, las conexiones de red se hacen automáticamente cuando estos aparatos se encuentren dentro del campo de alcance del hub. El campo de alcance de una red inalámbrica en ambientes estándares de oficinas puede ser de varios cientos de metros.

Las redes inalámbricas operan igual que las redes tradicionales y ofrecen los mismos beneficios y eficiencia en cuanto a productividad. Los usuarios podrán compartir archivos, aplicaciones, periféricos y acceso al Internet.

2.1.12 BENEFICIOS DE UNA RED INALÁMBRICA.

- Estar basada en estándares y contar con certificación Wi-Fi
- Instalación simple
- Robusta y confiable
- Escalabilidad
- Facilidad de uso
- Servidor Web para una administración más fácil
- Seguridad
- Una aplicación que detecte localidades

2.1.12.1 Basada en estándares y contar con certificación Wi-Fi

El Wi-Fi es un robusto estándar de redes, comprobado en la industria de transmisión de datos, que asegura que los productos inalámbricos ínter operarán con otros productos certificados de Wi-Fi de otros fabricantes de redes. Con un sistema basado en Wi-Fi, los usuarios gozarán de compatibilidad con el mayor número de productos inalámbricos y evitarán los altos costos y la selección limitada de las soluciones patentadas de un solo fabricante.

Además, la selección de una solución inalámbrica basada en estándares, que sea totalmente ínter operable con redes Ethernet y Fast Ethernet, le permitirá al usuario que su red inalámbrica trabaje sin interrupciones con su sistema existente de LAN tradicional.

2.1.12.2 Instalación simple

La solución inalámbrica debe ser del tipo plug and play; tomando solamente unos minutos para su instalación. Al conectarla, los usuarios empezaran a gozar de inmediato de los servicios en red. Para obtener una instalación aún más fácil, su solución deberá soporta el protocolo denominado Dynamic Host Configuration Protocol (DHCP), el cual asignará automáticamente direcciones IP a los clientes inalámbricos. En lugar de instalar un servidor DHCP en algún aparato independiente para obtener esta capacidad de ahorro de tiempo, los usuarios deben seleccionar hubs inalámbricos que ofrezcan servidores DHCP incorporados.

Si un usuario está agregando un sistema inalámbrico a su red Ethernet, sería una buena opción potenciar un punto de acceso a través de cables estándares de Ethernet; esto le permitirá hacer que el punto de acceso funcione utilizando un voltaje bajo de corriente CC en el mismo cable que es usado para transmitir datos: eliminando la necesidad de tener una toma de poder local y un cable para cada dispositivo de puntos de acceso.

2.1.12.3 Robusta y confiable

Considere soluciones inalámbricas robustas que tengan alcances de por lo menos 100 metros. Estos sistemas les ofrecerán a los empleados de una compañía una considerable movilidad dentro sus instalaciones. Un usuario puede optar por un sistema superior que automáticamente detecte el ambiente, para seleccionar la mejor señal de frecuencia de radio disponible y obtener máximos niveles de comunicaciones entre el punto de acceso y las PC cards. Para garantizar una conectividad a las velocidades más rápidas posibles -incluyendo largo alcance o ambientes ruidosos- el usuario debe asegurarse que su nuevo sistema pueda hacer cambios dinámicos de velocidades, basándose en las diferentes intensidades de señal y distancias del punto de acceso. Además, el usuario debe seleccionar PC cards inalámbricas para computadoras portátiles que ofrezcan antenas retractables para prevenir rupturas durante la movilización de los aparatos.

2.1.12.4 Escalabilidad

Un buen hub inalámbrico deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas en computadoras adicionales e impresoras listas para ser conectadas a la red. Las impresoras u otros dispositivos periféricos que no puedan conectarse en red tradicional, se conectan a su red inalámbrica con un adaptador USB inalámbrico o un Ethernet Client Bridge.

2.1.12.5 Facilidad de uso

Si un usuario planea conectar múltiples hubs inalámbricos a una red existente de cables, considere una solución que ofrezca conexiones automáticas a la red. Cuando un usuario se desplace fuera de los límites de un hub al campo de otro, una capacidad automática de conexión a la red transferirá sus comunicaciones -sin interrupciones- al siguiente aparato, aún al cruzar límites de routers, sin siquiera tener que reconfigurar la dirección IP manualmente. Esto resulta ser especialmente útil para aquellas compañías con múltiples instalaciones que están conectadas por medio de una red de área amplia (WAN). Como resultado, los usuarios podrán movilizarse libremente -dentro de sus instalaciones y más allá- y permanecer conectados a la red.

2.1.12.6 Servidor Web para una administración más fácil

Un usuario simplificará la administración de su red inalámbrica si selecciona un punto de acceso con un servidor Web incorporado. Esto le permitirá acceder y definir parámetros de configuración, monitorear el rendimiento y hacer diagnósticos desde un navegador Web.

2.2 IMPLEMENTACIÓN DE POLÍTICAS [8]

2.2.1 TIPOS DE INSEGURIDADES

Las inseguridades de las redes inalámbricas radican en:

- Configuración del propio “servidor” (puntos de accesos).
- La “escucha” (pinchar la comunicación del envió de paquetes).
- “Portadoras”.
- El sistema de encriptación (WEP, Wirelles Equivalent Privacy, el mas usado es de 128 Bits, pero depende del uso que se le de a la red.)

2.2.2 CONSEJOS DE SEGURIDAD

Para que un intruso se pueda ingresar a una red inalámbrica tiene que ser nodo o usuario, pero el peligro radica en poder escuchar la transmisión. Los siguientes son consejos para poder estar más tranquilos con la red inalámbrica.

2. Cambiar las claves por defecto cuando instalemos el software del Punto De Acceso.
3. Control de acceso seguro con autentificación bidireccional.
4. Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
5. Configuración WEP (muy importante) , la seguridad del cifrado de paquetes que se transmiten es fundamental en la redes inalámbricas, la codificación puede ser mas o menos segura dependiendo del tamaño de la clave creada y su nivel , la mas recomendable es de 128 Bits.
6. Crear varias claves WEP para el punto de acceso y los clientes y que varíen cada día.

---

[8] Seguridad en Redes Inalámbricas, http://www.zonagratuita.com/servicios/seguridad/wireles.html

7. Utilizar opciones no compatibles, si nuestra la red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que el posible intruso tenga que trabajar con un modelo compatible al nuestro.
8. Radio de transmisión o extensión de cobertura, este punto no es muy común en todos los modelos, resulta más caro, pero si se puede controlar el radio de transmisión al círculo de nuestra red podemos conseguir un nivel de seguridad muy alto y bastante útil.

2.2.3 SEGURIDAD

Si un usuario escoge una solución inalámbrica que ofrezca múltiples niveles de seguridad, incluyendo encriptación y autenticación de usuarios. Una solución segura también le ofrecerá una encriptación de por lo menos 40 bits de encriptación. Tanto para su facilidad de uso como para una protección más fuerte, seleccione una solución superior que automáticamente genere una clave nueva de 128 bits para cada sesión de red inalámbrica, sin tener que ingresar la clave manualmente. Además, el usuario debe considerar un sistema que ofrezca autenticación del usuario, requiriendo que cada usuario ingrese con una contraseña antes de acceder la red.

2.2.3.1 ¿802.11 seguridad? [9]

La IEEE 812.11 provee seguridad a través de la autenticación e encriptación. En el Ad Hoc o modo de servicio extendido de la red, la autenticación puede ser un sistema abierto o una la llave compartida. Una estación de la red que recibe una demanda puede conceder la autenticación a cualquier requerimiento o sólo a esas estaciones en una lista definida. En un sistema de clave compartida, únicamente aquellas estaciones en una lista definida que poseen una clave encriptada reciben autenticación.

[9] Red de Área Local Inalámbrica (WLAN), Wireless Security, Randall K. Nichols, Panos C. Lekkas, 2003

La IEEE 802.11 especifica una capacidad de encriptación opcional llamada Wired Equivalent Privacy Privacidad Equivalente Alambrada (WEP). Como el nombre lo indica, la intención es establecer una seguridad conmensurable a las redes alambradas. WEP emplea el algoritmo RC4. El algoritmo de RC4 encripta las transmisiones que van por el aire.

El dilema de seguridad para el 802.11 es que esa capacidad de encriptación para WEP no se extiende a la transmisión fin a fin. Solo protege la información de datos paquete y no protege la cabecera de la capa física mientras que otras estaciones en la red pueden escuchar la necesidad de control de datos para manejar la red. (Presumiblemente las otras estaciones no pueden descifrar las porciones de datos del paquete).

2.2.3.2 IEEE 802.11b

Como su predecesor, 802.11b trabaja en la banda de los 2.4 - 2.48 GHz y proporciona a los usuarios conectividad en cualquier país. También direccionado como Ad Hoc y servicios extendidos de red. Al contrario del 802.11, el IEEE 802.11b remueve FHSS como un modo de transmisión de datos y establece a la DSSS como una tecnología de la transmisión estándar. Eso porque la DSSS maneja bien las señales débiles. Con DSSS, los datos pueden ser extendidos de una interferencia de fondo sin tener que ser retransmitidos. Con DSSS como la técnica de transmisión seleccionada, la 842.11b establece también los rangos de velocidades de datos 5.5 y 11 Mbps.

Algunos equipos que cumplen con el estándar 802.11b ofrecen un esquema de encriptación opcional, de 128 bits, superior a su esquema de encriptación predecesor de 40 y 64 bits. También los vendedores están produciendo equipos 802.11b con tarjetas de interfase de red (NICs) las que poseen un único MAC y un único par de llaves publica-privada. Con estas mejoras, los administradores de WLAN pueden requerir todas las direcciones de hardware y las combinaciones de llave publica para ser ingresados en los puntos de acceso (APs) antes de

establecer la red, ellos pueden configurar los puntos de acceso para guardar las combinaciones que ellos encuentren y rechazan cualquier error. Haciendo esto, un administrador puede prevenir ataque en una red a través de una dirección spoofing MAC.

2.2.4 AMENAZAS

Una WLAN opera de la misma manera como una LAN alambrada sólo que los datos son transportados a través de un medio inalámbrico usualmente ondas de radio antes que los cables. Un puerto WLAN alberga la misma vulnerabilidad como una LAN alambrada, más algunas específicas a ella.

Esta sección discute amenazas comunes que enfrentan las WLANs, algunas de las medidas preventivas que se han diseñado para direccionar esas amenazas y las fortalezas y limitaciones de esas medidas preventivas.

2.2.4.1 Eavesdropping (Escuchar secretamente por medio de dispositivos electrónicos)

La amenaza principal es la potencial autorización para escuchar las señales de radio enviadas entre una estación inalámbrica y un AP, comprometiendo la confidencialidad de la información. Escuchar es un ataque pasivo. Cuando un operador de la radio envía un mensaje sobre una ruta de radio, todos los otros usuarios equipados con un receptor compatible dentro del rango de transmisión pueden escuchar el mensaje. Además, porque un eavesdropping puede escuchar un mensaje sin alterar a los datos, el remitente y el receptor del mensaje no siempre puede estar fuera de la intromisión.

Las LANs alambradas también son vulnerables a eavesdropping, pero no a la misma magnitud. Una LAN alambrada puede irradiar señales electromagnéticas a través de cableado, pero un eavesdropping debe estar cerca del cableado para

oír las señales con un dispositivo. Por el contrario, algunos eavesdropping en una WLAN pueden estar localizados a cierta distancia de la red e incluso pueden estar fuera de los confines físicos del ambiente en que la red opera. Esto es porque las señales de radio emitidas de una WLAN pueden propagarse más allá del área en la cual se origina, y puede penetrar paredes de edificios y otros obstáculos físicos, dependiendo de la tecnología del transmisor y la fuerza de la señal.

El equipo capaz de interceptar el tráfico de WLAN está disponible a los consumidores en forma de adaptadores inalámbricos y otros productos compatibles con el estándar 802.11. La dificultad eavesdropping es decodificar la señal digital a 2.4 GHz porque la mayoría de los sistemas de WLAN usa tecnología del Spread-Spectrum la cual es resistente al eavesdropping. Además, si la encriptación usada, los eavesdroppin deben descifrar el contenido encriptado. A pesar de estas dificultades, eavesdropping propone una amenaza significativa a las comunicaciones de WLAN.

2.2.4.2 Acceso no autorizado

Una segunda amenaza a la seguridad de WLAN es el potencial para un intruso para entrar en un sistema de WLAN enmascarado como un usuario autorizado. Una vez dentro, el intruso puede violar la confidencialidad y la integridad del trafico de la red enviando, recibiendo, alterando, o forjando los mensajes. Éste es un ataque activo, y puede llevarlo acabo usando un adaptador inalámbrico que es compatible con la red atacada, o usando un (por ejemplo, robado) dispositivo acomodado que se une a la red.

La mejor protección contra el acceso desautorizado es desplegar los mecanismos de la autenticación para asegurar, que solo los usuarios autorizados puedan acceder a la red. Tales mecanismos son regularmente desplegados en las LANs alambradas, no sólo para prevenir accesos desautorizados, sino también para descubrir las intrusiones cuando ellas ocurren. Descubrir intrusos que intentan acceder a la WLAN no es fácil. Esto es porque podrían interpretarse mal los

ataques infructuosos como esfuerzos de logon causados por el high bit error rate (BER) de radio transmisiones o por estaciones que pertenecen a otra WLAN.

Una variante de acceso desautorizado es un atacante que engaña las estaciones inalámbricas preparando un falso AP. Cuando una estación inalámbrica es primero energizada o cuando entra en un nueva micro celda, escoge un AP para enlazar, basado en la fuerza de la señal y observa las proporciones de error de paquete. Si es aceptada por el AP, la estación sintoniza al canal de radio que la AP está usando. Poniendo un AP falso con una señal poderosa, un atacante puede atraer una estación en red para capturar claves secretas y logon password. Alternativamente, el atacante puede rechazar los logon intentados pero graba los mensajes transmitidos durante el proceso de logon, para el mismo propósito.

El primer tipo de ataque descrito arriba es muy difícil de llevar a cabo, porque el atacante debe tener información muy detallada para poder engañar a la estación que cree que ha sido accesada a la red casera. Por otra parte, el ataque puede ser fácilmente detectado. El segundo tipo de ataque es más fácil de implementar, porque el atacante únicamente requiere un receptor y una antena que es compatible con las estaciones vistas. Este ataque también es difícil de ser detectado porque logons infructuoso son relativamente comunes en comunicaciones de WLAN. La mejor protección contra ambos tipos de ataques es usar un mecanismo de autenticación eficiente que permita a las estaciones inalámbricas autenticar a los APs sin revelar llaves confidenciales o passwords.

2.2.4.3 Interferencia y Jamming

Una tercera amenaza a la seguridad de las WLAN es la radio interferencia que puede degradar seriamente (el throughput de los datos). En muchos casos la interferencia es accidental. Porque las WLANs usan las ondas de radio ilícitas, otros dispositivos operan en los infrarrojos o la radio frecuencia de 2.4 GHz puede saturarse con el tráfico de la WLAN. Las fuentes potenciales de interferencia incluye a los aficionados de gran potencia, militar, industrial, científica y

transmisores militares (ISM). Los hornos de microonda son una posible fuente, pero la mayoría de los vendedores de las WLAN diseñan sus productos minimizan la interferencia de la microonda. Otra preocupación; en la operación de dos o más WLANs en la misma área cubierta. Algunas WLANs son diseñadas para operar en la proximidad de otros sistemas mientras operan o no.

Claro la interferencia también puede ser intencional. Si un atacante tiene un transmisor poderoso, él o ella pueden generar una señal de radio suficientemente fuerte para agobiar las señales débiles, rompiendo las comunicaciones. Ésta es una condición conocida como Jamming, es un rechazo al servicio atacado. Dos tipos de jammers que puede usarse contra el tráfico de LAN son pulsados en alta potencia de banda llana jammers que cubren la frecuencia entera usada por la señal en uso y bandas parciales y jammers de baja potencia que cubren únicamente parte de la frecuencia usada por la señal en uso.

Equipos de Jamming están disponibles a los consumidores o pueden ser construidos por atacantes con conocimiento. En suma, los atacantes Jamming pueden ser montados en una localización remota de la red en uso (por ejemplo de un vehículo estacionado al otro lado de la calle o un apartamento en el próximo bloque). Equipos de direccionamiento pueden detectar la fuente de las señales jamming, pero no necesariamente a tiempo para impedir el Jamimng.

2.2.4.4 Amenazas Físicas

Las WLANs pueden venirse abajo por daños o destrucción de la infraestructura física. Como un WLAN alambrado, un WLAN opera en el modo de infraestructura variada de componentes físicos, Incluyendo APs, cables, antenas, adaptadores inalámbricos y software. Daños en cualquiera de estos componentes podrían reducir la fuerza en la señal, limitar el área cubierta, o reducir el ancho de banda, mientras la habilidad de los usuarios para acceder a los datos y servicios de información (por ejemplo, servidores de archivo, impresoras y enlaces de

internet). Si es lo suficientemente severo, compromete la infraestructura física para apoyar las operaciones de la WLAN.

La infraestructura de los componentes es susceptible a las condiciones del medio ambiente en el que ellos operan, especialmente afuera. APs pueden ser obstruidas por la nieve, hielo, y distorsión de las señales de radio. Las antenas montadas encima de palos o edificios pueden ser golpeadas oblicuamente, por vientos, doblados por el hielo, cambiando el ángulo del ancho del haz usado para transmitir señales. Esto puede ser problemático especialmente para antenas con haces de banda estrecha, como las antenas de disco parabólico. Las antenas y APs también pueden ser dañados por el relámpago, intrusión de agua en el cableado y conectores que unen a la red alambrada. Finalmente los accidentes y usos inapropiados pueden dañar los adaptadores inalámbricos y las estaciones inalámbricas.

Los componentes físicos también pueden estar sujetos al ataque. Las WLANs generalmente confían en plantas físicas más pequeñas que las LANs alambradas, haciendo de ellas menos vulnerable al sabotaje, pero ellas no son completamente seguras. Por ejemplo, un atacante podría cortar el cable que conecta un AP a la red alambrada, aislando las micro celdas afectadas y rompiendo la potencia al receptor. Un atacante puede también estar apto para dañar o destruir un AP expuestos a la antena conectada a él. Un atacante también podría robar o podría comprometer una estación inalámbrica o un adaptador y podría usarlo para intentar interceptar el tráfico WLAN o para ganar el acceso desautorizado a la red. Finalmente, un atacante podría sabotear la red alambrada, rompiendo el funcionamiento de todas las WLANs conectadas a ella.

2.2.5 CONTRAMEDIDAS

Los sistemas de WLAN más comúnmente usan tecnología de Espectro-Extendido para transmitir datos. El Espectro-Extendido esta diseñado para resistir eavesdropping, la interferencia y ruido. A los escuchadores casuales, la señal

suena como ruido de fondo. El Espectro-Extendido consume más ancho de banda que las transmisiones de banda estrecha (las cuales concentran señales en una sola frecuencia), pero produce una señal que es fácil detectar si el receptor conoce los parámetros de la transmisión. El receptor usa el mismo código extendiendo usado por el transmisor para reagrupar la señal extendida a su forma original.

2.2.5.1 Wep

Aunque los sistemas WLAN pueden resistir un espionaje pasivo, la única manera de prevenir terceras partes del compromiso de los datos transmitidos es usar la encriptación. El propósito de WEP es asegurar que los sistemas WLAN tengan un nivel de privacidad que es equivalente a las LANs alambradas por la encriptación de las señales de radio: Un segundo propósito de la WEP es prevenir usuarios sin autorización de acceso a las WLANs (esto es proveer autentificación). El segundo propósito no es explicito en el estándar 802.11, pero es considerado como un importante aspecto de los algoritmos de la WEP.

La WEP es un elemento crítico para la seguridad de la confidencialidad e integridad de los datos de la base estándar, los sistemas WLAN como proveen control de acceso a través d la autentificación. Consecuentemente, la mayoría de los productos WLAN soportan WEP. La manera en la cual la WEP provee encriptación y autentificación se describe luego.

2.2.5.2 Encriptación

La WEP usa una clave secreta que es compartida entre una estación inalámbrica y un punto de acceso (AP). Todos los datos enviados y recibidos entre una estación inalámbrica y una AP puede estar encriptada usando esta clave compartida. El estándar 802.11 no especifica como la llave secreta esta establecida pero le permite un arreglo que ocasiona una única clave en cada

estación. En la práctica general una clave es compartida entre todas las estaciones y Aps de un sistema dado.

WEP proporciona encriptación de datos usando una clave secreta de 40 bits (débil) [802.11] o 128 bits (fuerte) [802.1lb] llave secreta y un RC4 Pseudo Random Number Generator (PRNG). Dos procesos son aplicados al texto simple de datos: uno encripta el texto simple, y el otro lo protege de modificaciones desautorizadas mientras esta en tránsito. La llave confidencial se encadena con un vector de inicialización randóm (IV) que agrega 24 bits a la llave resultante. La llave se inserta en el PRNG que genera una larga llave de flujo pseudo-aleatorio. El remitente XORs de la llave stream con el texto simple para generar el texto encriptado, o ciphertext, y lo transmite al receptor a lo largo con el IV. Una ves recibido el ciphertext, el receptor usa los IV y su propia copia de la llave confidencial para producir un stream que es idéntica a la llave stream generada por el transmisor. El receptor entonces XORs la llave stream con el ciphertext para revelar el texto simple original.

Para proteger el ciphertext contra modificaciones desautorizadas mientras esta en tránsito, WEP aplica un algoritmo de chequeo de integridad (CRC-32) al texto simple que produce un Valor de Chequeo de Integridad (ICV). El ICV es entonces concatenado al texto simple. El ICV es en efecto el fingerprint del texto simple. El ICV es adjuntado al ciphertext y enviado al receptor junto con los IV. El receptor combina el ciphertext con la llave stream para descubrir el plaintext. Aplicando el algoritmo de integridad al plaintext y compara la salida IVC a la ICV transmitida que verifican la desencriptación. Si los dos ICVs son idénticos, el mensaje se autentico; es decir, el fingerprint es igual. Figuras 7-6 y 7-7 ilustran la encriptación y desencriptación de WEP, respectivamente.

A pesar de la fuerza de potencial de WEP para proteger la confidencialidad e integridad de los datos, tiene limitaciones que sólo pueden ser direccionadas por el propio manejo. El primer problema stems de la reutilización de la IV. La IV esta incluido en la parte no encriptada de un mensaje de manera que el receptor sabe que IV se usa cuando genera la llave stream para desencriptar. El estándar

802.11 recomienda pero no es requerido que la IV sea combinada después de cada transmisión. Si la IV no cambia regularmente, pero es reutilizable para subsecuentes mensajes, un eavesdropper puede estar habilitado para criptoanalizar la llave stream generado por el IV y la llave secreta y de ahí desencriptar los mensajes que usa esa IV.

El problema de la reutilización IV potencialmente conduce hacía otro. A saber, una vez que el atacante sabe la secuencia de la llave para un mensaje encriptado, basado en la reutilización de IV, él o ella pueden usar esta información para construir una señal encriptada e insertarla dentro de la red. El proceso es para crear un nuevo mensaje, calcula el CRC-32, y modifica el mensaje original encriptado para cambiar el plaintext del nuevo mensaje. El atacante puede entonces transmitir el mensaje a un AP o a una estación inalámbrica, la cual la aceptarían como un mensaje válido. Cambiando el IV después de que cada mensaje es que una manera simple de prevenir problema y la secuela previamente descrita.

La distribución de llaves es otro problema. La mayoría de WLANs comporten una llave entre todas las estaciones APs en la red. Es improbable que una llave compartida entre muchos usuarios permanezca en secreto indefinidamente. Algunos administradores de la red direccionan este problema por la configuración de estaciones inalámbricas con la llave confidencial de ellos mismos, en lugar de permitir terminar a los usuarios realizan esta tarea. Ésa es una solución imperfecta; aunque, porque la llave compartida es guardada en las computadoras de los el usuarios dónde es vulnerable. Además, si una llave en una estación esta comprometida, todas las otras estaciones en el sistema deben ser reconfiguradas con un nuevo llave. La mejor solución es asignar una llave única para cada estación y cambiar la clave frecuentemente.

Aunque la encriptación WEP esta diseñada para ser eficientemente compatible, puede reducir el ancho de banda en uso. Según un informe, la encriptación de 40 bits reduce el ancho de banda por 1 Mbps, y la encriptación de 128 bits reduce el ancho de banda por 1 a 2 Mbps. Esta degradación de supresión es relativamente

pequeña, pero los usuarios todavía pueden notarlo, especialmente si la señal es transmitida vía FHSS la cual transmite señales a un máximo de sólo 3 Mbps. En muchos casos el impacto exacto dependerá del producto que se usa y el número de usuarios en el sistema.

2.2.5.3 Autenticación

La WEP provee dos tipos de autenticación: una por omisión del sistema predefinido, donde todos los usuarios están permitidos acceder a la WLAN, y compartir la clave de autenticación la cual controla el acceso a la WLAN y provee el acceso a la red desautorizada. De los dos niveles, la autenticación de llave compartida es el modo seguro. Usa una llave confidencial que es compartida entre todas las estaciones y APs en un sistema WLAN. Cuando una estación intenta asociarse con un AP, la AP contesta con el texto aleatorio en la forma de un desafío. Las estaciones deben usar la copia de su llave confidencial compartida para encriptar el texto del desafío y enviarlo de vuelta al AP para autenticarse ella misma. El AP desencripta la respuesta que usa la misma llave compartida y la compara con el texto del desafío enviado tempranamente. Si el texto es idéntico, el AP envía un mensaje de confirmación a la estación y acepta a la estación en la red. Si la estación no tiene una llave, o si le envía una contestación equivocada, el AP lo rechaza, previniendo a la estación que de accede a la red.

Note que la autentificación de clave compartida trabaja únicamente si la encriptación de WEP esta habilitada. Si no lo esta, el sistema fallara hacia el modo de Sistema Abierto, permitiendo casi a cualquier estación dentro del rango de un AP acceder a la red. Esto crea una ventana para los intrusos dentro del sistema, donde él o ella pueden enviar, recibir, alterar, o fabricar mensajes. Asegúrese que la WEP esta habilitada siempre que la autenticación segura se requiera. Incluso cuando la autenticación de llave compartida esta habilitada, todas las estaciones inalámbricas en un sistema WLAN puede tener la misma llave compartido, dependiendo cómo este instalado sistema. Para algunos

sistemas, autentificación individual no es posible; todos usuario-incluyendo los no autorizados con la clave compartida pueden acceder a la red. Esta debilidad puede resultar en un acceso no autorizado, sobre todo si el sistema incluye un gran número de usuarios. La mayoría de usuarios, el mayor probabilidad que la llave compartido pudiera entrar en las manos malas.

Finalmente, en muchos sistemas WLAN, la llave usada para la autenticación es la misma llave usada para el encriptación. Esta debilidad particular compone los problemas descritos anteriormente. Si un atacante tiene la llave compartida, él o ella no sólo pueden usarlo para acceder a la red sino también para descifrar los mensajes, creando una amenaza dual. La solución es distribuir llaves separadas a través del sistema uno para la autenticación y otro para la encriptación.

La WEP ha sido encontrada sumamente (aunque espectacularmente), agrietada para un daño serio sus demandas de seguridad y soportes. WLANs ha sido exitosamente sujeta a varias formas de ataque, incluso la desencriptación, basada en el análisis estático. La WEP tiene la vulnerabilidad adicional de ignorar algún tráfico sin autorización o una descriptación sin autorización, inyectados por atacante travieso al punto de acceso. Debido a esas desventajas, es probable que WEP sólo se use en el futuro en la conjunción VPNs.

2.2.6 OTRAS TÉCNICAS DE AUTENTICACIÓN

Es razonable considerar las técnicas de la autenticación como otras que comparten la llave de autenticación. Extended Services Set Identification (ESSID) es normalmente usada como técnica de autenticación. ESSID es un programa valioso en cada AP para identificar que subred de AP esta encendida. Este valor puede usarse para la autenticación para asegurar que solamente estaciones autorizadas puedan acceder la red. Si una estación no conoce el ESSID, no se le permite asociarse con el AP.

En suma, algunos fabricantes proveen una tabla de Control de Acceso al Medio (MAC) y direcciones en un access controd listt (ACL) que es incluida en el AP. Cuando una estación intenta asociarse con el AP, el enrutador en el AP lee la única dirección MAC en el adaptador inalámbrico de la estación y determina si está en la ACL. El acceso a la red esta restringido a aquellas estaciones en la lista; otras son rechazadas. Esto habilita a los administradores de la red incluir o excluir las estaciones inalámbricas. Esta capacidad provee una valiosa capa de seguridad adicional, no sólo para excluir estaciones foráneas también para excluir esas estaciones que pertenecen a la red pero han sido comprometidas (por ejemplo, una computadora robada).

2.2.7 SEGURIDAD FÍSICA

Se deben tomar precauciones para proteger los componentes físicos de una WLAN de accidentes, clima, y vandalismo. Esas precauciones deben ser correspondientes con el tipo de riesgos a que los componentes son expuestos, la probabilidad de que éstas ocurran, y el impacto que una ocurrencia llevaría a detener el funcionamiento de la WLAN. Si el equipo no puede ser protegido adecuadamente, debe fortalecerse para minimizar el impacto de estas condiciones. Deben montarse APs y antenas firmemente y localizadas en áreas que minimicen su exposición a las fuentes potenciales de interferencia, incluyendo los hornos de microonda y otros transmisores. Si los Aps y antenas están situadas en las afueras debería minimizarse la exposición a los vientos fuertes, nieve, y hielo, también deberían estar blindadas para detener relámpagos. Deben desplegarse para suprimir los efectos de golpes de relámpagos. El cableado debe estar con cubierta protectora, dónde sea posible, y cercanas cañerías y tanques de agua deberán ser mantenidos apropiadamente par prevenir fugas y derramamientos accidentales.

En suma, se debería negar el acceso a personal no autorizado al equipo de WLAN. Colocar los APs y antenas en las áreas seguras, lejos del trafico del publico y protegido con barreras apropiadas y controles de acceso. También

pueden usarse sistemas de descubrimiento de intrusión como circuito cerrado de televisión para supervisar los recursos remotos o expuestos.

Juntamente con las medidas físicas, se debe emplear controles administrativos apropiados. Estaciones inalámbricas asignadas a los usuarios de WLANs deberían ser apropiadamente logged y la identidad de los usuarios grabados. Las ACLs deberán ser mantenidas y regularmente puestos al día. Deben etiquetarse los equipos de WLAN apropiadamente para asegurar su identificación si se daña o se destruye. La etiqueta también puede detener el robo. Deben desarrollarse los procedimientos de respuesta en caso de que el equipo de WLAN este comprometido, dañado, o destruido.

Finalmente, debe educarse a los usuarios en la importancia de proteger sus estaciones del robo, daño, y mal uso. Por ejemplo, los usuarios nunca deben dejar sus estaciones desatendidas en las áreas públicas, y deberían salir fuera de la red si no están usándola. Además, los usuarios no deberían comer o beber cerca de su estación, y ellos deben evitar trabajar cerca de los posibles riesgos, como los hornos de microonda. Ellos también deben informar inmediatamente cualquier ocurrencia de actividad sospechosa que involucra a la WLAN, incluso los casos de compromiso o equipo robado.

2.2.8 UNA APLICACIÓN QUE DETECTE LOCALIDADES

Su solución de redes inalámbricas deberá incluir una aplicación para la detección de sus instalaciones. Esta aplicación le podrá ayudar al usuario a determinar la posición óptima de los hubs inalámbricos y el número de hubs que necesita para soportar a sus usuarios. Además, le ayudará a implementar una solución inalámbrica en forma efectiva y eficiente.

2.2.9 PROBLEMAS TÍPICOS DE SEGURIDAD Y SOLUCIONES [10]

La rápida expansión de las redes inalámbricas (wireless) basadas en los estándares 802.1x ha añadido un nivel adicional de complejidad al problema de la seguridad de redes. Aunque los mencionados estándares incorporan ciertas funciones de seguridad y que los diferentes fabricantes de equipos wireless han añadido diferentes mecanismos de protección, las redes inalámbricas representan un punto extremadamente vulnerable en la seguridad de una red.

Este documento explora siete problemas básicos que padecen las redes basadas en el estándar 802.11.

2.2.9.1 Puntos de Acceso Vulnerables

Las redes inalámbricas son fáciles de detectar. Con el objetivo de facilitar la conexión a los usuarios las redes emiten gran cantidad de información acerca de su configuración. Esta información es exactamente lo que un hacker necesita para lanzar un ataque.

Las redes 802.11 no utilizan ninguna función de seguridad para proteger esta información. Por tanto, cualquier usuario con una tarjeta wireless estándar 802.11 puede acceder a estos datos. Atacantes con antenas amplificadoras pueden acceder a redes ubicadas en otros edificios y a algunas calles de distancia.

Solución:

Lo ideal sería aislar la red inalámbrica de forma que las emisiones electromagnéticas de la red no salgan fuera del perímetro de la empresa, o fuera de las habitaciones en las que se utilizase la red. Sin embargo para la mayoría de empresas esta no es una solución factible.

---

[10] Redes Inalámbricas-Siete Problemas Típicos de Seguridad y Soluciones Recomendadas, www.totenguard.com

En muchos casos una solución eficiente es ubicar los puntos de acceso en redes DMZ (para mitigar cualquier intrusión) y en utilizar VPNs en la comunicación con los usuarios (para proteger el contenido de las transmisiones y poder contar con el sistema de autentificación del servidor de VPNs).

Otra medida de seguridad adicional es autentificar el acceso de los usuarios a través de la red inalámbrica con un servidor de autentificación. Por ejemplo, el estándar 802.1x soporta nuevos tipos de autentificación para integraciones con servidores RADIUS.

2.2.9.2 Puntos de Acceso no Autorizados

Las redes inalámbricas son fáciles de implementar y su precio está al alcance de cualquier usuario. Es relativamente sencillo comprar e instalar un punto de acceso wireless sin que éste sea advertido por los administradores de la red. En algunas ocasiones un departamento dentro de la empresa puede decidir instalar sus propios puntos de acceso sin coordinar dicha instalación con los responsables de seguridad.

Al funcionar prácticamente tan pronto como se conecta, la mayoría de puntos de acceso inalámbrico instalados sin supervisión utilizan la configuración por defecto. El problema principal es que esta configuración por defecto normalmente carece de todas las medidas de seguridad aplicables.

Solución:

Auditar las oficinas de la empresa de forma regular con un detector de redes inalámbricas o un Wireless Analyzer. Por ejemplo esto puede implicar asignar de forma regular un técnico para que se pasee por las oficinas con un ordenador portátil, o una agenda personal PDA, equipada con una herramienta para la detección de puntos de acceso wireless.

Existen varias herramientas en el mercado para el escaneo de redes inalámbricas. Algunas funcionan de forma pasiva detectando fuentes de emisión y analizando los datos transmitidos, mientras que otras intentan interrogar a los puntos de acceso que encuentran buscando información sobre los mismos.

2.2.9.3 Accesos a la Red no Autorizados

Muchas instalaciones de redes inalámbricas utilizan la configuración por defecto de los equipos realizando los cambios mínimos para que funcionen. Por lo general estas configuraciones no hacen uso de la encriptación WEP (incluida en el estándar 802.11).

Sin WEP es prácticamente inmediato acceder a una red 802.11, aunque se haya restringido el acceso mediante listas de códigos MAC autorizados. Un hacker equipado con un sniffer puede obtener direcciones MAC válidas en cuestión de segundos, realizar un spoof (falsificación) de la dirección MAC de su tarjeta wireless utilizando la de una tarjeta con acceso autorizado, y entrar en la red.

Solución:

La mejor forma para impedir los accesos no autorizados es utilizar un mecanismo de autentificación fuerte protegido mediante encriptación. Por ejemplo, Transport Layer Security (TLS), Protected EAP (PEAP) o Tunneled TLS (TTLS).

2.2.9.4 Rendimiento Limitado

Las redes inalámbricas tienen una capacidad muy limitada. El estándar 802.11b permite una velocidad nominal de transmisión de 11Mbps, mientras que el 802.11a alcanza los 54Mbps. Debido a la información de control necesaria para mantener la comunicación la velocidad real (práctica) suele ser la mitad que la

velocidad nominal. Además, se trata de una capacidad de transmisión (ancho de banda) que es compartida entre todos los usuarios.

La capacidad de transmisión inalámbrica puede saturarse de diferentes maneras:

- Un punto de acceso puede recibir a través de su conexión a la red física un flujo de datos superior al que el canal de radio puede emitir. Un atacante podría lanzar un ataque PING FLOOD desde un segmento de red Fast Ethernet y saturar rápidamente el punto de acceso.
- Utilizando paquetes de Broadcast, es posible saturar dos puntos de accesos conectados mediante cable.
- Sin estar conectado a ningún punto de acceso, un atacante puede inyectar datos en el canal de radio y saturar el medio. El estándar 802.11 ha sido diseñado para permitir la coexistencia de varias redes en un mismo canal de radio. Todo lo que el atacante ha de hacer es llenar de tráfico a un ritmo elevado el canal de radio utilizado por un punto de acceso, y este punto de acceso se saturará ya que intentará acomodar el nuevo tráfico.

Es especialmente importante recordar que en muchos casos el tráfico normal de una red es suficiente para saturar una red, y no tiene necesariamente que ser tráfico malintencionado o tratarse de un ataque. Aplicaciones Cliente / Servidor pueden transmitir ficheros de datos de gran tamaño de forma simultanea a varios clientes provocando una saturación de los puntos de acceso wireless.

Solución:

Monitorear las redes con un analizador de redes inalámbricas. Es necesario estudiar el tipo de conexiones según su velocidad y tipo de paquetes transmitidos. Un elevado porcentaje de conexiones de baja velocidad pueden indicar la existencia de una interferencia externa, o indicar que los puntos de accesos están demasiado lejos de los usuarios (o que existen obstáculos físicos entre los puntos de acceso y los usuarios). También es interesante averiguar la velocidad en los diferentes canales de radios a lo largo del tiempo para determinar la evolución del

ancho de banda disponible. La saturación de un canal en concreto puede indicar que existe demasiado tráfico y puede ser deseable asignar los usuarios a puntos de acceso alternativos.

2.2.9.5 MAC Spoofing y Secuestro de Sesiones

Al igual que las redes Ethernet, las redes 802.11 no realizan autentificación de “frames” (paquetes) de datos. Cada “frame” tiene una dirección de origen, pero no existe ninguna garantía de que la estación de origen fuese la que realmente emitió los datos. Hackers pueden falsificar paquetes de datos y alterar la tabla ARP de enrutamiento de datos, o pueden simplemente examinar el tráfico y extraer las direcciones MAC correspondientes a los usuarios para luego suplantar a los usuarios reales.

Otra técnica de ataque también utilizada es instalar un punto de acceso que pretende formar parte dela red. No existe ningún mecanismo que permita verificar que se trate de un punto de acceso legítimo.

Las tarjetas wireless de los usuarios automáticamente detectarán este punto de acceso e intentan conectarse, revelando datos sobre su configuración y claves WEP (en caso de utilizar WEP).

Para evitar estos problemas se está trabajando en estos momentos en mecanismos de autentificación para las redes 802.11. En junio del 2001 se aprobó el estándar 802.1x, que requiere que los usuarios se autentifiquen antes de acceder a la red inalámbrica. Sin embargo todavía no hay acuerdo sobre los mecanismos de gestión de claves necesarios para implementar esta autentificación. Estos mecanismos se incluirán en el estándar 802.11i todavía pendiente de aprobación.

Solución:

Hasta que no se apruebe el estándar 802.11i, y se comercialicen equipos que los implementen, es necesario mitigar el problema de la falsificación (Spoofing) de direcciones MAC. Para ello es necesario aislar la red Wireless de la red física. En estos momentos la mejor forma de conseguirlo es implementar un protocolo VPN con encriptación fuerte como por ejemplo IPSec, y no permitir el tráfico en ningún otro protocolo.

2.2.9.6 Análisis de Tráfico y Sniffing

Nada impide a un atacante el “escuchar” el tráfico de radio de una red wireless y observar el tráfico de forma pasiva. Armado con esta información, o utilizando un analizador de redes, un hacker puede averiguar toda la información necesaria para realizar un ataque. El protocolo 802.11 no dispone de ningún mecanismo para evitar que los datos transmitidos sean interceptados. Desgraciadamente el Wired Equivalente Privacy (WEP), que inicialmente tenía que prevenir estos problemas, solamente encripta una parte de los paquetes. Los paquetes de datos para el control y gestión de las transmisiones no son encriptados ni autentificados. Además, el sistema de encriptación utilizado por WEP tiene fallos y es fácilmente descifrable.

Las implementaciones actuales de WEP han corregido muchos de los fallos originales que permitían a un usuario equipado con las herramientas WEPcrack o AirSnort calcular las claves criptográficas en unos pocos minutos. Algunos fabricantes también han implementado un sistema para cambiar las claves WEP cada 15 minutos. De esta manera aunque la red genere grandes cantidades de datos, estos no son suficientes para poder descifrar las claves WEP antes de que éstas sean cambiadas.

Solución:

Al igual que en el punto anterior, la mejor solución es emplear protocolos seguros como el SSH, SSL o IPSec. Hasta que el estándar 802.11i no esté disponible solamente el uso de estos protocolos seguros puede garantizar la seguridad contra escuchas e interceptación del tráfico.

2.2.9.7 Topología de la Red

Una red inalámbrica es difícil de contener, y el medio que utiliza se propaga más allá del espacio físico de la empresa. Muchas redes físicas disponen de extraordinarias medidas de seguridad perimetrales (VPNs, firewalls, detectores de intrusiones, servidores de autentificación, certificados digitales, monitorización continua, etc.). Sin embargo una vez en el interior existen pocos mecanismos de seguridad para detectar un intruso. Al conectar una red wireless directamente a la red interna estamos creando un punto de fallo único, y si la seguridad de esta red wireless falla entonces la seguridad de toda la red interna se ve comprometida con independencia de todas las medidas de seguridad perimetrales.

Solución:

Es imperativo tratar a toda red inalámbrica, por muchas medida de seguridad que tenga, como una red insegura. Una práctica muy recomendada es tratar a las redes wireless como redes DMZ, y conectar los diferentes puntos de acceso a una red DMZ independiente que a su vez está conectada al firewall corporativo. De esta forma se puede regular exactamente que tipos de tráfico y que recursos de la red interna son accedidos desde la red inalámbrica.

2.3 CONTROL DE ACCESO [11]

2.3.1 ARQUITECTURA DE CONTROL DE ACCESO A REDES DE ÁREA LOCAL INALÁMBRICAS 802.11

El auge de las redes inalámbricas de área local ha sacado a la luz toda una serie de deficiencias en lo que a mecanismos de seguridad se refiere. En este artículo se presenta el diseño de una arquitectura de control de acceso para redes inalámbricas basada en el estándar IEEE 802.1X. Dicho sistema hace uso de certificados digitales para proporcionar a los usuarios tanto servicios de autenticación como de autorización. Además, el sistema gestiona también la confidencialidad de la comunicación, integrando el protocolo WEP con el mecanismo de control de acceso.

2.3.1.1 Introducción

Hoy en día es común llegar a un lugar público, como un aeropuerto o un hotel, y encontrarse con una infraestructura de red inalámbrica de área local (WLAN) que ofrece servicio a los usuarios que así lo solicitan. En relación con la tecnología de transmisión WLAN, en los últimos años han ido apareciendo una serie de estándares o especificaciones que tratan de cubrir las distintas áreas de esta tecnología. El más ampliamente extendido es el estándar IEEE 802.11, aunque también existen otras propuestas alternativas, e incompatibles entre sí, como HiperLAN o Bluetooth, este último más enfocado a las redes de área personal. Este tipo de tecnologías ofrece a los usuarios mayor versatilidad a la hora de acceder a los servicios de red, proporcionando múltiples ventajas en lo que se refiere a mantenimiento de la red, implantación y movilidad de los usuarios. Sin embargo, el uso de un canal compartido y de elementos de acceso a la red cableada directamente accesibles por cualquier persona plantea también ciertos

[11] Control de Acceso http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

problemas de seguridad que deben ser resueltos, de entre los cuales el control de acceso de usuarios a la red será el eje principal de este artículo.

En general, el mecanismo más utilizado para realizar un control de conexiones ha sido el uso de bases de datos en las que se introducen manualmente los datos de los usuarios autorizados, ya sean sus identificadores de usuario o direcciones MAC. Sin embargo, esta solución presenta problemas de escalabilidad cuando las bases de datos crecen demasiado o los usuarios cambian frecuentemente.

Como se analizará más adelante, existen hoy en día varias propuestas enfocadas a proporcionar servicios de control de acceso a redes WLAN. Dichas propuestas van desde la provisión de mecanismos de filtrado de direcciones de red o control de identificadores de sesión, hasta arquitecturas completas que proporcionan mayor versatilidad en cuanto a servicios. El trabajo aquí presentado está basado en la especificación IEEE 802.1X, un estándar que define claramente las entidades y protocolos necesarios para llevar a cabo procesos de control de acceso a cualquier servicio ofrecido por una red. 802.1X plantea un escenario con tres entidades básicas como son el cliente, el elemento que proporciona la conectividad a la red (punto de acceso) y el servidor de autenticación encargado de averiguar si un determinado cliente ha sido autorizado a hacer uso de dicha red. En lo que respecta a los protocolos que componen la especificación 802.1X, la propuesta es bastante flexible al no limitar los mecanismos de autenticación a ninguna solución concreta, sino que es posible hacer uso de cualquier tipo de especificación convenientemente adaptada al marco 802.1X. Esta flexibilidad nos va a permitir hacer uso de protocolos basados en certificados digitales como elementos fundamentales a la hora de constatar la autenticidad de los participantes. La importancia del uso de certificados digitales radica en su capacidad para aliviar los problemas de escalabilidad asociados a las soluciones fundamentadas en el uso de bases de datos. Estos elementos permiten que un usuario desconocido para el sistema pueda hacer uso de la red con solo proporcionarle el certificado adecuado. Además en este certificado pueden incluirse ciertos atributos acerca del usuario, como el tiempo máximo que puede utilizar la red, los servicios a los que puede acceder o los recursos que puede

utilizar. El sistema aquí presentado aborda las cuestiones relacionadas con la identificación de clientes que entran en el área de cobertura de un punto de acceso, la especificación del tipo de servicio que el cliente desea obtener de la red, la comprobación por parte del sistema de si dicho cliente ha sido autorizado a disfrutar de los privilegios que solicita, la generación de claves de cifrado de la comunicación entre cliente y punto de acceso (independientes para cada usuario), y el control de la movilidad del usuario. Para ello se han diseñado extensiones para los protocolos básicos del marco 802.1X.

2.3.1.2 Análisis

2.3.1.2.1 Objetivo

El objetivo de este estudio es analizar los diferentes componentes necesarios para desarrollar un sistema de control de acceso a redes WLAN basado en autenticación y autorización. Adicionalmente, se desea además contrastar las limitaciones de los sistemas actuales de cifrado de comunicación de cara a plantear también soluciones al respecto.

2.3.1.2.2 Redes inalámbricas de área local

Ya se ha comentado que en el campo de las redes inalámbricas han aparecido una serie de normas que intentan cubrir todos los ámbitos de su uso. De entre éstas, el estándar IEEE 802.11 es el más extendido en la actualidad.

Este estándar describe una arquitectura basada en unidades elementales, o celdas, donde un conjunto de dispositivos intentan acceder al medio haciendo uso de una misma función de coordinación. Estas unidades pueden conectarse entre sí mediante una red o sistema de distribución. El elemento que sirve de puente entre la red inalámbrica y la red cableada es el punto de acceso, el cual jugará también un papel crucial en el proceso de control de conexiones. Antes de que un

equipo que se conecta a un punto de acceso pueda transmitir los datos, éste debe realizar una fase de asociación en la que da a conocer su identificador al punto de acceso para que éste informe al resto de la red de que dicho equipo se encuentra bajo su área de cobertura. Es tras esta fase cuando debe realizarse el proceso de control de acceso para ver si realmente el cliente tiene permiso para hacer uso de la red.

Uno de los mecanismos utilizados por las redes 802.11 para intentar proporcionar un cierto nivel de seguridad es el cifrado de los datos que se transmiten entre el cliente y el punto de acceso. Para ello se utiliza el protocolo WEP, el cual está basado en el uso de un secreto compartido, o clave WEP, entre los dos extremos de la comunicación. Debido a la naturaleza de este mecanismo, principalmente basado en el algoritmo de cifrado RC4, en los últimos años se han descubierto varias vías de ataque que permiten a un intruso descifrar la comunicación protegida mediante WEP. Con la finalidad de solucionar dicho problema, se recomienda el uso de claves de longitud no inferior a 128 bits así como su continua actualización con el fin de limitar la cantidad de información cifrada con la misma clave.

2.3.1.2.3 IEEE 802.1X

La especificación IEEE 802.1X es un estándar de control de acceso desarrollado por el IEEE que permite utilizar diferentes mecanismos de autenticación. Su funcionamiento se basa en el concepto de puerto, visto éste como el punto a través del que se puede acceder a un servicio proporcionado por un dispositivo, que en este caso será el punto de acceso. En principio todos los puertos están desautorizados, excepto uno que el punto de acceso utiliza para comunicarse con el cliente. Cuando un nuevo cliente entra en su área de cobertura, le pasa al punto de acceso información de autenticación, dependiente del mecanismo utilizado, que éste reenvía al servidor de autenticación. Cuando éste le contesta, si la respuesta es que el cliente puede hacer uso de la red, autoriza un puerto

para que lo utilice el cliente. La Figura 9 muestra la estructura general de un sistema IEEE 802.1X.

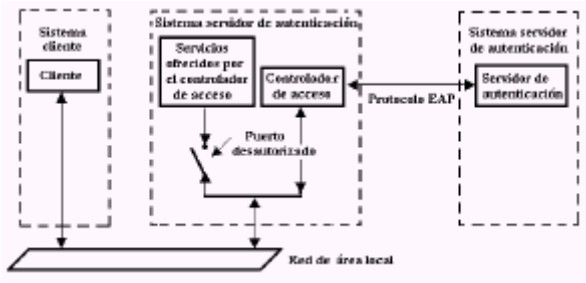


Fig 9. Arquitectura IEEE 802.1X
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

En esta arquitectura, la información de autenticación se encapsula en el protocolo EAP (Extensible Authentication Protocol), un mecanismo genérico de transmisión de datos de autenticación que puede ser materializado en distintos subprotocolos entre los que, por ejemplo, se encuentra EAP-MD5, que basa la autenticación del cliente en el uso de login y password, o EAP-TLS, que se basa en el uso del protocolo TLS y permite autenticación mutua entre los dos extremos. El sistema aquí presentado hará uso de EAP-TLS principalmente por dos motivos: el primero es que que durante la fase de establecimiento de la conexión este protocolo hace uso de certificados X.509 para identificar a las partes, lo cual constituye un mecanismo robusto de autenticación; el segundo es que dicha fase genera una clave compartida por los dos extremos que puede utilizarse para derivar claves para el cifrado de las transmisiones inalámbricas, lo cual es uno de los objetivos de nuestra arquitectura. Finalmente, los paquetes EAP se transmiten mediante el protocolo EAPOL, el cual especifica cómo encapsular los paquetes EAP en una red de área local tanto Ethernet como 802.11.

2.3.1.2.4 *Servidores de autenticación*

Aunque en la especificación 802.1X se habla de los servidores de autenticación en términos genéricos, en la práctica se trata de elementos diseñados según los

criterios del marco AAA (Authentication, Authorization and Accounting). Este marco define los elementos básicos necesarios para autenticar usuarios, manejar peticiones de autorización y realizar la contabilidad del sistema. Un servidor AAA debe ser capaz de recibir peticiones, examinar el contenido de dichas peticiones, determinar qué autorización se está pidiendo, recuperar las políticas que necesite de un repositorio, evaluar la petición y obtener la respuesta a la petición, o bien reenviar la petición a otro servidor AAA. RADIUS es un protocolo encuadrado dentro del marco AAA y utilizado principalmente en entornos donde los clientes son elementos de acceso a la red (como los puntos de acceso). Estos elementos mandan información al servidor cuando un nuevo cliente intenta conectarse, tras lo cual el servidor realiza el proceso de autenticación del usuario y devuelve al elemento de acceso la información de configuración necesaria para que éste trate al cliente de la manera adecuada. Toda la comunicación entre el elemento de acceso y RADIUS se encuentra cifrada mediante un secreto compartido que nunca se transmite por la red. Otro servidor de autenticación AAA es DIAMETER [5], el cual introduce algunas ventajas significativas respecto a RADIUS en materia de gestión de elementos de acceso complejos, si bien se encuentra aún en un estado menos avanzado de definición. La arquitectura presentada en este artículo se basa en el uso de servidores RADIUS dado que satisfacen completamente los requisitos del sistema al tener soporte para el protocolo EAP-TLS

2.3.1.2.5 *E. Autorización en WLAN*

Una de las alternativas para implementar mecanismos de autorización, si no se quiere mantener una base de datos con los permisos de cada usuario, es la utilización de certificados digitales. Un certificado es una estructura que contiene información del usuario en cuanto a identidad o permisos, y que va firmado digitalmente por una entidad de confianza. Dado que los certificados de clave pública X.509 (los más ampliamente extendidos) se utilizan exclusivamente para propósitos de identidad, se decidió incorporar a nuestra arquitectura el uso de certificados SPKI (Simple Public Key Infrastructure), una especificación que

permite plasmar de forma sencilla los privilegios asociados a un usuario individual o a un grupo de usuarios en conjunto. Este tipo de certificados pueden ser utilizados también para representar la pertenencia de un usuario a distintos grupos de privilegios (o roles). La especificación SPKI además define un algoritmo para obtener decisiones de autorización basándose en un conjunto de certificados presentados como pruebas, una solicitud de acceso y una política de seguridad del sistema.

2.3.1.3 Diseño

Una vez analizado un subconjunto los componentes que formarán parte de la arquitectura, es necesario ilustrar cuál ha sido el diseño de la arquitectura de control de acceso desarrollada.

La Figura 10 muestra un entorno típico de aplicación de la arquitectura. En ella se pueden ver varios puntos de acceso y un servidor de autenticación conectados mediante un sistema de distribución, y un conjunto de clientes que cuando entran por primera vez en el área de cobertura de un punto de acceso inician el proceso de conexión. Este proceso consta básicamente de tres fases: autenticación, autorización y distribución de la clave de cifrado WEP. Una vez conectado el cliente, el sistema realizará periódicamente un proceso de renegociación de la clave WEP. Del mismo modo, también gestionará la posibilidad de que el usuario se desplace hacia el área de cobertura de otro punto de acceso, todo ello con el fin de reaprovechar la asociación para que el proceso de conexión a través del nuevo punto de acceso se realice de forma eficiente.

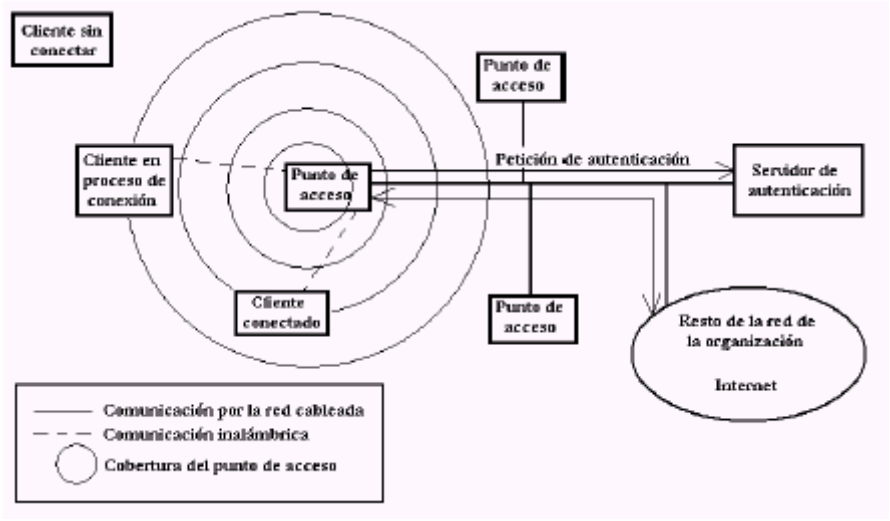


Fig 10. Arquitectura general del sistema
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

La Figura 11 presenta un esquema de las fases del protocolo, las cuales se detallan en los siguientes subapartados.

2.3.1.3.1 Fase de autenticación

La primera fase funciona siguiendo el estándar IEEE 802.1X, es decir, cuando el cliente entra en el área de cobertura del punto de acceso, este le pide su identidad, y el cliente se la proporciona.

Fig 11. Esquema del protocolo
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

Tras esta fase inicial se realiza el proceso de establecimiento de conexión TLS entre los extremos, donde según el estándar tanto el cliente como el servidor de autenticación se autentican mutuamente mediante certificados X.509 y negocian los parámetros de configuración necesarios para establecer el canal de comunicación seguro. En nuestra arquitectura hemos relajado el criterio de la autenticación mutua hasta el punto de poder configurar si el cliente debe también desvelar su identidad, proporcionando por tanto también soporte para escenarios en los que el anonimato sea un requisito. Una vez terminada la negociación, se establece un canal TLS entre el cliente y el servidor de autenticación basado en la posesión por ambas partes de un secreto compartido (Master Secret) que posteriormente se utilizará para derivar la clave WEP.

2.3.1.3.2 *Fase de autorización*

En esta fase, tal y como muestra la figura 12, el cliente indica al servidor de autenticación cual es el tipo de conexión que desea en cuanto al ancho de banda requerido y el tiempo que va a estar conectado, junto con los certificados SPKI que demuestran que dicho usuario está autorizado a realizar el uso de la red que pide. Entonces el servidor evalúa los certificados y comprueba si todo es correcto y si el nivel de privilegios del cliente es el necesario, continuando con el protocolo si todo va bien y desautorizando al cliente a acceder a la red si hay algún problema. De esta forma no es necesario acceder a ninguna base de datos de usuarios para comprobar los permisos de los mismos, sino que sólo se necesita confiar en las entidades emisoras de dichos certificados de autorización.

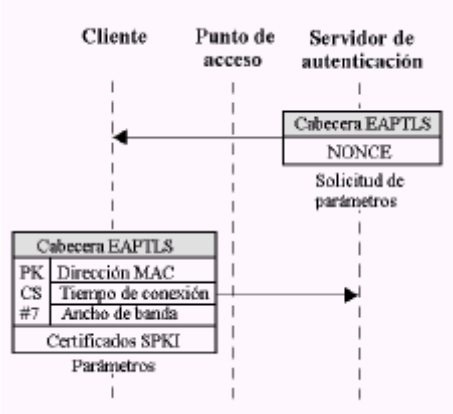


Fig 12. Fase de Autorización

http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

Los parámetros del cliente se mandan en una estructura firmada PKCS#7, de manera que el servidor de autenticación pueda estar seguro de que nadie ha modificado estos parámetros. Además, toda la información relativa a la autorización del cliente, parámetros y certificados, se manda a través del canal TLS establecido anteriormente, de manera que solo pueden haber sido enviados por parte del cliente con el que se ha iniciado el proceso de conexión. Dicha estructura PKCS#7 contiene el certificado del cliente con el que se ha realizado la firma para que el servidor pueda verificar que la firma es correcta. En el mensaje mediante el cual el servidor le pide al cliente sus parámetros de conexión, se incluye un identificador de 4 octetos aleatorio, que posteriormente se utilizará para derivar la clave WEP junto con la dirección MAC del punto de acceso y la clave maestra de la conexión TLS anteriormente establecida.

2.3.1.3.3 *Fase de distribución de clave*

En esta fase del protocolo, representada en la figura 13, únicamente participan el punto de acceso y el servidor de autenticación, y consiste en que éste último le pase al primero un descriptor de la clave WEP que debe utilizar con el cliente, así como el tipo de servicio que el cliente espera que se le ofrezca. Esta clave WEP la habrá generado el servidor como resultado de una función de resumen digital

MD5 aplicada sobre la concatenación de la clave maestra generada por EAP-TLS, la dirección MAC del punto de acceso,. Por su parte, el punto de acceso debe comprobar que en su situación actual puede soportar las necesidades del nuevo cliente, es decir debe comprobar que la suma total del ancho de banda necesitado por todos los usuarios que actualmente hay conectados, junto con el requerido por el nuevo cliente, no sobrepase su capacidad; y que vaya a estar disponible el tiempo que el cliente requiere; informando al servidor de autenticación sobre la decisión que tome.

Tras estas fases, el proceso de conexión ha terminado, y si todo se ha realizado correctamente, el servidor de autenticación notifica al punto de acceso la autorización por su parte a que el cliente haga uso de la red. El punto de acceso traslada entonces al cliente esta decisión para que inicie la comunicación. El cliente, que habrá generado la misma clave WEP que obtuvo el punto de acceso, puede comenzar a hacer uso de la red, con la garantía de que sus mensajes son sólo descifrables por el punto de acceso, dado que la clave WEP generada es distinta para cada usuario.

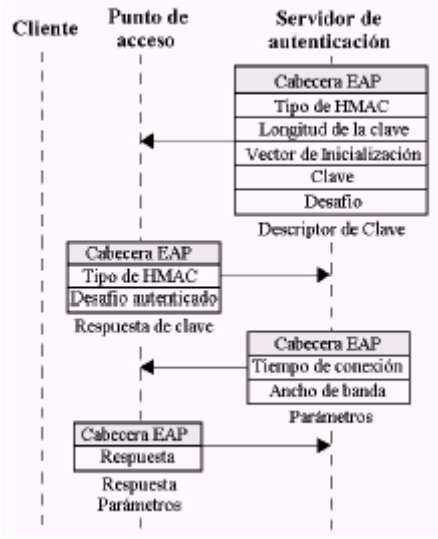


Fig 13. Fase de distribución de claves y parámetros
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

En este punto del diseño hay que dejar una puerta abierta a una probable modificación futura, ya que es posible que al aumentar la potencia de los ordenadores, una clave WEP de hasta 16 octetos (tamaño del resumen MD5) no proporcione suficiente seguridad, por lo que el protocolo dejaría de ser seguro. Por ello, en el caso de necesitar una clave WEP de mayor tamaño, podría utilizarse el método de extensión de longitud de claves mostrado en la Figura 14.

$$WEP_0 = MD5(clave, MAC, nonce)$$
$$WEP_n = WEP_{n-1} \,||\, MD5(clave, MAC, nonce, WEP_{n-1})$$

Figura 14. Obtención de la clave WEP
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

2.3.1.3.4 *Fase de renegociación*

Periódicamente, y dependiendo esta periodicidad del nivel de seguridad que quiera el usuario, es posible renegociar la clave WEP que se está utilizando para cifrar la comunicación entre el cliente y el punto de acceso. Para ello, el cliente inicia un proceso de renegociación de conexión TLS. En esta ocasión, no será necesario que el cliente mande sus parámetros, a no ser que quiera cambiarlos, sino que únicamente se realiza esta fase para indicar al cliente cual es la nueva cadena aleatoria para generar la clave WEP.

De esta manera al terminar el nuevo proceso de conexión, tanto el punto de acceso como el cliente tendrán la nueva clave WEP a utilizar para cifrar sus comunicaciones.

2.3.1.3.5 *Fase de movilidad*

Esta fase se apoya en la anterior, ya que cuando un cliente detecta que está en el área de cobertura de un nuevo punto de acceso, en lugar de iniciar el proceso de

conexión descrito desde el principio, inicia un proceso de renegociación de conexión TLS. Al basarse la nueva conexión en la anterior, la generación del secreto compartido se puede realizar de forma más ligera, y además se evita que el servidor de autenticación tenga que validar de nuevo al usuario. Una consecuencia directa es también que de forma automática se inicia la fase de renegociación de clave WEP, lo cual implica un cambio de la misma para trabajar con el nuevo punto de acceso.

2.3.1.4 Implementación

La implementación del prototipo de este protocolo se ha basado en una serie de aplicaciones y librerías ya existentes a las que se ha añadido el soporte para las nuevas fases.

2.3.1.4.1 HostAP

HostAP 2 es un driver para Linux que permite que un ordenador con una tarjeta inalámbrica funcione como punto de acceso, además de incluir una implementación del estándar IEEE 802.1X.

En cuanto a las modificaciones realizadas sobre este software, se han centrado en añadirle soporte para la fase de generación de claves WEP. Durante el resto del protocolo, este dispositivo únicamente funciona como elemento puente, es decir reenvía todo lo que le llega desde el cliente al servidor de autenticación y viceversa.

2.3.1.4.2 XSupplicant

XSupplicant es una aplicación que pertenece al proyecto Open1X, un intento de obtener una implementación completa y abierta del estándar IEEE 802.1X para Unix, pero que actualmente solo tiene disponible el cliente.

Las modificaciones realizadas sobre XSupplicant se centran básicamente en la fase de autorización, la fase de renegociación de clave y la de movilidad. Una vez que todo el proceso de conexión ha terminado y XSupplicant recibe la autorización de hacer uso de la red, es necesario establecer la clave WEP de la forma ya descrita.

2.3.1.4.3 FreeRADIUS

FreeRADIUS 3 es una implementación abierta para UNIX de RADIUS, que tiene la ventaja de que se ha comprobado su interoperabilidad con XSupplicant. La mayor parte de los cambios realizados se han producido en FreeRADIUS debido a que, ya sea con el cliente o con el punto de acceso, el servidor de autenticación siempre está implicado en alguna fase del protocolo.

2.3.1.4.4 OpenSSL

OpenSSL 4 es una implementación de SSL de código abierto. Esta librería es necesaria para poder instalar tanto FreeRADIUS como XSupplicant, ya que al usar EAP-TLS necesitan de una implementación de TLS que aquí se proporciona. Además, también se ha empleado como librería criptográfica con soporte para PKCS#7 y resúmenes digitales.

2.3.1.5 Trabajo Relacionado

El control de acceso a redes WLAN es un campo de investigación bastante abierto. Encuadrados dentro del marco 802.1X han surgido varios protocolos EAP, además de los comentados EAP-MD5 y EAP-TLS, que ofrecen distintos niveles de seguridad. Por ejemplo, el protocolo LEAP (Lightweight EAP), al igual que nuestra arquitectura, también incluye mecanismos para generar claves únicas de cifrado, si bien tiene grandes limitaciones al estar basado en el modelo EAP-MD5. Otras propuestas son EAP-TTL y PEAP, las cuales son capaces de trabajar con varios tipos distintos de datos de autenticación, si bien no tienen soporte para autorización, renegociación o movilidad. En lo que respecta a arquitecturas completas de control de acceso, y no sólo a protocolos de autenticación EAP, existen otras propuestas como el sistema NoCatAuth, basado en el uso del Web como medio de autenticación frente al punto de acceso, o como la propuesta de Nikander, basada en 802.1X aunque demasiado limitada al filtrado de direcciones MAC como principal medio de control. La principal diferencia de la arquitectura que aquí se presenta respecto a estas otras propuestas está en el uso de la certificación digital y en el tratamiento global a todas las fases involucradas en el proceso de control de conexiones, no sólo la autenticación sino también la gestión de claves de cifrado, la especificación de la calidad de servicio deseada y la gestión de la movilidad.

2.3.1.6 Como asegurar una red inalámbrica [12]

- Autentificación de Punto de Acceso y de los usuarios.
- Encriptación de datos WEP, Wirelles Equivalent Privacy.

[12] Seguridad en Redes Inalámbricas, http://www.zonagratuita.com/servicios/seguridad/wireles.html

2.3.1.7 Autentificación de puntos de acceso y de los usuarios.

Extensible Authentication Protocol (AP) o Extendido de Servicios (Extended Service Set - ESS) son formas de establecer una buena barrera de seguridad para poder identificar redes inalámbricas intrusas en una red o usuarios no permitidos. Utilizar estas opciones es muy recomendable ya que se establecen unos valores de seguridad usando la compatibilidad de nuestros propios productos. Si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro, también se determina si los dispositivos de control pertenecen a nuestra red o al conjunto Extendido de Servicios, el AP revisa si el identificador de ESS es idéntico al nuestro, si no lo son, aún siendo el mismo fabricante y mismo modelo de AP, no podrán participar en la red y no puede recibir ni enviar ningún paquete de datos.

2.3.1.8 Encriptación de datos WEP, Wirelles Equivalent Privacy.

WEP básicamente es la encriptación de nuestros datos o paquetes enviados por nuestra red, esto añade cierto grado de seguridad para evitar intrusos en nuestra red. Muchos usuarios son reacios al uso del WEP ya que se a demostrado que el cifrado puede ser ineficaz en algunas ocasiones, pero también puede ser un gran muro de seguridad si se realiza con ciertas reglas de uso.

2.4 PERÍMETROS DE SEGURIDAD

Las primeras fuentes de problemas se basan en el alcance de las redes mismas, como no es un medio cerrado como pueden ser los cables o la fibra óptica, esta aun más expuesto a ataques no controlados. Por esta misma razón es visible desde todos los lugares del edificio, esto es valido para todos los tipos de redes (WI-FI).

Este problema no es tan fácil de solucionar (si lo que se quiere es limitar el alcance de estas redes) aunque no imposible se puede limitar el alcance apantallando las paredes de los edificios es decir colocando un aislante en las paredes o muros falsos de la empresa, sin embargo esta solución es costosa.
La alternativa a esto es simplemente colocar la red aislada por medio de un firewall. Y hacer que todas las comunicaciones fluyan de forma codificada es decir por medio de una VPN.

2.5 SEGURIDAD DE APLICACIONES

Es un hecho generalmente aceptado que muchos de los problemas de seguridad informática que se sufren en la actualidad tienen que ver con el poco cuidado que se pone en la codificación durante la creación de sistemas, protocolos y aplicaciones. Si se tiene en cuenta que, además, es muy difícil que ese código sea modificado por los propios usuarios, lo que tampoco tiene sentido, se ve claramente el tremendo impacto de no disponer de un código cuidadosamente creado. Así, pues, parece lógico exigir que los creadores del software que de forma legal se usa sigan unas pautas de diseño de sistemas y aplicaciones en las que aparezca como criterio la seguridad informática. En principio, todos los fabricantes de software dicen seguir unas muy concretas, pero todos los siguen apareciendo noticias de nuevas vulnerabilidades.

Por esta razón, hay ya una serie de estándares, con mayor o menor peso en la industria, para tratar de asegurar esas normas mínimas que es razonable exigir. El propio IETF ha estandarizado una interfaz de programación de aplicaciones, GSS-API (Generic Security Services – Application Programming Interface). Se trata esencialmente de una serie de servicios de seguridad subyacentes en todas las comunicaciones de datos en redes IP (RFC 2478, 2479, 2743, 2744 y 2853). En este caso, el usuario típico de esta interfaz es un protocolo de comunicaciones que la utiliza para proteger sus comunicaciones con servicios de seguridad de autenticación, integridad y privacidad. Permiten utilizar tecnologías de clave privada y de clave pública.

CAPITULO III

ANÁLISIS Y DISEÑO DE UN PROTOTIPO BASICO DE RED INALÁMBRICA

3.1 METODOLOGIA

Una descripción sobre la forma de implementar y llevar a cabo un proyecto de seguridad en redes inalámbricas, la forma de diseñarlo, presentarlo, implementarlo, gestionarlo y brindarle un soporte y mantenimiento para disminuir en gran medida el nivel de amenazas presentes tanto afuera como al interior de la empresa o entidad.

Se definen de una manera general todos los aspectos que hay que tener en cuenta dentro de un proyecto de seguridad y se resalta la importancia de entender muy bien el papel que juegan los diferentes protocolos de comunicaciones y las amenazas actuales en seguridad para proteger la información.

El estudio se basa en dos aspectos principales que son:

Seguridad
Ataques

3.1.1 ASPECTOS DE SEGURIDAD

Se hace énfasis en los protocolos de comunicación para la interconexión de redes inalámbricas. Se definen los modelos de seguridad a seguir y algunos aspectos

estratégicos para la consecución de un buen diseño y políticas de seguridad adecuadas de acuerdo a las circunstancias y requerimientos.

3.1.2 ATAQUES

Esta sección trata de los otros protocolos y entornos de seguridad en ambientes como las redes inalámbricas WirelessLAN, Wlan, describen las amenazas, vulnerabilidades y ataques en las redes inalámbricas.

3.2 REQUERIMIENTOS

Para establecer un principio de seguridad para la seguridad de las comunicaciones inalámbricas, los requisitos mínimos son:

- Confidencialidad
- Autenticación
- Integridad
- No repudiación
- Acceso remoto seguro

El acceso remoto de seguridad implica comunicación confidencial de ítems específicos como contraseñas, los diálogos desafío-contestación, claves criptográficas, y llaves de sesión, o vectores de inicialización (IVs), Estos valores deben corroborarse a través de autentificación de servidores los cuales aprueban o desaprueban según las políticas de seguridad especificadas.

Hay otros aspectos de seguridad de comunicaciones de hecho, así como hay también otros tipos de ataques:

- Negación de servicio
- Bloqueando

- Interceptación

La negación de servicios (DOS) es el tipo de ataque más publicitada en el mundo del paquete de comunicaciones. El daño ocurre cuando los hackers inundan los servidores de SYN demandas que finalmente destruyen la funcionalidad. El miedo de interceptación esta siempre prevaleciendo en el mundo de las comunicaciones inalámbricas en algunas redes más que otras.

3.2.1 TAXONOMIA DE LOS SISTEMAS DE COMUNICACIÓN

La multitud de posibles aplicaciones en las comunicaciones inalámbricas demanda que nosotros organizamos aplicaciones e interacciones dentro de las clasificaciones entendidas. Los modelos computados deben ser mapeados en la fábrica de comunicaciones.

Con el mapa en las manos, nosotros podemos empezar a prever que necesitamos para la seguridad, y que ha sido propuesto para direccionar esas necesidades.

Los dispositivos de comunicación son esencialmente computadoras equipadas con CPUs bien de la variedad CISC y RICS o procesadores DSP con programas de memoria y memoria de los datos. Sus capacidades computables pueden alcanzar desde magro a verdaderamente imponentes dependiendo de la necesidad funcional, calidad de diseño, y, por supuesto la necesidad de precios de las tiendas asignadas. Los modelos de taxonomía computable están más allá de las aplicaciones inmediatas a los dispositivos de comunicación

3.2.2 CALIDAD Y SERVICIO (QoS)

Básicamente garantiza la latencia de la red y throughput, está instituyéndose a través de una serie de estructuras de la señalización de la red inalámbrica,

señalando congestión y alarmas los cambios, determinando acciones para su seguridad. Éstos simplemente son unos pocos puntos para tomar en cuenta en el desarrollo de seguridad en redes inalámbricas.

3.3 ANALISIS

3.3.1 CONCEPTOS DE SEGURIDAD

Las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

3.3.1.1 Valor de los datos

Establecer el valor de los datos es relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad. Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

El tema no está restringido únicamente a Internet. Aunque no se esté conectado a Internet, una red está expuesta a distintos tipos de ataques electrónicos, incluidos los virus.

Por esto, y por cualquier otro tipo de consideración que se tenga en mente, es realmente válido pensar que cualquier organización que trabaje con computadoras - y hoy en día más específicamente con redes inalámbricas, debe tener normativas que hacen al buen uso de los recursos de la información**.**

3.3.1.2 Definiciones

- Seguridad: es “calidad de seguro”, y, seguro está definido como “libre de riesgo”.
- Información: es “acción y efecto de informar”.
- Informar: es “dar noticia de una cosa”.
- Redes: es “el conjunto sistemático de caños o de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinado fin”.

Uniendo todas estas definiciones, podemos establecer qué se entiende por Seguridad en redes.

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Al fin de cuentas, los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.

3.3.1.3 Impacto en la organización

En realidad, la implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativa
.

3.3.1.4 Implementación

La implementación de medidas de seguridad, es un proceso técnico-administrativo. Como este proceso debe abarcar toda la organización, sin

exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Hay que tener muy en cuenta la complejidad que suma a la operatoria de la organización la implementación de estas medidas. Será necesario tener en cuenta la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

3.3.2 POLÍTICAS GENERALES DE SEGURIDAD

3.3.2.1 Políticas de seguridad informática (PSI)

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

3.3.2.2 Elementos de una política de seguridad informática

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no-cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

Las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes:

3.3.2.3 Algunos parámetros para establecer políticas de seguridad

- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.
- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

- Un último consejo: no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

3.3.2.4 Proposición de una forma de realizar el análisis para llevar acabo un sistema de seguridad informática

Se comienza realizando una evaluación del factor humano que interviene teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad, de los mecanismos con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos), luego, el medio ambiente en que se desempeña el sistema, las consecuencias que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las amenazas posibles.

Una vez evaluado todo lo anterior, se origina un programa de seguridad**,** que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea. Luego, se pasa al plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino.

Con el propósito de asegurar el cumplimiento de todo lo anterior, se realizan los controles y la vigilancia.

Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a simular eventos que atenten contra la seguridad del sistema. Como el proceso de seguridad es un proceso dinámico, es necesario realizar revisiones al programa de seguridad, al plan de acción y a los procedimientos y normas.

Es claro que el establecimiento de políticas de seguridad es un proceso dinámico sobre el que hay que estar actuando permanentemente, de manera tal que no

queden desactualizados; que, cuando se le descubran debilidades, éstas sean subsanadas y, finalmente, que su práctica por los integrantes de la organización no caiga en desuso.

A continuación, mencionamos algunas recomendaciones para concienciar sobre la seguridad informática:

- Desarrolle ejemplos organizacionales relacionados con fallas de seguridad que capten la atención de sus interlocutores.
- Asocie el punto anterior a las estrategias de la organización y a la imagen que se tiene de la organización en el desarrollo de sus actividades
- Articule las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información. Muestre una valoración costo-beneficio, ante una falla de seguridad.
- Justifique la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización.

La seguridad tiene varios estratos:

- El marco jurídico adecuado.
- Medidas técnico-administrativas, como la existencia de políticas y procedimientos o la creación de funciones, como administración de la seguridad o auditoria de sistemas de información interna.

Ambas funciones han de ser independientes y nunca una misma persona podrá realizar las dos ni existir dependencia jerárquica de una función respecto de otra.

3.3.2.5 Riesgos

La autenticación suele realizarse mediante una contraseña, aún cuando sería más lógico que se pudiera combinar con características biométricas del usuario para impedir la suplantación. Entre éstas pueden estar: la realización de la firma con reconocimiento automático por ordenador, el análisis del fondo de ojo, la huella digital u otras.

Al margen de la seguridad, nos parece que el mayor riesgo, aún teniendo un entorno muy seguro, es que la Informática y la Tecnología de la Información en general no cubran las necesidades de la entidad; o que no estén alineadas con las finalidades de la organización.

Limitándonos a la seguridad propiamente dicha, los riesgos pueden ser múltiples. El primer paso es conocerlos y el segundo es tomar decisiones al respecto; conocerlos y no tomar decisiones no tiene sentido.

Hay daños de menores consecuencias, siendo los errores y omisiones la causa más frecuente normalmente de poco impacto pero frecuencia muy alta y otros, como por ejemplo:

- El acceso indebido a los datos (a veces a través de redes),
- la cesión no autorizada de soportes magnéticos con información crítica
- Los daños por fuego, por agua (del exterior como puede ser una inundación, o por una tubería interior),
- la variación no autorizada de programas, su copia indebida, y tantos otros, persiguiendo el propio beneficio o causar un daño, a veces por venganza.

Otra figura es la del “hacker”, que intenta acceder a los sistemas sobre todo para demostrar (a veces, para demostrarse a sí mismo/a) qué es capaz de hacer, al superar las barreras de protección que se hayan establecido.

3.3.2.6 Niveles de trabajo

- Confidencialidad
- Integridad
- Autenticidad
- No Repudio
- Disponibilidad de los recursos y de la información
- Consistencia
- Control de Acceso
- Auditoria

3.3.2.6.1 Confidencialidad

Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

3.3.2.6.2 Integridad

Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:

- Causadas por errores de hardware y / o software.
- Causadas de forma intencional.
- Causadas de forma accidental

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

3.3.2.6.3 Autenticidad

En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

3.3.2.6.4 No – repudio

Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

3.3.2.6.5 Disponibilidad de los recursos y de la información

De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

3.3.2.6.6 Consistencia

Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

3.3.2.6.7 Control de acceso a los recursos

Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

3.3.2.6.8 Auditoria

Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

En cuanto a los dos últimos puntos resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre “espiar” y “monitorear” a los mismos. La ética es algo que todo buen administrador debe conocer y poseer. Finalmente, todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios. De esta manera, es posible sentar de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos que los usuarios conozcan sus derechos y obligaciones (es decir, las políticas), de tal forma que no se sientan agredidos por los procedimientos organizacionales.

3.3.2.7 Algoritmo

Cuando se piensa establecer una estrategia de seguridad, la pregunta que se realiza, en primera instancia, es: ¿en qué baso mi estrategia?. La respuesta a esta pregunta es bien simple. El algoritmo Productor / Consumidor.

Hay que tener muy en cuenta que, al realizar el análisis de riesgos, se deben identificar todos los recursos cuya seguridad está en riesgo de ser quebrantada.

Los recursos que deben ser considerados al estimar las amenazas a la seguridad son solamente seis:

Hardware:

Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.

Software:

Programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Datos:

Durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, en tránsito sobre medios de comunicación.

Gente:

Usuarios, personas para operar los sistemas.

Documentación:

Sobre programas, hardware, sistemas, procedimientos administrativos locales.

Accesorios:

Papel, formularios, cintas, información grabada.

3.3.2.8 Procedimiento para determinar los buenos passwords

Aunque no lo parezca, la verificación de palabras claves efectivas no es algo frecuente en casi ninguna organización. El procedimiento debe explicar las normas para elegir un password:

Se debe explicitar

- La cantidad de caracteres mínimo que debe tener,
- No tiene que tener relación directa con las características del usuario.
- Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.
- Determinar, si es posible, el seguimiento de las palabras claves (llevar registros de las palabras claves anteriores elegidas por el usuario).

Una vez que el usuario ha elegido su password, se le debe correr un “programa crackeador” para tener idea de cuán segura es, en base al tiempo que tarda en romper la palabra.

3.3.2.9 Procedimientos de verificación de accesos

Debe explicar la forma de realizar las auditorias de los archivos logísticos de ingresos a fin de detectar actividades anómalas. También debe detectar el tiempo entre la auditoria y cómo actuar en caso de detectar desviaciones.

Normalmente, este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar. Escanean archivos de “log” con diferentes fechas tomando en cuenta las reglas que se le han dado. Ante la detección de un desvío, generan reportes informando el mismo.

En el procedimiento debe quedar perfectamente indicado quién es el responsable del mantenimiento de estos programas y cómo se actúa cuando se generan alarmas.

3.3.3 TIPOS DE ATAQUES Y VULNERABILIDADES

En el presente apartado, se describirán los modos de ataques que podrían ocurrir más frecuentemente en las redes de información. Debido a la pérdida de dinero y de tiempo que estos ataques pueden ocasionar, se presentarán también algunas formas de prevención y de respuesta a los mismos.

3.3.3.1 Negación de servicios

Denial of service es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos.

3.3.3.2 Modos de ataque

Algunos ataques de negación de servicio se pueden ejecutar con recursos muy limitados contra un sitio grande y sofisticado. Este tipo de ataque se denomina “ataque asimétrico”. Por ejemplo, un atacante con una vieja PC y un módem puede poner fuera de combate a máquinas rápidas y sofisticadas. Últimamente, esto es común con ataques de los denominados “nukes” en los cuales caen instalaciones grandes, por ejemplo, de clusters Windows NT.

Hay tres tipos de ataques básicos de negación de servicios:

a.- Consumo de recursos escasos, limitados, o no renovables
b.- Destrucción o alteración de información de configuración
c.- Destrucción o alteración física de los componentes de la red

3.3.4 DESTRUCCIÓN O ALTERACIÓN DE LA INFORMACIÓN DE CONFIGURACIÓN

Una computadora incorrectamente configurada puede no funcionar bien o directamente no arrancar. Un hacker puede alterar o destruir la información de configuración de su sistema operativo, evitando de esta forma que usted use su computadora o red.

Veamos algunos ejemplos:

Si un hacker puede cambiar la información de ruteo de sus routers, su red puede ser deshabilitada.

Si un hacker puede modificar la registry en una máquina Windows NT, ciertas funciones pueden ser imposibles de utilizar, o directamente el sistema puede no volver a bootear.

3.3.4 DESTRUCCIÓN O ALTERACIÓN FÍSICA DE LOS COMPONENTES DE LA RED

Es muy importante la seguridad física de la red. Se debe resguardar contra el acceso no autorizado a las computadoras, los routers, los racks de cableado de red, los segmentos del backbone de la red, y cualquier otro componente crítico de la red.

Firewall:

Un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o

entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

Existen varias técnicas de firewall:

- Filtrado de paquetes: Examinar a cada paquete que deje o entre a la red, y aceptarlo o rechazarlo basado en reglas definidas por el usuario. El filtrado de paquetes es efectivo y transparente a los usuarios, pero es difícil de configurar. Adicionalmente, es susceptible a IP spoofing

- Gateway de aplicación: Aplica mecanismos de seguridad a aplicaciones específicas como FTP y Telnet. Es muy efectivo, pero puede provocar degradaciones de performance.

- Gateway al nivel de circuito: Aplica mecanismos de seguridad cuando una conexión TCP es establecida. Una vez establecida los paquetes circulan sin más inspección.

- Proxy server: Intercepta todos los mensajes que entran y dejan la red. Un proxy server oculta en forma efectiva las direcciones reales de red. En la práctica, un firewall utiliza alguna o varias de estas técnicas en conjunto.

- Firewall Router: Filtro de paquetes que filtra el tráfico basándose en la dirección destino y fuente.

3.4 DISEÑO

3.4.1 TOPOLOGÍAS QUE PUEDE ADOPTAR UNA RED WIRELESS [14]

3.4.1.1 Modo Ad-Hoc

Esta topología se caracteriza por que no hay Punto de Acceso (AP), las estaciones se comunican directamente entre si (peer-to-peer), de esta manera el área de cobertura está limitada por el alcance de cada estación individual.

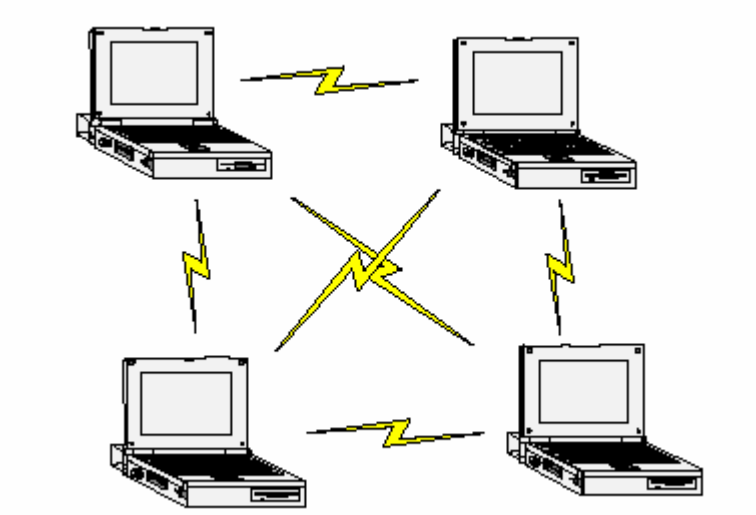


Fig. 16 Topología Modo Ad-Hoc,, http://www.matarowireless.net

3.4.1.2 Modo Infraestructura

Como mínimo se dispone de un Punto de Acceso (AP), las estaciones wireless no se pueden comunicar directamente, todos los datos deben pasar a través del AP. Todas las estaciones deben ser capaces de “ver” al AP.

La mayoría de las redes wireless que podemos encontrar en las empresas utilizan modo infraestructura con uno o más Puntos de Acceso. El AP actúa como un HUB en una LAN, redistribuye los datos hacia todas las estaciones.

---

[14] (In) seguridad en redes 802.11b, http://www.matarowireless.net

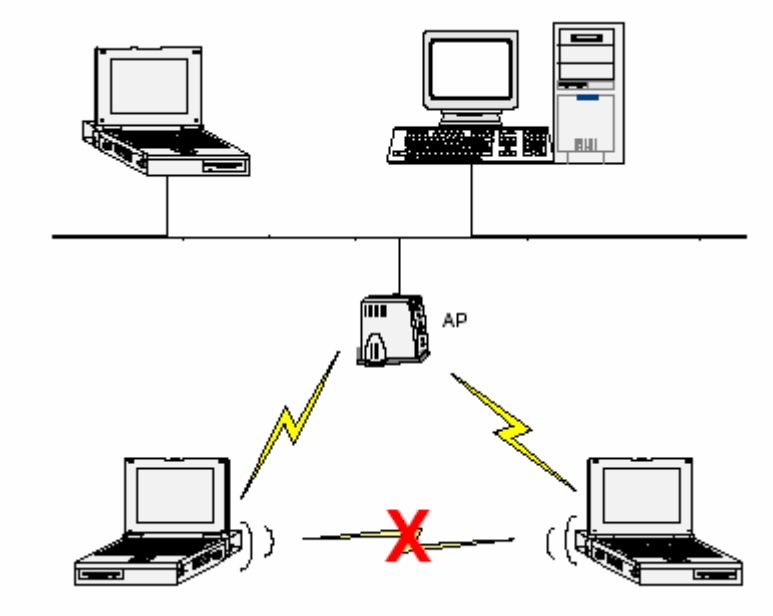


Fig. 17 Topología Modo Infraestructura,, http://www.matarowireless.net

3.4.2 ESSID

Cada red wireless tiene un ESSID (Extended Service Set Identifier), que la identifica. El ESSID consta de cómo máximo 32 caracteres y es *case-sensitive*. Es necesario conocer el ESSID del AP para poder formar parte de la red wireless, es decir, el ESSID configurado en el dispositivo móvil tiene que concordar con el ESSID del AP.

3.4.3 BEACON FRAMES

Los Puntos de Acceso mandan constantemente anuncios de la red, para que los clientes móviles puedan detectar su presencia y conectarse a la red wireless. Estos “anuncios” son conocidos como BEACON FRAMES, si analizamos con el snifer las tramas de una red wireless podremos ver que normalmente el AP manda el ESSID de la red en los BEACON FRAMES, aunque esto se puede

deshabilitar por software en la mayoría de los AP que se comercializan actualmente.

3.4.4 WEP

Las redes Wireless (WLANs) son de por sí más inseguras que las redes con cables, ya que el medio físico utilizado para la transmisión de datos son las ondas electromagnéticas. Para proteger los datos que se envían a través de las WLANs, el estándar 802.11b define el uso del protocolo WEP (Wired Equivalent Privacy). WEP intenta proveer de la seguridad de una red con cables a una red Wireless, encriptando los datos que viajan sobre las ondas radioeléctricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace).

El protocolo WEP está basado en el algoritmo de encriptación RC4, y utiliza claves de 64bits o de 128bits. En realidad son de 40 y 104 bits, ya que los otros 24 bits van en el paquete como Vector de Inicialización (IV). Se utiliza un checksum para prevenir que se inyecten paquetes spoofeados. Más adelante veremos más a fondo como funciona la encriptación WEP.

3.4.5 MEDIDAS DE SEGURIDAD

Las medidas de seguridad más comúnmente utilizadas en las redes wireless son las siguientes:

- ACL’s basadas en MAC’s: sólo permitir la comunicación con el AP a las direcciones MAC que el AP conoce (hay que añadir las MACs de los clientes que pueden tener acceso a la WLAN a mano en el AP).

- No emitir Beacon Frames (o emitirlos sin el ESSID)

- Utilizar WEP para cifrar los datos.

3.4.6 COMO FUNCIONA WEP

Para entender las vulnerabilidades, WEP utiliza el algoritmo RC4 para la encriptación con llaves de 64 bits, aunque existe también la posibilidad de utilizar llaves de 128 bits. Veremos que en realidad son 40 y 104 bits, ya que los otros 24 van en el paquete como Vector de Inicialización (IV).

3.4.6.1 Llaves

La llave de 40 ó 104 bits, se genera a partir de una clave (passphrase) estática de forma automática, aunque existe software que permite introducir esta llave manualmente. La clave o passphrase debe ser conocida por todos los clientes que quieran conectarse a la red wireless que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente.

A partir de la clave o passphrase se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP.

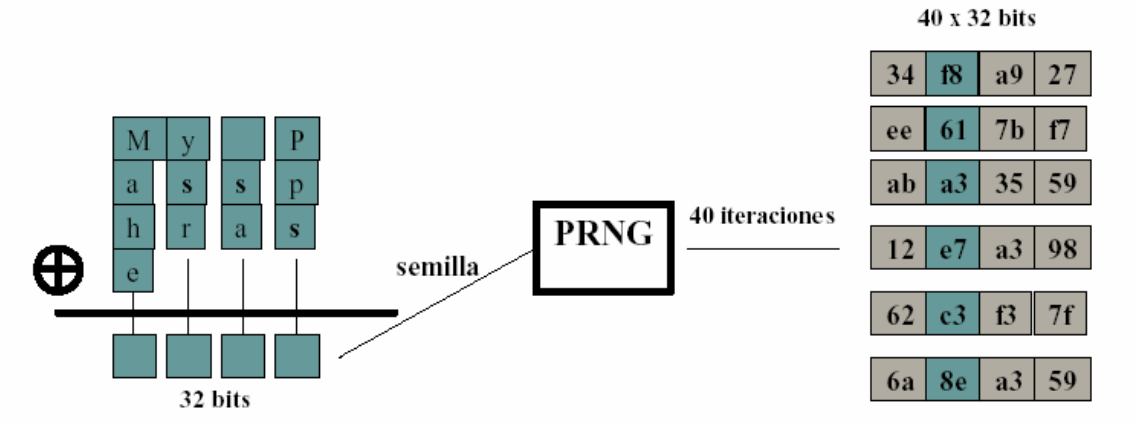


Fig. 18 Proceso para Generar Llaves, http://www.matarowireless.net

Este es el proceso que se realiza para generar las llaves: Se hace una operación XOR con la cadena ASCII (*My Passphrase*) que queda transformada en una

semilla de 32 bits que utilizará el generador de números pseudoaleatorios (PRNG) para generar 40 cadenas de 32 bits cada una. Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits. De estas 4 llaves sólo se utilizará una para realizar la encriptación WEP.

3.4.7 ENCRIPTACIÓN

Para generar una trama encriptada con WEP se sigue el siguiente proceso:

Partimos de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (Header) y contiene unos datos (Payload). El primer paso es calcular el CRC de 32 bits del payload de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único del payload en concreto, que nos servirá para verificar que el payload recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como **valor de chequeo de integridad** (ICV: Integrity Check Value):

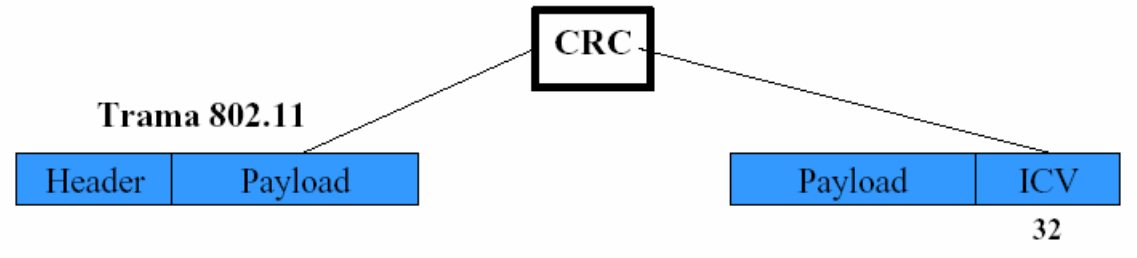


Fig. 19 Valor de Chequeo de Integridad, http://www.matarowireless.net

Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles:

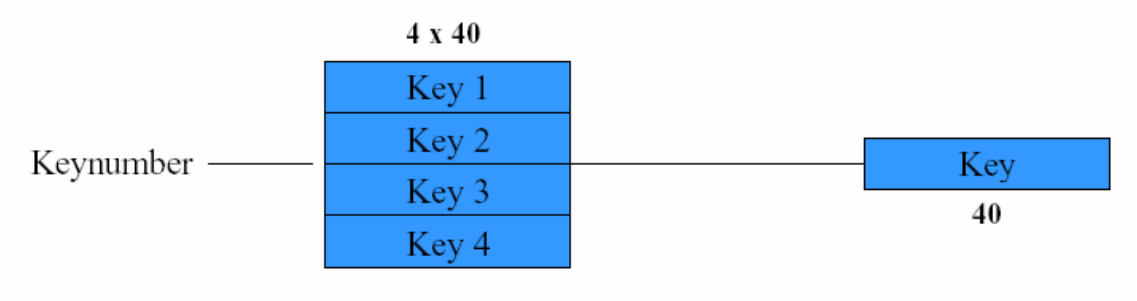


Fig.20 Selección de llave de 40 bits, http://www.matarowireless.net

Y añadimos el **Vector de Inicialización** (IV) de 24 bits al principio de la llave seleccionada:

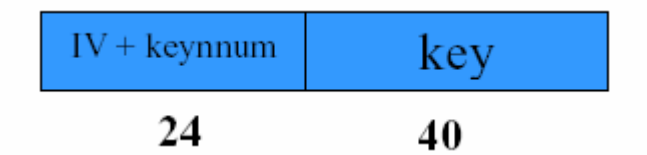


Fig.21 Vector de Inicialización, http://www.matarowireless.net

El IV es simplemente un contador que suele ir cambiando de valor a medida que vamos generando tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para encriptar la trama. En el caso de utilizar encriptación de 128 bits tendríamos 24 bits de IV y 104 de llave.

Llegado a este punto, aplicamos el algoritmo RC4 al conjunto IV + Key y conseguiremos el keystream o flujo de llave. Realizando una operación XOR con este keystream y el conjunto Payload + ICV obtendremos el Payload + ICV cifrado, este proceso puede verse en el siguiente grafico.

Se utiliza el IV y la llave para encriptar el Payload + ICV:

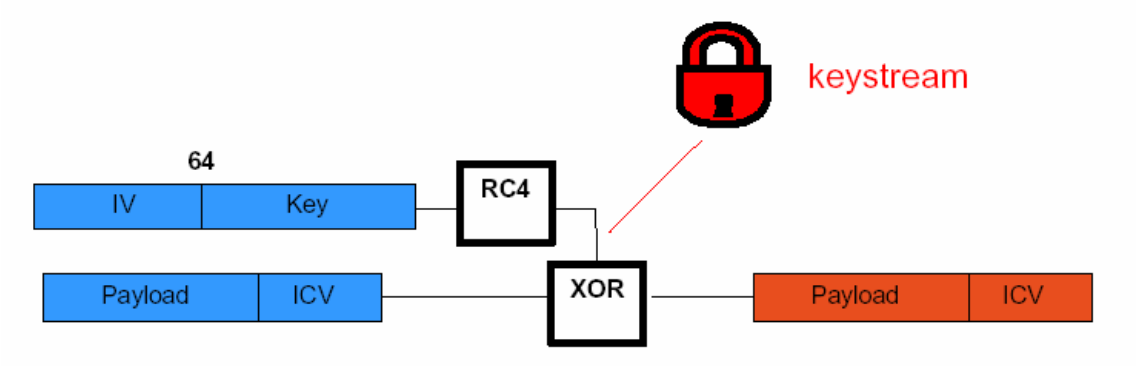


Fig.22 Aplicación del algoritmo RC4 al conjunto IV + Key, http://www.matarowireless.net

Después añadimos la cabecera y el IV+Keynumber sin cifrar. Así queda la trama definitiva lista para ser enviada:

Fig.22 Trama para ser enviada, http://www.matarowireless.net

El proceso de encriptación en conjunto se ve resumido en este esquema:

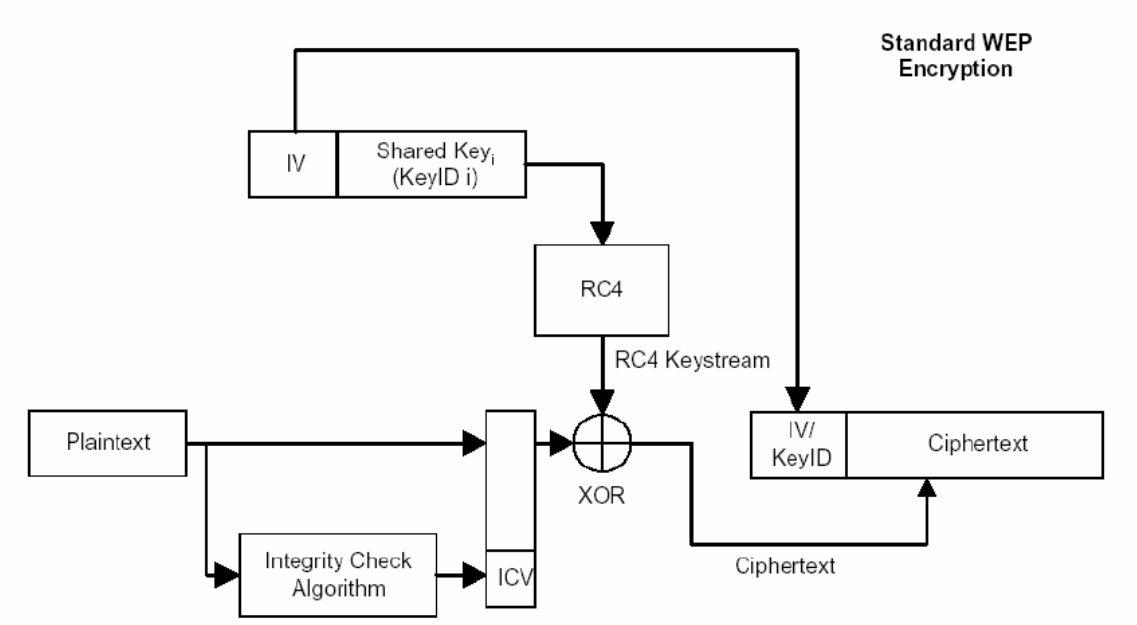


Fig.23 El proceso de encriptación, http://www.matarowireless.net

3.4.8 DESENCRIPTACIÓN

Ahora vamos a ver el proceso que se realiza para desencriptar una trama encriptada con WEP:

Se utiliza el número de llave que aparece en claro en la trama cifrada junto con el IV para seleccionar la llave que se ha utilizado para cifrar la trama:

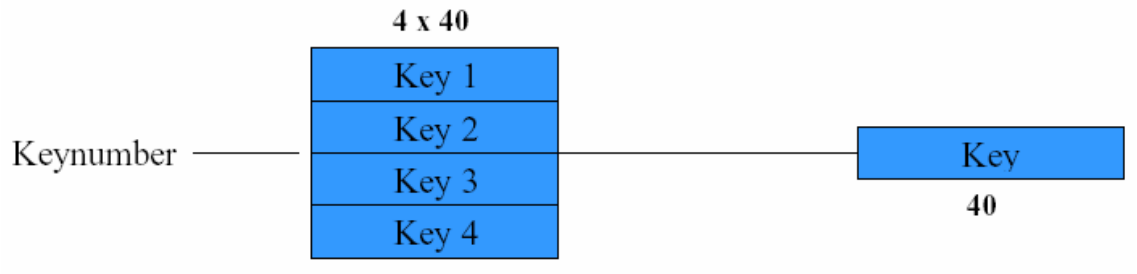


Fig.24 Selección de la llave que se ha utilizado para cifrar la trama, http://www.matarowireless.net

Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64 bits de llave. Aplicando RC4 a esta llave obtenemos el keystream válido para obtener la trama en claro (plaintext) realizando una XOR con el Payload+ICV cifrados y la llave completa como se describe a continuación:

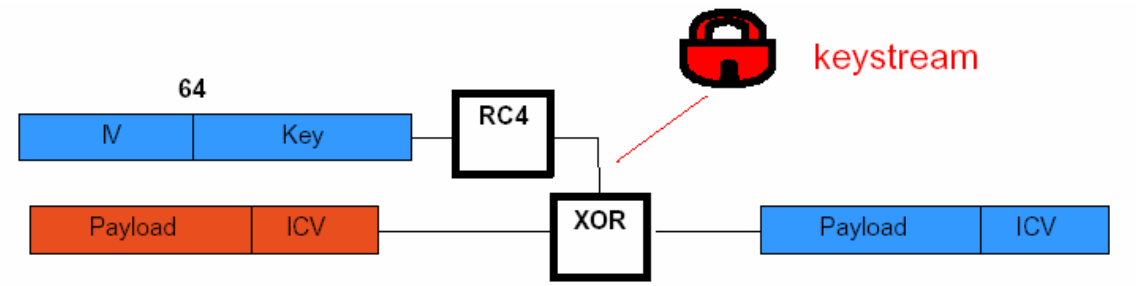


Fig.25 Obtención de la trama en claro (plaintext), http://www.matarowireless.net

Una vez obtenido el plaintext, se vuelve a calcular el ICV del payload obtenido y se compara con el original. El proceso completo puede verse en el siguiente esquema:

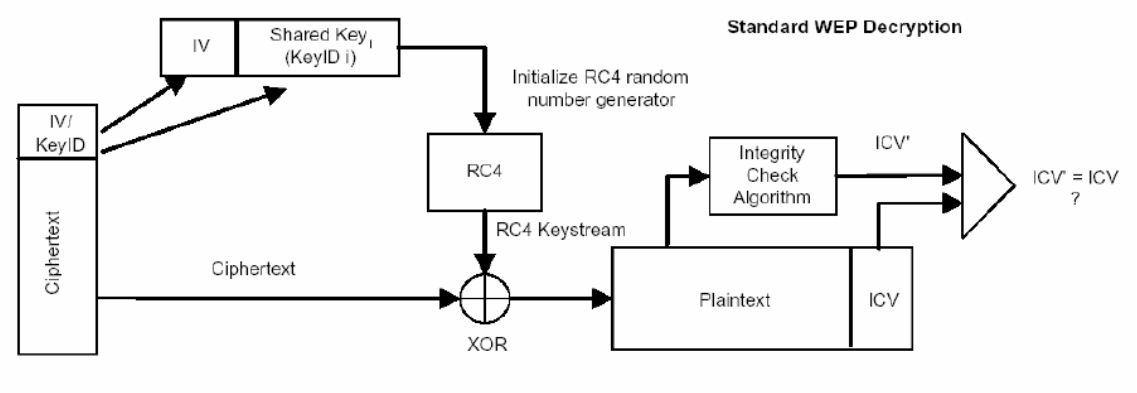


Fig.26 El proceso de Desencriptación, http://www.matarowireless.net

3.4.9 CONEXIÓN A UNA WLAN

El siguiente diagrama de estados muestra los pasos que debe realizar un cliente para asociarse con un AP:

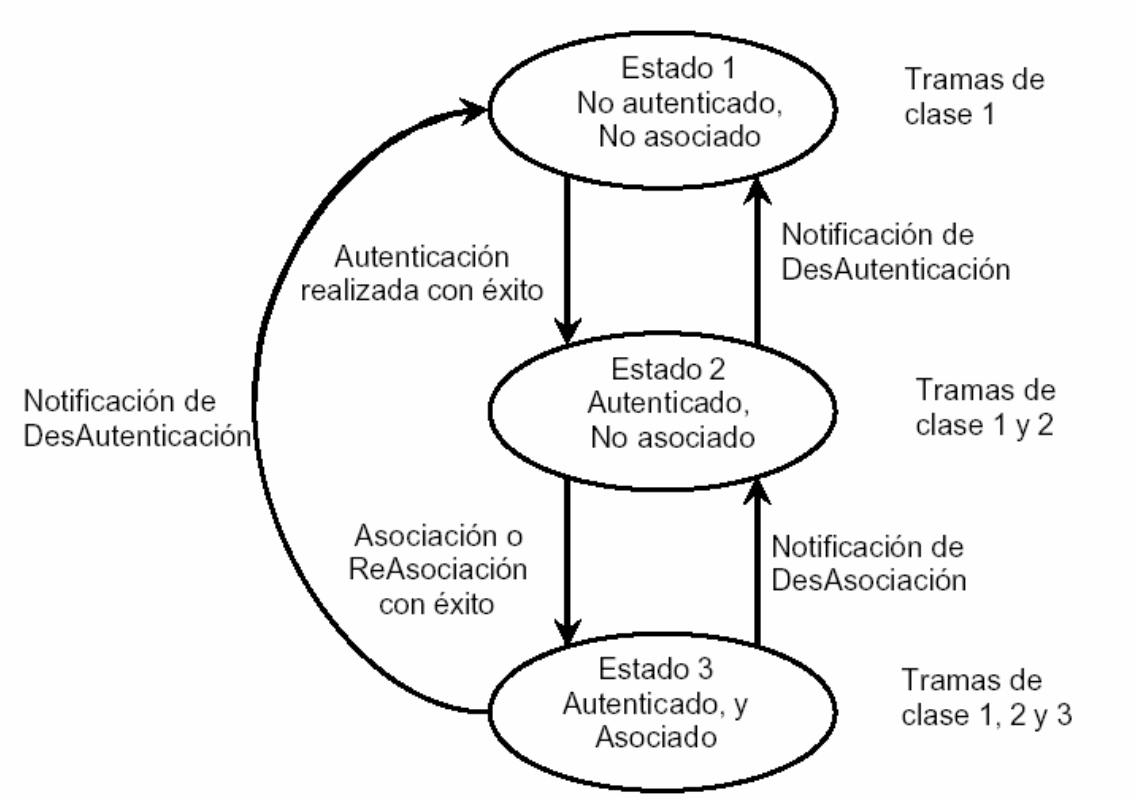


Fig.27 Pasos para asociarse con un AP, http://www.matarowireless.net

El proceso de asociación tiene dos pasos, envueltos en 3 estados:

1. No autenticado y no asociado
2. Autenticado y no asociado
3. Autenticado y asociado

En la transición por los diferentes estados, ambas partes (cliente y AP) intercambian mensajes llamados “management frames”.El proceso que realiza un cliente wireless para encontrar y asociarse con un AP es el siguiente:
Los AP transmiten BEACON FRAMES cada cierto intervalo de tiempo fijo. Para asociarse con un AP y unirse a una red en modo infraestructura, un cliente escucha en busca de BEACON FRAMES para identificar Puntos de Acceso. El cliente también puede enviar una trama “PROVE REQUEST” que contenga un ESSID determinado para ver si le responde un AP que tenga el mismo ESSID.

Después de identificar al AP, el cliente y el AP realizan autenticación mutua intercambiando varios management frames como parte del proceso. Hay varios mecanismos de autenticación posibles que veremos con más detalle un poco más adelante. Después de una autenticación realizada con éxito, el cliente pasa a estar en el segundo estado (autenticado y no asociado). Para llegar al tercer estado (autenticado y asociado) el cliente debe mandar una trama “ASSOCIATION REQUEST” y el AP debe contestar con una trama “ASSOCIATION RESPONSE”, entonces el cliente se convierte en un host más de la red wireless y ya está listo para enviar y recibir datos de la red.

3.4.10 MECANISMOS DE AUTENTICACIÓN

3.4.10.1 Open System Authentication

Es el protocolo de autenticación por defecto para 802.11b. este método autentica a cualquier cliente que pide ser autenticado. Es un proceso de autenticación NULO, las tramas se mandan en texto plano aunque esté activado el cifrado WEP.

3.4.10.2 Shared Key Authentication

Este mecanismo utiliza una clave secreta compartida, que conocen cliente y AP. El siguiente esquema muestra el proceso de autenticación descrito a continuación:

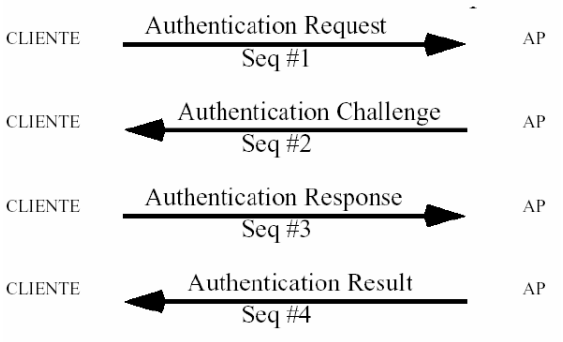


Fig.28 Proceso de Autenticación, http://www.matarowireless.net

La estación que quiere autenticarse (cliente), envía una trama AUTHENTICATION REQUEST indicando que quiere utilizar una “clave compartida”. El destinatario (AP) contesta enviando una trama que contiene 128 octetos de texto (desafío) al cliente. El texto del desafío se genera utilizando el PRNG (generador de números pseudoaleatorios de WEP) con la clave compartida y un vector de inicialización (IV) aleatorio.

Una vez el cliente recibe la trama, copia el contenido del texto de desafío en el payload de una nueva trama, que encripta con WEP utilizando la clave compartida (*passphrase*) y añade un nuevo IV (elegido por el cliente). Una vez construida esta nueva trama encriptada, el cliente la envía al AP, y éste desencripta la trama recibida y comprueba que:

- El ICV (Integrity Check Value) sea valido (CRC de 32 bits).
- El texto de desafío concuerde con el enviado en el primer mensaje.

Si la comprobación es correcta, se produce la autenticación del cliente con el AP y entonces se vuelve a repetir el proceso pero esta vez el primero que manda la trama con el AUTHENTICATION REQUEST es el AP. De esta manera se asegura una autenticación mutua.

En la siguiente figura se muestra el formato de una trama de autenticación. Este formato es utilizado para todos los mensajes de autenticación:

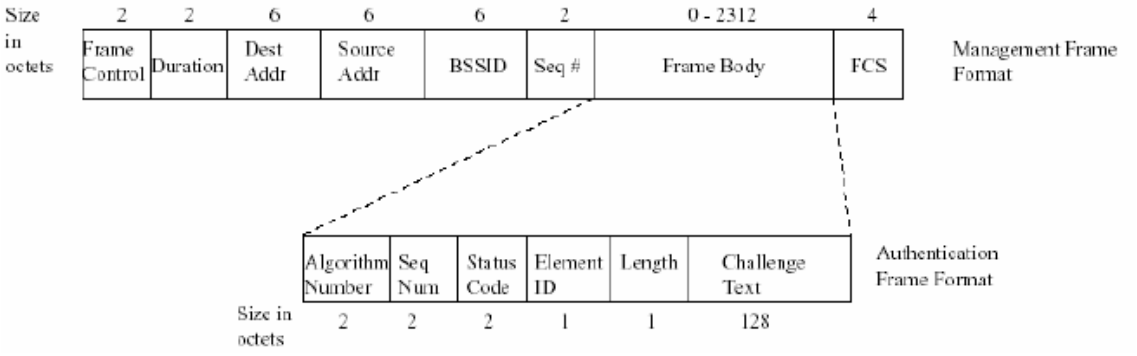


Fig.29 Formato de una trama de Autenticación, http://www.matarowireless.net

Si el campo “Status Code” tiene valor ‘0’ indica que la autenticación ha sido realizada con éxito, si no contiene un código de error.

El campo “Element identifier” indica que la trama contiene el texto de desafío.
El campo “Length” indica la longitud del texto de desafío y está fijado a 128 bits.

El campo “Challenge text” incluye el texto de desafío aleatorio.
La siguiente tabla muestra los posibles valores de los campos y cuando está presente el texto de desafío, según el número de secuencia (Seq #) del mensaje: Sequence Number Status Code Challenge Text Se usa WEP

Sequence Number	Status Code	Challenge Text	Se usa WEP
1	Reservado	No presente	No
2	Status	Presente	No
3	Reservado	Presente	Si
4	Status	No presente	No

Fig.30 Posibles valores de los campos cuando está presente el texto de desafío, http://www.matarowireless.net

3.4.11 VULNERABILIDADES

3.4.11.1 Deficiencias en la encriptación WEP

3.4.11.1.1 Características lineares de CRC32

Como hemos visto anteriormente, el campo ICV (Integrity Check Value) de una trama encriptada con WEP contiene un valor utilizado para verificar la integridad del mensaje. Esto provee de un mecanismo de autenticación de mensajes a WEP, por lo tanto el receptor aceptará el mensaje si el ICV es válido. El ICV se genera simplemente haciendo un CRC (Cyclic Redundancy Check) de 32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas:

- Los CRCs son independientes de la llave utilizada y del IV
- Los CRCs son lineares: $CRC(m \oplus k) = CRC(m) \oplus CRC(k)$

Debido a que los CRCs son lineares, se puede generar un ICV valido ya que el CRC se combina con una operación XOR que también es linear y esto permite hacer el '*biflipping*' como veremos a continuación:

- Un atacante debe interceptar un mensaje m (conocido o no) y modificarlo de forma conocida para producir m':

$$m' = m \oplus \Delta$$

- Como el CRC-32 es linear, puede generar un nuevo ICV' a partir del ICV de m:

$$IC' = IC \oplus h(\Delta)$$

- ICV' será valido para el nuevo cyphertext c'

$$c' = c \oplus \Delta = k \oplus (m \oplus \Delta) = k \oplus m'$$

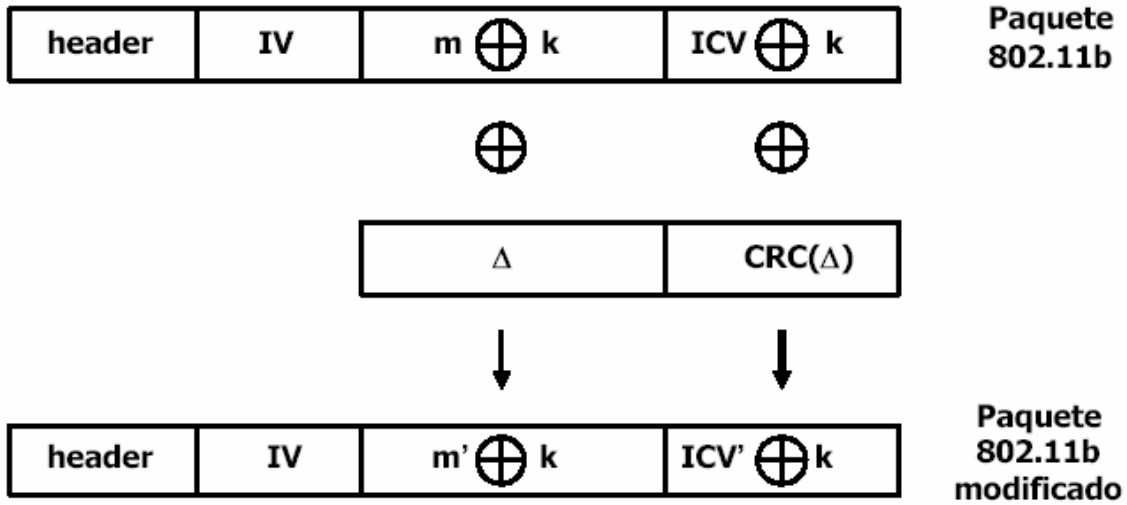


Fig.31 Paquete 802.11b Modificado, http://www.matarowireless.net

3.4.11.1.2 MIC Independiente de la llave

Esta vulnerabilidad en WEP es conocida en inglés como “Lack of keyed MIC”:

Ausencia de mecanismo de chequeo de integridad del mensaje (MIC) dependiente de la llave.

El MIC que utiliza WEP es un simple CRC-32 calculado a partir del payload, por lo tanto no depende de la llave ni del IV. Esta debilidad en la encriptación da lugar a que conocido el plaintext de un solo paquete encriptado con WEP sea posible inyectar paquetes a la red. Esto es posible de la siguiente manera:

- El atacante captura un paquete $\mathbf{c = m \oplus k}$ donde m es conocido (por ejemplo, el atacante envía un e-mail a la victima)
- El atacante recupera el flujo pseudo-aleatorio $\mathbf{k = c \oplus m}$ para el IV concreto del paquete
- Supongamos que el atacante quiere inyectar un mensaje m’, debe realizar lo siguiente:

$$\mathbf{ICV' = CRC32(m')}$$

- El atacante ya puede ensamblar la parte encriptada del paquete:

$$\mathbf{c = (m' | ICV') \oplus k}$$

- El atacante obtiene un paquete válido y listo para ser inyectado a la red:

Fig.32 Paquete a ser enviado, http://www.matarowireless.net

3.4.11.1.3 Tamaño de IV demasiado corto

Otra de las deficiencias del protocolo viene dada por la corta longitud del campo IV en las tramas 802.11b. El vector de inicialización (IV) tiene sólo 24 bits de longitud y aparece en claro (sin encriptar).

Matemáticamente sólo hay 2^24 (16.777.216) posibles valores de IV. Aunque esto pueda parecer mucho, 16 millones de paquetes pueden generarse en pocas horas en una red wireless con tráfico intenso:

Un punto de acceso que constantemente envíe paquetes de 1500 bytes (MTU) a 11Mbps, acabará con todo el espacio de IV disponible después de 1500*8/(11*10^6)*2^24 = ~1800 segundos, o 5 horas. Este tiempo puede ser incluso más pequeño si la MTU es menor que 1500.

La corta longitud del IV, hace que éste se repita frecuentemente y de lugar a la deficiencia del protocolo que veremos a continuación, basada en la posibilidad de realizar ataques estadísticos para recuperar el plaintext gracias a la reutilización del IV.

3.4.11.1.4 Reutilización de IV

Se basa en que WEP no utiliza el algoritmo RC4 “con cuidado”: el Vector de Inicialización se repite frecuentemente. Se pueden hacer ataques estadísticos contra cyphertexts con el mismo IV. Si un IV se repite, se pone en riesgo la confidencialidad Supongamos que *P*, *P’* son dos plaintexts encriptados con el mismo IV.

Supongamos*)* $Z = RC4(key, IV)$; entonces los dos ciphertexts son
$C = P \oplus Z$ y $C' = P' \oplus Z$.

Nótese que $C \oplus C' = (P \oplus Z) \oplus (P' \oplus Z) = (Z \oplus Z) \oplus (P \oplus P') = P \oplus P'$ por lo que la XOR de ambos plaintexts es conocida. Si hay redundancia, se pueden descubrir ambos plaintexts. Si podemos adivinar un plaintext, el otro puede también ser descubierto estadísticamente de forma trivial, así que si RC4 no se usa con cuidado, se vuelve inseguro, WEP no usa RC4 con cuidado. (El Estándar 802.11 especifica que cambiar el IV en cada paquete es opciona)

El IV normalmente es un contador que empieza con valor cero y se va incrementando de uno en uno, por lo tanto:

- Rebotar causa la reutilización de IV's
- Sólo hay 16 millones de IV's posibles, así que después de interceptar suficientes paquetes, seguro que hay IV's repetidos

Un atacante capaz de escuchar el tráfico 802.11 puede descifrar ciphertexts Interceptados incluso sin conocer la clave.

3.4.11.1.5 Deficiencias en el método de autenticación Shared Key

El método de autenticación *Shared Key Autentication* descrito anteriormente se puede explotar fácilmente mediante un ataque pasivo: El atacante captura el segundo y el tercer *management messages* de una autenticación mutua (*Authentication Challenge* y *Authentication Response*). El segundo mensaje contiene el texto de desafío en claro, y el tercer mensaje contiene el desafío encriptado con la clave compartida. Como el atacante conoce el desafío aleatorio (plaintext, P), el desafío encriptado (cyphertext, C), y el IV público, el atacante puede deducir el flujo pseudo-aleatorio (keystream) producido usando WEP utilizando la siguiente ecuación:

$$WEP_{PR}^{K,IV} = C \oplus P$$

El tamaño del keystream será el tamaño de la trama de autenticación, ya que todos los elementos de la trama son conocidos: número de algoritmo, número de secuencia, status code, element id, longitud, y el texto de desafío. Además, todos los elementos excepto el texto de desafío son los mismos para TODAS las *Authentication Responses*.

El atacante tiene por lo tanto todos los elementos para autenticarse con éxito sin conocer la clave secreta compartida K. El atacante envía un *Authentication Request* al AP con el que se quiere asociar. El AP contesta con un texto de desafío en claro. El atacante entonces, coge el texto de desafió aleatorio, R, y el flujo pseudo-aleatorio WEP k,IV PR y genera el cuerpo de una trama *Authentiation Response* válido, realizando una operación XOR con los dos valores. El atacante entonces debe crear un nuevo ICV valido aprovechando la vulnerabilidad de *Características lineares de CRC32*. Una vez creado el nuevo ICV, el atacante acaba de completar la trama de *Authentication Response* y la envía, de esta manera se asocia con el AP y se une a la red.

Con este proceso el atacante sólo esta autenticado, pero todavía no puede utilizar la red. Como el atacante no conoce la clave compartida, para poder utilizar la red debe implementar algún ataque al protocolo WEP.

3.4.12 ATAQUES

3.4.12.1 Ataques al WEP

3.4.12.1.1 Ataque de fuerza bruta

La semilla de 32 bits que utiliza el PRNG es obtenida a partir de la passphrase. La passphrase normalmente contiene caracteres ASCII, por lo cual el bit más alto de cada carácter siempre es cero. El resultado de la operación XOR de estos bits también es cero y esto provoca una reducción de la entropía de la fuente, es

decir, las semillas sólo podrán ir desde 00:00:00:00 hasta 7F:7F:7F:7F en lugar de hasta FF:FF:FF:FF.

El uso del PRNG con esta semilla también reduce la entropía. De la semilla de 32 bits sólo utilizan los bits del 16 al 23. El generador es un generador lineal congruente (LGC: linear congruential generator) de módulo 2^32, esto provoca que los bits mas bajos sean “menos aleatorios” que los altos, es decir, el bit 0 tiene una longitud de ciclo de 2^1, el bit 1 de 2^2, el bit 2 de 2^3, etc. La longitud de ciclo del resultado será por tanto 2^24. Con esta longitud de ciclo sólo las semillas que vayan de 00:00:00:00 a 00:FF:FF:FF producirán llaves únicas.

Como las semillas sólo llegan hasta 7F:7F:7F:7F y la última semilla que tiene en cuenta el PRNG es 00:FF:FF:FF, sólo necesitamos considerar las semillas desde 00:00:00:00 hasta 00:7F:7F:7F por lo que la entropía total queda reducida a 21 bits.

El conocimiento de estos datos nos permite hacer ataques de fuerza bruta contra la encriptación WEP generando llaves de forma secuencial utilizando las semillas desde 00:00:00:00 hasta 00:7F:7F:7F. Utilizando este proceso, un procesador PIII a 500MHZ tardaría aproximadamente 210 días en encontrar la llave, aunque se puede usar computación en paralelo para obtener la llave en un tiempo más razonable.

También existe la posibilidad de utilizar un diccionario para generar sólo las semillas de las palabras (o frases) que aparezcan en el diccionario, con lo que si la passphrase utilizada está en el diccionario conseguiríamos reducir sustancialmente el tiempo necesario para encontrarla.

3.4.12.1.2 Ataque Inductivo Arbaugh

Se basa en explotar la vulnerabilidad de MIC independiente de la llave aprovechando también la redundancia de información producida por el CRC.

Para realizar el ataque hay que conocer parte del plaintext que viaja encriptado en una trama, que podemos obtener por ejemplo identificando mensajes "*DHCPDISCOVER*" de los que conocemos que la cabecera IP tendrá como origen 0.0.0.0 y como destino 255.255.255.255 y tienen longitud fija. Una vez identificada la trama con el mensaje "*DHCPDISCOVER*" realizamos una XOR del plaintext conocido con el cyphertext que hemos recibido, obteniendo así n (en este caso 24) bytes del keystream para el IV concreto del paquete.

Una vez tengamos estos 24 bytes conocidos del keystream hay que generar un paquete de tamaño n-3, es decir 24-3 = 21 bytes de longitud. Este paquete debe ser algo de lo que podamos esperar una respuesta, por ejemplo un ping o un ARP Request.

Calculamos el ICV del paquete generado y añadimos sólo los primeros 3 bytes del ICV que hemos calculado. Realizamos una XOR con el resto del keystream añadiendo el último byte del ICV en el byte n+1 (al final del paquete) tratando de adivinar el siguiente byte del keystream tal y como se muestra en la figura:

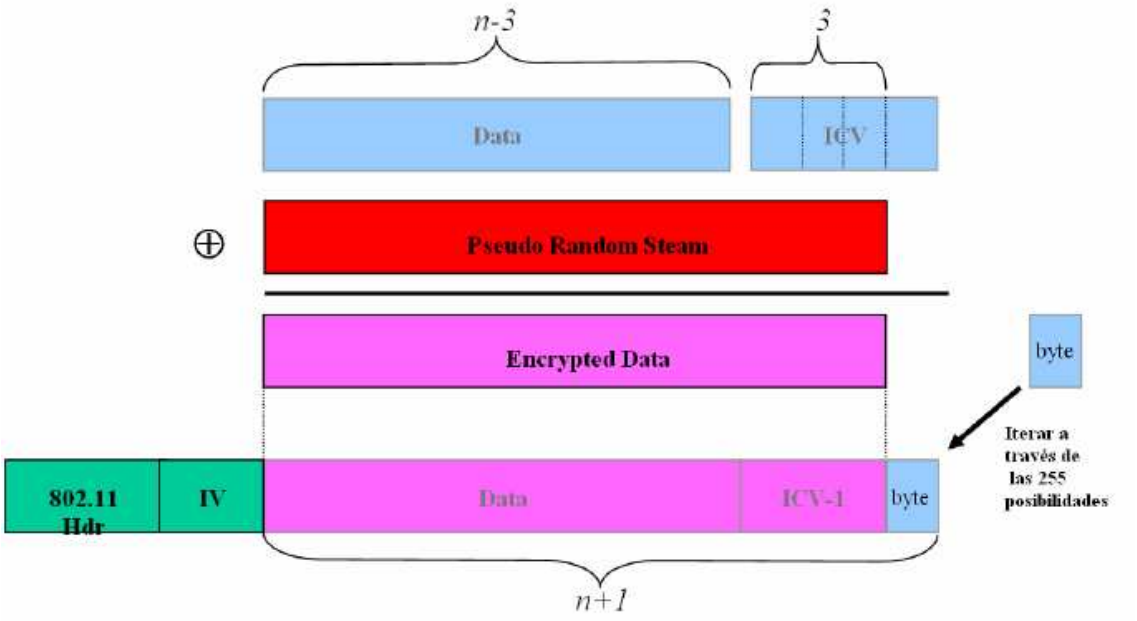


Fig.33 Ataque Inductivo Arbaugh, http://www.matarowireless.net

Una vez generado el paquete completo lo enviamos y esperamos una respuesta (echo reply, ARP reply…), si no hay respuesta tendremos que ir probando las 255 posibilidades restantes modificando el último byte (n+1). Si hay respuesta podemos afirmar que el byte n+1 era el último byte del ICV, así que tenemos un plaintext que concuerda con el cyphertext y que a su vez nos da el byte n+1 del keystream que es lo que nos interesa. Realizando este proceso repetidas veces obtendremos el keystream completo.

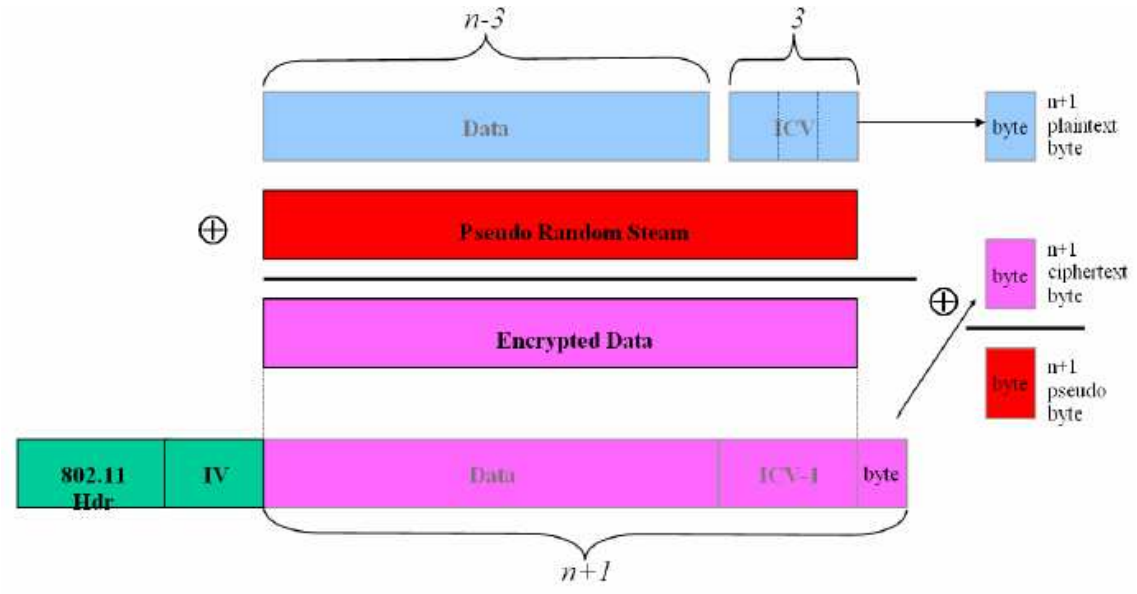


Fig.34 Ataque Inductivo Arbaugh, http://www.matarowireless.net

Asumiendo que un atacante puede realizar aproximadamente 100 pruebas por segundo, tardaría una media de 36 minutos en encontrar un keystream completo de 1500 bytes valido para un IV determinado.

Una vez tenemos un keystream entero, los 224 – 1 restantes son fáciles de obtener: El atacante tiene que volver a generar un paquete del cual se le devuelva una respuesta, (lo mejor es enviar broadcast pings, así recibimos múltiples respuestas por cada paquete que enviamos). El atacante conoce el plaintext de la respuesta y el que responde cada vez enviará el paquete con un IV diferente, así es posible construir una tabla de keystreams completos para cada IV que el atacante puede utilizar para descifrar el tráfico encriptado con WEP en tiempo real.

El atacante necesita almacenar 1500 bytes de keystream por cada IV, por lo que la tabla ocuparía 224x1500 = 24GB y tardaría una media de 30 horas en construir la tabla. Si el ataque se realiza en paralelo 4 hosts atacantes tardarían 7,5 horas y 8 hosts atacantes 3.75 horas.

Cuando el atacante recibe un paquete mira en la tabla a que keystream corresponde el IV recibido y hace una XOR del keystream con el cyphertext del paquete para obtener el plaintext.

3.4.12.1.3 Debilidades en el algoritmo key Scheduling de RC4

La demostración teórica de la vulnerabilidad más devastadora de las existentes hasta ahora en la encriptación WEP.

Demostraron que usando sólo la primera palabra de un keystream, podían obtener información de la clave secreta compartida. Se buscan IVs que causen que no haya información de la llave en el keystream. Los autores llamaron a esta condición "*resolved condition*" o condición resuelta. Cada uno de estos paquetes resueltos sólo tiene ausencia de información de un byte de la llave, y este byte debe ser adivinado correctamente para que el siguiente paquete pueda ofrecer información del siguiente byte de la llave. Para realizar el ataque más rápidamente sólo se buscan los IVs débiles que cumplen esta condición. Hay una posibilidad del 5% de adivinar el byte de la llave correctamente cuando encontramos un paquete resuelto (con un IV débil). Pero como hay gran cantidad de paquetes resueltos viajando por la red, las posibilidades son aún mayores.

Adam Stubblefield, un trabajador de AT&T Labs, fue la primera persona que implementó este ataque con éxito. Añadió que en el tráfico IP se añade una cabecera 802.2 extra, y esto hace que el ataque sea más sencillo de implementar, ya que cada paquete IP tiene el mismo primer byte de plaintext. Para realizar el ataque con éxito, durante la primera fase del ataque, los primeros pocos bytes

deben ser adivinados correctamente. Stubblefield utilizo dos métodos para conseguirlo.

El primer método es apuntar los paquetes resueltos para disminuir las posibles combinaciones de bytes de la llave. Se puede comprobar si las llaves son correctas mediante el ICV de los paquetes desencriptados.
El segundo método se centra en la manera en que se distribuyen las llaves WEP. Se supone que el usuario introducirá una clave fácil de recordar en el software de configuración. Una llave fácil de recordar debe contener caracteres ASCII. Comprobando si los bytes de la llave concuerdan con caracteres ASCII cómo letras o símbolos etc. Las posibilidades de adivinar la llave correcta aumentan.

Cuando se han recolectado suficientes IVs débiles para un valor concreto de un byte de la llave, el análisis estadístico muestra una tendencia hacia un valor en particular para ese byte de la llave. Se le da una puntuación a cada una de las 256 posibilidades según la probabilidad de ser el valor correcto.

La llave se intenta adivinar a partir de los valores con mayor puntuación en el análisis estadístico (Hay un 95% de posibilidades de que un IV no revele información sobre un byte de la llave).Los IV’s débiles no están distribuidos de forma lineal a través del espacio de IV’s.

El número de paquetes que necesitamos recolectar antes de descubrir un byte de la llave varía en función de en que valor se encuentre el contador de IV’s de las tarjetas que estemos monitorizando. Hay 9.000 IV's débiles en los 16 millones de IV's posibles.

¿Cuántos paquetes encriptados necesitamos recolectar para crackear la llave WEP?

- La mayoría de las llaves pueden ser adivinadas después de encontrar aproximadamente 2000 paquetes resueltos.

- Algunas llaves requieren que capturemos incluso más de 4000 paquetes resueltos.

Podremos adivinar la llave después de recolectar de 5 a 10 millones de paquetes encriptados.

3.4.12.1.4 Ataques a redes Wireless

Vista la manera romper la encriptación WEP ya no debería ser un problema para nosotros, por eso en la implementación de los ataques que vamos a ver a continuación no vamos a hablar de WEP ya que si la WLAN que estamos "auditando" tiene encriptación WEP ya disponemos de las herramientas necesarias para obtener la clave y por tanto, podremos realizar los distintos ataques tanto si existe encriptación WEP como si no.

3.4.12.1.5 Romper ACL's basados en MAC

Una de las medidas más comunes que se utilizan para asegurar una red wireless es restringir las máquinas que podrán comunicarse con el Punto de Acceso haciendo filtrado por dirección MAC en éste. Para esto se suele crear una tabla en el punto de acceso que contiene todas las MACs de los clientes que están autorizados para conectar. Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente envía, y hacernos pasar por uno de los equipos que si que tienen acceso a la red.

Para llevar a cabo el ataque basta con utilizar el snifer durante un momento el tráfico y fijarnos en la MAC de cualquiera de los clientes, sólo hace falta que nos pongamos su misma MAC y ya habremos saltado la restricción.

3.4.12.1.6 Ataque de Denegación de Servicio (DoS)

Para realizar este ataque basta con esnifar durante un momento la red y ver cual es la dirección MAC del Punto de Acceso. Una vez conocemos su MAC, nos la ponemos y actuamos como si fuéramos nosotros mismos el AP. Lo único que tenemos que hacer para denegarle el servicio a un cliente es mandarle continuamente notificaciones (*management frames*) de desasociación o desautenticación. Si en lugar de a un solo cliente queremos denegar el servicio a todos los clientes de la WLAN, mandamos estas tramas a la dirección MAC de broadcast.

3.4.12.1.7 Descubrir ESSID ocultados

Como hemos comentado anteriormente, para que un cliente y un AP se puedan comunicar, ambos deben tener configurado el mismo ESSID, es decir, deben pertenecer a la misma red wireless.

Una medida de seguridad bastante común es “ocultar” el ESSID, es decir, hacer que el AP no mande BEACON FRAMES, o en su defecto no incluya el ESSID en éstos. En este caso, para descubrir el ESSID deberíamos utilizar el snifer y esperar a que un cliente se conectara, y veríamos el ESSID en la trama PROVE REQUEST del cliente (en el caso de que no se manden BEACON FRAMES), o en la trama PROVE RESPONSE del AP.

Pero también podemos “provocar” la desconexión de un cliente, utilizando el mismo método que en el ataque DoS, pero mandando sólo una trama de desasociación o de desautenticación en lugar de mandarlas repetidamente, es decir, nos ponemos la dirección física del AP y mandamos una trama DEAUTH o DISASSOC a la dirección MAC del cliente (o a la de broadcast), entonces el cliente intentará volver a asociarse o autenticarse, con lo que podremos ver el ESSID en los *management frames*.

3.4.12.1.8 Ataque Man in the middle

El ataque de *Man in the middle*, también conocido como *Monkey in the middle* consiste en convencer al cliente (la victima) de que el host que hay en el medio (el atacante) es el AP, y hacer lo contrario con el AP, es decir, hacerle creer al AP que el atacante es el cliente.

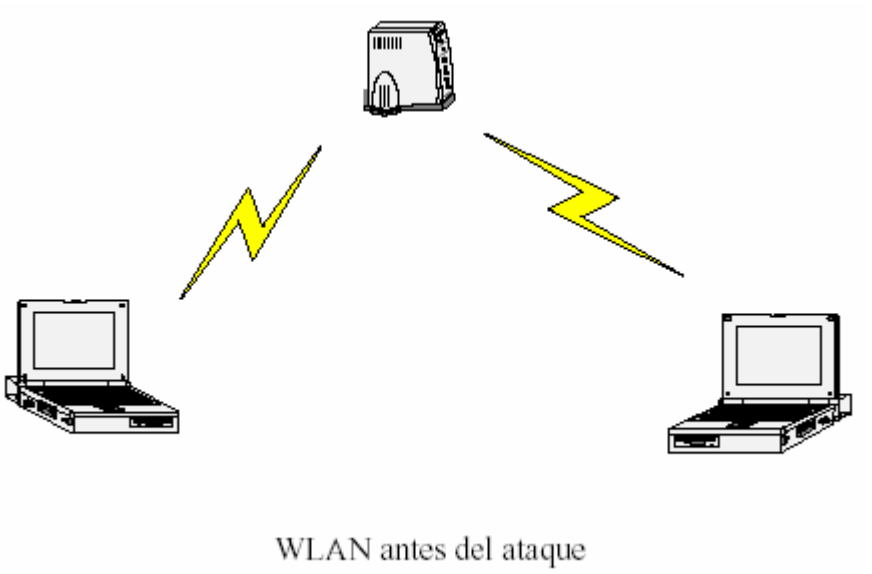


Fig.35 WLAN antes del Ataque, http://www.matarowireless.net

Para realizar este ataque, primero debemos utilizar el snifer para obtener:

- El ESSID de la red (si esta ocultado, usaremos el método anterior)
- La dirección MAC del AP
- La dirección MAC de la victima

Una vez conocemos estos datos, utilizamos el mismo método que en el ataque DoS, para desautenticar a la victima del AP real, es decir, el atacante spoofea su MAC haciéndose pasar por el AP y manda tramas DEAUTH a la victima. La tarjeta wi-fi de la victima empezará entonces a escanear canales en busca de un AP para poderse autenticar, y ahí es donde entra en juego el atacante. El

atacante hace creer a la victima que él es el AP real, utilizando la misma MAC y el mismo ESSID que el AP al que la victima estaba autenticada anteriormente, pero operando por un canal distinto. Para realizar esto la tarjeta wi-fi del atacante debe estar en modo master**.**

Por otra parte, el atacante debe asociarse con el AP real, utilizando la dirección MAC de la victima. De esta manera hemos conseguido insertar al atacante entre la victima y el AP, veamos como quedaría la WLAN después de realizar el ataque.

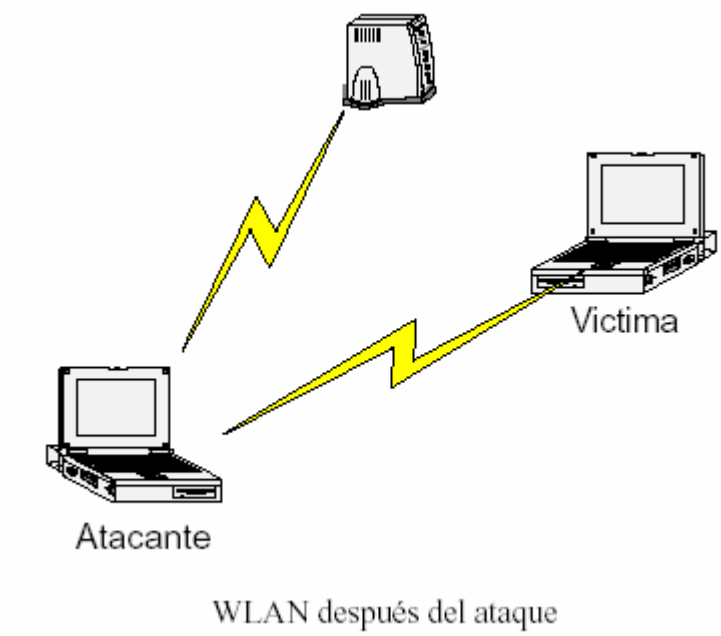


Fig.36 WLAN después del Ataque, http://www.matarowireless.net

De esta manera todos los datos que viajan entre la victima y el AP pasan a través del atacante. Como el ataque ha sido realizado a nivel de enlace (nivel 2), el atacante puede ver y capturar e incluso modificar las tramas en los niveles superiores del modelo OSI. Es muy fácil implementar este tipo de ataques utilizando el driver air-jack con la herramienta monkey-jack.

Hay que tener en cuenta que muchas soluciones de seguridad están pensadas asumiendo que las capas 1 y 2 son seguras, esto como hemos visto es incierto para las redes wireless y por tanto el uso de según que tipo de solución podría no ser adecuado para estas redes.

3.4.12.1.9 Ataque ARP Poisoning

El *ARP cache poisoning* es un ataque que sólo se puede llevar a cabo cuando el atacante está conectado a la misma LAN lógica que las victimas, limitando su efectividad a redes conectadas con switches, hubs y bridges, pero no routers. La mayoría de los Puntos de Acceso 802.11b actúan como bridges transparentes de capa 2, lo que permite que los paquetes ARP pasen de la red wireless hacia la LAN donde está conectado el AP y viceversa. Esto permite que se ejecuten ataques de *ARP cache poisoning* contra sistemas que están situados detrás del Punto de Acceso, como por ejemplo servidores conectados a un switch en una LAN a los que se pueda acceder a través de la WLAN.

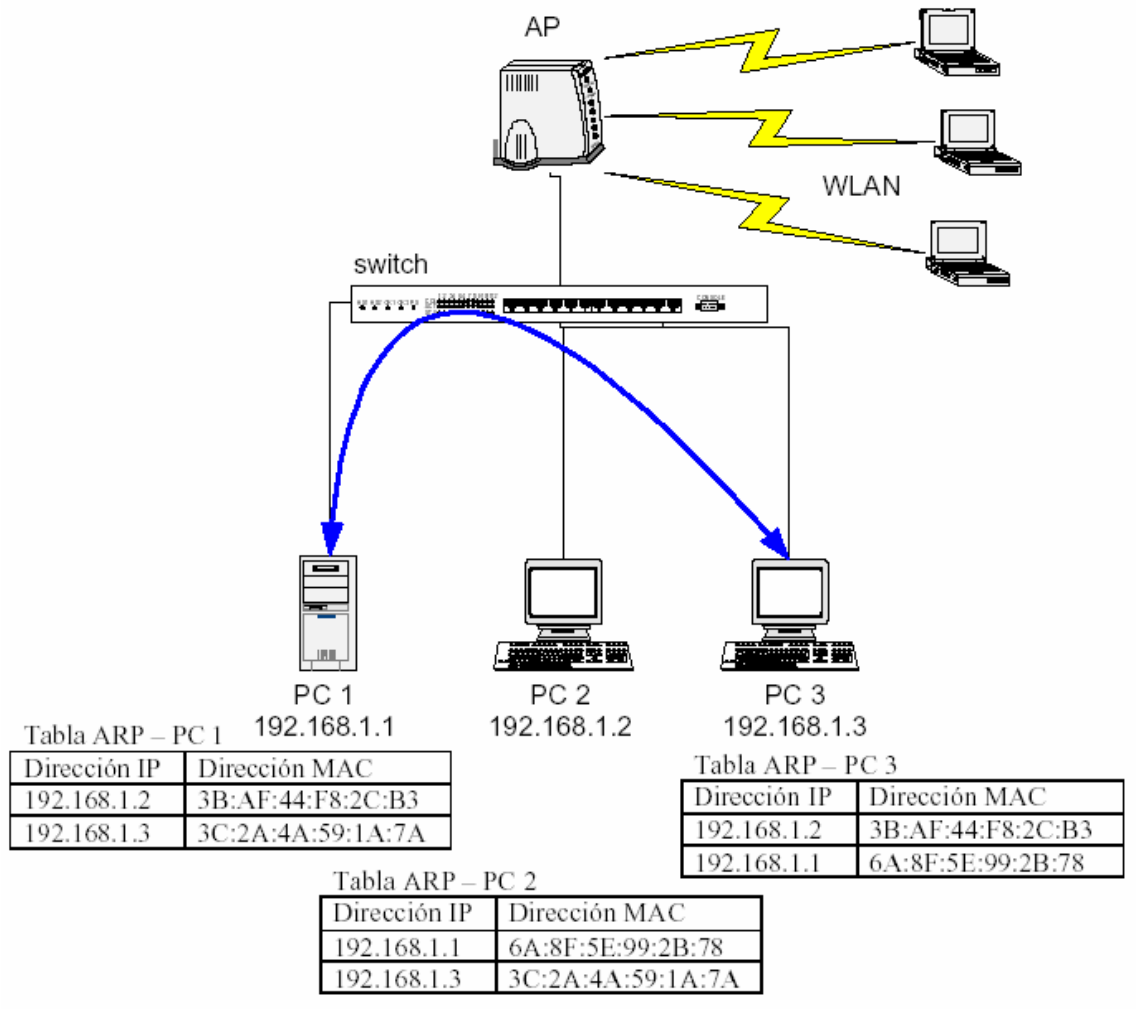


Fig.37 Comunicación sin Ataque, http://www.matarowireless.net

El servidor PC 1 se comunica con PC 3 a través del switch, si un atacante desde la WLAN envenena la tabla de ARP's de PC 1 y de PC 3 podrá realizar un ataque del tipo *Man in the Middle* situándose entre los dos hosts de la red con cables.

Así es como se efectuaría la comunicación después del ataque:

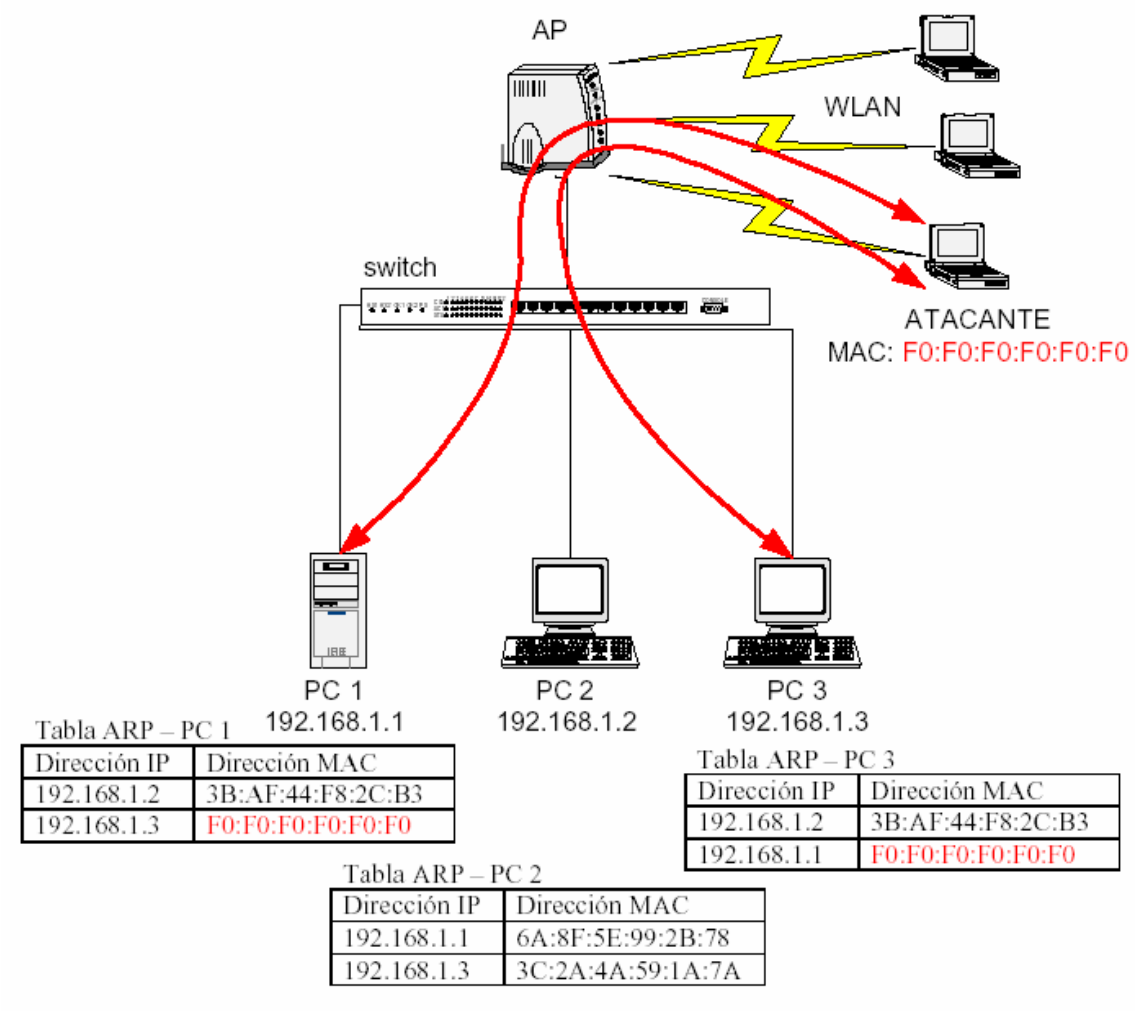


Fig.36 Comunicación después Ataque, http://www.matarowireless.net

El atacante manda paquetes *ARP REPLY* a PC 2 diciendo que la dirección IP de PC 1 la tiene la MAC del atacante, de esta manera consigue “envenenar” la caché de ARP’s de PC 2. Luego realiza la misma operación atacando a PC 1 y haciéndole creer que la dirección IP de PC 2 la tiene también su propia MAC.
Como ARP es un protocolo *stateless*, PC 1 y PC 2 actualizan su caché de acuerdo a la información que el atacante ha inyectado a la red.

Como el switch y el AP forman parte del mismo dominio de broadcast, los paquetes ARP pasan de la red wireless a la red con cables sin ningún problema.

3.4.13 IFERENCIAS ENTRE LAS TECNOLOGÍAS BLUETOOTH Y WIFI (802.11B) [15]

3.4.13.1 Diferencias entre las tecnologías Bluetooth y 802.11b

El Bluetooth y el 802.11b son tecnologías casi totalmente complementarias. Las soluciones Bluetooth están diseñadas para redes personales con un énfasis en movilidad y economía.

Estas soluciones permiten conectar todos sus aparatos Bluetooth: computadoras portátiles, dispositivos de mano, teléfonos celulares y otros más. Además, usted tendrá acceso parcial al LAN y a la WAN, a través de un punto de acceso o conexión de marcado.

Por otro lado, las redes 802.11b están diseñadas para extender o reemplazar a las redes convencionales de cables, usando potencias de radio más altas en canales fijos de mayor ancho de banda, para poder ofrecer el rendimiento necesario para soportar una gama completa de servicios de LAN e Internet.

3.4.13.2 Tecnologías Bluetooth y 802.11b

Hoy en día si pueden coexistir las dos tecnologías con ciertos límites. Aunque el potencial de interferencia es bastante bajo, usted necesita saber que existe la posibilidad de que las dos tecnologías interfieran entre sí, pero solamente cuando estén transmitiendo simultáneamente en localidades muy cercanas.

Si la interferencia ocurre, es probable que sea debido a una interrupción de la señal del 802.11b; es posible que haya pérdida de datos, pero no habrá daños físicos a ninguno de los sistemas. Aunque es muy probable que los usuarios no

---

[15] Diferencias principales entre WiFi y Bluetoth, http://www.paradigma.cl/ordenadorbt/diferencias/diferencias.html

noten este tipo de interferencia, en los casos en los que sea evidente, es suficiente apartar los aparatos para resolver el problema. No obstante, hay ocasiones en las que será necesario cesar la operación de uno de los dos aparatos.

3.4.13.3 Interferencia entre el Bluetooth y el 802.11b?

La interferencia no se nota en muchos de los casos. Si llegara a ocurrir, los usuarios de ambas tecnologías tendrán que operar manualmente sus dispositivos para eliminar la interferencia en alguna de las siguientes dos maneras: la primera, separando físicamente a los aparatos; o, la segunda, cesando la operación de uno de los dos radios.

Cahners In-Stat Group declara que cuando los radios están a más de dos metros de distancia, generalmente no hay ninguna degradación perceptible en ninguno de los dos aparatos; de dos metros a medio metro de distancia, se presentará una ligera degradación; y, cuando los aparatos se encuentran aproximados o colocados muy de cerca, la degradación podría ser bastante notoria.

El SIG del Bluetooth y el IEEE están trabajando en el desarrollo de tecnología para reducir - y sucesivamente eliminar - la interferencia entre estos sistemas. No hay razón para retardar la implementación de ninguna de las dos tecnologías por miedo a problemas de coexistencia.

El Bluetooth y el 802.11b pueden trabajar - y trabajarán - juntos para permitir que los usuarios tengan acceso a su información, a cualquier hora y desde cualquier lugar. El Bluetooth será utilizado como el reemplazo de los cables y como un medio de comunicación en aparatos con restricciones de potencia y tamaño, tales como teléfonos celulares, dispositivos de mano, cámaras, bocinas, auriculares y otros más.

El 802.11b será usado para extender o reemplazar a los LANs por cable, brindando acceso de Internet y una gama completa de características LAN a los usuarios, sin la necesidad de cables. Además, son fáciles de instalar, haciendo que las redes en el hogar sean más razonables.

3.4.13.4 Diferencias principales entre WiFi (802.11b) y Bluetooth?

La tecnología inalámbrica Bluetooth y WiFi son complementarias y realizan distintas tareas. Bluetooth se ha diseñado para reemplazar las conexiones por cables USB o de otro tipo entre los teléfonos móviles, portátiles y otros dispositivos informáticos y de comunicación a corto alcance. WiFi es una Ethernet inalámbrica que proporciona la extensión o reemplazo de las redes por cables para varios dispositivos informáticos.

1. Bluetooth es el equivalente inalámbrico de la conectividad USB.
2. WiFi equivale a una Ethernet inalámbrica (conexión de red).
3. Bluetooth puede ofrecer mayor versatilidad, sin embargo, WiFi está más adaptada a transferencias de datos de mayor volumen.
4. Bluetooth y WiFi usan la banda sin licencia y de disponibilidad universal ISM de 2,4 GHz.
5. Bluetooth funciona dentro de una cobertura de 50-250 metros y WiFi entre 300-400 metros.
6. Bluetooth consume un quinto de las baterías utilizadas por WiFi.

3.4.13.5 Cuadro Comparativo Bluetooth-WiFi

Distinciones Técnicas	Bluetooth	WiFi
Banda de radio	ISM 2,45 Ghz	2,4 Ghz
Frecuencia de Salto	1600 saltos/seg.	Sin salto
Velocidad de transmisión de voz y datos	721 kb/seg.	11Mbps (aunque la velocidad real de transmisión depende en última instancia del número de usuarios conectados a un punto de acceso)
Cobertura	Rango entre 50- 250 mts. Dependiendo del dispositivo Bluetooth	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos
Dispositivos con que trabaja	Alrededor de 600 dispositivos.	alrededor de 450 aparatos
Popularidad	Nueva tecnología, con un rápido crecimiento	Adoptado masivamente
Acceso Público	El número de Hotspots crece exponencialmente	El número de Hotspots crece exponencialmente
Consumo Batería	Aprox. Un quinto del consumo que utiliza WiFi	
Seguridad	128 bit encriptación	64 bit encriptación

CAPITULO IV

IMPLEMENTACIÓN Y PRUEBAS

4.1 CONFIGURACIÓN

Para la implementación del prototipo básico haremos una descripción de los equipos, la instalación, configuración de tarjetas y la tecnología que se utilizarán.

4.1.1 TECNOLOGÍA

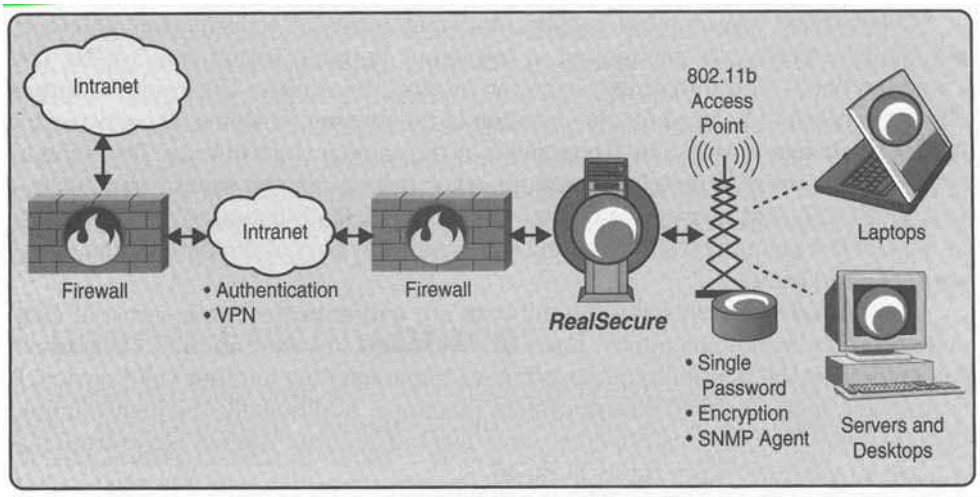
La tecnología Wireless Fidelity (WiFi) es la tecnología inalámbrica que se utilizara para la implementación del prototipo básico por que presenta mejores características que la tecnología Bluetooth.

Wireless Fidelity usa potencias de radio más altas y mayor ancho de banda lo que hace que soporte más servicios transmite mayor volumen de datos y tiene mayor alcance.

Wireless Fidelity remplaza a las LAN por cable, permite el acceso al Internet y proporciona una gama completa de características LAN a los usuarios.

Wireless Fidelity es más de cinco veces más rápido que las soluciones inalámbricas de la generación anterior, y su rendimiento es más que suficiente para la mayoría de las aplicaciones de negocios.

La siguiente figura muestra el diseño del prototipo básico de red, donde se puede probar las seguridades que se presentan en los diferentes medios internos y externos, siendo lo suficiente para el prototipo de red inalámbrico básico.



4.1.2 CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS

4.1.2.1 Equipos portátiles

1 Computador laptop

Marca:	Compaq
Modelo:	Armada 110
Sistema Operativo:	Microsoft Windows XP Profesional Versión 2002
Procesador:	Intel Pentium III
Velocidad:	846 MHz
Memoria:	184 MB de RAM

2 Computadores laptop

Marca:	IBM
Modelo:	ThinkPad
Sistema Operativo:	Microsoft Windows XP
	Profesional
	Versión 2002
Procesador:	Intel Pentium III
Velocidad:	447 MHz
Memoria:	192 MB de RAM

4.1.2.2 Equipos Wireless

2 Adaptadores Inalámbricos

Marca:	D-Link
Modelo:	DWL-G650+

Hasta 8x de mayor velocidad de transferencia de datos que 802.11b
Mayor seguridad en red con encriptación WEP de 256-bit
Conexión de hasta 100m en interiores / 400m en exteriores
Configuración y utilidades de diagnostico amigables para el usuario

1 Wireless Router

Marca:	D-Link
Modelo:	DI-624+

Hasta 8x de mayor velocidad de transferencia de datos que 802.11b
Compartición de conexión Internet con conmutador de 4 puertos integrado
Firewall avanzado y seguridad
Mayor seguridad en red con encriptación WEP de 256-bit
Totalmente compatible con estándar 802.11b
Soporta multisesiones con VPN pass-through

Avanzada capacidad de registro
Conexión de hasta 100m en interiores / 400m en exteriores
Asistente de configuración para instalación rápida

4.2 PLAN DE PRUEBAS

Se establece un esquema de pruebas para analizar el funcionamiento y manejo de seguridades frente a las siguientes amenazas ó ataques que se pueden perpetrar en el prototipo básico de red implementado.

Ataque del wep
Ataque de negación de servicios
Ruptura de ACL MAC Address

Estos ataques son los más frecuentes en el uso de redes inalámbricas por eso se considera hacer el análisis de estas posibles instrucciones.

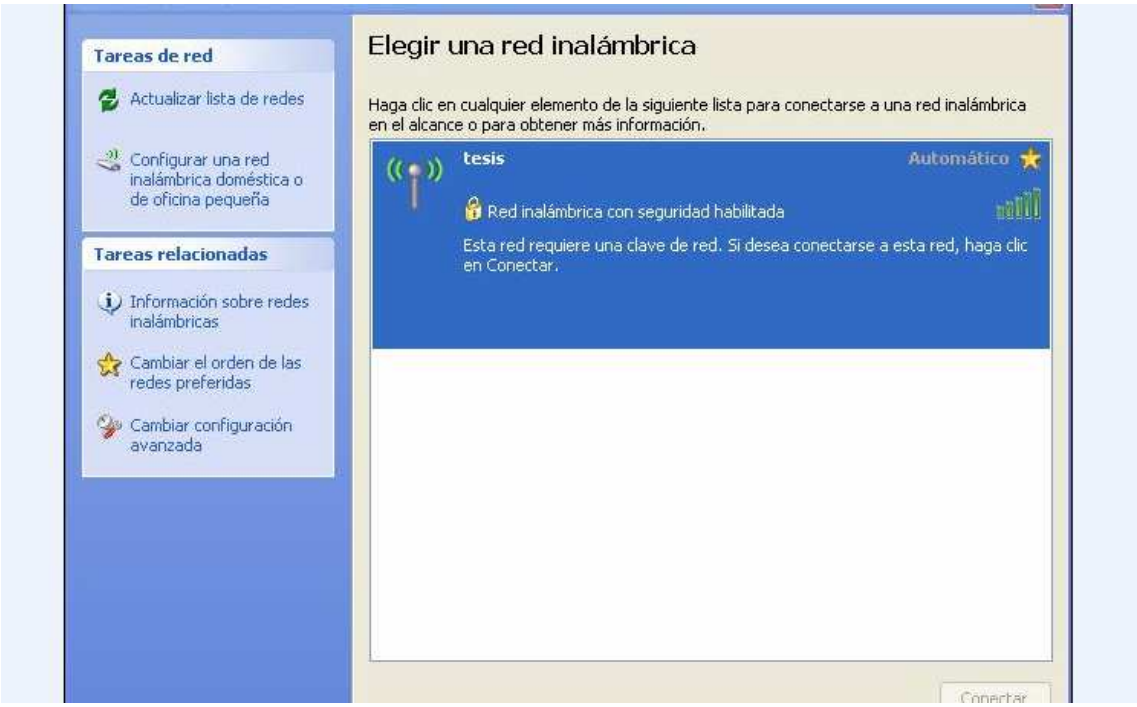
El análisis es considerado en los puntos de acceso interno (LAN / WIRELESS) Y acceso externo (WAN), con los dispositivos que constituye el prototipo básico de red inalámbrica.

4.2.1 CONFIGURACIÓN BÁSICA DE SEGURIDAD

Para el funcionamiento y manejo de seguridades, se establece un estándar de configuración básica de inicio. Esto permite tener una secuencia de análisis para diferentes tipos de pruebas.

4.2.1.1 Configuración de red inalámbrica (Wireless)

La configuración de la red inalámbrica se realiza para habilitar una seguridad estable, para estar en un modo seguro previamente se configura el equipo ruteador inalámbrico cuyo manual de configuración se encuentra en el ANEXO 1.



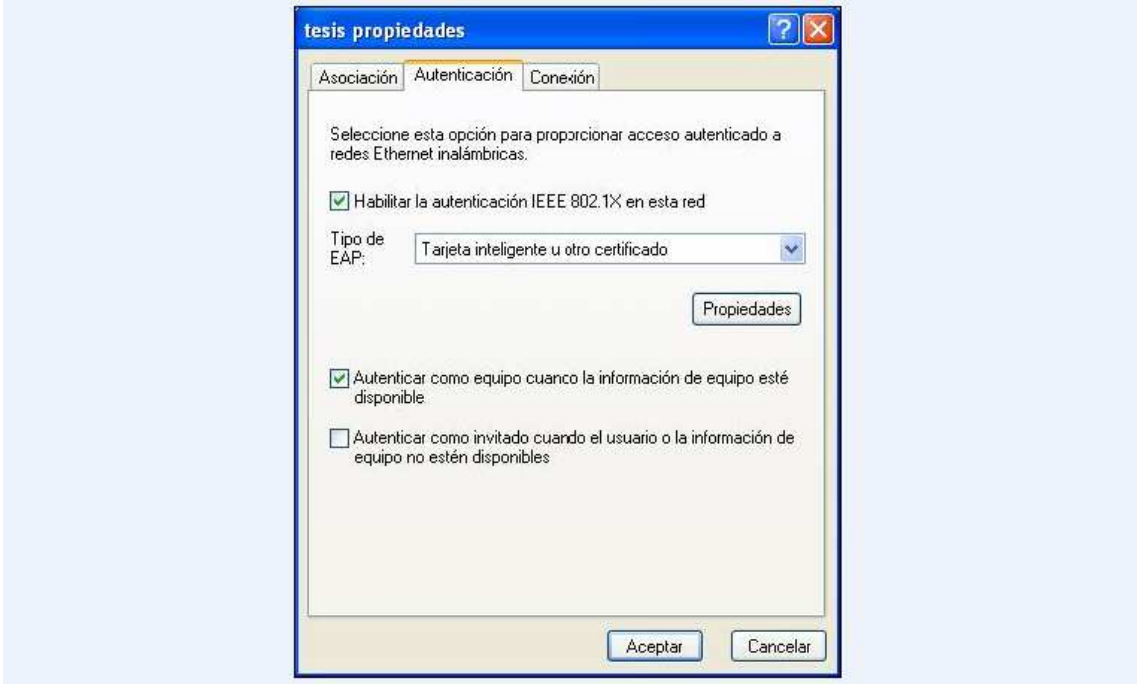
La selección de la red inalámbrica depende de la aplicación

La configuración maneja el protocolo TCP/IP, por ser el que cumple con las características necesarias para el estudio del prototipo básico.

Se procede a seleccionar la red que cumpla con los requisitos para la aplicación que se le va a dar.

Se define el identificador de la red inalámbrica, la autenticación y el cifrado; como parámetros de seguridad.

Seleccionamos la opción para habilitar la Autenticación en la red inalámbrica.



Se selecciona una entidad para emitir certificados de autenticación, permite garantizar y saber de quien es el emisor de la información

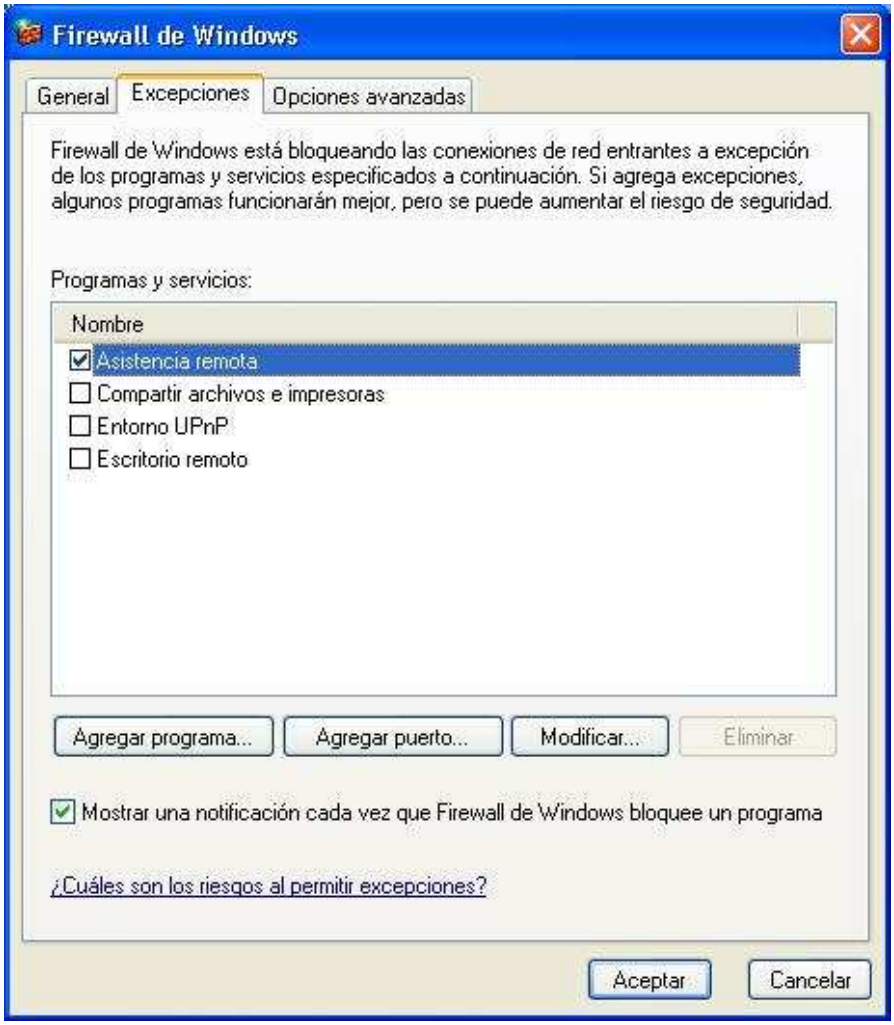
Para proteger el equipo y la red se habilita el Firewall

4.2.1.2 Configuración de acceso Interno

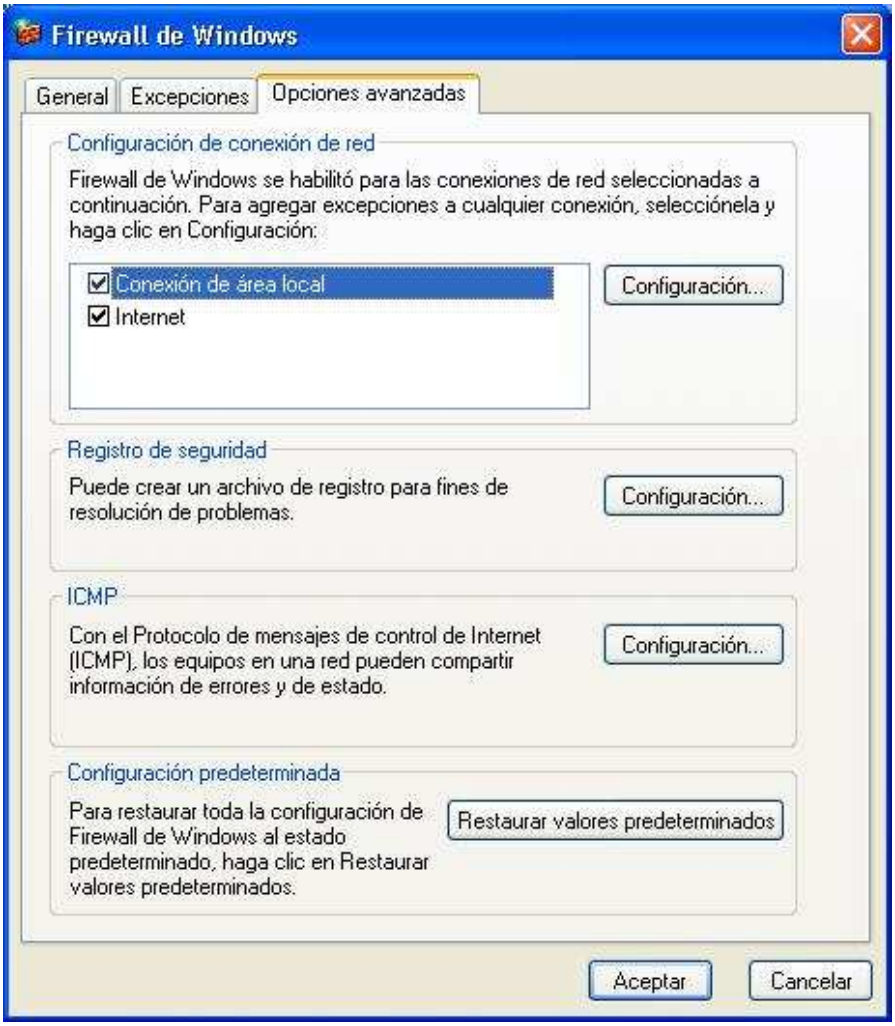
El acceso interno se maneja con las seguridades de la red inalámbrica (sección 4.2.1.2), y las seguridades del interfase del acceso (interno/externo) que se hace referencia en el manual de configuración ANEXO 1

La configuración de firewall de Windows se utiliza para delimitar y asegurar el acceso interno.

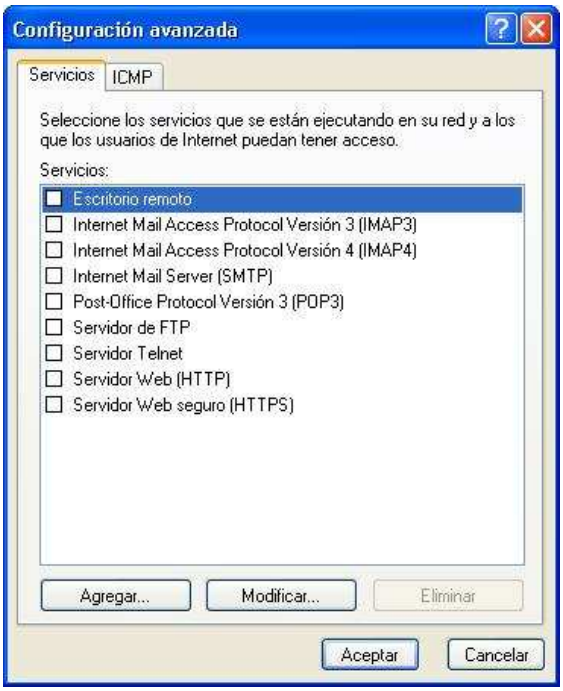
Se selecciona los programas y servicios que se le permite el ingreso a nuestra red, de manera que no afecta ni compromete a la seguridad de nuestra red.



En este punto se determina el tipo de conexión de red, registros de seguridad y con control de mensajes

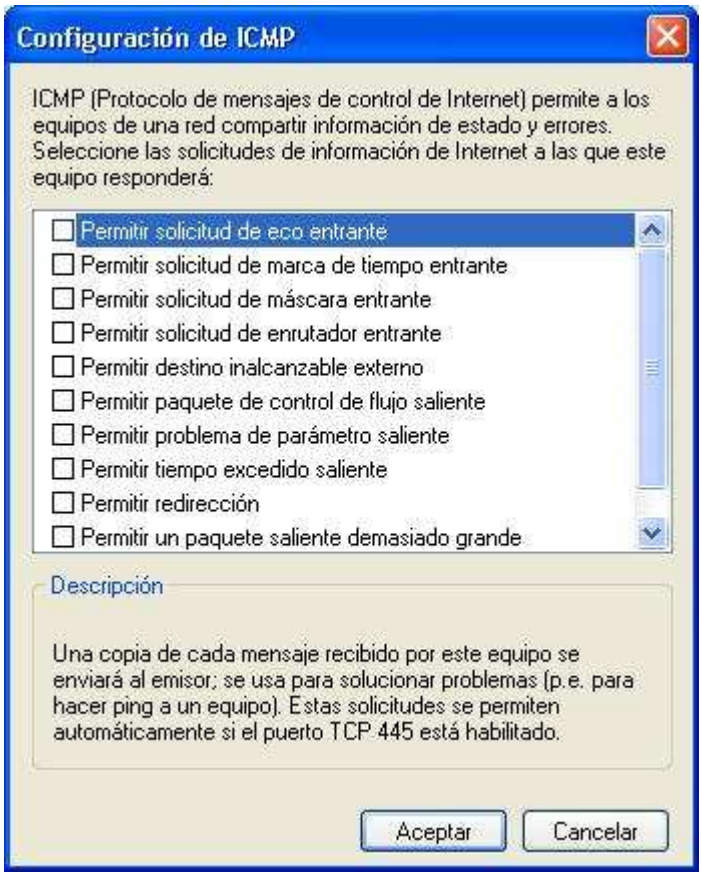


La configuración avanzada determina que tipos de servicios se utiliza



Se determina el registro que maneja nuestra red, con esto miramos el flujo de información.

ICMP permite ver la forma de compartir la información.

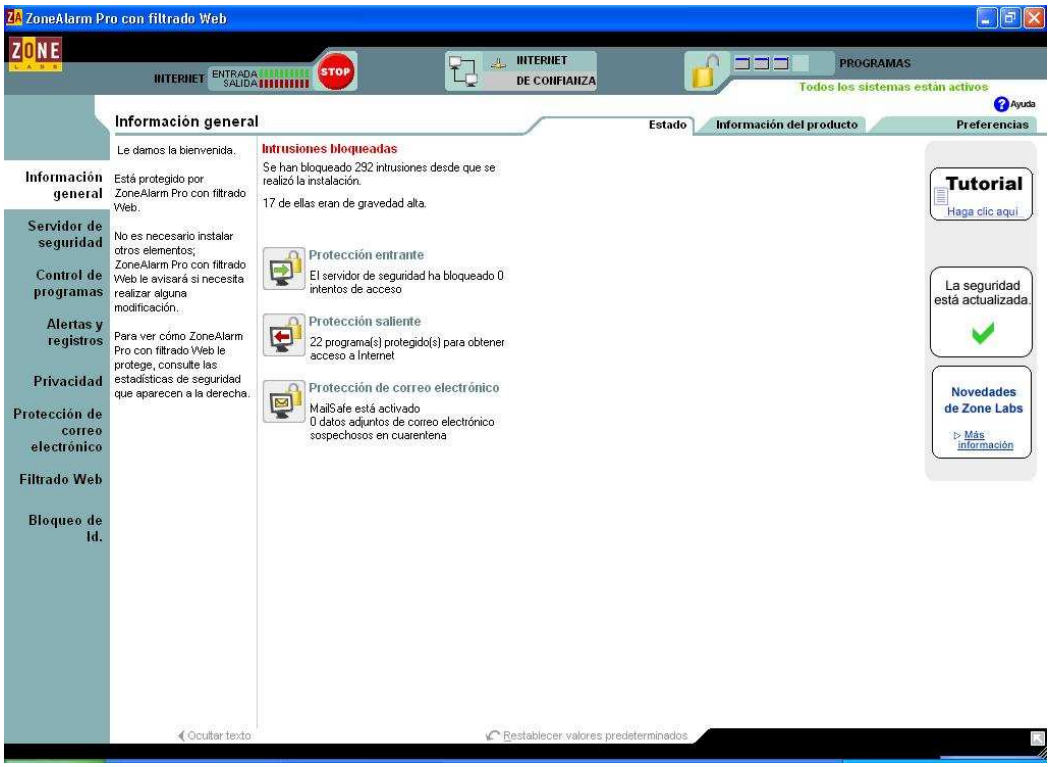


4.2.1.3 Configuración de acceso Externo

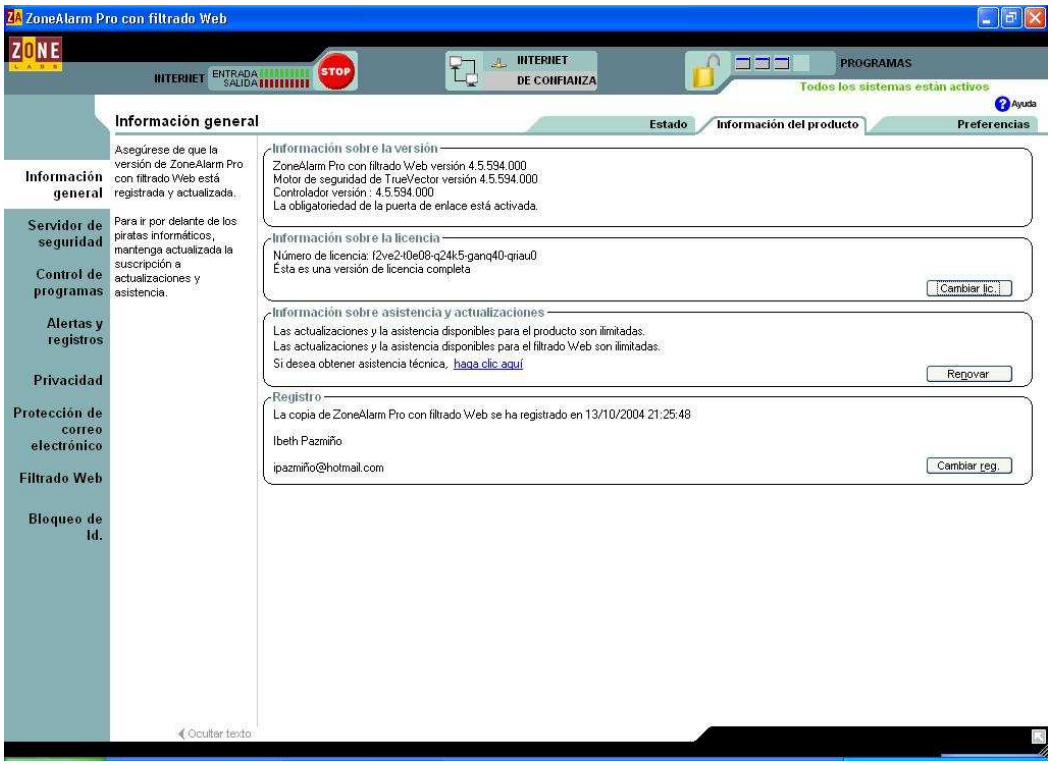
El acceso externo se maneja las seguridades del interfase del acceso (interno/externo) que se hace referencia en el manual de configuración ANEXO 1 y seguridad del medio externo, la protección para el acceso externo se lo realiza con un firewall robusto que permite asegurar el prototipo básico de red.

La configuración se inicia para detectando la red para trabajar en una relación de confianza y de Internet.

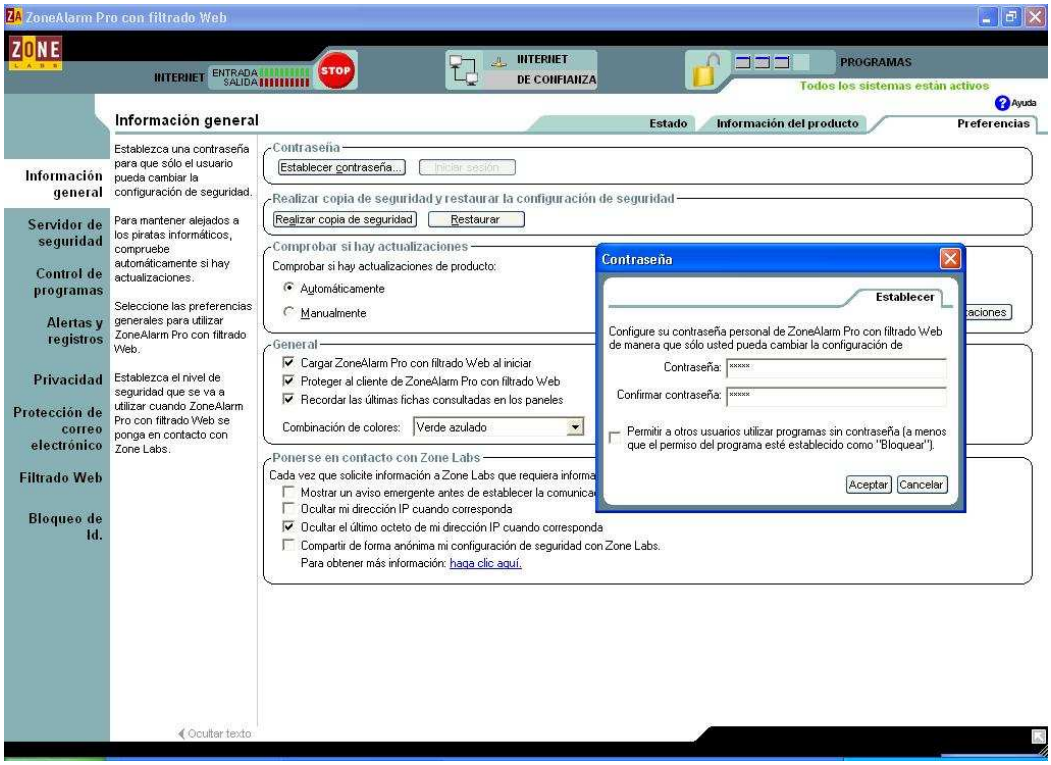
Analizamos el estado del firewall y los accesos que vamos a asegurar.



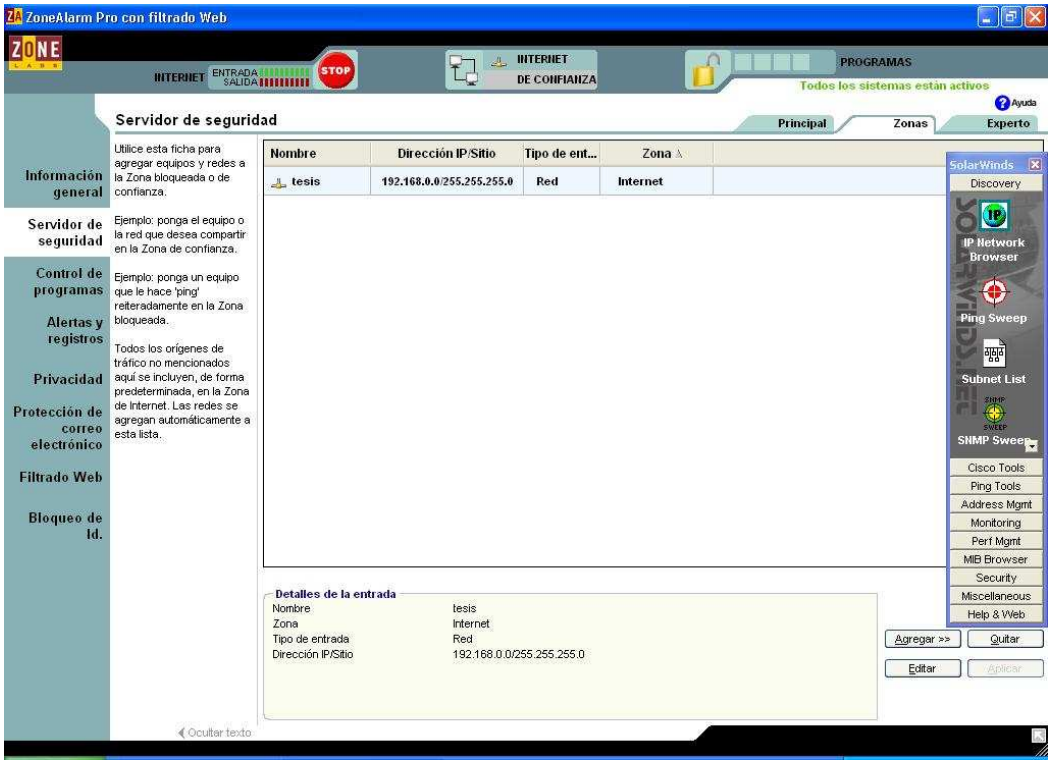
Se muestra la información y características del firewall.



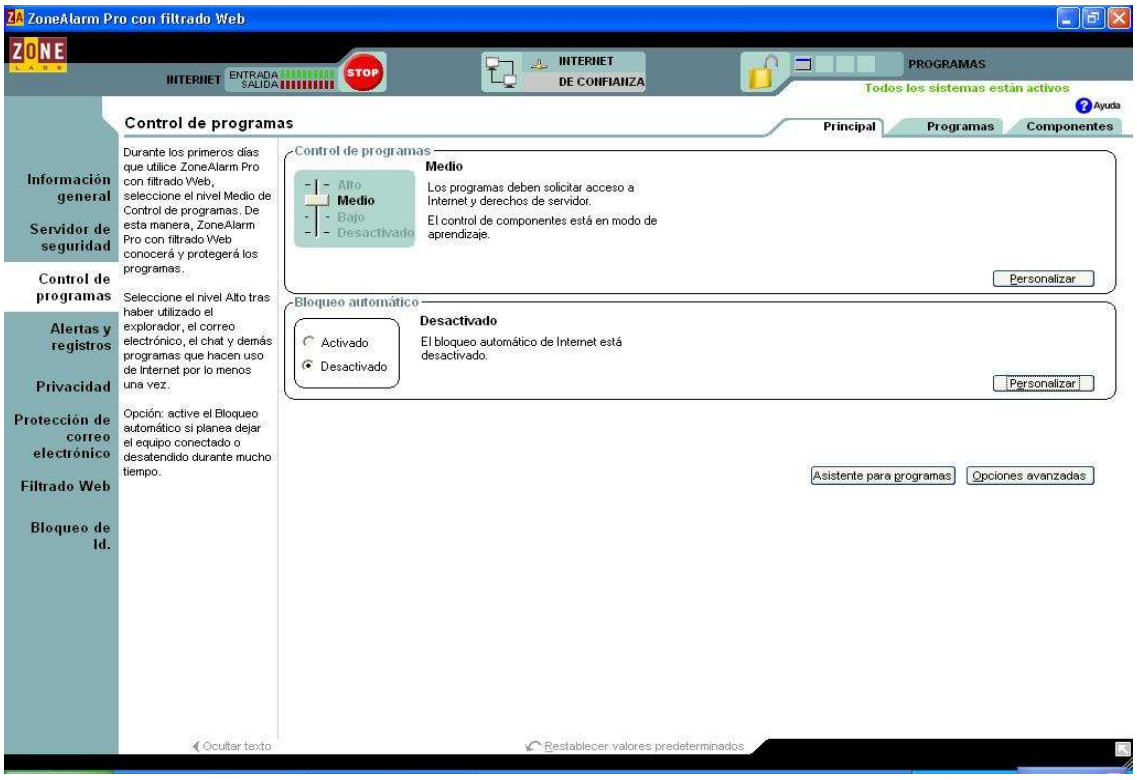
Configuración de contraseña de administración, actualización de productos de seguridad y almacenamiento de configuración de seguridad..



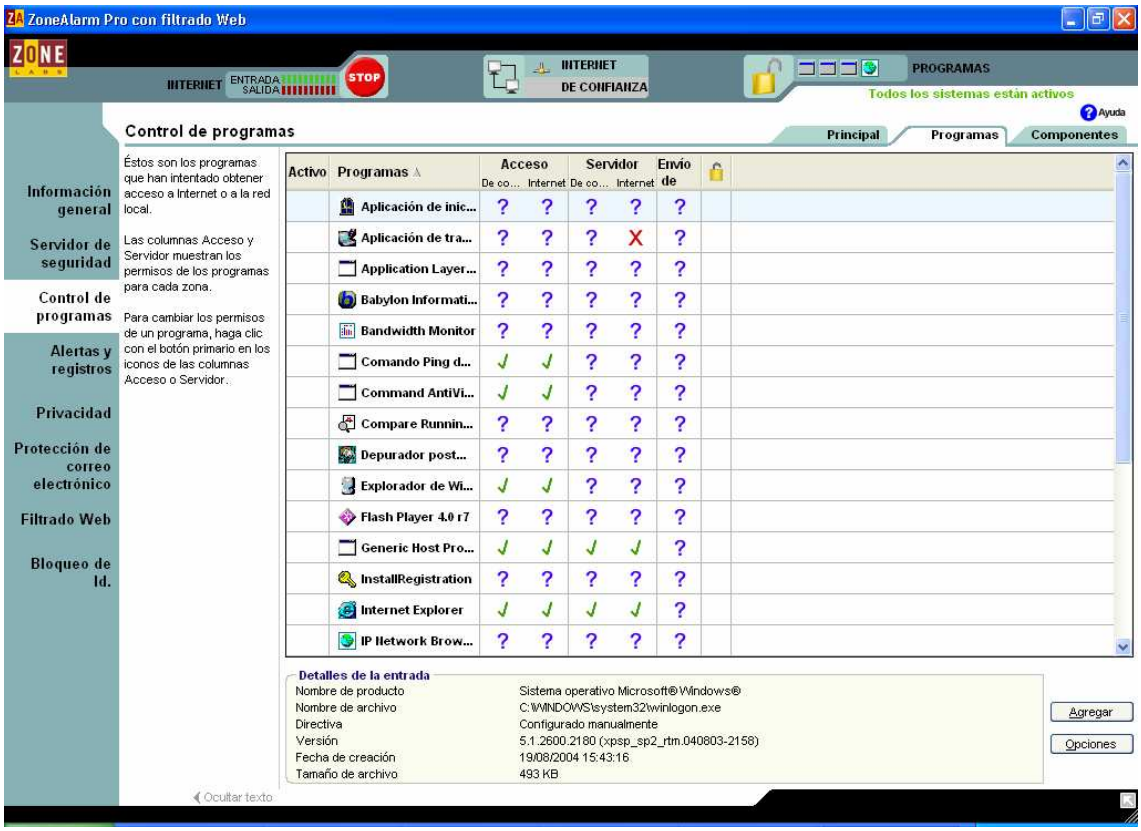
Establecemos nuestro servidor de seguridad y la zona en la que vamos a trabajar, observaremos el origen de tráfico que se genere interno y externo.



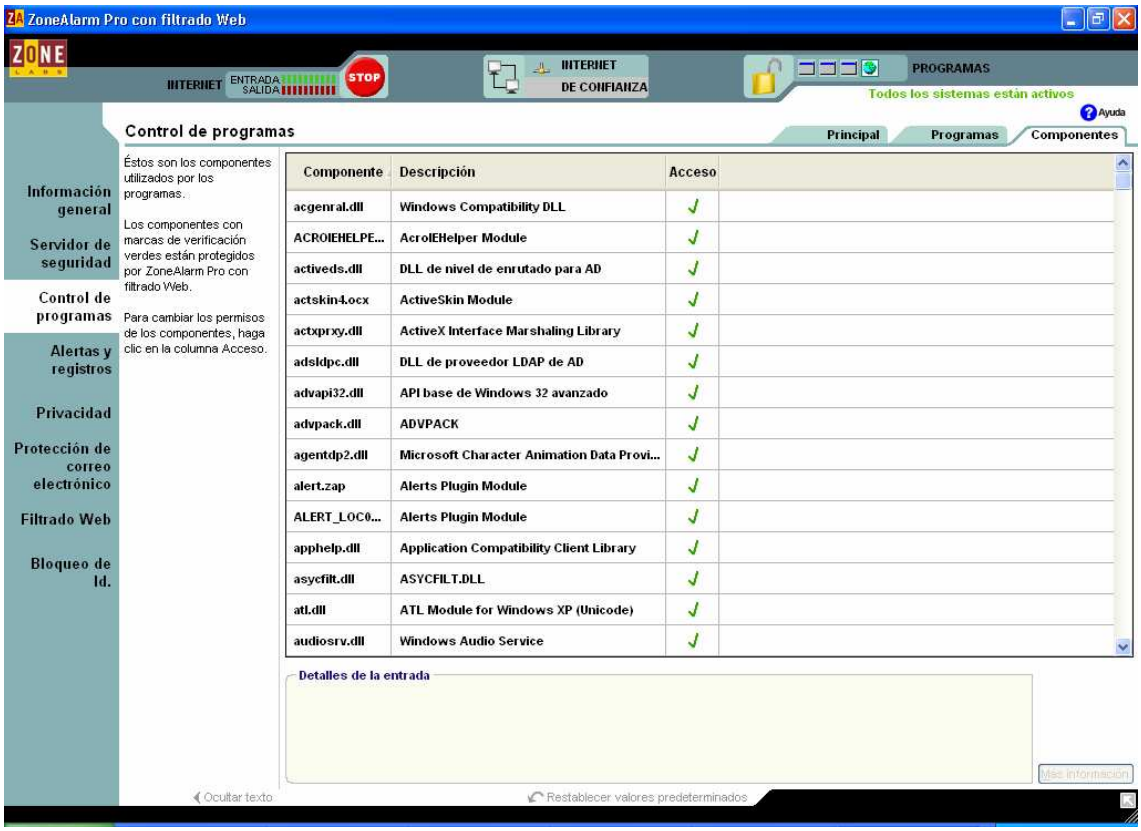
Se maneja el nivel de seguridad para el control de programas y el bloqueo de programas. Esto asegura que los dispositivos no sean violentados.



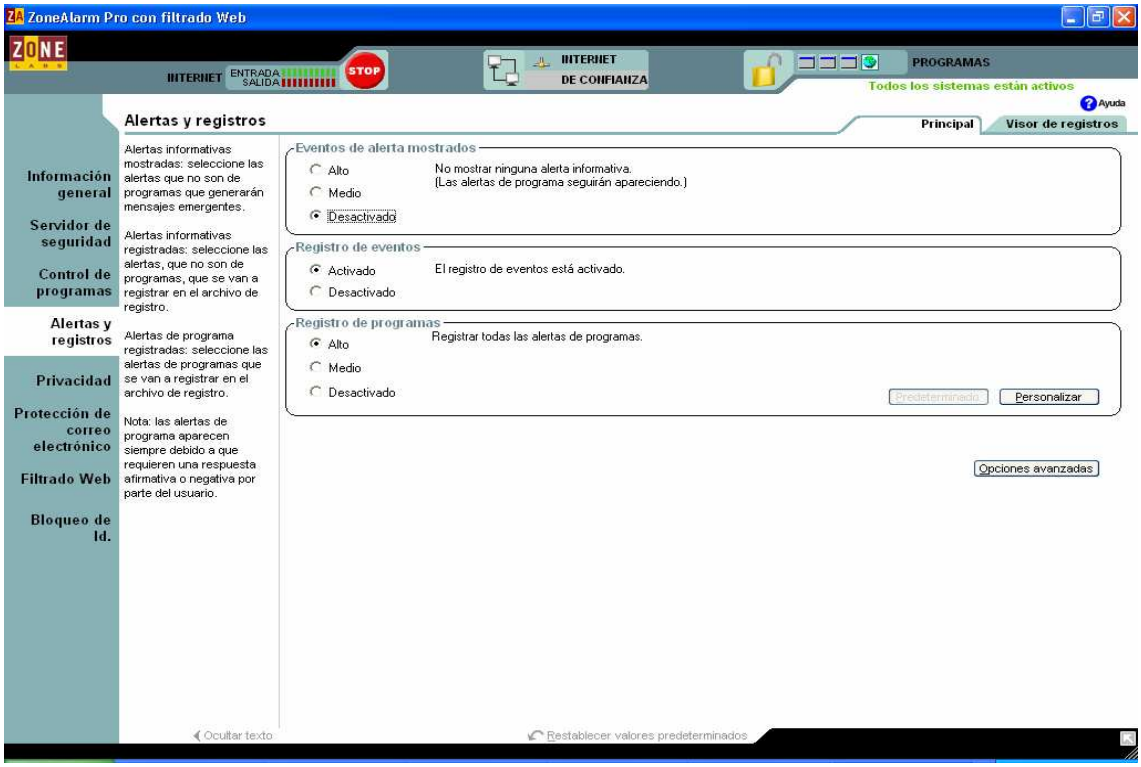
Se establece que programas vamos a permitir el acceso y en que zona trabaja (confianza ó Internet).



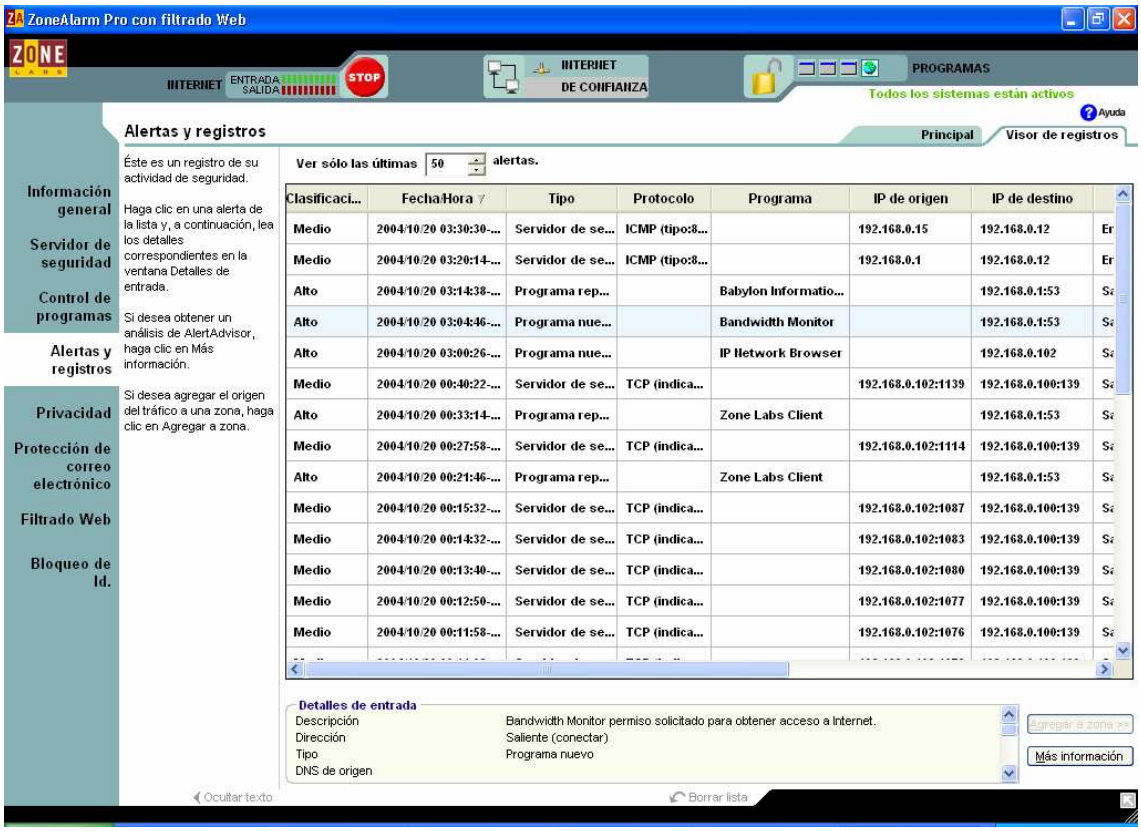
Establecemos el acceso de los componentes que van a estar protegidos.



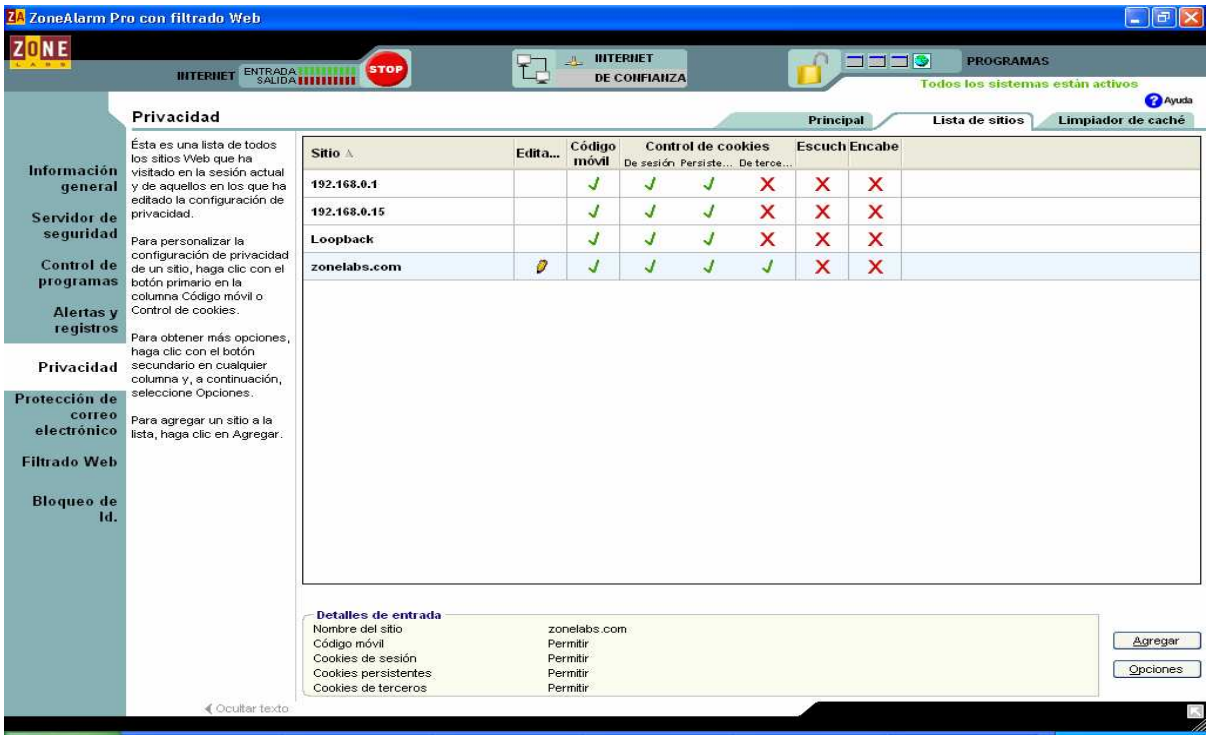
Configuramos los niveles de alerta, eventos y registros de programas



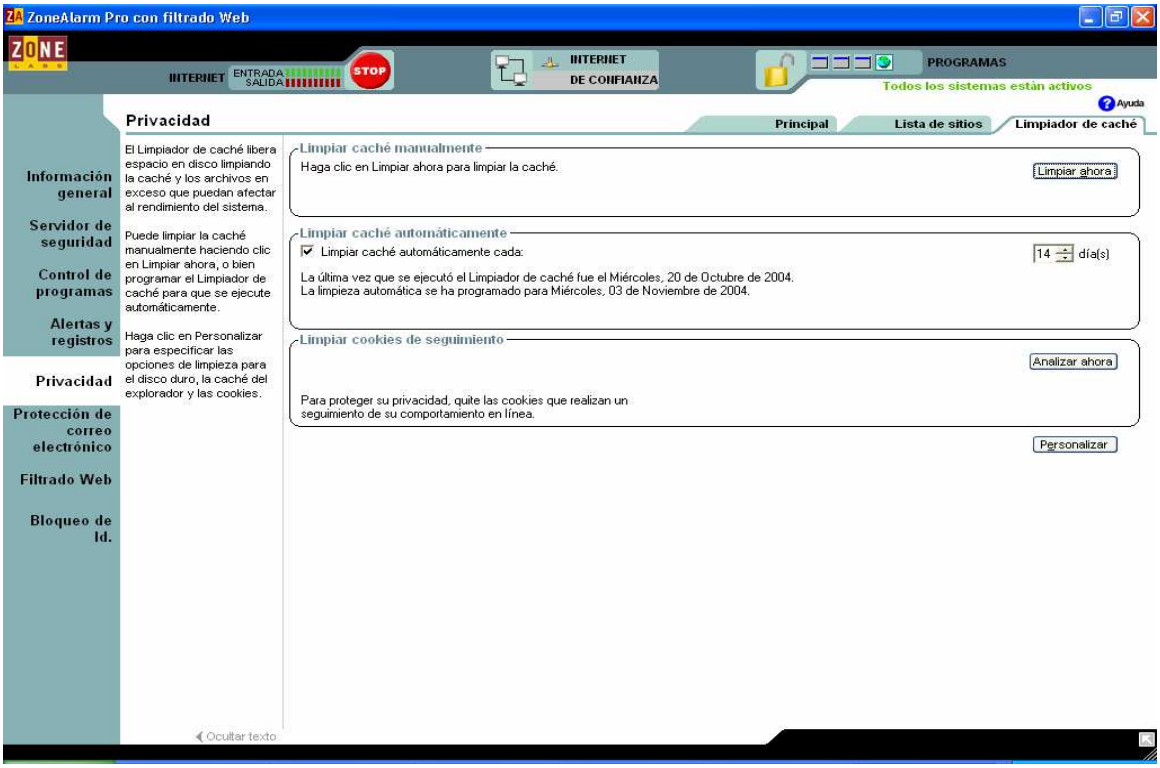
Se maneja un registro de actividad de seguridad.



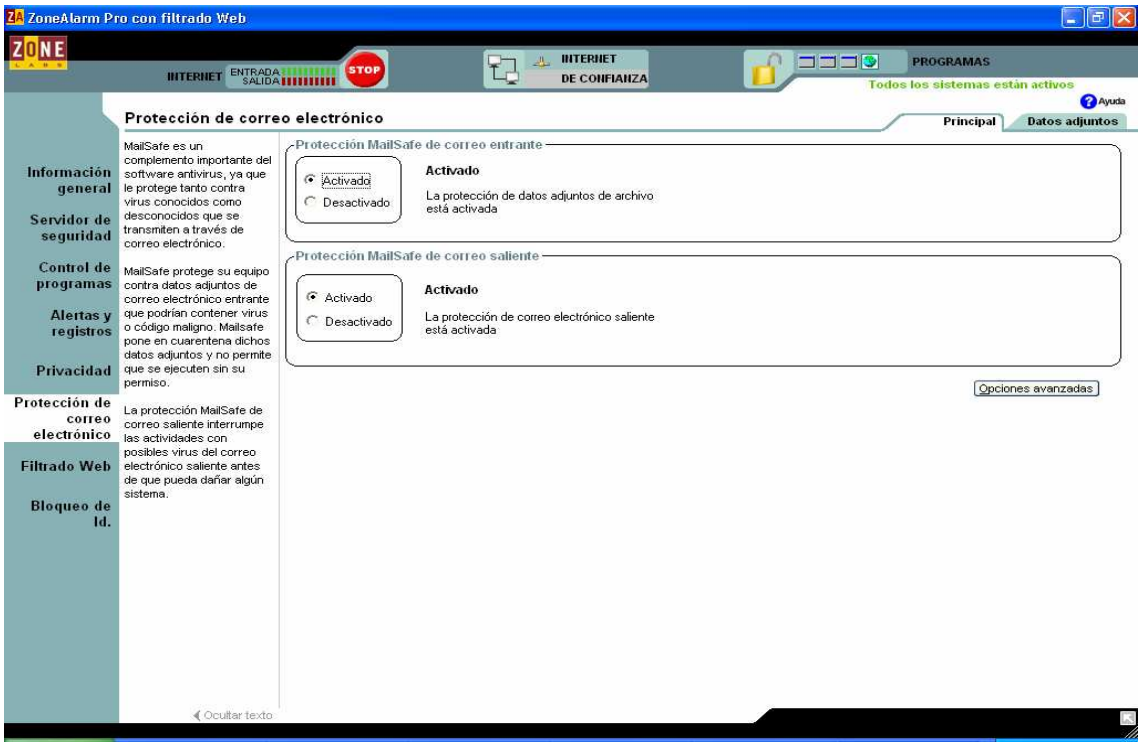
Determinamos la privacidad en los sitios o puntos de acceso



Configuramos la privacidad, manejando el seteo de caché y cookies.

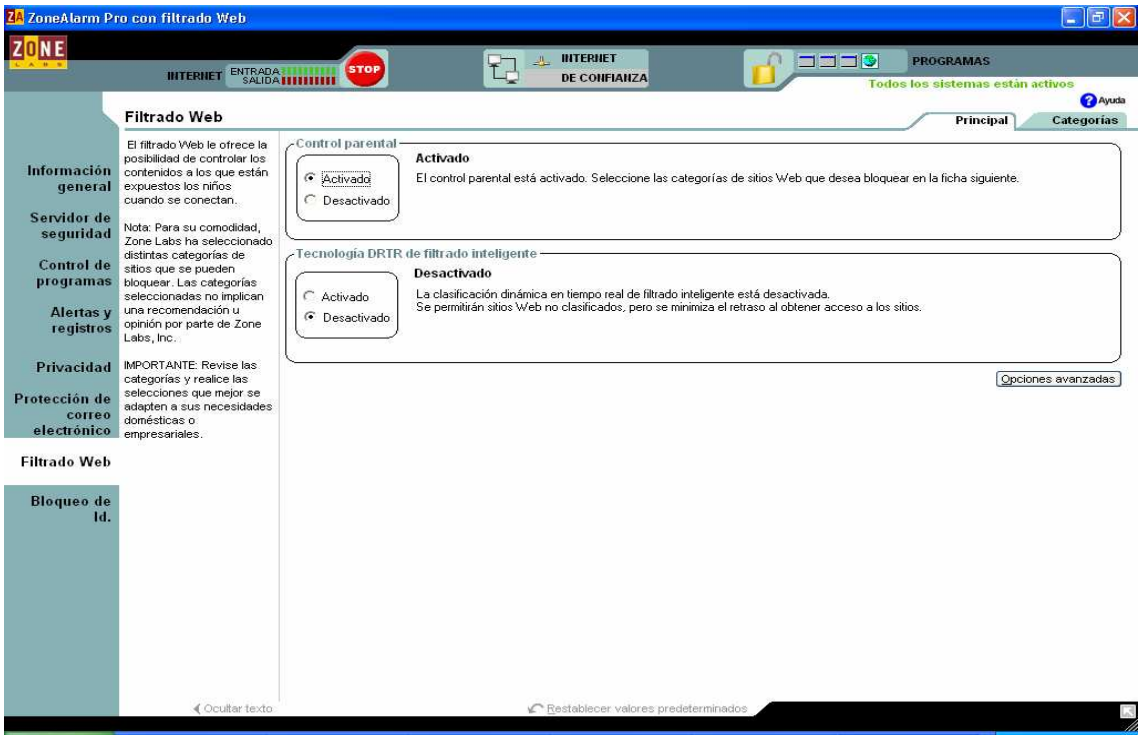


Se configura los niveles de seguridad para proteger el correo electrónico.

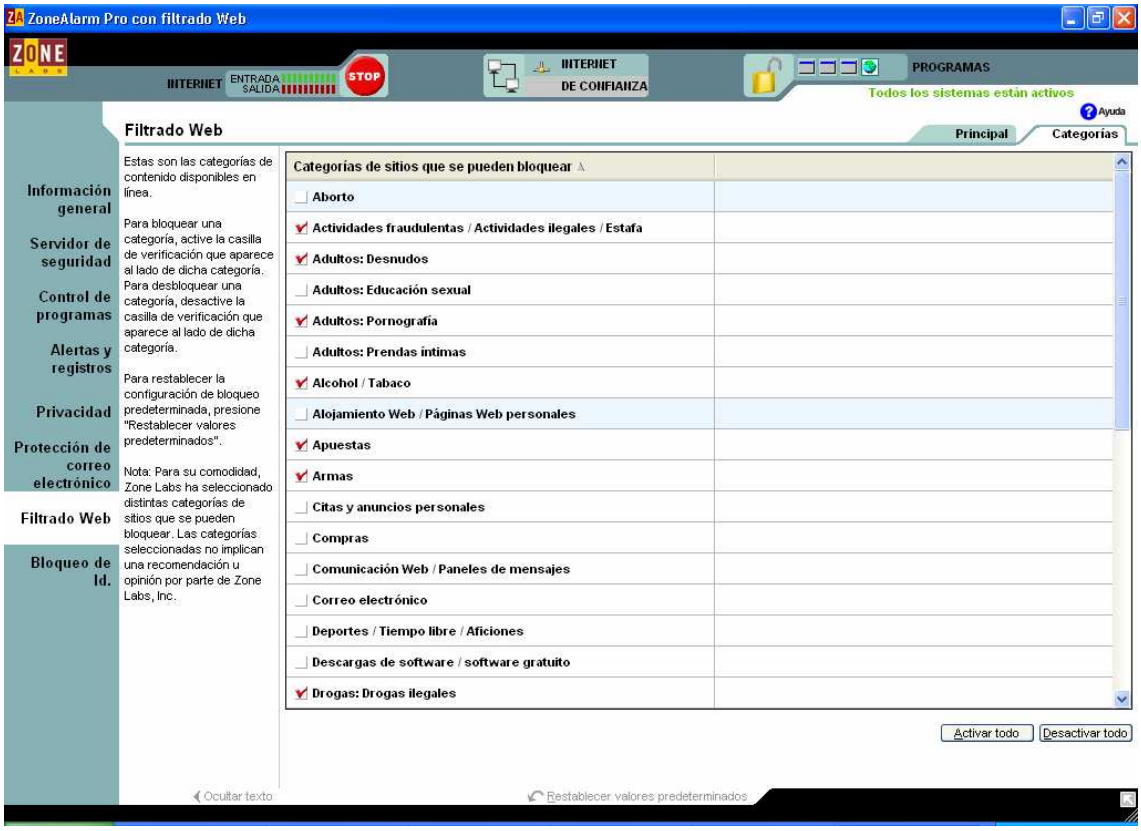


El manejo de los datos adjuntos y extensiones, se configura para permitir el acceso.

Permite realizar un filtrado de los contenidos de la información del web.



Se determina las diferentes categorías, que vamos a permitir el acceso.



Se establece la protección de la información personal.

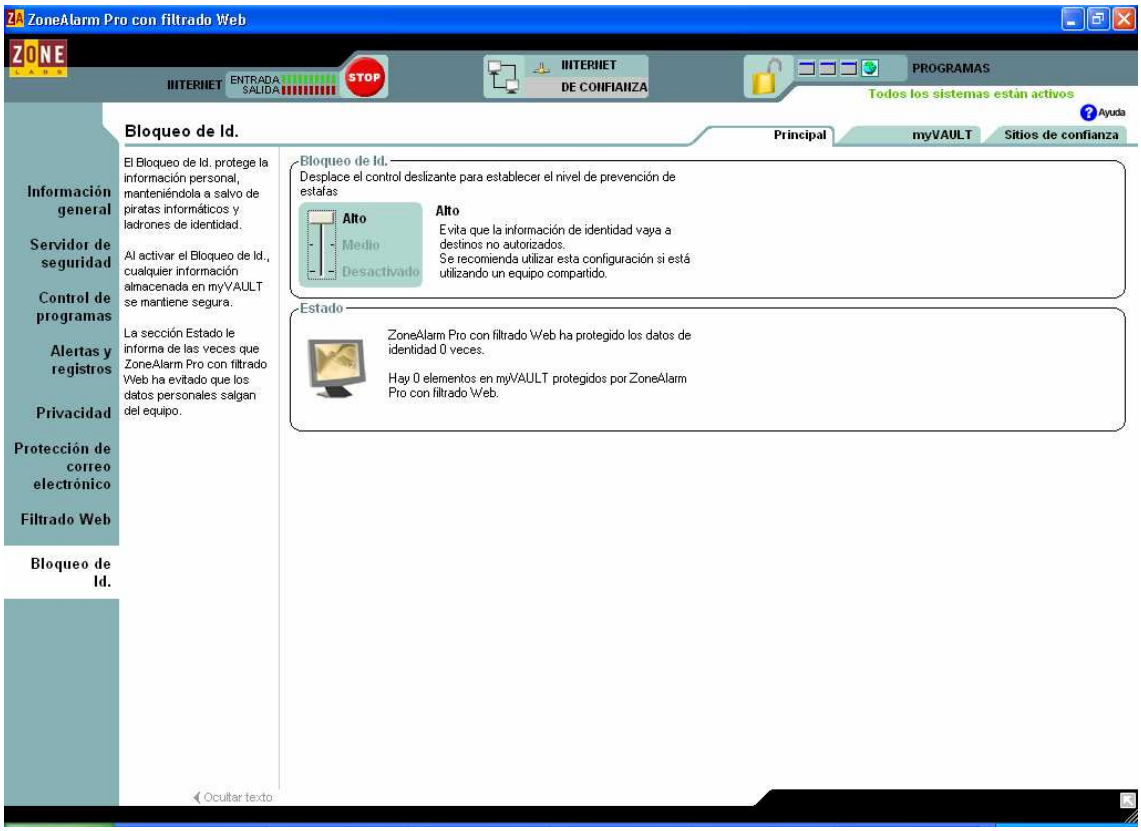


Tabla de configuración inicial del prototipo básico de red Inalámbrica

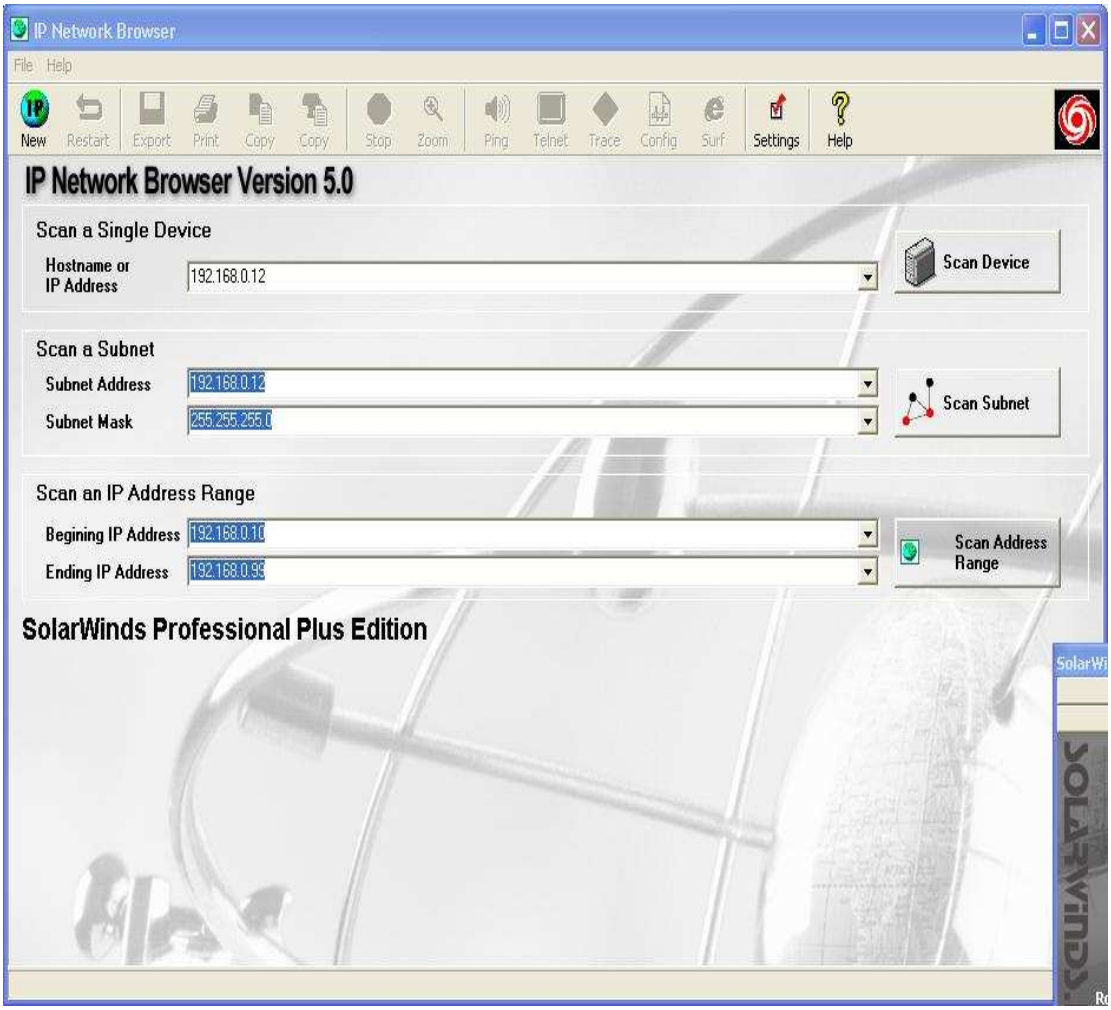
	WIRELESS 1	WIRELESS 2	LAN	WAN	ROUTER
OPERACIÓN	OK	OK	OK	OK	OK
CONEXIÓN	SEGURA	SEGURA	SEGURA	SEGURA	SEGURA
SEGURIDAD	FIREWALL WINDOWS	FIREWALL WINDOWS	FIREWALL WINDOWS	FIREWALL ZONEALERT	FIREWALL D LINK
FILTRADO	OK	OK	OK	OK	OK
AUTENTICADO	OK	OK	OK		OK
CIFRADO				OK	
ENCRIPTADO	OK	OK	OK		OK
FILTRADO WEB				OK	
ANTIVIRUS	OK	OK	OK		

4.2.2 ANÁLISIS Y MONITOREO DE RED

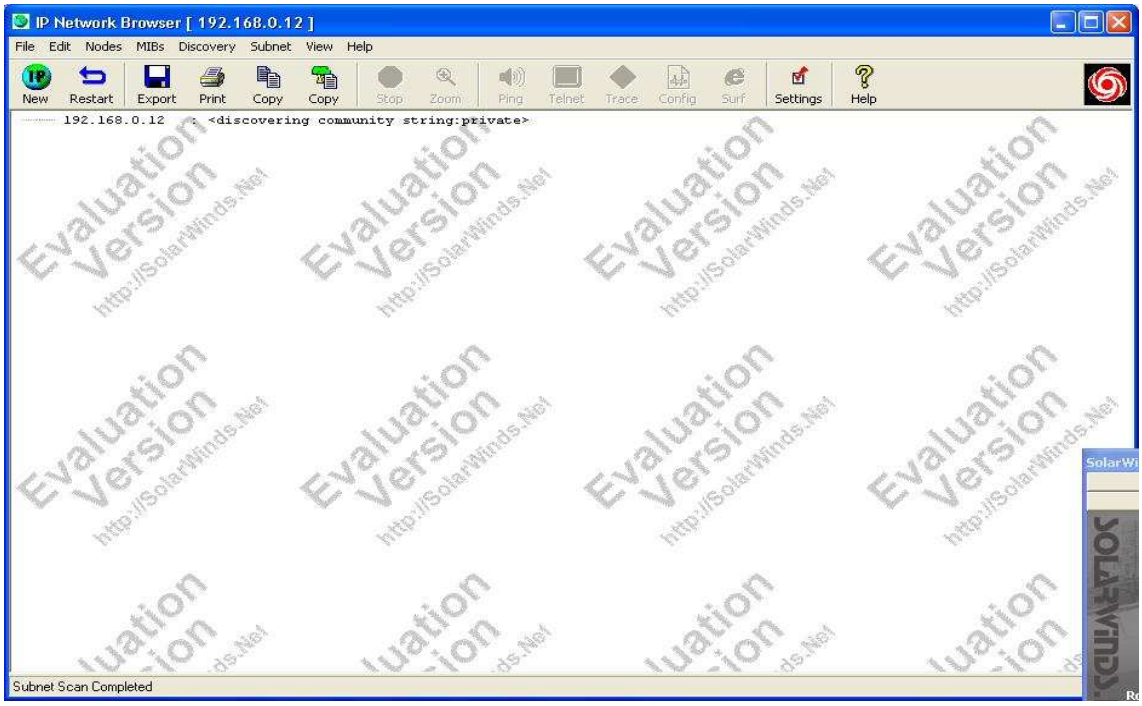
Se verifica, analiza y monitorea la información que se da para cada uno de los medios, usando las diferentes herramientas de verificación.

4.2.2.1 Análisis de red básica

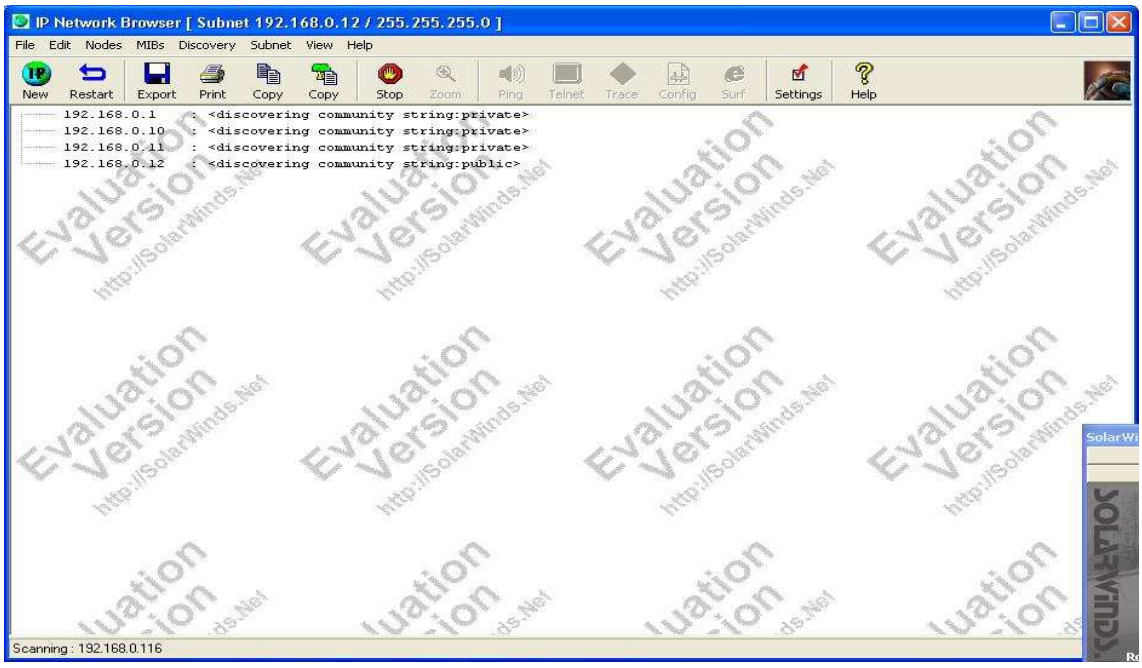
Aquí se analiza la constitución básica de nuestra red, para ver los dispositivos conectados y el rango de manejo. La utilización de este analizador permite saber las condiciones que se encuentra conformado el prototipo básico de red.



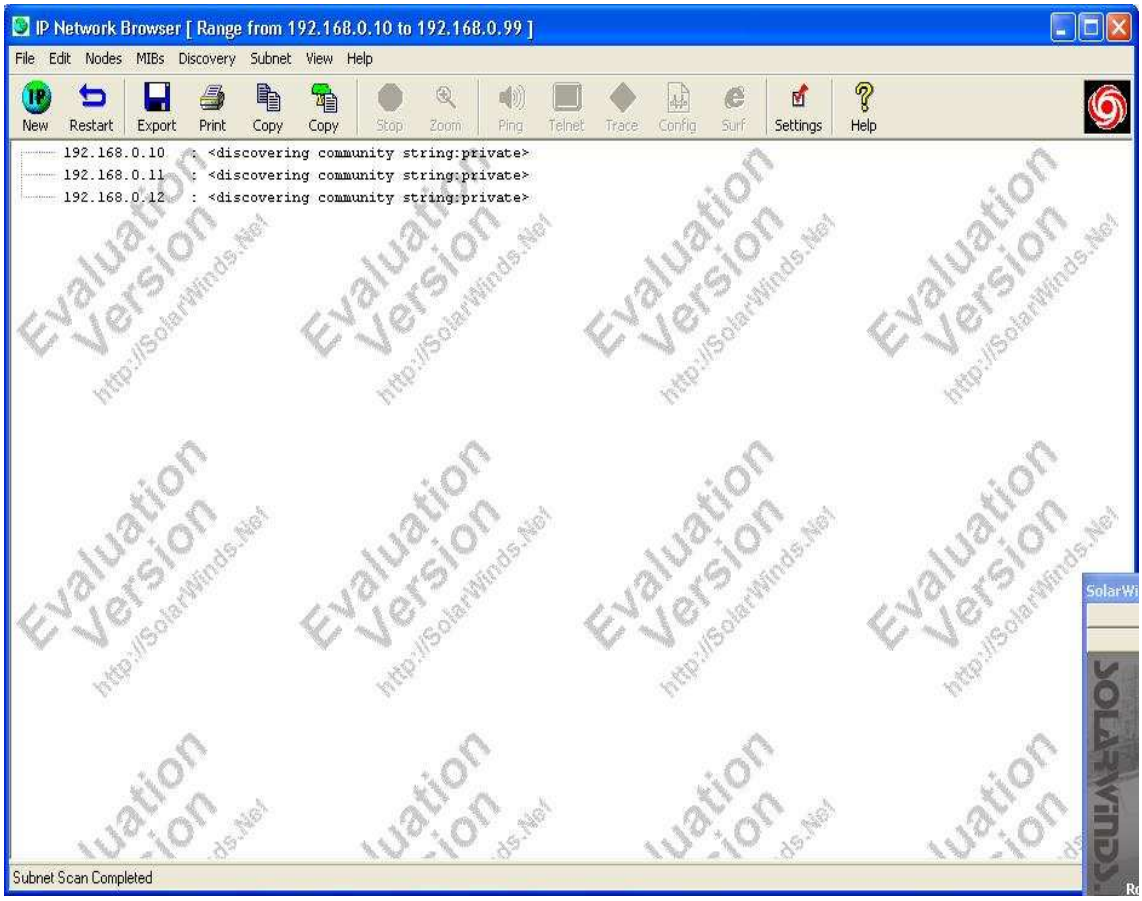
Verificamos el dispositivo en la red. Esta figura indica como esta constituido el servidor y a que comunidad pertenece pública ó privada, esto permite determinar características de seguridad.



Se escanea la red respecto, cuyo resultado presenta a los dispositivos que están en el prototipo básico de red, a las comunidades que presentan bajo ese servidor y se verifica que no haya dispositivos extraños a el prototipo básico de red.



Se establece un análisis de la red pero en rango ampliado, como parte de verificación de intrusos dentro de nuestro prototipo básico de red.

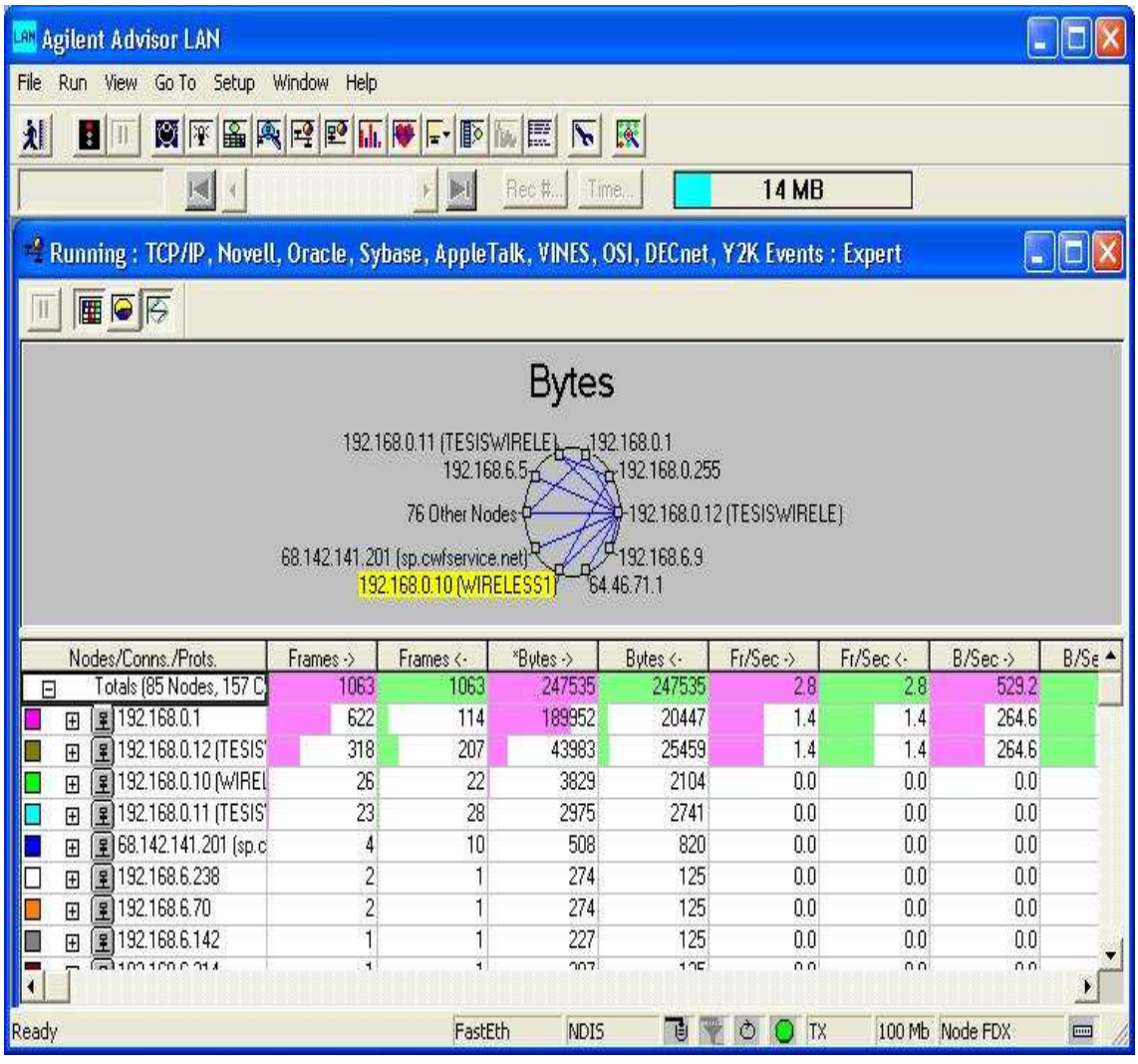


4.2.2. Monitoreo de la red

Se monitorea el trabajo que realiza la red a nivel interno como externo, se verifica que la información que se procesa este siendo entregada a quien pertenece, la velocidad de transmisión se mantiene constante para los dispositivos inalámbricos.

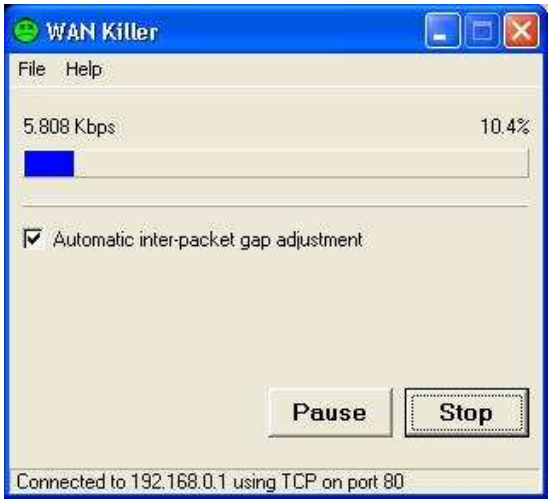
Rango de estudio de los dispositivos inalámbricos:

Línea de vista (200 +/- 25) metros con algunos obstáculos en el medio.
Aptitud omnidireccional vertical (15 +/- 3) metros con algunos obstáculos en el medio.



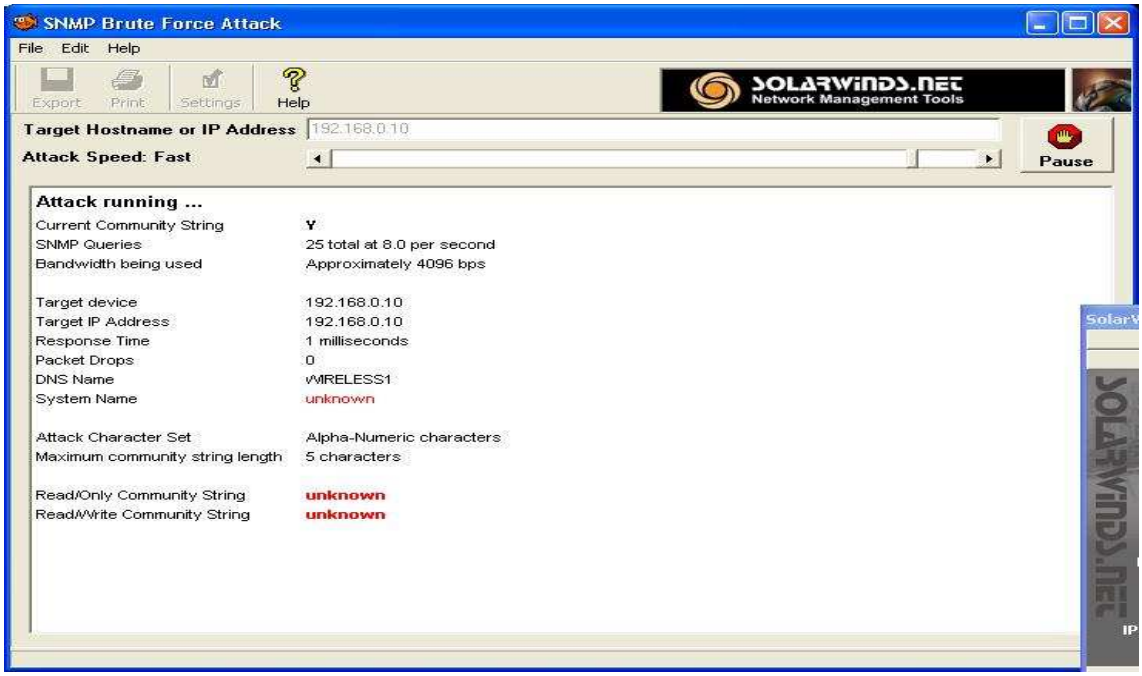
4.2.2.3 Análisis de red con simulación de ataques internos y externos

Se utiliza un simulador de ataque externo, un aniquilador de WAN hace un análisis de los paquetes que están en el medio eliminando tramas, provocando reenvíos y congestionando el medio.

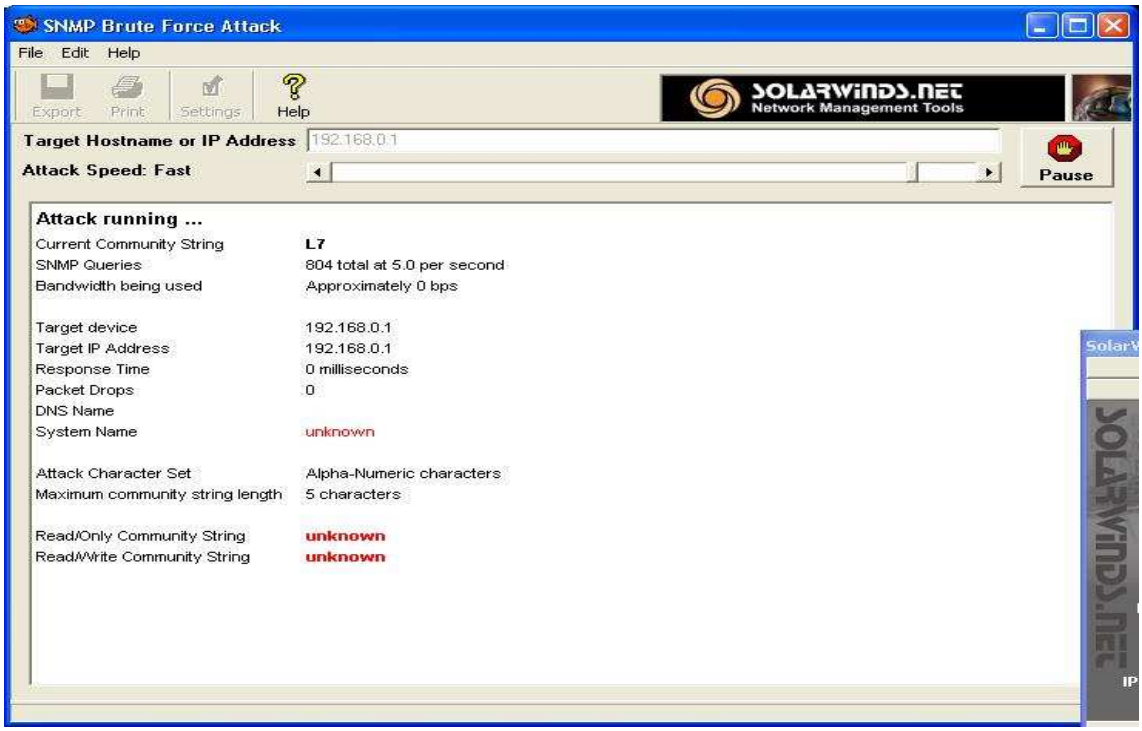


El Simulador de ataque interno nos hace un ataque alfa-numérico a la red sin importar a la comunidad que este pertenezca ya sea pública o privada, detecta a los equipos y perpetra nuestra seguridad, pudiendo modificar los datos de configuración, tal como MAC Address.

Análisis en la parte inalámbrica.

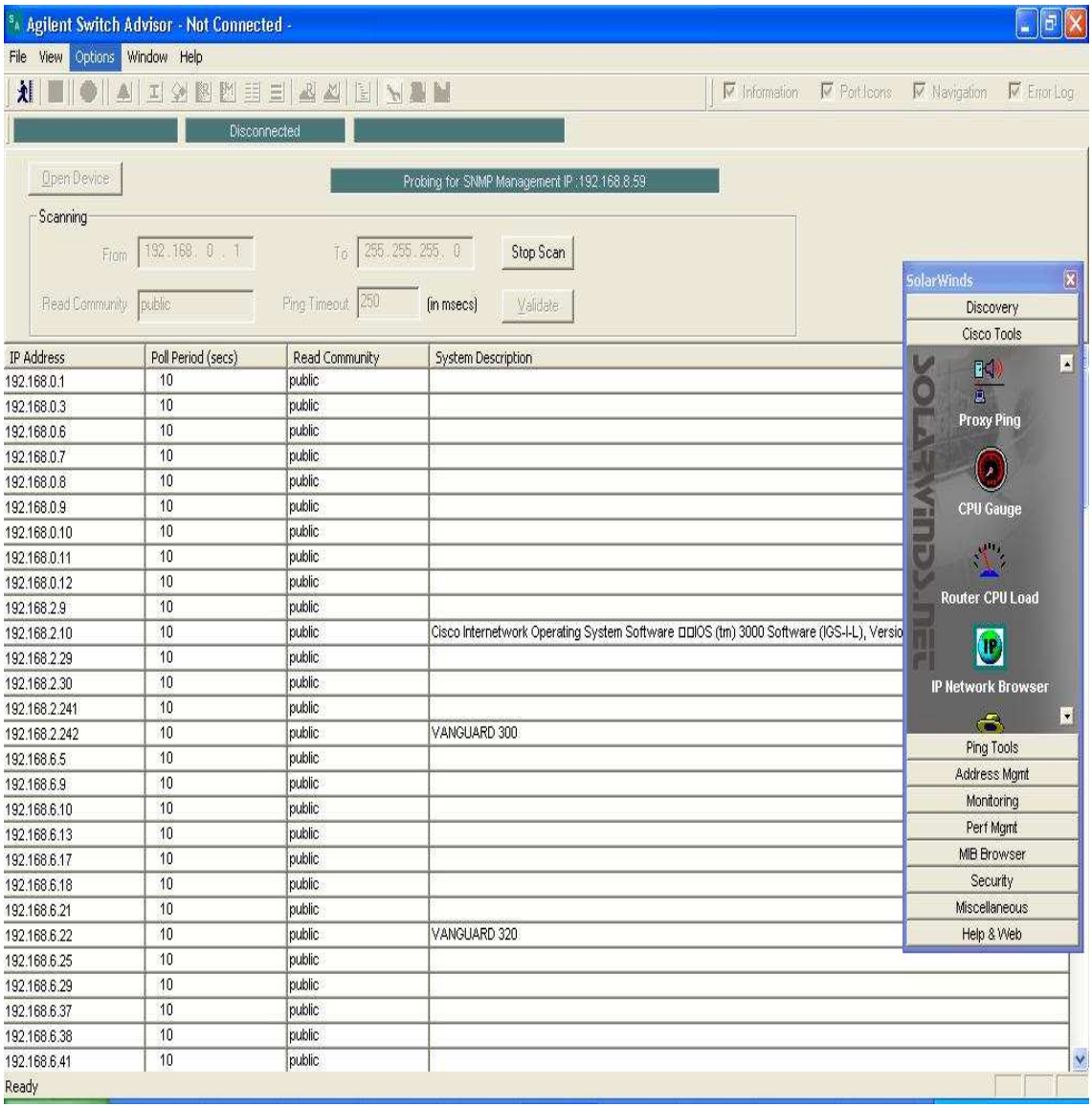


Análisis en la parte del ruteador.

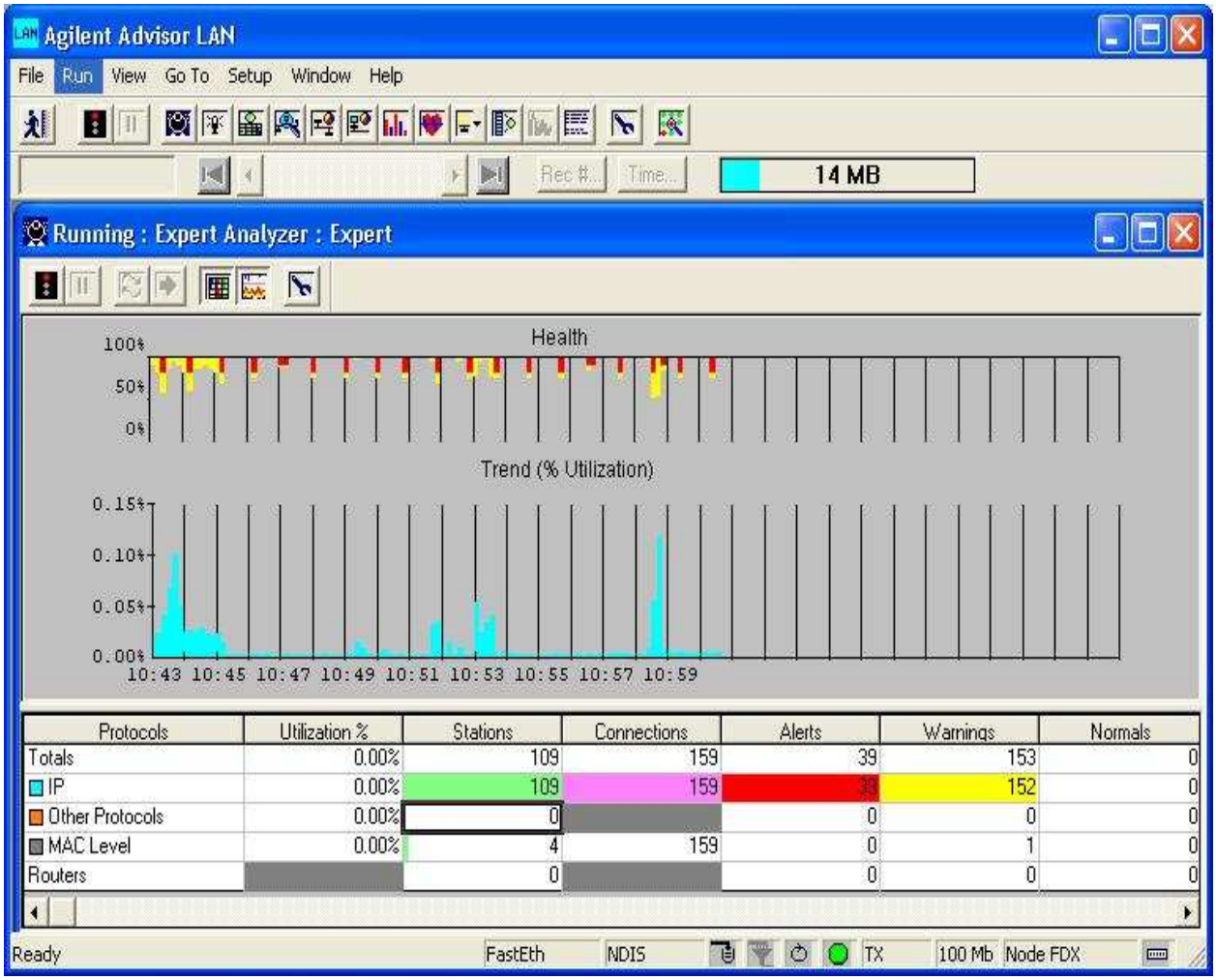


Análisis en la parte del servidor de seguridad.

Presentación de comportamiento de la red frente a los ataques, escaneando la dirección IP, puerto de análisis y comunidad a la que pertenece, nótese que el prototipo básico de red no ha sido perpetrado.



Analizamos los recursos que se están utilizando, las conexiones que están estableciendo y las alertas frente a los ataques. Se denota un incremento de tráfico de información en el monitor, debido a la utilización de los simuladores de ataques.

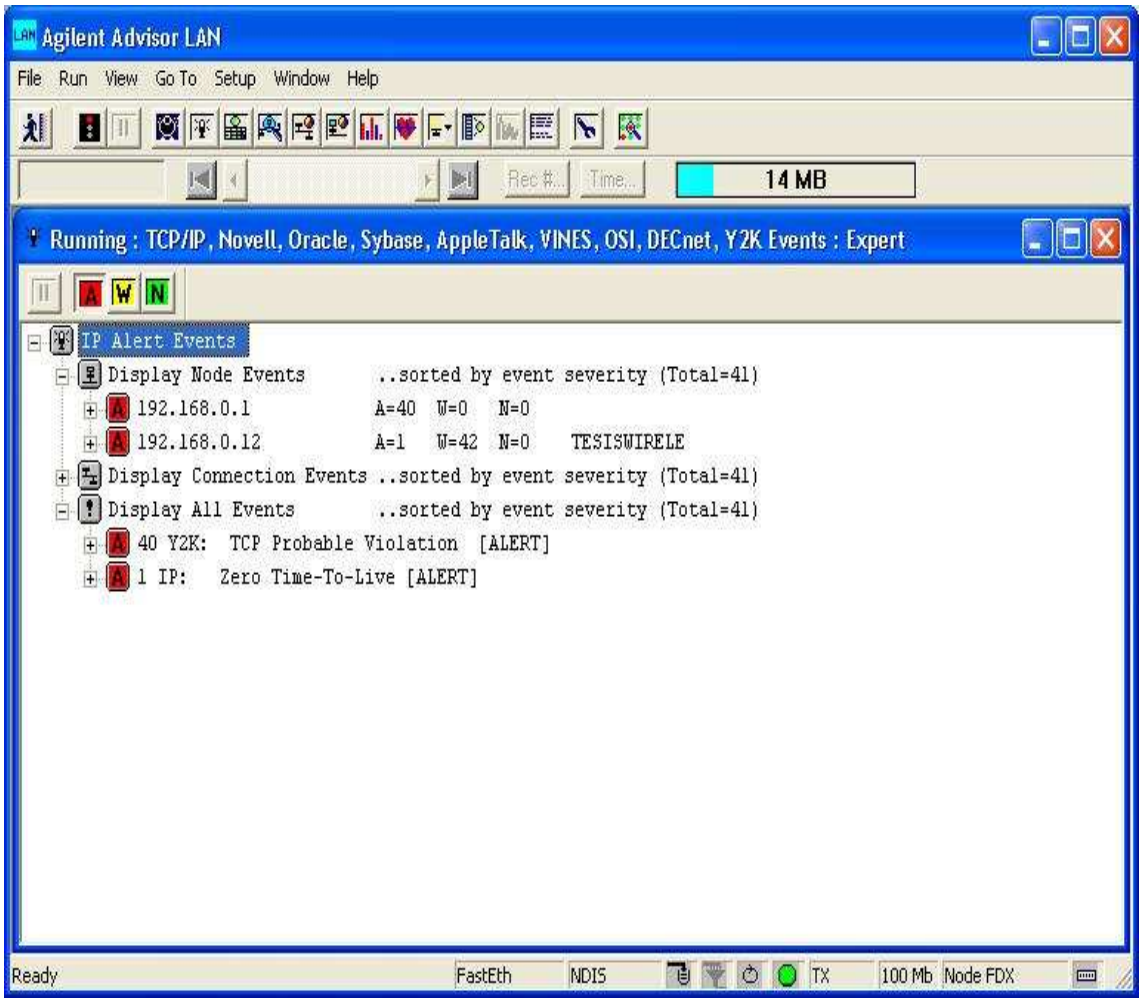


Observamos las alertas de eventos en el análisis del prototipo básico de red, esto se da más en el servidor de seguridad y en el ruteador, esto nos permite tomar precauciones para el manejo de seguridad. Los niveles de alertas son:

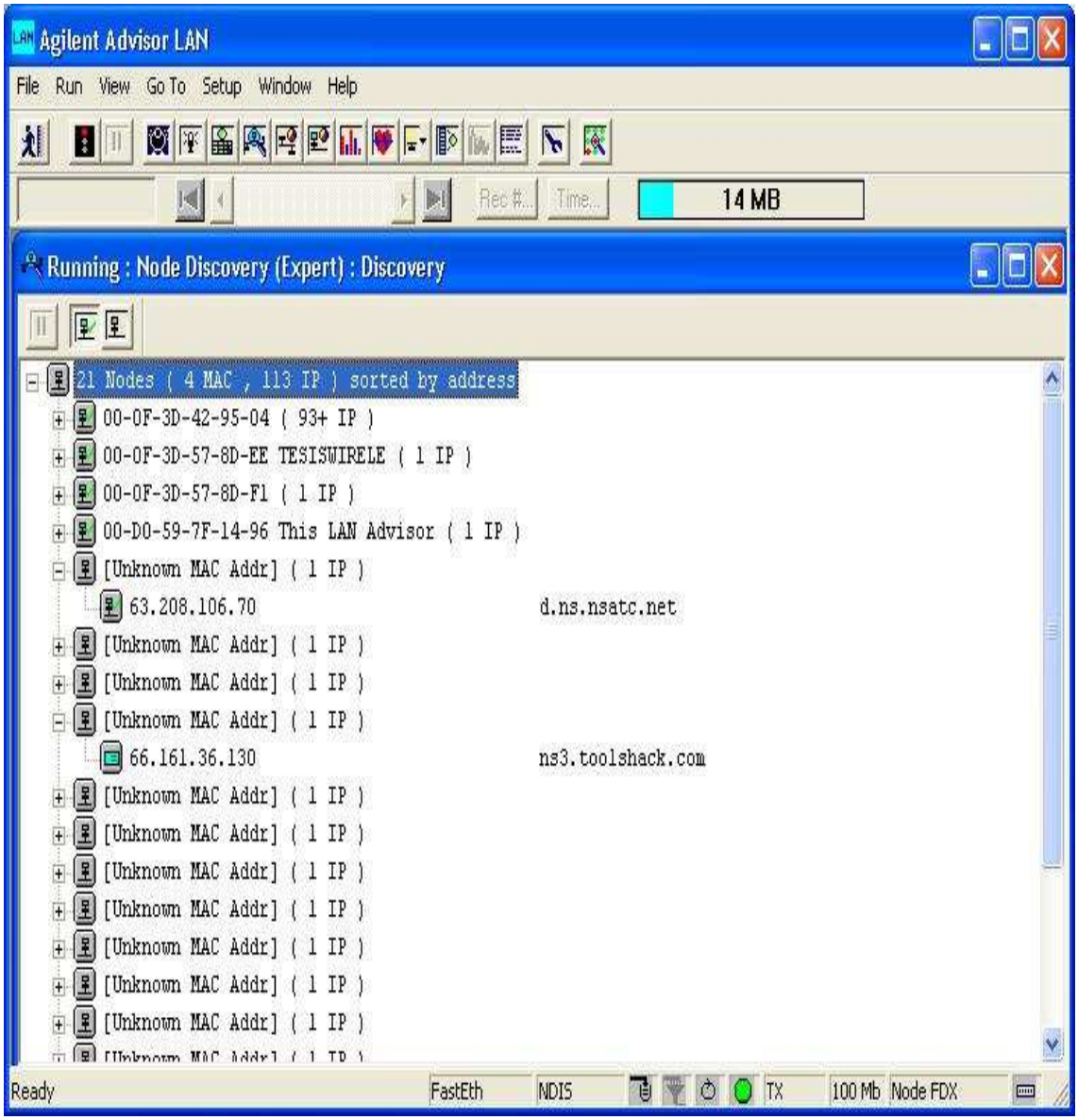
A Alarma

W Precaución

N Normal



Observamos el análisis del MAC Address, estos son detectado por el esnifer en un medio interno y externo. Este es un probable intento de ataque.



4.3 ANÁLISIS DE RESULTADOS

El Análisis de los resultados nos indica que el prototipo básico de red inalámbrico mantiene una seguridad estable y permite el manejo de alertas, y además tomar acciones ante posibles violaciones.

Se maneja un nivel de conexión y seguridad en la red inalámbrica constante, el alcance de los equipos responde a una calidad lineal tomando en cuenta la característica lineal de vista.

Al negar el servicio, se accede a un determinado número de intentos, pero las seguridades implementadas asignan el número máximo a ejecutarse.

Se observo que se trato de violentar el acceso con el simulador utilizado, alterando o destruyendo información, donde las direcciones más visitadas son las del servidor de seguridad y la del router, la red no fue deshabilitada.

Se hizo un resguardo contra el acceso no autorizado, ante posibles intrusiones los dispositivos que conforman la red o a otro componente crítico de la red.

Un sistema de seguridad diseñado para evitar accesos no autorizados es mediante el uso de Firewalls para el prototipo. Todos los mensajes que dejan o entran a la red pasan a través del firewall, permite tomar alternativas de seguridad como el de bloquear aquellos que no cumplan con determinado aspecto de seguridad que se ha configurado tales como:

- El filtrado de paquetes es efectivo y transparente a los usuarios.
- Aplica mecanismos de seguridad a aplicaciones específicas como FTP y Telnet.
- Aplica mecanismos de seguridad cuando una conexión TCP es establecida. Una vez establecida los paquetes circulan sin más inspección.
- Filtro de paquetes que filtra el tráfico basándose en la dirección destino y fuente.

Se protegió la información contra la lectura no autorizada, explícitamente contra la modificación sin el permiso. Se comprobó que los datos no fueron modificados durante su transferencia.

El sistema fue constante como de la forma esperada, el controlar el uso de los recursos es el optimó se pudo terminar qué es lo que sucede en el prototipo básico de red.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

- Las redes inalámbricas sin seguridades son vulnerables, todo el tráfico puede ser desencriptado fácilmente, cualquier persona puede unirse a la red inalámbrica cuando quiera, modificar y reenviar el tráfico. Hoy en día las redes Wireless se están implantando en muchas empresas, esta tecnología está ahora en fase de crecimiento y va evolucionando cada vez más rápido. La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite, sin embargo, una gran cantidad de redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

- Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), de si es una red ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores. La restricción de acceso mediante direcciones MAC es insuficiente para cualquier red, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta cualquiera.

- El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

- El uso de las VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

- La alternativa de 802.1x y EAP es la adecuada si los equipos de la red inalámbrica se pueden actualizar, o si se va a montar una red nueva. Puede usarse la solución de WEP con clave dinámica, o la de WPA; ambas ofrecen un excelente grado de protección.

- Todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa.

- Bluetooth es una norma abierta para una tecnología de punta que posibilita la conexión inalámbrica de corto alcance de voz y datos entre computadoras de escritorio y portátiles, agendas digitales personales, teléfonos móviles, impresoras, escáneres, cámaras digitales e incluso dispositivos de casa, a través de una banda disponible a nivel global (2,4 GHz) y mundialmente compatible. En otras palabras, Bluetooth desenchufa tus periféricos digitales y convierte a la atadura de los cables en cosa del pasado.

- Las redes inalámbricas pueden tener mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en la industria, esta tecnología puede ser utilizada junto con los lectores ópticos.

- El uso de las redes se ha extendido por todas partes de forma notoria, lo que no carece de fundamento: son eficaces (todos los usuarios conectados utilizan los mismos datos), ahorran dinero (se utiliza la misma impresora) y ofrecen diversión (las redes locales son ampliamente utilizadas para juegos).

- La instalación de una red inalámbrica puede ser una de las tareas más simples a nivel administrativo debido a la gran facilidad de configuración, lo cual no implica que sea inmediatamente segura. Cuando se instala una red inalámbrica se deben considerar que es una red completamente abierta desde el punto de vista físico, las consideraciones lógicas y de seguridad comienzan a ser un punto crítico en toda la comunicación.

- Las consideraciones de seguridad comienzan por la estructura misma de la red. Y los accesos que va a tener un dispositivo conectado a la misma, esto es debido principalmente a que si se compromete el punto de acceso, por alguna causa, pues esto seria devastador. Por lo que los usuarios con accesos a la red inalámbrica deberán tener un perfil diferente a los usuarios tradicionales, para los usuarios que utilizan ambas redes se recomienda crear un doble perfil que les permita acceder a su información en ambas formas, de manera segura.

- Los usuarios de la red inalámbrica no deben compartir desde ningún punto de vista recursos con usuarios tradicionales sin clave, es decir todo recurso que se alcance desde la red inalámbrica debe estar protegido por clave y debe limitarse al mínimo la interacción con el sistema de este.

- Activar el control de acceso por medio de las dirección MAC (Media Access Card) es una de las estrategias mas usadas en las redes inalámbricas de hoy debido a que todos los fabricantes de dispositivos nuevos y antiguos soportan esta característica, con esta activación se garantiza que la red esta asegurada de intrusos que puedan estar rastreando el acceso con fines desconocidos.

- Activar la característica de WEP aunque no ofrece gran seguridad desde el punto de vista criptográfico, si puede prevenir bastantes tipos de intrusiones básicas. La seguridad esta dada por el algoritmo de tipo RC4.

- La encriptación puede ser tan buena únicamente como la llave que se le suministre, es decir la clave que se le coloque, si se desea una seguridad mas alta se debe colocar una clave que no sea tan fácil de adivinar.

- Es recomendable usar el máximo de seguridad disponible en la red para encriptación, en la mayoría de los casos es de 128 bits.

- Cambiar de manera periódica la clave del sistema.

- No permitir que se administre el dispositivo de acceso o (Wireless Access Point o WAP) vía inalámbrica, esto puede ser catastrófico para la red pues si un intruso logra acceso a la interfaz de administración puede tener acceso a toda la red.

- Cambiar el password predeterminado del dispositivo.

- Si se desea mantener los datos de manera muy confidencial se debe activar el modo de VPN en la red es la mejor forma de hacer la red inalámbrica mas segura.

- A pesar de las ventajas de trabajar con la red inalámbrica, las WLANs son vulnerables a las amenazas de seguridad. Las amenazas comunes incluyen eavesdropper, el acceso desautorizado, la interferencia y bloqueo, y el daño físico. Dependiendo cómo un WLAN se diseña o se configura, pueden prevenirse tales amenazas o pueden mitigarse. Por ejemplo, sistemas que usan la tecnología del Spread-Spectrum son resistentes al eavesdropping pasivo e interferencia. Sistemas que usan el algoritmo de encriptación WEP son resistentes al eavesdropping activo y proporcionan

la autenticación del cliente. Si WEP es empleada, de cualquier modo, deben tomarse las medidas para asegurar que las llaves de encriptación sean manejadas apropiadamente. Finalmente los componentes físicos de una WLAN pueden ser protegidos de daños físicos con la instalación de salvaguardas físicas y proporcionando entrenamiento a los usuarios.

REFERENCIAS BIBLIOGRAFICAS

Ref [1] Red de Area Local Inalámbrica (WLAN),
Wireless Security, Randall K. Nichols, Panos C. Lekkas, 2003

Ref [2] Redes Inalámbricas,
http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

Ref [3] Red de Area Local Inalámbrica (WLAN),
Wireless Security, Randall K. Nichols, Panos C. Lekkas, 2003

Ref [4] Redes Inalámbricas,
http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

Ref [5] Bluetooth,
Wireless Security, Randall K. Nichols, Panos C. Lekkas, 2003

Ref [6] Que es Bluetooth,
http://www.zonabluetooth.com/que_es_bluetooth.htm

Ref [7] Redes Inalámbricas,
http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

Ref [8] Seguridad en Redes Inalámbricas,
http://www.zonagratuita.com/servicios/seguridad/wireles.html

Ref [9] Red de Area Local Inalámbrica (WLAN),
Wireless Security, Randall K. Nichols, Panos C. Lekkas, 2003

Ref [10] Redes Inalámbricas-Siete Problemas Típicos de Seguridad y Soluciones Recomendadas, www.totenguard.com

Ref [11] Control de Acceso
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

Ref [12] Seguridad en Redes Inalámbricas,
http://www.zonagratuita.com/servicios/seguridad/wireles.html

Ref [13] Preguntas Frecuentes: Tecnología Bluetooth

Ref [14] (In) seguridad en redes 802.11b,
http://www.matarowireless.net

Ref [15] Diferencias principales entre WiFi y Bluetoth,
http://www.paradigma.cl/ordenadorbt/diferencias/diferencias.html

LISTADO DE FIGURAS

http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

Fig. 12. Fase de Autorización
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

Fig. 13. Fase de distribución de claves y parámetros
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

Fig14. Obtención de la clave WEP
http://skywalker.dif.um.es/~lolo/ficheros/XIV_jornadas.pdf

Fig. 15 Introducción a las WLAN, José Manuel Huidrobro

Fig. 16 Topología Modo Ad-Hoc,,
http://www.matarowireless.net

Fig. 17 Topología Modo Infraestructura,,
http://www.matarowireless.net

Fig. 18 Proceso para Generar Llaves,
http://www.matarowireless.net

Fig. 19 Valor de Chequeo de Integridad,
http://www.matarowireless.net

Fig.20 Selección de llave de 40 bits,
http://www.matarowireless.net

Fig.21 Vector de Inicialización,
http://www.matarowireless.net

Fig.22 Aplicación del algoritmo RC4 al conjunto IV + Key,
http://www.matarowireless.net

Fig.34 Ataque Inductivo Arbaugh,
http://www.matarowireless.net

Fig.35 WLAN antes del Ataque,
http://www.matarowireless.net

Fig.36 WLAN después del Ataque,
http://www.matarowireless.net

Fig.37 Comunicación sin Ataque,
http://www.matarowireless.net

Fig.36 Comunicación después Ataque,
http://www.matarowireless.net

ANEXO 1

MANUAL DE CONFIGURACIÓN DEL WIRELESS ROUTER DI-624+

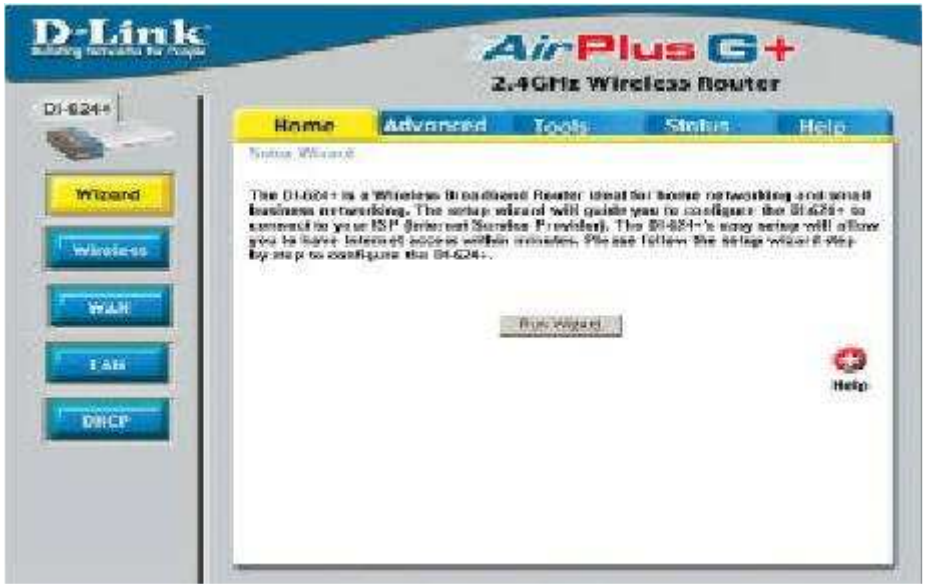
Siempre que se quiera configurar la red o la DI-624+, se debe acceder a la configuración del menú abriendo el web-browser y tipeando la dirección IP de la DI-624+.

Tipee **admin** user name fail.

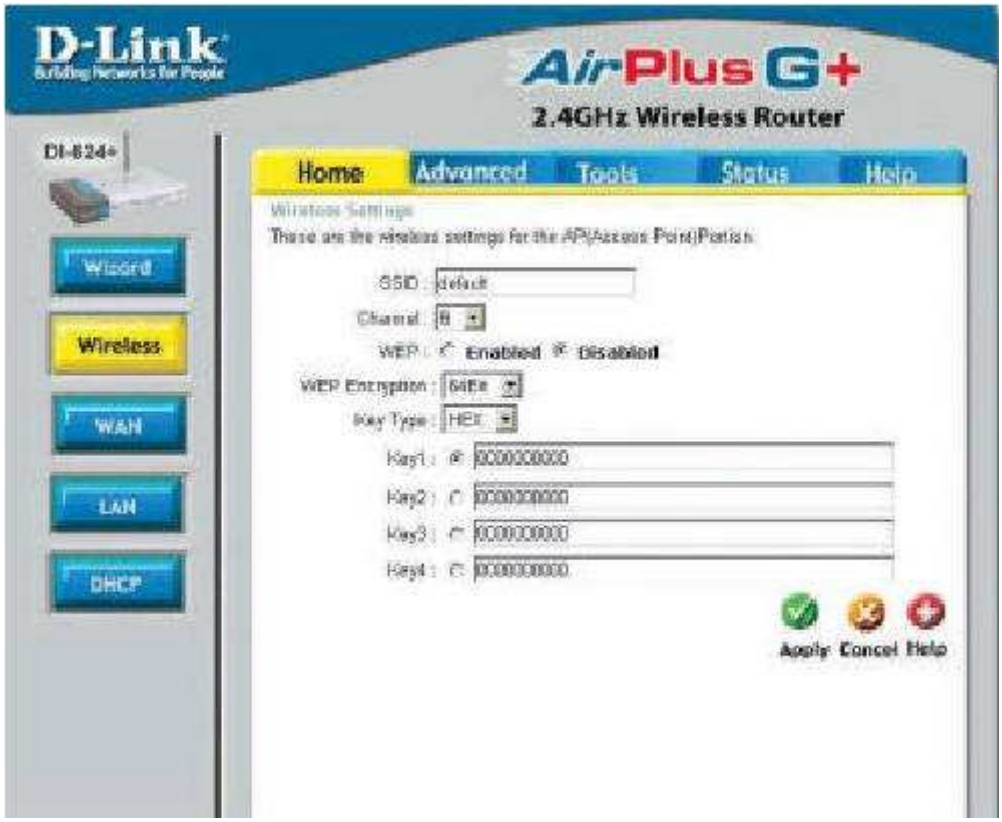
Home

Home > Wizard

En la pantalla aparece Home > Wizard.



Home > Wireless



SSID: Service Set Identifier es el nombre designado para la especificación WLAN.

Channel: El canal por default es 6. Todos los dispositivos de la red pueden compartir el mismo canal.

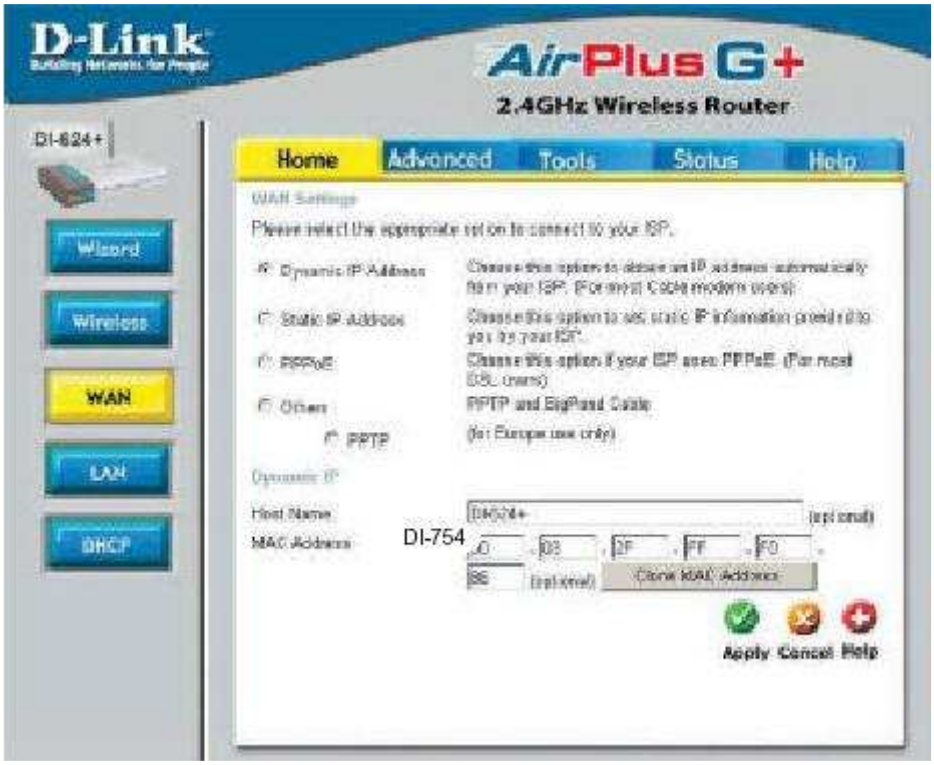
WEP: Wired Equivalent Privacy (WEP) es un protocolo de seguridad inalámbrico para redes de área local inalámbrica (WLAN). WEP provee seguridad para encriptación de datos que son enviados a través de la WLAN. Seleccionar **Enabled** o **Disabled. Disabled** es el seteo por default.

WEP Encryption: Seleccionar el nivel de encriptación deseado: 64-bit, o 128-bit.

Key Type: Seleccionar **HEX** o **ASCII**

Keys 1-4: La entrada sobre cuatro teclas WEP, seleccione una que desee usar.

Home > WAN > Dynamic IP Address



Dynamic IP Adress: Escoja Dynamic Ip Adress para obtener información de la dirección IP automáticamente del ISP. Seleccionar esta opción si el ISP no da ningún número IP para uso. Esta función es comúnmente usada para servicio de cable moden.

Host Name: El Host Name es opcional pero puede ser requerido algún ISP. Por default el host name es el nombre del dispositivo router y puede ser cambiado.

MAC Address: Por default la dirección MAC esta seteado a la dirección MAC de la interface física de la WLAN en el ruteador de banda ancha. No es recomendable que se cambie el la dirección MAC a pesar de ser requerido por su ISP.

Clone MAC Address: Por default la dirección MAC es seteada para la interface física de la WLAN.

Primary/Secondary DNS Address: Ingresar una dirección DNS si no se desea usar una proveída por el ISP.

MTU: Ingresar un valor de MTU solo si es requerido por el ISP. De otra forma dejarlo en el seteo por default.

Home > WAN > Static IP Address

Static IP Address: Escoger una dirección IP estática si toda la información IP de la WAM es proveída por el ISP. Se necesitara ingresar en la dirección IP, mascara de la subred, dirección gateway, y dirección DNS proveída por el ISP. Cada dirección IP ingresada en el archivo debe estar en la forma apropiada la cual es, cuatro octetos separados por un punto. El router no aceptara la dirección IP si esta no esta en este formato.

IP Address: Ingresar la dirección IP pública proveída por el ISP.

Subnet Mask: Ingresar la mascara de la subred. (Todos los dispositivos en la red pueden tener la misma mascara de la subred.)

ISP GAteway Address: Ingresar la dirección IP publica del ISP al que esta conectada.

Primary DNS Address: Ingresar el DNS primario (Domain Name Server) dirección IP proveída por el ISP.

Secundary DNS Address: Este es opcional.

MTU: Ingresar el valor del MTU solo si es requerido por el ISP. De otra manera dejarlo en el seteo por default.

Home > WAN > PPPoE

Se escoge PPPoE (Point to Point Protocol over Ethernet) si el ISP usa una conexión PPPoE. El ISP proveerá un nombre de usuario y clave. Esta opción es típicamente usada por los servicios DSL. Seleccione la PPPoE dinámica para obtener su conexión PPPoE. Seleccione la PPPoE estática para usar una dirección IP estática para su conexión PPPoE.

PPPoE: Escoger esta opción si el ISP usa PPPoE.
Dynamic PPPoE- recibe una dirección IP automáticamente desde el ISP.
Static PPPoE - Tiene asignada una dirección IP estática.

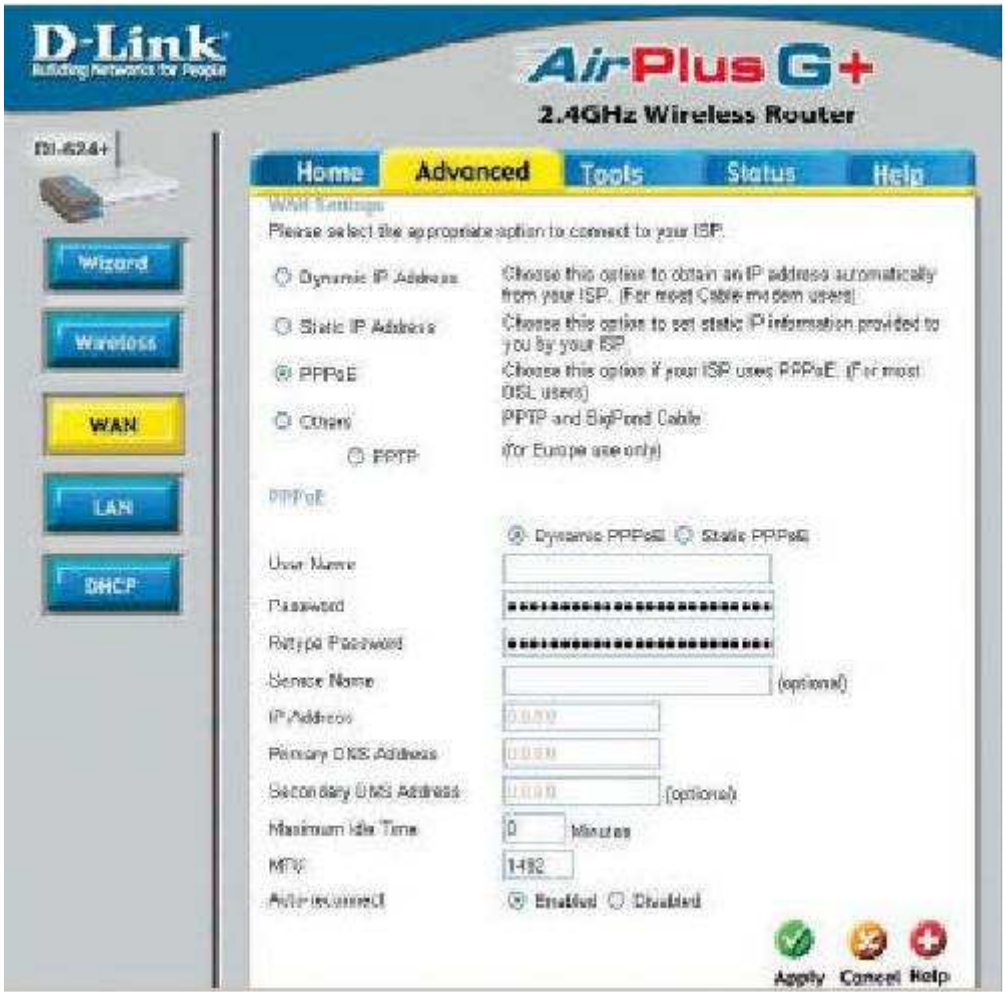
User Name: El user name proveído por el ISP

Retype Password: Re ingrese el password PPPoE

Service Name: Ingrese el Nombre de Servicio proveído por el ISP (opcional).

IP Address: Esta opción solo esta disponible para PPPoE estática. Ingrese la dirección IP estática de la conexión PPPoE.

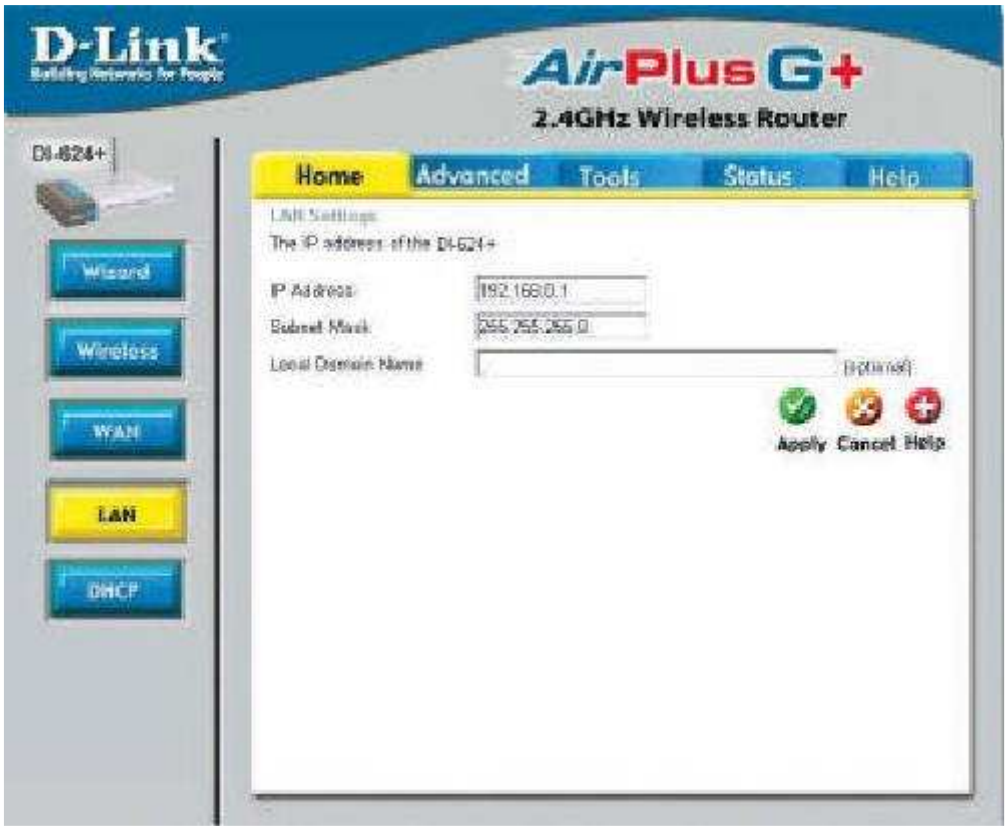
Primary DNS Address: Dirección IP del DNS primario proveída por el ISP



MTU: Unidad de Transmisión Máxima-1492 es el seteo por default Se puede cambiar el MTU para un optimo rendimiento con su especifico ISP.

Auto-reconnect: Si habilita la DI-624+ automáticamente se conectara a su ISP luego su sistema se restablecerá o si la conexión PPPoE es interrumpida,

Home > LAN



La LAN es corta para la red de área local. Esta está considerad para su red interna. Estos son los seteos IP de la interface LAN para la DI-624+.Estos seteos pueden ser referidos como seteos privados. Se puede cambiar la dirección de la LAN IP si es necesario. La dirección IP LAN es privada a la red interna y no puede ser vista en el Internet.

IP Address: La dirección IP de la interface LAN. Por default la dirección IP es: **192.168.0.1**

Subnet Mask: La mascara de la subred de la interface LAN. Por default la dirección IP es: **225.225.225.0**

Local Domain: Este archivo es opcional. Ingresar el nombre del dominio local.

Home > DHCP

Los soportes DHCP para Dynamic Host Control Protocol. La DI-624+ tiene un servidor construido en la DHCP. El servidor DHCP automáticamente asignara una dirección IP a los computadores la red LAN / privada. Asegurese setear los computadores para los clientes DHCP seteando los seteos TCP / IP para obtener un direccionamiento automático IP.

DHCP Server: Seleccionar **Enabled** o **Disabled.** Por defecto esta seteado **Enabled**.

Starting IP Address: La dirección IP de inicio para la asignación IP del servidor DHCP.

Ending IP Address: La dirección IP final para la asignación IP del servidor DHCP.

Lease Time: La longitud lease time para el IP lease. Ingrese el tiempo. Seteo por default es una hora.

Advanced

Advanced > Virtual Server

EL DI-624+ puede ser configurado como un servidor virtual de manera que los usuarios remotos accedan a la Web, a los servicios FTP a través de la dirección IP publica que puede ser automáticamente redireccionada hacia los servidores locales en la LAN.

Las características Firewall de la DI-624+ filtran paquetes no reconocidos para proteger su red LAN de manera que todos los computadores en red con la DI-624+ son invisibles al mundo exterior.

Virtual Server: Seleccionar **Enabled** o **Disabled**

Name: Ingresar el nombre referido al servicio virtual

Private IP: El servidor en la LAN que será el proveedor de los servicios virtuales.

Protocol Type: Protocolo usado por el servicio virtual

Private Port: Número de puerto del servicio usado por el computador privado IP

Public Port: El número del puerto en el lado de la WAN será usado para acceder al servicio virtual.

Schcrdule: La programación de tiempo cuando el servicio virtual sea habilitado. La programación puede ser seteada **Always**, lo cual permitirá al servicio particular siempre ser habilitado. Si se setea a **Time** selecciona el cuadro de tiempo para el servicio a ser habilitado.

Advanced > Applications

Algunas aplicaciones requieren múltiples conexiones, estas aplicaciones tiene dificultad para trabajar a través de la NAT aplicaciones especiales hacen que algunas de estas aplicaciones trabajen con la DI-624+

Name: Este es el nombre que se refiere a la aplicación especial

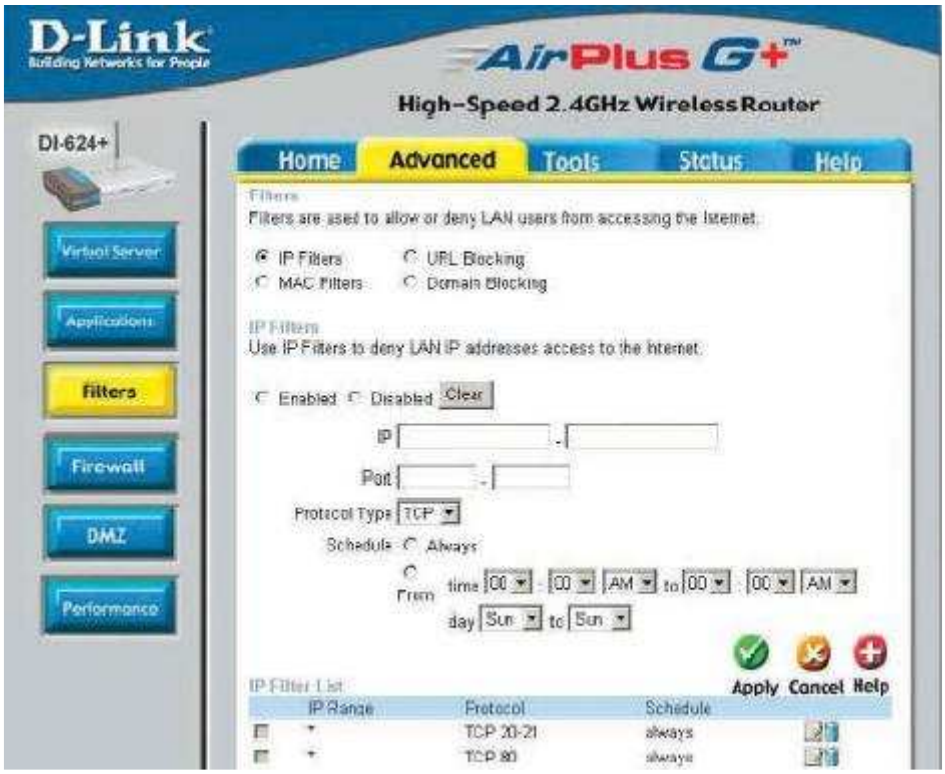
Trigger Port: Puerto usado para disparar la aplicación puede ser bien un puerto simple o un rango de puertos

Trigger Type: Protocolo usado para dispara una aplicación especial.

Public Port: Número de puerto en el lado de la WAN que será usado para acceder a la aplicación. Se puede definir un puerto único o un rango de puertos.

Public Type: Protocolo usado para la aplicación especial.

Advanced > Filters > IP Filters



Los Filtros son usados para negar o permitir a los computadores de la LAN acceso al Internet. La DI-624+ puede ser seteado para denegar a los computadores internos por sus direccionamientos IP o MAC.

IP Filters: Usar los filtros IP para negar las direcciones LA IP del acceso del Internet. Se puede negar números de puertos específicos o todos los puertos para la dirección IP específica.

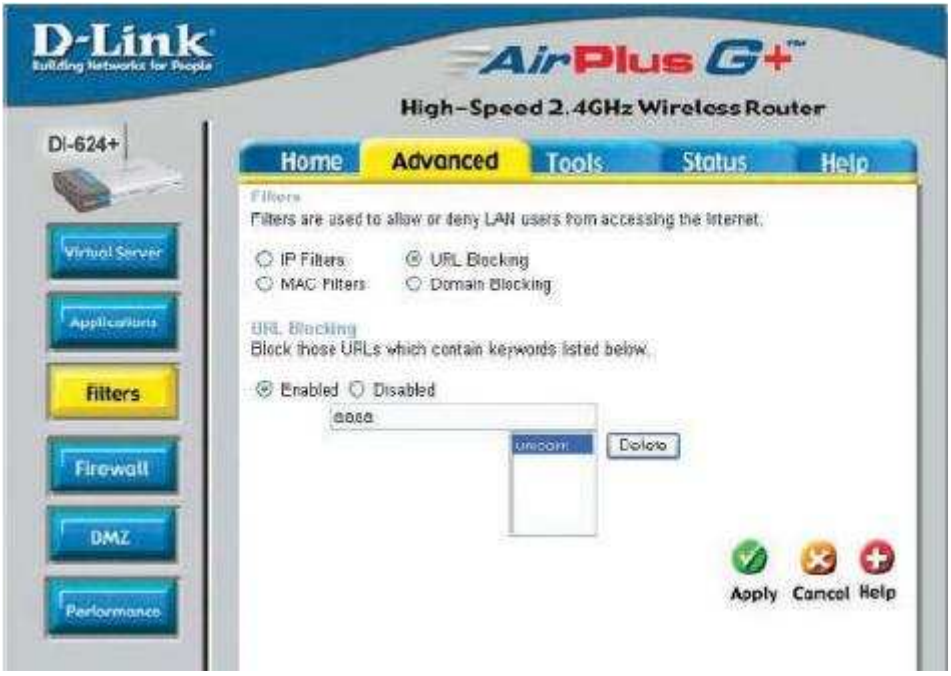
IP: Dirección IP del computador LAN que negara el acceso al Internet.

Port: Puerto único o rango de puertos que negara el acceso al Internet.

Protocol Type: Seleccionar el tipo de protocolo

Schedule: Es la programación de tiempo cuando el filtro IP sea habilitado.

Advanced > Filters > URL Blocking



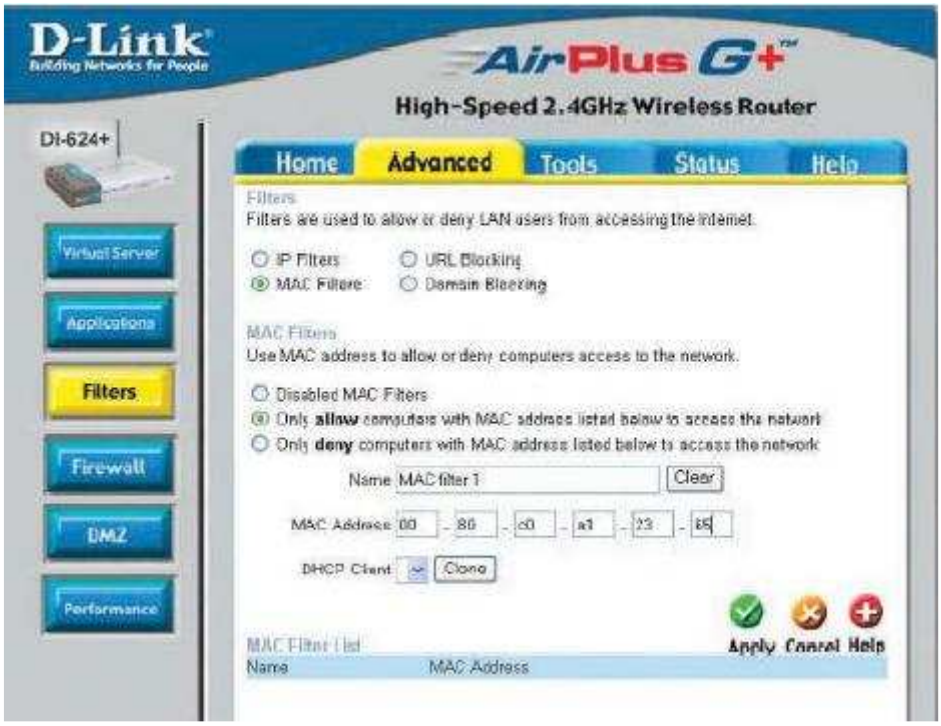
URL Blocking es usado para negar a los computadores del acceso de los sitios Web específicos por la URL. Una URL es una cuerda de texto formateado específicamente que define un lugar en el Internet.

Filters: Seleccionar el filtro que se desea usar en este caso el URL Blocking fue escogido

URL Blocking: Seleccionar **Enabled** o **Disabled**

Keywords: Los Bloques URLs los cuales contiene Keywords listados abajo. Ingrese el Keywords en el espacio.

Advanced > Filters > MAC Filters



Usar MAC (Media Access Control) Filters par permitir o negar a los computadores LAN por sus direcciones MAC del acceso a la red. Se puede manualmente añadir una dirección MAC o seleccionar la dirección MAC de la lista de clientes que son corrientemente conectados al servidor de banda ancha.

Filters: Seleccionar el filtro que se desee usar, en este caso **MAC filters** fueron escogidos.

MAC Filters: Escojer los filtros MAC **Disable**; direciones MAC **allow** listadas abajo o las direcciones MAC **deny** listadas abajo.

Name: Ingresar aquí el nombre

MAC Address: Ingresar la dirección MAC

DHCP Client: Seleccione un cliente DHCP de la lista. Haga click en **Clone** para copiar esa dirección MAC

Advanced > Filters > Domain Blocking

Domain Blocking es usado para permitir o negar a los computadores LAN del acceso de los dominios específicos en el Internet. El bloqueo del dominio negara todas las requisiciones a un dominio específico como la http y ftp. También puede permitir a los computadores acceder a sitios específicos y negar todos los otros sitios.

Filters: Seleccionar el filtro que desea usar, en este caso **Domain Blocking** fue escogido.

Domain Blocking:

Disabled: Seleccionar **Disabled** para desabilitar **Domain Blocking**

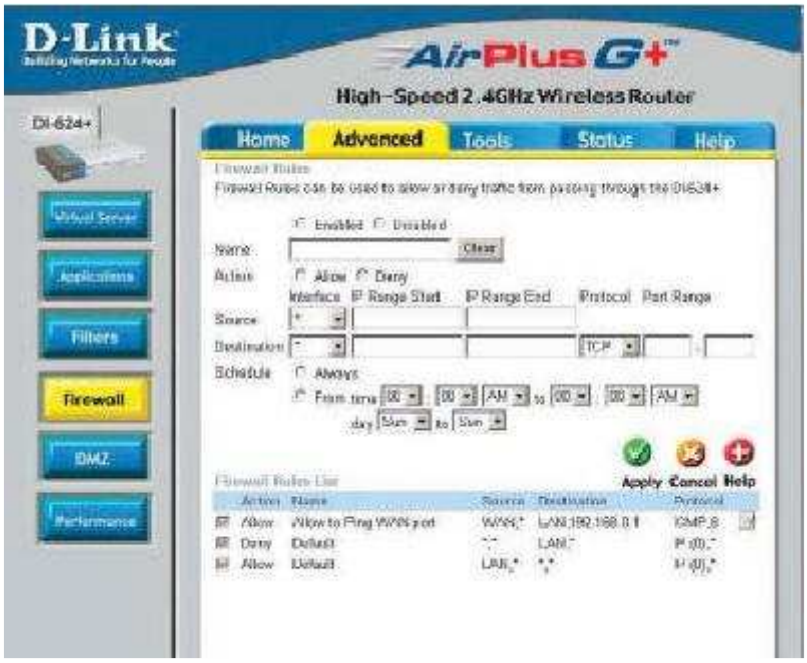
Allow: Permite a los usuarios acceder a todos los dominios excepto a los dominios bloqueados.

Deny: Niega a los usuarios el acceso a todos los dominios excepto los dominios permitidos

Permitted Domains: Ingresar el dominio permitido en este campo

Blocked Domains: Ingresar el dominio bloqueado en este campo

Advanced > Firewall



Firewall Rules es una característica avanzada usada para negar o permitir el tráfico de paso a través de La DI-624+. Trabaja de la misma forma como los filtros IP con seteos adicionales.

Firewall Rules:	**Enabed** o **Desabled** el Firewall
Name:	Ingresar el nombre
Action:	**Allow** o **Deny**
Source:	Ingresar el rango de la dirección IP
Destination:	Ingresar el rango de dirección IP; el protocolo y el rango de puerto
Schedule:	Seleccionar **Allways** o ingresar el **Time range**

Advanced > DMZ

Si se tiene un cliente PC que no puede correr las aplicaciones IP apropiadamente de la parte de atrás de la DI-624+ , entonces se puede poner al cliente arriba para accesos de a Internet no restringidos.

DMZ: **Enabled** o **Disable** la DMZ. La DMZ permite a un computador único estar expuesto al Internet. Por default la DMZ es **disabled.**

IP Address: Ingresar la dirección IP de la computadora para estar en la DMZ.

Advanced > Performance

En esta ventana se muestran las características de rendimiento inalámbrico por el punto de acceso parcial de la DI-624+.

Beacon Interval: Beacons son paquetes enviados por un Acces Point para sincronizar una red inalámbrica. Especifica un valor. 100 es el valor por default y es el recomendado.

RTS Threshold: Este valor podría recordar a su seteo default de la 2432. Si el flujo de datos inconsistente es un problema solo una modificación menor podría ser hecha.

Fragmentación: El lumbral de fragmentación, el cual es especificado en bytes determina que paquetes serán fragmentados.

DTIM interval: 3 es un seteo por default, Una DTIM es una información de cuenta regresiva de clientes de la siguiente ventana para escuchar la transmisión y los mensajes multicast

Preamble Type: Seleccionar **Short** o **Long Preamble**, el preamble define la extensión de la longitud del bloque CRC para la comunicación entre los ruteadores inalámbricos y los adaptadores de red de roamming inalámbricos.

SSID Broadcast: Elegir **Enbled** para transmitir la SSID a través de la red todos los dispositivos en una red deben compartir la misma SSID para establecer una comunicación. Elija **Disabled** si no desea transmitir la SSID sobre la red.

802.11g only mode: Seleccionar este modo para restringir la red hacia únicamente esos dispositivos que emplean los estándares de la 802.11g. Habilitando este modo se asegura tener la mas alta velocidad de conectividad.

CTS Mode: CTS (Clear To Send) es una función usada para minimizar colisiones entre dispositivos inalámbricos en una LAN inalámbrica. La CTS nos asegurara que la red inalámbrica esta limpia antes de que un cliente intente enviar datos inalámbricos. Habilitando el CTS

Super G Mode: Es un grupo de características de alto rendimiento que incrementa las aplicaciones finales de usuario en una red 802.11g.

Tools

Tools > Admin

En esta pagina el administrador DI-624+ puede cambiar el sistema de clave. Hay dos cantidades que pueden acceder a la interface de manejo WEP del ruteador de banda ancha ellos son admin y user. Admin tiene lectura/escritura de acceso mientras el user tiene únicamente lectura de acceso. El user solo puede ver los seteos pero no puede hacer ningún cambio.

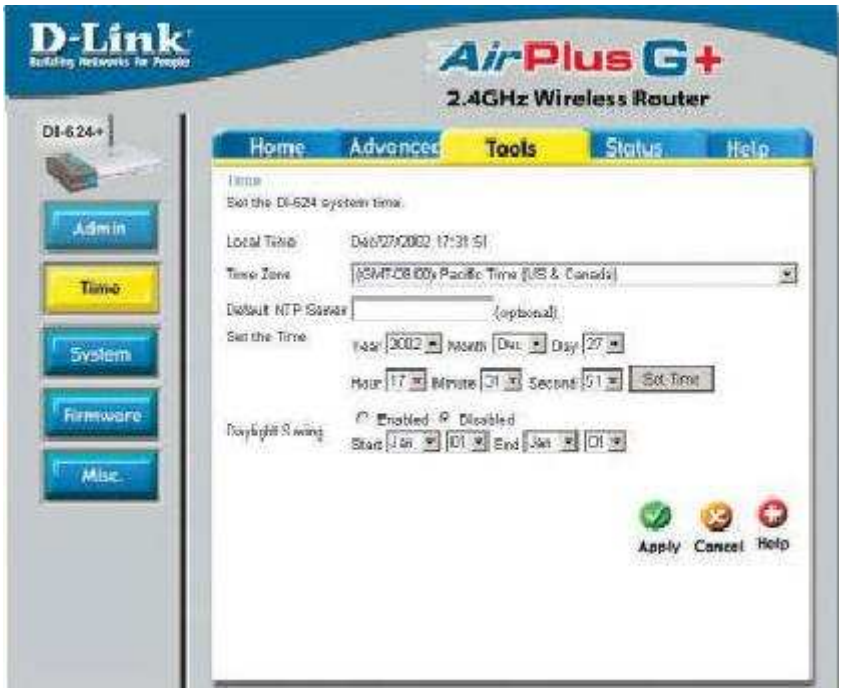
Administrator: **admin** es el login name del administrador

Password: Ingresar la clave para luego ser confirmada

User: **user** es el login name del usuario

Password: Ingresar la clave para luego ser confirmada

Tools > Time



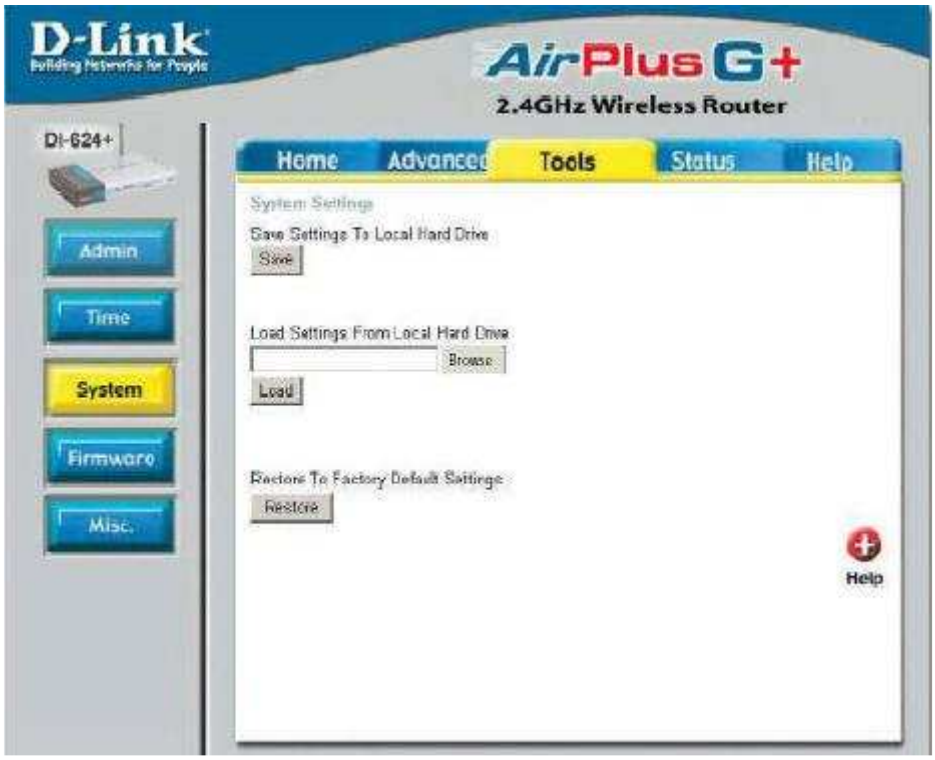
Time Zone: Seleccionar la zona de tiempo

Default NTP Server: NTP es el nombre corto para Network Time Protocol. NTP sincroniza el reloj de la computadora en una red de computadoras. Esto es opcional.

Set the Time: Ingresar manualmente en esta archivo los valores para año, mes, día, hora, minuto y segundo. Hacer Click en **Set Time**.

Daylight Saving: Para seleccionar manualmente el tiempo de ahorro de luz del día, seleccione **enabled** o **disabled**, y ingrese una fecha de inicio y una fecha final para tiempo de ahorro de luz del día.

Tools > System



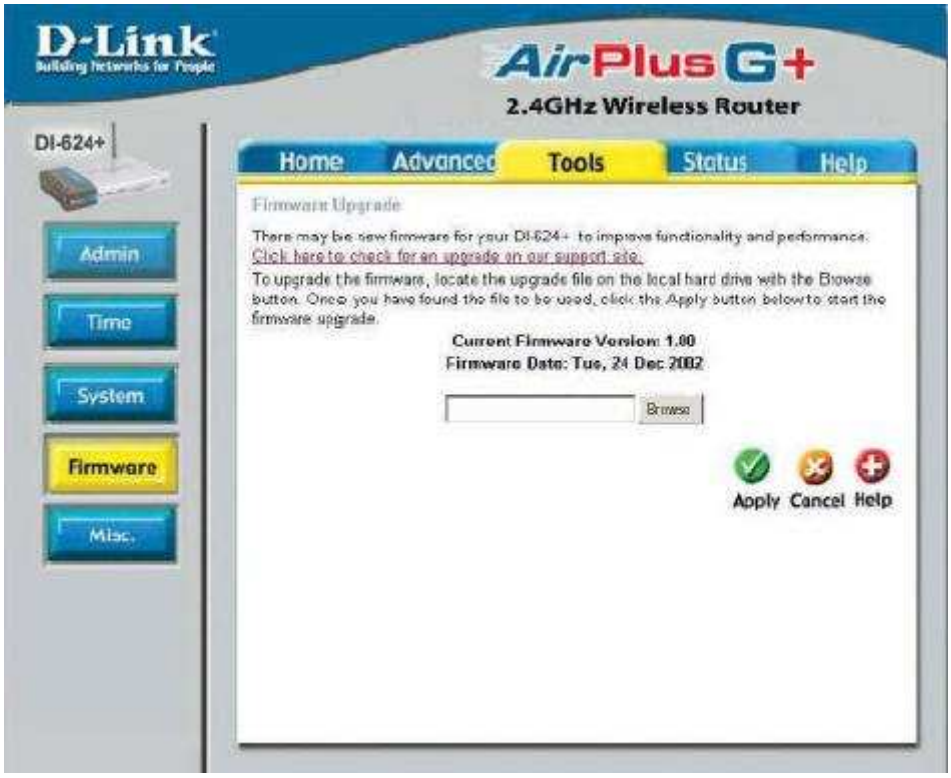
Los seteos del sistema actual pueden ser guardados como un archivo en el disco duro local. El archivo guardado o cualquier otro archivo de seteo guardado puede ser cargado de vuelta en el ruteador de banda ancha.

Save Settings to Local Hard Drive: Click **Save** para guardar el seteo actual en el disco duro local.

Load Settings from Local Hard adrive: Click en el **Browse** para encontrar el seteo, luego click en **Load**.

Restore to Factory Default Settings: Click en **Restoren** para recuperar el seteo por default.

Tools > Firmware

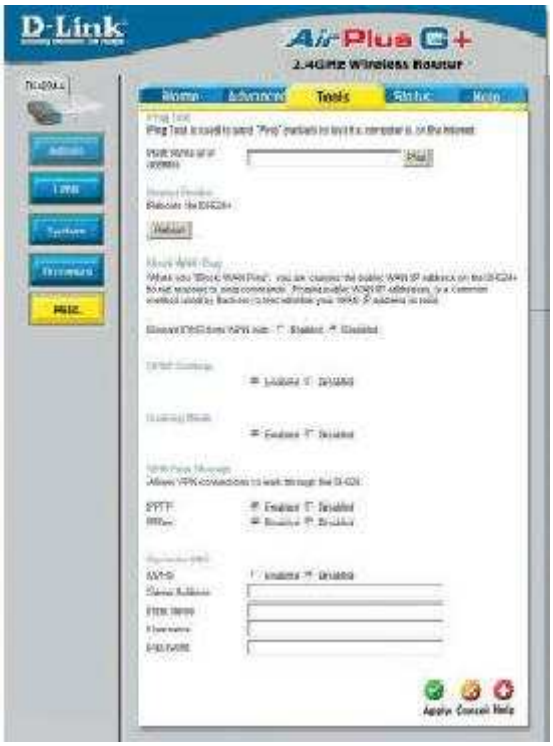


Aquí se puede mejorar el Firmware del ruteador. Asegurarse que el firmware que hay que usar este en el disco duro local del computador. Hagaclick en Browse para explorar el disco duro local y localizar el firmware a se usado por una fecha posterior.

Firmware Upgrade: Hacer click en el enlace de esta pantalla para encontrar si hay un firmware de fecha posterior.

Browse: Después de que ha descargado el nuevo firmware, Haga click en Browse en esta ventana para localizar el firmware de fecha superior en su disco duro. Haga click en Apply para completar el firmware superior.

Tools > Misc



Ping test: El Ping Test es usado para enviar paquetes Ping para probar si un computador esta en el Internet. Ingresar la dirección IP que desea hacer ping y hacer click en **Ping**.

Restar Device: Hacer click en **Reboot** para recetear la DI-624+

Block WAN Ping: Si escoge bloquear WAN pin: la dirección WAN IP de la DI-624+ no responderá a los pings. Bloquear el ping puede generar una s seguridades extras de las hackers

UPNP: Para usar las características del Universal Plug and Play hacer click en **Enabled**.

Gaming Mode: El modo gaming permite una forma de paso _ a través para ciertos juegos de internet.

Dynamic DNS: Dinamic Domain Name System es un método de almacenamiento de un nombre de dominio enlazado a una dirección de cambio IP esto es una carteristica muy útil desde

que muchos computadores no usaban una dirección estática IP

VPN Pass Through: La DI-624+ soporta VPN (Virtual Private Network) paso a traves para ambos PPTP y IPSec. Una vez que la VPN es habilitada, no necesita abrir un servicio virtuale.

Status

Status > Device Info

Aquí se muestra la información actual para la DI_624^ . Mostrara la información de LAN , WAM y dirección MAC

WAN: IP Address: WAN/Public IP Address
Subnet Mask: WAN/Public Subnet Mask
Gateway: WAN/Public Gateway IP Address
Domain Name Server: WAN/Public DNS IP Address
WAN Status: WAN Connection Status

LAN: IP Address: LAN/Private IP Address of the DI-624+
Subnet Mask: LAN/Private Subnet Mask of the DI-624+

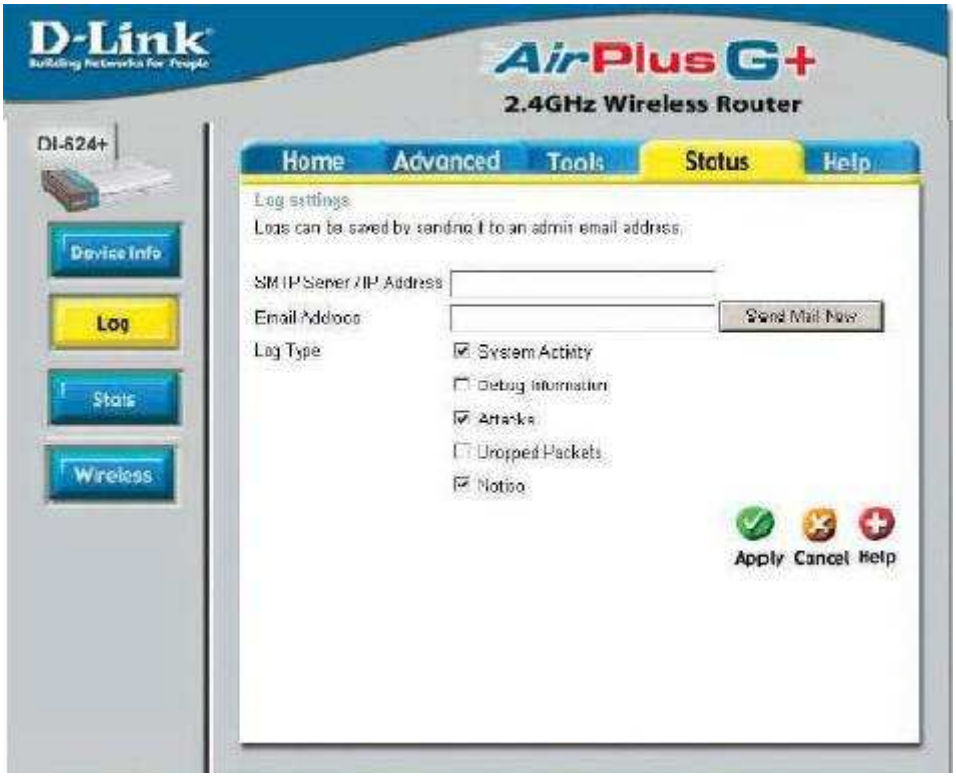
Wireless: MAC Address: Displays the MAC address
SSID: Displays the current SSID
Channel: Displays the current channel
WEP: indicates whether WEP is enabled or disabled

Status > Log

El ruteador de banda ancha guarda un log corrido de eventos y actividades que ocurrieron en el ruteador. Si el dispositivo es rebooted; los log son automáticamente limpiados . Se puede almacenar los archivos log bajo los seteos log.

View Log: **First Page –** Primera pagina del log
Last Page – Ultima pagina del log
Previous – Mueve hacia atrás una pagina log
Next – Mueve hacia adelante una pagina log
Clear – Limpia completamente los logs
Log Settings – Trae la pagina para configurare el log

Status > Log > Log Settings



No solo hace que el ruteador de banda ancha muestre los log de actividades y ventos ; el puede setearlo y enviarlo esos log a otra locacion

SNTP Server / IP Address : La dirección del servidor de SMTP puede ser usado para enviar los logs.

Email Address: La dirección email para lo cual los logs deben ser enviados. Click en **Send Mail Now** para enviar el email.

Status > Stats

Aquí se muestra las estadísticas de tráfico. Se puede ver la cantidad de paquetes que pasan a través de la DI-624+ en los pórticos WAN y Lan. EL contador de trafico se reseteara si el dispositivo es rebooted.

Status > Wireless

La tabla de clientes inalámbrico muestra una lista de los clientes inalámbrico conectados actuales. Esta tabla también muestra el tiempo de conexión y la dirección MAC de los clientes inalámbricos conectados.