REDES INALÁMBRICAS +

Redes con Seguridad Robusta +

Instalación de una red Inalámbrica +

Redes Inalámbricas en Medellín

ALEJANDRO PÉREZ QUINTERO

UNIVERSIDAD EAFIT

DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS

MEDELLÍN

2008

REDES INALÁMBRICAS +

ALEJANDRO PÉREZ QUINTERO

PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE INGENIERO DE SISTEMAS

ASESOR

JUAN GUILLERMO LALINDE PULIDO

DOCTOR EN TELECOMUNICACIONES

UNIVERSIDAD EAFIT

DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS

MEDELLÍN

2008

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

PRESIDENTE DEL JURADO

_____

JURADO

_____

JURADO

Medellín, 30 de Julio del año 2008

DEDICATORIA

A MIS PADRES Y HERMANOS, A DIANA

A TODO AQUEL QUE NO PREGUNTO PARA CUANDO ESTABA LISTA

A LA UNIVERSIDAD, A LOS AMIGOS

A TODOS AQUELLOS DE LOS QUE HE APRENDIDO

AGRADECIMIENTOS

El autor expresa su agradecimiento a todas las personas que de una u otra forma contribuyeron al desarrollo de este proyecto.

Al Doctor Juan Guillermo Lalinde P. por el apoyo, conocimiento, tiempo y paciencia que tuvo durante todo el largo proceso de asesoría en cada uno de los proyectos que fue descartado antes de este.

Al Jurado por su tiempo y constancia en la revisión de este trabajo, así como por las correcciones y sugerencias que realizaron.

A Diana Sandoval, por su comprensión, su incondicionalidad y ser un gran aliciente para la finalización de este proyecto.

A mis padres y hermanos, que nunca perdieron la confianza y siempre me dieron su apoyo.

A mis amigos Jorge Mario y Juan Gonzalo, por ser como son. A Nanda y Dea por su palabras siempre en el momento correcto.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Lista de Imágenes

LISTA DE GRÁFICOS

I PARTE – INTRODUCCIÓN

Esta primera parte, cubre aspectos generales sobre las redes inalámbricas, una definición amplia del concepto de red inalámbrica, ¿cómo funciona una red inalámbrica?, los beneficios que trae esta tecnología, los tipos de redes clasificados según su cobertura y un primer y breve acercamiento a la seguridad de las redes inalámbricas, esta parte fue escrita pensando en que cualquier persona se pueda aproximar al texto y tener una comprensión clara de los conceptos presentados que posteriormente se trataran más profunda y técnicamente.

1. FUNDAMENTOS

El concepto de redes inalámbricas se refiere principalmente a cualquier tipo de red computacional o electrónica que es inalámbrica, comúnmente se asocia con una red de transmisión de datos formada al conectar dos dispositivos sin el uso de cables. Una red inalámbrica se implementa normalmente con algún tipo de mecanismo de transmisión remota de información que usa ondas electromagnéticas, como las ondas de radio.

1.1. ¿CÓMO FUNCIONAN LAS REDES INALÁMBRICAS?

Al igual que en todo sistema de comunicación, se tiene un emisor que transmite, un receptor que recibe, un medio por el que se transmite y un mensaje a transmitir, en todos los casos inalámbricos el medio es el aire, o más exactamente el espectro electromagnético, el mensaje viaja por el aire usando una frecuencia de radio; el emisor y el receptor ya se habrán reconocido previamente, así aunque usen un medio que no es directo, podrán saber que el mensaje que han enviado llegará a su destino y que el mensaje que han recibido estaba destinado para ellos.

En las redes inalámbricas el receptor y el emisor intercambian su papel continuamente, para facilitar la descripción llamemos a uno la estación (EST) y al otro el punto de acceso (PA), en inglés Access Point. Todo el proceso de comunicación comienza cuando la estación envía un mensaje a un punto de acceso especificó indicando que quiere tener una comunicación directa con él o también puede comenzar porque el punto de acceso está programado para periódicamente enviar un mensaje sin destinatario directo indicando que allí está, listo para establecer comunicación cuando sea necesario, si una EST está cerca e interesada en iniciar una comunicación, responderá con un mensaje indicando que se quiere comunicar con ese PA.

Luego de este primer mensaje donde se solicita el inicio de la comunicación, la EST y el PA establecen una comunicación usando protocolos preestablecidos, donde se identifican, así a pesar de usar un

medio abierto para enviar sus mensajes, tienen la seguridad[1] de tener un canal de comunicación solo para los dos.

1.2. ¿POR QUÉ INSTALAR UNA RED INALÁMBRICA?

La principal razón para instalar una red inalámbrica es la conveniencia, la naturaleza inalámbrica de la red permite a los usuarios acceder los recursos de red que necesite desde casi cualquier locación que se encuentre dentro del radio de cobertura de la misma. Esto aplica para los teléfonos inalámbricos, para los controles remotos que se usan a diario, para los dispositivos que se conectan por Bluetooth o para el acto de conectarse a internet desde un computador portátil o un asistente personal (PDA). Qué gran inconveniente existiría si todas esas conexiones inalámbricas que se acaban de nombrar, solo pudiera realizarse con cables, habría que tener a disposición siempre una docena de cables y adaptadores para realizar tareas que se pueden realizar usando el espectro electromagnético, con ondas de radio, microondas, infrarrojo u ondas en otras frecuencias igual de útiles. Lo mejor de toda esta movilidad es que se puede obtener sin sacrificar la tasa de transferencia ni la funcionalidad en la mayoría de los casos.

Otra ventaja que se desprende de la anterior, es la facilidad de instalación, al no tener que mover o agregar cables en paredes o techos o en esa masa de cables llenos de polvo que muchas veces se encuentra en la parte posterior de los computadores. Incluso en algunas edificaciones preservadas por su valor histórico es obligatorio el uso de redes inalámbricas ya que no se puede modificar ningún aspecto de la construcción. A la facilidad de instalación se suma el que ahora la mayoría de computadores que se consiguen en el mercado ya vienen equipados con toda la tecnología inalámbrica necesaria e incluso los proveedores de internet, ofrecen los PA en sus planes de servicio, para que el usuario no tenga que comprarlos.

Por esto es que instalar una red inalámbrica es tan atractivo y el mercado de dispositivos inalámbricos ha crecido continuamente en los últimos años, con unos costos para el usuario cada vez menores.

1.3. TIPOS DE REDES INALÁMBRICAS

Las redes inalámbricas se pueden clasificar de muchas formas, por su velocidad, por la tecnología que usan para transmitir, o por la cobertura que tienen, desde un punto de vista de la arquitectura y la cobertura de las redes inalámbricas a continuación se presentan los principales tipos:

[1] Por las características del medio, no es posible estar completamente seguro de que la comunicación se esté realizando solo entre las dos partes. Puede existir un agente intermedio interviniendo, esto se tratará más profundamente en “Seguridad, vulnerabilidades y amenazas”

Redes inalámbricas de cobertura personal: estas redes requieren poca o ninguna infraestructura y operan en distancias cortas que van desde los pocos centímetros (infrarrojo) hasta una decena de metros (Bluetooth), normalmente funcionan en un mismo cuarto. Estas redes por ejemplo proveen los servicios que permiten la comunicación entre un teclado o un mouse inalámbrico y un computador o entre un teléfono celular y un computador portátil.

Redes inalámbricas de cobertura local: es el conjunto de elementos inalámbricos ubicados en un área geográfica limitada, como una casa, un piso de oficinas o una universidad, que tienen capacidades de radio comunicación, estas redes usualmente se encuentran implementadas como una extensión a una red cableada de cobertura local, con el fin de proveer una mayor movilidad a los usuarios. El estándar dominante para este tipo de redes es IEEE 802.11 o Wireless-Fidelity (Wi-Fi®). La IEEE es una organización profesional sin ánimo de lucro, que trabaja por el avance de la tecnología y que entre muchas de sus actividades, está la creación de estándares industriales. Este documento trata en general sobre las redes inalámbricas de cobertura local y los estándares que las definen, sus formas más comunes son 802.11a, 802.11b, 802.11g y 802.11n las que se identifican genéricamente como 802.11a/b/g/n y 802.11i, este ultimo estándar se refiere a la seguridad de las redes y se detallaran más adelante.

Redes inalámbricas de cobertura metropolitana: estas redes pueden proveer conectividad a múltiples individuos en diferentes lugares, separados por varios kilómetros, estas redes proveen acceso de banda ancha a personas en áreas metropolitanas, el estándar más utilizado es el IEEE 802.16 mejor conocido por su nombre comercial: WiMAX.

Redes inalámbricas de cobertura amplia: estas redes conectan individuos o dispositivos sobre amplias zonas geográficas, son usadas típicamente para las comunicaciones celulares de voz y datos, y para comunicaciones satelitales

1.4. SEGURIDAD EN LAS REDES INALÁMBRICAS DE COBERTURA LOCAL

Todas las variaciones del estándar IEEE 802.11 incluyen una característica de seguridad conocida como Privacidad Equivalente al Cable o en inglés Wired Equivalent Privacy (WEP), WEP fue desarrollada para proveer un nivel de seguridad comparable al de las redes cableadas de cobertura local y proteger mediante una clave las transmisiones inalámbricas, pero en 2001 se encontraron debilidades que permiten vulnerar las claves WEP con relativa facilidad, la IEEE consciente de estos problemas y en asocio con Wi-Fi Alliance (una asociación global, sin ánimo de lucro con más de 300 miembros dedicada a promover el crecimiento de las redes inalámbricas de cobertura local) crean estrategias a corto y largo plazo para inicialmente mitigar los problemas y luego solucionarlo completamente. A comienzos de 2003 se desarrolla WPA (Wi-Fi Protected Access) una mejora en la seguridad ideada con el fin de

reemplazar WEP, en junio de 2004 la IEEE finaliza el estándar 802.11i diseñado para superar las debilidades de WEP, mejorar WPA y proveer a las redes 802.11 con mecanismos robustos de seguridad.

II PARTE – ASPECTOS TÉCNICOS

En esta segunda parte, se cubren aspectos generales de las redes inalámbricas, para luego profundizar en las redes inalámbricas de cobertura local, que son las redes que comúnmente se conocen como redes Wi-FI y técnicamente en inglés como Wireless Local Area Networks (WLAN), también se cubre el tema de la seguridad de estas redes, las vulnerabilidades que tienen y las amenazas que afrontan, para finalmente hablar de las redes con seguridad robusta, un tipo de redes inalámbricas que se basan en un estándar internacional y que proporcionan un alto nivel de protección a las redes contra la mayoría de ataques existentes.

1. IDEA GENERAL DE LAS TECNOLOGÍAS INALÁMBRICAS

La comunicación inalámbrica es la transmisión de información sin usar cables, la distancia puede ser corta como la de un control remoto en un televisor o muy larga, hasta miles de kilómetros si se piensa en las comunicaciones de radio que usan los satélites artificiales. Lo inalámbrico reúne muchas tecnologías, los radios de dos vías, lo teléfonos celulares, los dispositivos GPS, los controles que abren puertas de garajes, un teclado inalámbrico, la televisión por satélite, los teléfonos inalámbricos y muchos otros dispositivos mas. Los dispositivos que se comunican entre sí inalámbricamente, forman redes de comunicación y estas redes pueden ser clasificadas según el área de cobertura que tienen. Desde unos centímetros como en el caso de los infrarrojos, hasta miles de kilómetros como en los teléfonos satelitales.

1.1. REDES INALÁMBRICAS DE COBERTURA PERSONAL

Son redes inalámbricas a pequeña escala que requieren poca o ninguna infraestructura, normalmente son usadas por unos cuantos dispositivos en un solo cuarto para comunicarse sin necesidad de cables. Algunas tecnologías usadas por este tipo de redes son:

Bluetooth: desarrollado por el grupo 802.15.1 de la IEEE, con el fin de facilitar la comunicación inalámbrica entre pequeños dispositivos portátiles. Algunos ejemplos incluyen la sincronización de un PDA con un computador, proveer servicios de impresión, habilitar la comunicación inalámbrica entre un teclado o un mouse inalámbrico y un computador, permitir que unos audífonos o un dispositivo manos libres se comunique con un teléfono celular. Todos los dispositivos Bluetooth operan en la banda ISM (Industrial, Scientific and Medical) 2.4GHz usando el método de transmisión de Salto de Frecuencia Espectro Amplio, en inglés Frequency Hopping Spread Spectrum (FHSS). Bluetooth en su versión 1.1 y 1.2 ofrece tasas de transferencia máximas de hasta 720 kilobits por segundo (Kbps); Bluetooth en su versión 2.0 +EDR puede alcanzar tasas de transferencia de hasta 3 Mbps.

Ultra-Wideband (UWB) Ultra-Banda Ancha: UWB está definido por el borrador de estándar 802.15.3a de la IEEE, es un estándar de bajo costo y baja potencia, que usa un amplio rango de frecuencias para evitar la interferencia con otras transmisiones inalámbricas, puede alcanzar tasas de transferencia de hasta 480 Mbps en distancias cortas (menores a un metro) y puede soportar todas las aplicaciones que de una red inalámbrica de cobertura personal se esperan, uno de los usos esperados de esta tecnología es la habilidad para detectar formas a través de barreras físicas como paredes y cajas, lo cual puede ser útil para aplicaciones policiales o de búsqueda y rescate.

Zigbee: este es el nombre usado comúnmente para el estándar 802.15.4 de la IEEE, también conocido como ultra-banda ancha de baja velocidad, Zigbee es un protocolo sencillo para redes inalámbricas de cobertura personal, ideado para ser más simple y barato que otras tecnologías como Bluetooth, tiene como características una baja velocidad de transmisión, bajo consumo de energía y una comunicación segura

1.2. REDES INALÁMBRICAS DE COBERTURA LOCAL

Una Red inalámbrica de cobertura local, es una red de cobertura local que transmite inalámbricamente sobre un radio de cobertura de unos 100 metros del transmisor, utilizando radio comunicación, estas redes usualmente se encuentran implementadas como una extensión a una red cableada de cobertura local, con el fin de proveer una mayor movilidad a los usuarios. IEEE 802.11 o Wireless-Fidelity (Wi-Fi) ® es el estándar dominante para este tipo de redes, aunque existen otros estándares como High Performance Radio Local Area Network (HIPERLAN) del instituto europeo de estándares en telecomunicaciones. Este documento trata en general sobre las redes Wi-Fi, este estándar y sus formas más comunes son 802.11a, 802.11b, 802.11g y el más reciente 802.11n los que se identifican genéricamente como 802.11a/b/g/n y 802.11i estándar dedicado exclusivamente a la especificación de mecanismos de seguridad para redes inalámbricas.

IEEE 802.11a/b/g/n, En 1997 la IEEE ratificó el estándar 802.11, con tasas de transferencia de 1 o 2 Mbps y transmitiendo en la frecuencia ISM de 2.4GHz con un rango de cobertura entre 20 metros bajo techo y 100 metros a campo abierto aproximadamente. En 1999 la IEEE hace dos enmiendas al estándar 802.11 (802.11a y 802.11b), 802.11a transmite en la frecuencia UNII, en inglés Unlicensed National Information Infrastructure, de 5GHz con una tasa de transferencia teórica de 54Mbps, pero al usar una frecuencia más alta su tasa de transferencia se ve severamente afectada por obstáculos y disminuye exponencialmente al aumentar la distancia, así es que desarrolla su tasa de transferencia máxima a una distancia no mayor de 20 metros, a los 90 metros la tasa de transferencia se ve reducida a 6Mbps o menos, este factor es el que hace que el estándar 802.11b sea mucho mas aceptado, 802.11b transmite en la frecuencia ISM 2.4GHz con una tasa de transferencia teórica de 11Mbps, con una cobertura de 100 metros a máxima velocidad de transmisión. En 2003 la IEEE presenta la enmienda 802.11g usando un método de transmisión que usa la frecuencia ISM 2.4GHz y soportando tasas de transferencia máximas hasta de 54Mbps, este estándar tiene compatibilidad con los equipos diseñados para el estándar

802.11b, se han realizado experimentos a campo abierto que han permitido realizar conexiones a distancias superiores a los 30 kilómetros usando antenas direccionales de alta ganancia.

IEEE 802.11n oficialmente no es un estándar aún, se encuentra en las últimas etapas de aprobación, su principal características será su tasa de transferencia, que es de 300Mbps y una cobertura bajo techo de 70 metros y de 250 metros a campo abierto, para sus transmisiones usa las frecuencias 2.4GHZ y 5GHz, es posible encontrar en el mercado productos usando las especificaciones de los últimos borradores de IEEE 802.11n.

Los productos que transmiten en la frecuencia ISM 2.4GHz pueden tener problemas de interferencia, porque esta frecuencia también es utilizada por hornos microondas, dispositivos Bluetooth, radios monitores de bebes y teléfonos inalámbricos.

IEEE 802.11i, el estándar 802.11i es la sexta enmienda al estándar original, e introduce muchas mejoras al modelo de seguridad, con tecnologías maduras y probadamente seguras. 802.11i introduce el concepto de Red con Seguridad Robusta, en inglés Robust Security Network (RSN), una RSN se define como una red inalámbrica en la que solo se permite la creación de Asociaciones de Red con Seguridad Robusta, en inglés Robust Security Network Associations (RSNA), una RSNA es una conexión lógica entre elementos 802.11 estableciendo una conexión a través del esquema de manejo de claves 802.11i, el cual es llamado apretón de manos de cuatro tiempos, el apretón de manos es un protocolo que valida que ambos elementos compartan una clave maestra, sincroniza la instalación de claves temporales y confirma la selección y configuración de la confidencialidad de los datos y la integridad de los protocolos.

1.3. REDES INALÁMBRICAS DE COBERTURA METROPOLITANA

Estas redes pueden proveer con conectividad a usuarios localizados a varios kilómetros unos de otros, el uso más común de estas redes IEEE 802.16 o WiMAX (World Interoperability for Microwave Access) por su nombre comercial, existen dos tipos de WiMAX, WiMAX fijo IEEE 802.16d, con un rango de cobertura de 45 kilómetros con visibilidad directa al enlace o 7.5 kilómetros si no hay visibilidad directa al enlace, el rango también depende de una serie de condiciones ambientales como el viento o la lluvia, en optimas condiciones el WiMAX fijo tiene una tasa de transferencia de hasta 75Mbps. También está el WiMAX móvil IEEE 802.16e, este es una evolución que incluye los ajustes necesarios para permitir la movilidad de los usuarios y mejorar las características de alcance y velocidad.

Otras redes que caben dentro de la descripción de redes inalámbricas de cobertura metropolitana son las redes celulares de datos, las redes celulares modernas 3G son un claro ejemplo de redes inalámbricas de cobertura metropolitana.

2. REDES INALÁMBRICAS DE COBERTURA LOCAL

Las tecnologías para las redes inalámbricas de cobertura local o WLAN por sus siglas en inglés y la industria que de ellas se desprende existen desde mediados de 1980, cuando la comisión federal de comunicaciones de Estados Unidos (FCC) pone por primera vez a disposición de la industria privada el espectro de radio frecuencia, en el resto de la década de los ochentas y a comienzos de los noventa el crecimiento fue relativamente lento, sin embargo en la actualidad las redes WLAN están teniendo un gran crecimiento, debido principalmente al aumento en el ancho de banda que ha sido posible gracias al estándar 802.11 y sus evoluciones.

2.1. HISTORIA

La primera WLAN de la que se tiene noticia fue desarrollada en 1970, por la universidad de Hawaii, usando radios de bajo costo crearon una red que se llamo ALOHAnet, esta red conectaba a siete computadores distribuidos en 4 islas, con un computador central. Luego de esto se tiene noticia de experimentos con infrarrojos e incluso con aparatos diseñados por radio operadores aficionados

Pero no es sino hasta mediados de la década de los noventas que las primeras tecnologías WLAN modernas fueron puestas en el mercado, cuando algunos vendedores usando diseños particulares, transmitiendo en la frecuencia de 900MHz y entregando tasas de transferencia de alrededor de 1Mbps sacan a la venta sus productos dedicados al mercado de consumo general, la velocidad de 1Mbps era muy inferior a las 10Mbps que se encontraba en la mayoría de redes cableadas para esa época, lo que influyo a que no fuera ampliamente adoptado. Anterior a esto la IEEE ya estaba trabajando en un estándar que agrupara vendedores y evitará las proliferación de productos diseñados con protocolos cerrados, el estándar resultante fue 802.11, pero no fue sino hasta 1999, que los productos diseñados para ambientes domésticos llegan al mercado con precios accesibles, uno de los primeros productos que cumplió con estas características es el AirPort de Apple, presentado en julio de 1999 en una conferencia, antes de esto, WLAN era muy costoso y solo lo usaban algunas grandes compañías que podían pagar por la tecnología.

2.2. COMPONENTES Y TOPOLOGÍAS

Componentes

En el mercado existen cientos de dispositivos y tecnologías inalámbricas, pero son algunos dispositivos específicos los que conforman la mayoría de redes inalámbricas.

Dispositivos clientes: estos dispositivos en una red inalámbrica son conocidos como estaciones (EST) y sirven como dispositivos inalámbricos finales. Las EST permiten a los usuarios tener acceso y utilizar

recursos proveídos por las redes inalámbricas. Algunos ejemplos comunes de este tipo de dispositivos son los asistentes digitales, los teléfonos celulares, los computadores portátiles y otros aparatos electrónicos de consumo con capacidades inalámbricas.

Puntos de acceso: un punto de acceso (PA) conecta lógicamente dispositivos clientes (EST) entre sí y provee el acceso a una red cableada, si está conectado a ella. Un PA normalmente se compone de un puerto para redes cableadas (puerto RJ-45) y al menos un radio para proveer la conectividad inalámbrica. Los PA basados en el estándar IEEE 802.11 tienen un rango de cobertura de aproximadamente 100 metros, los cuales dependen de una serie de características del dispositivo y del ambiente donde se opera. Los PA inalámbricos le dan al usuario la capacidad de moverse libremente dentro del área de cobertura del PA manteniendo la conectividad entre la EST y el PA. Si se configuran correctamente los PA puede ser enlazados usando una infraestructura cableada o inalámbrica para permitir a los usuarios, "saltar" entre PA dentro del área de cobertura extendida de una edificación o de un campus universitario.

Puentes inalámbricos: un Puente inalámbrico enlaza dos redes cableadas que generalmente están operando en dos locaciones físicas diferentes. Los puentes se utilizan a menudo para conectar dos edificios o dos redes, cuando una conexión por cable no es posible o eficiente en términos de costos. Los puentes inalámbricos son parecidos a los PA, pero generalmente solo sirven para proveer enlaces inalámbricos punto-a-punto, aunque algunos puentes inalámbricos también pueden cumplir funciones de PA.

Topologías

Hay dos tipos de topologías generales para las redes inalámbricas: infraestructura y ad-hoc. Las redes en modo infraestructura comprenden las redes inalámbricas de cobertura local, las redes celulares y otros tipos de redes que requieren de un PA. Una conexión de infraestructura se puede definir como una red inalámbrica de cobertura local que comprende uno o más Conjuntos Básicos de Servicios, en inglés Basic Service Set (BSS), un BSS incluye un PA y una o más EST, el PA en un BSS conecta la EST a un sistema de distribución, el sistema de distribución es el medio mediante el cual las EST pueden comunicarse con la red cableada y redes externas, como Internet, la figura-1, muestra el modo de infraestructura con dos BSS conectados a un sistema de distribución.

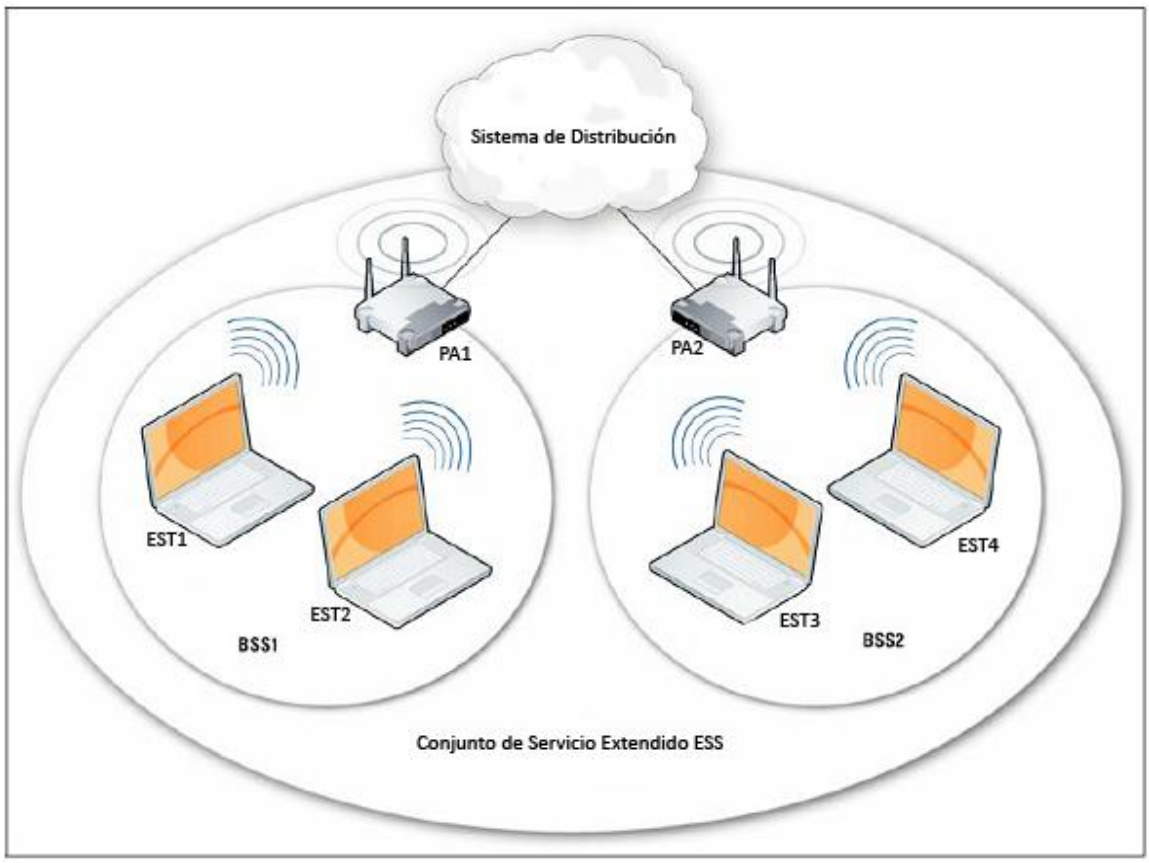

Figura 1 WLAN en modo infraestructura (tomada de [2] traducida por el autor)

El uso de múltiples PA conectados a un sistema de distribución único, permite la creación de una red inalámbrica del tamaño y la complejidad que se quiera, según el estándar 802.11, una red en la que se encuentren varios BSS se llama Conjunto de Servicio Extendido, en inglés Extended Service Set (ESS).

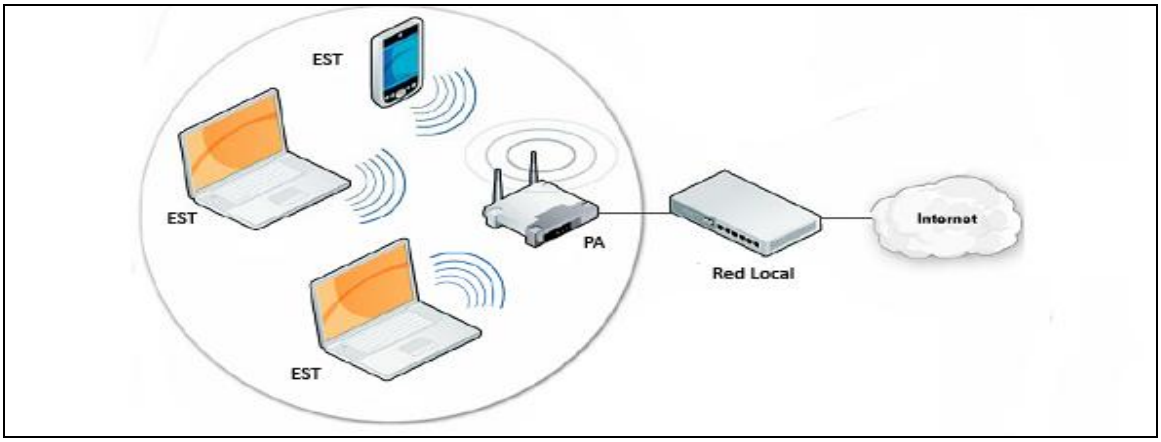

Figura 2 posible configuración de una WLAN casera (tomada de [2] traducida y adaptada por el autor)

En la figura-2, se puede ver un BSS, con dos computadores portátiles y un asistente PDA, conectados a un PA, el cual a su vez está conectado a la red cableada de una casa y esta así mismo conectada a internet, con esta configuración, se pueden tener varias EST compartiendo recursos y conexiones a internet.

Las redes ad-hoc, están diseñadas para conectar dinámicamente dispositivos como celulares, portátiles y asistentes personales entre sí, sin usar dispositivos de infraestructura, estas redes son llamadas ad-hoc o par-a-par (peer to peer P2P) por la topología dinámica de la red. Donde las redes de infraestructura usan un esquema de red fija, las redes ad-hoc mantienen una configuración de red dinámica, confiando en otros dispositivos pares para el manejo de las comunicaciones. Las conexiones ad-hoc solo se dan entre dispositivos EST, un conjunto de dispositivos EST conectados de esta forma se llaman un Conjunto Independiente Básico de Servicios, en inglés Independent Basic Service Set (IBSS), en la figura-3, se presenta un IBSS simple que incluye un computador portátil, un teléfono celular y un asistente digital PDA, el círculo negro determina el área de cobertura dentro del cual las estaciones pueden mantener la conexión, una característica de un IBSS es que no define mecanismos de enrutamiento o reenvió de información, por lo tanto todos los dispositivos deben mantenerse dentro del rango de alcance del radio de los demás.

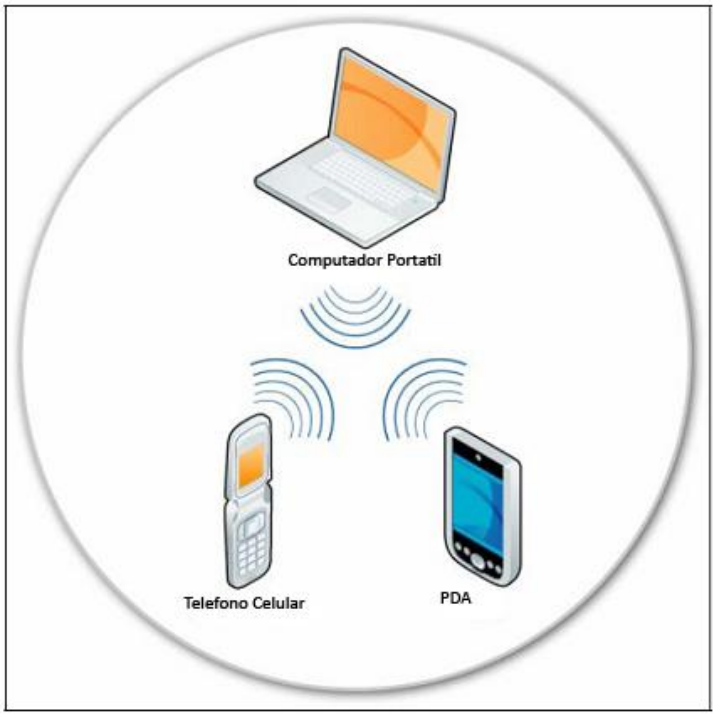

Figura 3 WLAN en modo Ad-Hoc (tomada de [2] traducida por el autor)

Una de las ventajas claves de las conexiones ad-hoc es que pueden ser formadas en cualquier momento y en cualquier parte, permitiendo a varios usuarios crear una conexión inalámbrica fácil y rápidamente.

Una red ad-hoc puede crearse por muchas razones, como permitir a los clientes compartir archivos entre sí. Sin embargo los clientes que se conecten usando este tipo de conexión, no pueden conectarse a ninguna red inalámbrica de infraestructura, la conexión ad-hoc que mantienen pueden causar interferencia con una red de infraestructura que se encuentre en el mismo espacio inalámbrico.

2.3. FRECUENCIAS, TASAS DE TRANSFERENCIA Y ALCANCE

802.11g es el más reciente de los estándares inalámbricos aprobado completamente por la IEEE, entrega una tasa de transferencia de 54Mbps, usa La Multiplexación por División de Frecuencias Ortogonales, en inglés Orthogonal Frequency Division Multiplexing (OFDM) como método de transmisión y opera en la frecuencia ISM (industrial, scientific and medical) 2.4GHz, es compatible con el estándar 802.11b lo cual fue una de las características deseadas al momento de su diseño, este es el estándar más popular actualmente. 802.11b tiene una tasa de transferencia de 11Mbps, usa Espectro amplio por secuencia directa, en inglés Direct Sequence Spread Spectrum (DSSS) como método de transmisión y opera en la frecuencia ISM 2.4GHz. 802.11a tiene una tasa de transferencia de 54Mbps, usa OFDM como método de transmisión y opera en la frecuencia UNII de 5GHz. 802.11n tiene una tasa de transferencia de 248Mbps, usa Múltiples Entradas Múltiples Salidas, en inglés Multiple-Input Multiple-Output (MIMO) como método de transmisión y opera en las frecuencias ISM 2.4GHz y UNII 5GHz. La tabla-1 resume esto.

Característica	**802.11**	**802.11b**	**802.11g**	**802.11a**	**802.11n**
Capa Física – Método de transmisión	FHSS	DSSS	OFDM y DSSS manteniendo compatibilidad con 802.11b	OFDM	MIMO
Banda – Frecuencia	ISM 2.4 GHz	ISM 2.4 GHz	ISM 2.4 GHz	UNII 5GHz	ISM 2.4 GHz UNII 5GHz
Tasas de transmisión Máximas	2Mbps	11Mbps	54Mbps	54Mbps	248Mbps
Rango de Operación	20 Mts bajo techo 100 Mts campo abierto	38 Mts bajo techo 140 Mts campo abierto	38 Mts bajo techo 140 Mts campo abierto	35 Mts bajo techo 120 Mts campo abierto	70 Mts bajo techo 250 Mts campo abierto

Tabla 1 Frecuencias, tasas de transferencia y alcance en redes 802.11 (adaptada de [2])

Los rangos de operación confiable dependen de muchos factores, como fuentes de interferencia, características físicas del espacio, potencia, conectividad y antena, el rango típico bajo techo es de unas

decenas de metros con mucho mayor alcance en campo abierto, usando antenas direccionales de alta ganancia se han reportado conexiones a mas de 30 kilómetros.

Los PA también pueden servir como puentes, conectando dos redes cableadas y aumentando así su cobertura, la figura-4, muestra como dos PA, conectan a dos edificios, se ubica un PA en cada edificio y así todas las comunicaciones que se originen en la red cableada del edificio A con destino al edificio B, se transmiten inalámbricamente al edificio B, allí son recibidas por el PA y enviadas a la red cableada del edificio B. Efectivamente conectando dos sitios alejados, que posiblemente no se puedan conectar de otra manera.

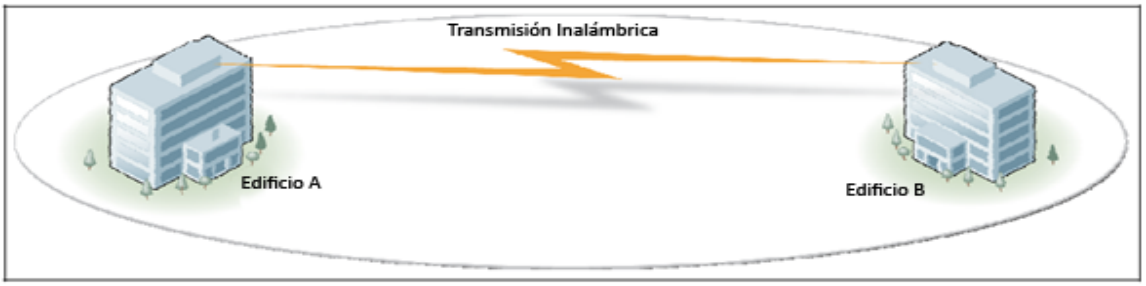

Figura 4 dos puntos de acceso funcionando como puentes (tomada de [2] traducida por el autor)

2.4. BENEFICIOS

Las WLAN tienen muchos beneficios para sus usuarios, los principales son:

Movilidad: el usuario puede acceder a archivos u otros recursos de la red, e incluso conectarse a Internet, sin tener que conectarse físicamente a la red cableada, los usuarios pueden ser móviles y aún así mantener una conexión a alta velocidad.

Instalación: el tiempo requerido para la instalación se reduce, ya que no es necesaria la instalación de cables a través de muros y techos. Por esta razón las WLAN son usadas en edificios protegidos por leyes de preservación histórica.

Flexibilidad: se pueden agregar o remover una WLAN según se necesite, por ejemplo si se vive en una casa de varios pisos y en algún momento se necesita acceso inalámbrico a la red en una zona que no tiene cobertura, se puede agregar y más tarde si ya no se necesita se puede remover, con la mayor facilidad.

Escalabilidad: la topología de la red WLAN puede ser fácilmente modificada para suplir las necesidades que se tengan, y escalar desde una red con un solo PA para un área definida, a una red mucho más compleja y con mayor cobertura.

A causa de estos beneficios, el mercado de las WLAN ha crecido continuamente en los últimos años y continúa ganando popularidad.

2.5. OPERACIONES DE LAS REDES 802.11

El protocolo de la capa de enlace IEEE 802.11 especifica las funcionalidades requeridas en una WLAN para poder proveer una entrega confiable de los datos de un usuario sobre un medio potencialmente ruidoso y poco confiable como el inalámbrico. Este protocolo implementa un intercambio de paquetes en el cual una EST que recibe un paquete de datos responde con una confirmación del paquete que recibió o notifica al originador algún error en el paquete recibido. Las EST reciben, decodifican y responden a todos los paquetes que recibe, con la excepción de algunos paquetes que se envían a todas las estaciones o que envía el PA indicando su existencia.

En la figura-5, se muestra un intercambio típico de paquetes, una EST envía una petición de asociación al PA, esta petición solicita conectarse a la WLAN con SSID "NoSegura". El PA que tiene el SSID puede responderle a la EST con un aviso de éxito o de falla. Si la respuesta es de éxito, se crea una asociación entre la EST y el PA.

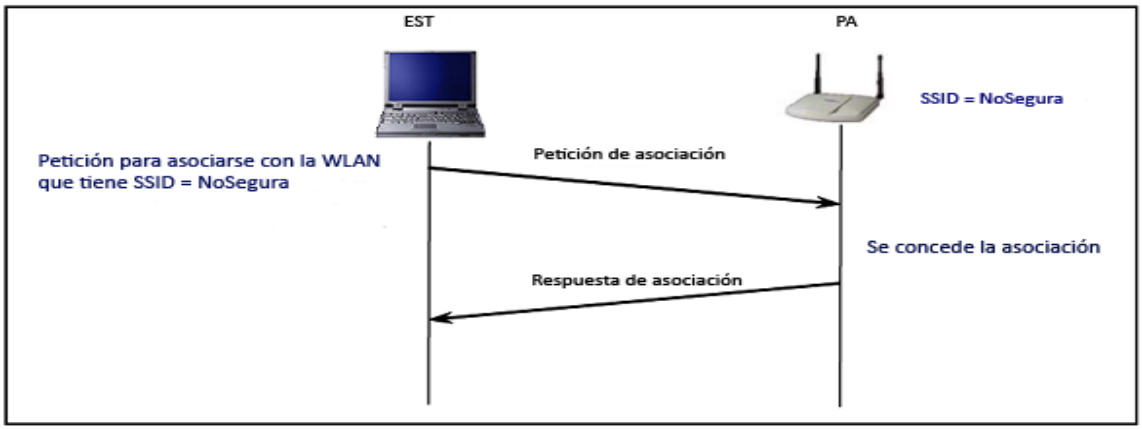

Figura 5 Intercambio de paquete al solicitar conexión a una WLAN (tomada de [3] traducida por el autor)

2.5.1. Tipos de paquetes usados por IEEE 802.11

El protocolo de intercambio de paquetes comprende tres tipos de paquetes, que son los siguientes:

- Paquetes de datos. Los paquetes de datos llevan información de niveles superiores, como IP, los paquetes IP pueden contener datos de aplicaciones como, el correo electrónico o una página web. Los paquetes de datos permiten el envió de información desde y hacia aplicaciones en niveles superiores a las EST o al PA. [3]

- Paquetes administrativos. Los paquetes administrativos transportan la información necesaria para llevar a cabo funciones administrativas, como la autenticación o la asociación.

- Paquetes de control. Estos paquetes se usan para solicitar y controlar el acceso al medio inalámbrico. El paquete de confirmación de recepción es un paquete de control, que se utiliza para asegurar la confiabilidad. Su principal propósito es alertar al remitente que el último paquete enviado fue recibido correctamente y no hay necesidad de retransmitirlo. Siempre se espera la confirmación del paquete, si no se recibe la confirmación se considera perdido el paquete. [3]

La tabla-2 muestra los subtipos de paquetes administrativos.

Subtipo de paquete	Descripción
Solicitud de asociación	Lo usa la EST para solicitar una asociación, en este paquete se debe proveer el SSID de la WLAN.
Respuesta de asociación	Se usa para indicar el estado de la solicitud de asociación (éxito o fallo).
Solicitud de re-asociación	Lo usa una EST que estaba asociada con un BSS, para solicitar la asociación a otro BSS con el mismo SSID. En este paquete se incluye la misma información que se envía en la solicitud de asociación, más la dirección del PA actual.
Respuesta de re-asociación	Se usa para indicar el estado de la solicitud de re-asociación (éxito o fallo).
Solicitud de Existencia	Es usado por una EST para encontrar rápidamente una WLAN rápidamente, este paquete sirve para localizar cualquier WLAN o una con un SSID en particular.
Respuesta de existencia	Lo usa el PA para responder a la solicitud de existencia, este paquete incluye básicamente la misma información que el

	paquete señal.
Señal	Lo transmite periódicamente el PA para que las EST lo puedan localizar fácilmente e identificar un BSS
Autenticación	Lo usa una EST o un PA para verificar la identidad de otra EST
Des-autenticación	Lo usa una EST para señalar la terminación de una relación de autenticación.
Des-asociación	Lo usa una EST para señalar la terminación de una asociación
Anuncio de indicación de tráfico	Lo usa una EST conectada en modo ad-hoc para indicar a otras EST que pueden estar en modo ahorro de energía que ya tiene suficientes datos esperando para ser transmitidos

Tabla 2 subtipos de paquetes administrativos (adaptada de [3])

En la figura-6 se ilustra un flujo de paquetes administrativos en un intercambio de paquetes entre tres EST y un PA en una BSS. El PA periódicamente envía un paquete de señal, alertando a todas las estaciones que una WLAN está operando. Luego de completar el intercambio de paquetes para la autenticación, las EST pueden conectarse al PA para asociarse a él. EST1 y EST2 hacen el intercambio solicitud de asociación - respuesta con el PA. La EST3 se une a la red luego de que la señal fue transmitida, por esto la EST envía una solicitud de existencia y recibe una respuesta de solicitud.

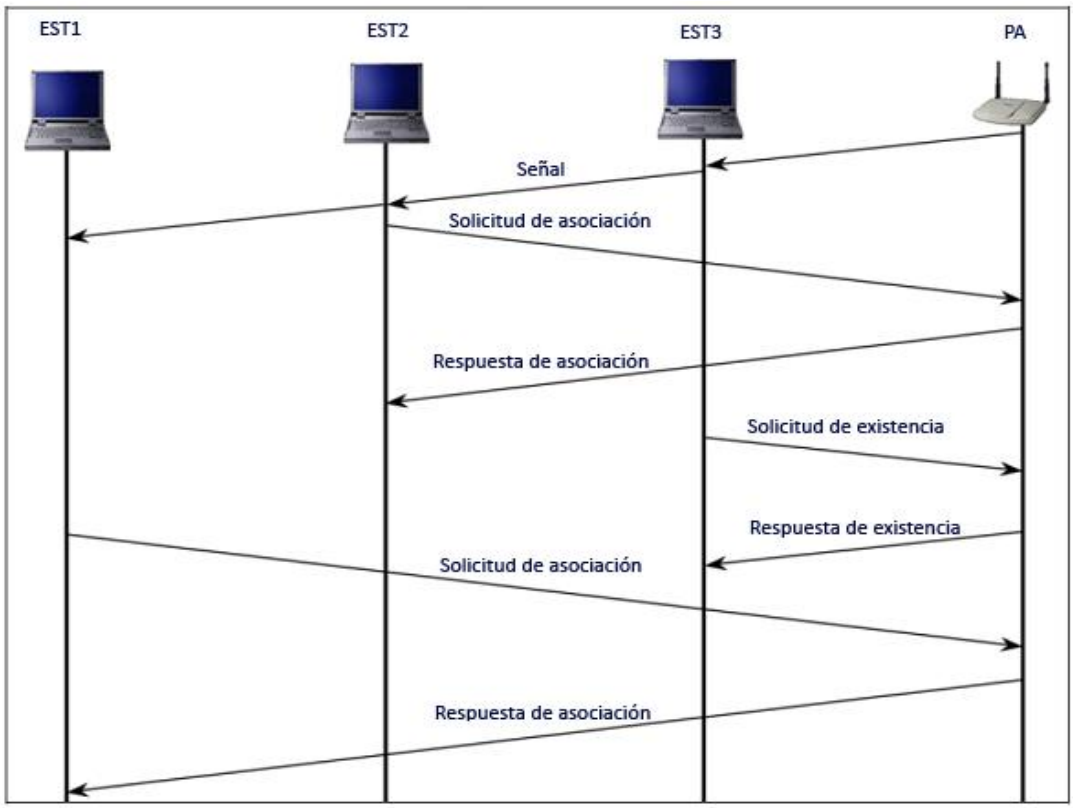

Figura 6 Flujo de paquetes administrativos Típico (tomado de [3] traducido por el autor)

2.6. SEGURIDAD

Las redes cableadas y las redes inalámbricas tienen como objetivo proveer las siguientes características desde el punto de vista de la seguridad:

Confidencialidad: Asegurar que la comunicación no pueda ser leída por partes no autorizadas. [3]

Integridad: Detectar cualquier cambio intencional o fortuito que pueda ocurrir durante la transmisión de los datos. [3]

Disponibilidad: Asegurar que los dispositivos e individuos puedan acceder a la red y a sus recursos cuando lo requieran. [3]

Control de acceso y autenticidad: Restringir los derechos para acceder a la red y a sus recursos a los dispositivos e individuos, verificando que las partes estén identificadas y autorizadas. [3]

La mayoría de amenazas que tienen las WLANs involucran a un atacante con acceso al enlace de radio entre un AP y una EST o entre dos EST, estos ataques muchas veces requieren interceptar el tráfico de datos y transmitir comunicaciones en la red, esto deja expuesta la principal diferencia entre proteger

una red inalámbrica y un red cableada, al no estar precisamente delimitada la red inalámbrica, se pierde control sobre la seguridad física, se puede comparar con mantener una conversación en un sitio público, cualquier extraño que esté lo suficientemente cerca para escuchar lo hará e incluso puede que intervenga. En cambio en una red cableada el atacante tiene que obtener acceso físico a los equipos o haber comprometido remotamente un sistema que esté conectado a la red, volviendo a las comparaciones, esto sería como tener una conversación telefónica, si alguien quiere escuchar debe interceptar la comunicación físicamente.

Anteriormente se habló de WEP, el protocolo de seguridad que se utilizó inicialmente para proteger redes inalámbricas, este protocolo fue sustituido por WPA, ya que WEP tiene múltiples vulnerabilidades que han sido aprovechadas para romper su seguridad, una red inalámbrica protegida por una clave WEP, puede ser vulnerada en par de minutos, WPA fue ideado para ser fuerte en los puntos en los que WEP era débil, pero también como una solución transitoria antes de que se tuviera listo el estándar IEEE 802.11i[2], otro problema que se tuvo luego de identificar las debilidades de WEP fue que los vendedores intentaron mitigarlas con sus propias soluciones, pero estas soluciones disminuían la interoperabilidad entre las redes sí se hacía una mezcla de proveedores.

En las próximas páginas se presentaran las características y fallos que tenían los modelos anteriores a 802.11i, concentrándose en: control de acceso y autenticación, cifrado, integridad de datos, protección contra retransmisión y disponibilidad

Control de acceso y autenticación, originalmente 802.11 definía solo dos medios para validar las identidades de los dispositivos inalámbricos que querían tener acceso a una WLAN, autenticación de sistema abierto y autenticación de clave compartida, ninguno de estos métodos es completamente seguro, es requisito que los dispositivos 802.11 soporten la autenticación de sistema abierto y es opcional la implementación de la autenticación de clave compartida, la autenticación de sistema abierto, es un mecanismo de autenticación nulo que no brinda una verdadera verificación. [3]

En la práctica, una EST se autentica con un PA al proporcionar el identificador de servicio del PA, en inglés, Service Set Identifier (**SSID**), el SSID es el nombre de la WLAN, permite que las ESTs, distingan un PA de otro, el SSID lo transmite periódicamente el PA, así un intruso que este escuchando el tráfico puede conocer el SSID de una WLAN, también debe proporcionar la dirección **MAC** de la EST, la dirección MAC, en inglés Media Access Control, es un identificador único que se asigna a la tarjeta de red inalámbrica, muchas implementaciones de 802.11 permiten que un administrador defina una lista de direcciones MAC que pueden tener accesos a un PA, entonces el PA solo le permitirá el acceso a los dispositivos cuyas direcciones MAC estén en la lista, esto se conoce Filtrado por dirección MAC, sin embargo las direcciones MAC se transmiten inalámbricamente sin ser cifradas, esto hace mas sencillo para un atacante identificar direcciones MAC que tengan permitido pasar el filtro de direcciones, además es relativamente trivial cambiar una dirección MAC, lo que significa que un atacante puede conseguir el acceso fácilmente.

[2] 802.11i y RSNA se explicará profundamente en la sección " Redes con seguridad robusta"

En una conexión en la que se utilizó la autenticación de sistema abierto la EST no tiene forma de verificar que el PA es realmente el PA con el que se quiere conectar, puede ser un PA impostor que está usando el mismo SSID, por lo tanto la autenticación de sistema abierto no asegura de una forma razonable las identidades de los dispositivos que intervienen en una conexión.

La autenticación de clave compartida está basada en una clave criptográfica conocida como clave WEP, esta clave es compartida por las ESTs y PA legítimos. La autenticación de clave compartida es un esquema bastante simple de desafío-respuesta, que se basa en el principio de que la EST que quiere tener acceso a la WLAN conoce la clave de esta, como se presenta en la figura-7, la EST inicia una petición de autenticación al PA, y el PA genera un valor de desafío y lo envía a la EST, la EST usando la clave WEP cifra el desafío y reenvía el valor resultante al PA, el PA descifra el valor recibido usando la misma clave WEP y le permite el acceso a la EST solo si el valor que resulta luego de descifrarlo es igual al valor desafío que envió inicialmente.

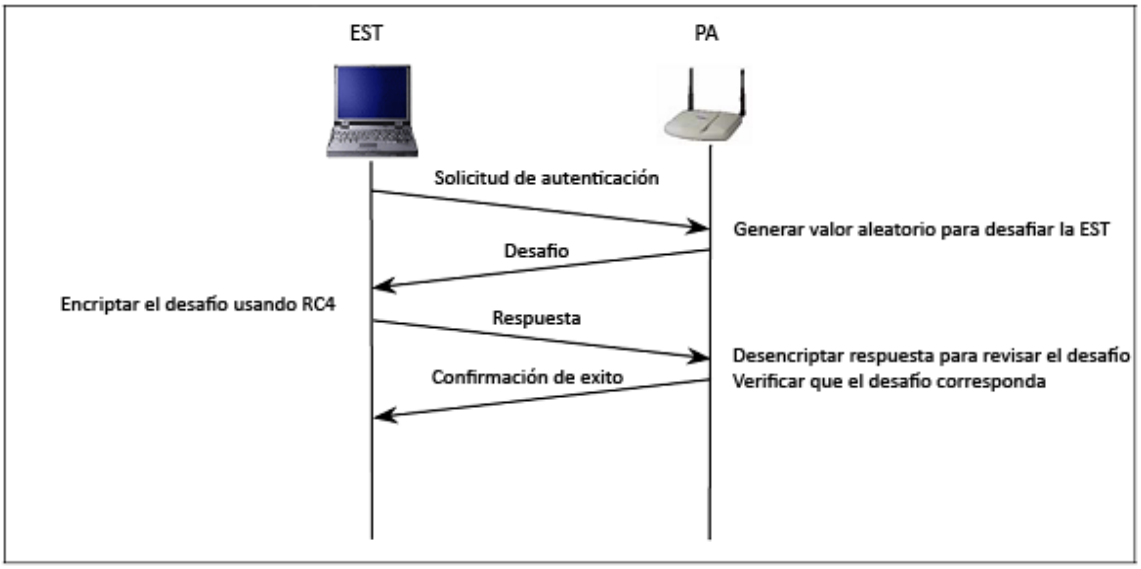

Figura 7 Autenticación usando WEP (tomada de [3] traducida por el autor)

Con la autenticación de clave abierta, el PA no se autentica con la EST, por esto no hay seguridad de que la EST se esté comunicando con un PA legítimo, con el esquema WEP tampoco se autentica a los usuarios, si un atacante accede a una EST que tenga la clave WEP puede usar esa clave para obtener acceso a la WLAN. El esquema de desafío-respuesta como el que se ilustra acá es conocido por su debilidad a menos que se tenga en cuenta la necesidad de generar un desafío lo suficientemente aleatorio, usar claves de una longitud apropiada, usar una función de cifrado fuerte y asegurar todo el diseño del protocolo.

Un atacante puede vulnerar este esquema de autenticación, al usar un ataque como el de hombre en el medio, interceptando las comunicaciones entre dos partes, obteniendo así claves y datos, luego el atacante se puede hacer pasar por una parte autorizada. Otro método de ataque es que un atacante

que este escuchando el tráfico, guarde el desafío enviado por el PA y la respuesta cifrada de la EST, luego usando fuerza bruta analizar los datos para encontrar la clave.

Como las claves deben estar en los PA y en las ESTs, si la clave es vulnerada, debe ser cambiada en todos los dispositivos, las claves WEP no se usan para controlar el acceso sino para proteger la confidencialidad y la integridad.

Adicional a todos estos problemas, algunos PA se comienzan a usar utilizando la clave que viene predefinida de fabrica o unas claves triviales como todo cero o todo uno, la clave para ser efectiva debe ser lo más aleatoria posible, para que no se puede adivinar fácilmente y si un atacante intenta encontrarla usando fuerza bruta sea mucho más difícil.

Cifrado, el protocolo WEP usa un tipo de cifrado llamado RC4 para cifrar las comunicaciones inalámbricas, lo que protege el contenido de las comunicaciones de los receptores no autorizados, el estándar WEP detalla que se debe soportar solamente una llave con longitud de 40 bits; sin embargo algunos fabricantes ofrecen extensiones no estándar para que WEP pueda soportar longitudes de llave de 128 o incluso 256 bits. Para formar su llave WEP también usa un valor de 24 bits conocido como el Vector de Inicialización, en inglés Inicialization Vector (IV), como un valor semilla para inicializar el flujo de la llave criptográfica, así una llave WEP con longitud de 104 bits con 24bits de IV se convierte en una llave de 128 bits. Idealmente una llave más larga se traduce en una protección mejor, pero las técnicas criptográficas usadas por WEP tienen falencias conocidas que no se solucionan con una llave más larga. [3]

La mayoría de intentos de ataques contra WEP tienen que ver con vulnerabilidades en el IV. Por ejemplo la parte del IV de una llave RC4 se transmite sin ser cifrada, lo que hace posible que un atacante que este escuchando el tráfico de red, pueda analizar poco tráfico y deducir la llave WEP completa, aprovechando el conocimiento del valor IV, el poco tamaño que tiene el IV y algunas debilidades del algoritmo RC4. En la especificación de WEP no es claro como los valores IV deben ser iniciados o como se deben cambiar, algunos fabricantes usan un valor inicial preestablecido. Si dos mensajes tienen el mismo IV y el texto de uno de los mensajes se conoce, es relativamente sencillo para un atacante descifrar el contenido del otro mensaje. Incluso el tráfico que se genera mientras se aumenta secuencialmente el valor IV es susceptible de ser atacado, hay menos de 17 millones de IV, 2^{24} IVs exactamente, en una red con una buena cantidad de tráfico todos los IVs serán usados en pocas horas. Cuando el valor IV es aleatorio, que parece ser la mejor opción a elegir, por la paradoja del cumpleaños[3], existe una probabilidad de 50% de tener dos valores IV iguales luego de 2^{12} paquetes de datos. [3]

[3] La paradoja del cumpleaños, se refiere a que en un grupo personas seleccionadas al aleatoriamente un par de ellas tendrán la misma fecha de cumpleaños, en un grupo de 23 o mas personas, hay una probabilidad de mas del 50% de que un par de personas tengan la misma fecha de cumpleaños [http://mathworld.wolfram.com/BirthdayProblem.html]

Integridad de datos, WEP verifica la integridad de los datos transmitidos entre una EST y un PA, asimismo está diseñado para rechazar cualquier paquete de datos que haya sido modificado durante la transmisión, la integridad en WEP es comprobada por medio de una suma de chequeo de 32 bits, chequeo de redundancia cíclica, en inglés cyclic redundancy check (CRC32) que se computa con cada paquete de datos antes de ser transmitido, el receptor descifra el paquete de datos, vuelve a computar el chequeo y lo compara con el valor que recibió con el paquete de datos, si los valores no son iguales, el paquete de datos transmitido fue modificado durante la transmisión y se descarta inmediatamente. [3]

Desafortunadamente, CRC32 puede ser burlado, ya que un atacante puede saber cuáles bits del chequeo cambiaran si se cambian ciertas partes del mensaje, lo que hace posible modificar los datos sin que el chequeo lo detecte. WEP intenta solucionar este problema al cifrar el CRC32 y producir un valor de integridad de chequeo, en inglés integrity check value (ICV), los creadores de WEP pensaron que al cifrar el valor CRC, sería más difícil modificar los datos, pero por las características del algoritmo RC4 si un bit cambia de valor, este sobrevive el proceso de cifrado, por lo tanto ICV en WEP no ofrece ninguna protección adicional contra el cambio de bits. [3]

La integridad debería ser verificada por un método de chequeo criptográfico no por CRC, estos métodos son conocidos como hashes con clave o Códigos de autenticación de mensaje, en inglés Message Authentication Codes (MAC), estos métodos protegen efectivamente contra los cambios de bits que CRC no detecta, aunque CRC es más efectivo en términos computacionales, solo está diseñado para proteger contra cambios aleatorios de bits, no contra cambios premeditados. [3]

Protección contra retransmisión, la implementación de WEP no tiene ninguna protección contra la retransmisión de paquetes de datos, para protegerse debería tener un contador incremental de los paquetes o una marca de tiempo, que permita detectar el tráfico retransmitido sencillamente. [3]

Disponibilidad, existen al menos tres ataques que afectan la disponibilidad de una red inalámbrica, el primero es cuando un dispositivo que transmite en la misma frecuencia de radio de la WLAN, transmite más fuerte que los otros dispositivos y crea un bloqueo en las frecuencias, la energía transmitida hace que no se pueda usar la WLAN, este bloqueo puede ser generado deliberadamente por un atacante o fortuitamente cuando por ejemplo un horno microondas o un teléfono inalámbrico bloquea la señal. El segundo ataque ocurre cuando un atacante envía una gran cantidad de paquetes de datos a un PA continuamente, el PA no es capaz de responder a la cantidad de datos que recibe, esto ocasiona que las EST genuinas no puedan seguir comunicándose con el PA. El tercer ataque ocurre cuando un atacante crea un PA ficticio con el mismo SSID de un PA genuino y transmite con mayor potencia, esto puede llevar a una pérdida de disponibilidad para los clientes. Una vulnerabilidad adicional que tiene 802.11 es que los paquetes administrativos no viajan autenticados, entonces un atacante puede enviarle a un PA un mensaje haciéndose pasar por un cliente genuino, en el que solicita desconectarse de la red y el PA desconectará al cliente de la red, el atacante en este momento puede hacerse pasar por el cliente o monitorear el tráfico para el momento en el que la EST solicita reconectarse y extraer de allí la clave de la red.

En la tabla-3 se presentan algunas de las amenazas más comunes.

Tipo de Amenaza	Descripción
Negación del Servicio	Un atacante previene o impide el uso normal o la administración de una red o de un dispositivo de red.
Espiar	Un atacante monitorea pasivamente las comunicaciones en busca de datos, como claves u otra información "interesante".
Hombre en el medio	Un atacante activamente intercepta las comunicaciones entre dos partes, obteniendo así claves y datos. Luego un atacante se puede hacer pasar por una parte autorizada.
Enmascarar	Un atacante suplanta un usuario autorizado y obtiene acceso a recursos no autorizados
Modificación del mensaje	Un atacante altera un mensaje legitimo, borrando, agregando o modificando los datos
Retransmisión del mensaje	Un atacante monitorea pasivamente las comunicaciones y las retransmite, actuando como si el atacante fuera un usuario legítimo
Análisis de Tráfico	Un atacante monitorea pasivamente las comunicaciones para identificar patrones de comunicación y partes envueltas en ellas.

Tabla 3 Principales amenazas inalámbricas (adaptada de [2])

3. SEGURIDAD, VULNERABILIDADES Y AMENAZAS

Para comenzar leamos algunas definiciones de los términos que vamos a usar. Para ello usare las definiciones encontradas en inglés en el "Webster's Third New International Dictionary" [21] ya que se ajustan más al tema que estamos tratando, luego traduciré libremente la definición al Español.

Security – Seguridad:

Freedom from danger, fear, anxiety, care, uncertainty, doubt; basis for confidence; measures taken to ensure against surprise attack, espionage, observation, sabotage; resistance of a cryptogram to cryptanalysis usually measured by the time and effort needed to solve it.

Libre de peligro, miedo, ansiedad, cuidado, incertidumbre, duda; base para la confianza; medidas tomadas para asegurarse contra un ataque sorpresa, espionaje, observación, sabotaje; Resistencia de un criptograma al análisis criptográfico usualmente medido por el tiempo y esfuerzo necesario para solucionarlo.

Availabity – Disponibilidad:

Present or ready for immediate use.

Presente o listo para su uso inmediato

Integrity – Integridad:

Unimpaired or unmarred condition; soundness; entire correspondence with an original condition; adherence to a code of moral, artistic or other values; the quality or state of being complete or undivided; material wholeness.

Intacto o sin ninguna mutilación; coherencia; correspondencia completa con una condición original; adherencia a un código moral, artístico u otros valores; la cualidad o estado de estar completo o sin división; completitud material

Authenticity – Autenticidad:

Quality of being authoritative, valid, true, real, genuine, worthy of acceptance or belief by reason of conformity to fact and reality.

Característica de estar autorizado, ser válido, verdadero, real, genuino, digno de aceptación o confianza por razón de conformidad a los hechos o a la realidad

Confidentiality – Confidencialidad:

Quality or state of being private or secret; known only to a limited few, containing information whose unauthorized disclosure could be prejudicial to the national interest.

Característica o estado de ser privado o secreto; conocido solamente por unos pocos, contener información cuya exhibición no autorizada puede ser perjudicial a los intereses nacionales

Possession – Posesión:

Act or condition of having or taking into one's control or holding at one's disposal; actual physical control of property by one who holds for himself, as distinguished from custody; something owned or controlled.

Acto o condición de tenencia o tomar para uno mismo control o de tener a su propia disposición; control físico de una propiedad de uno que la tiene para si mismo, a diferencia del que lo tiene en custodia; algo poseído o controlado.

Se ha hablado de cinco conceptos fundamentales para la seguridad informática, la disponibilidad, la integridad, la autenticidad, la confidencialidad y la posesión o propiedad. Cada uno de estos conceptos que tiene su propia definición según un diccionario se pueden igualmente definir en términos de seguridad de la información, así [25]:

- Disponibilidad: capacidad de la información para ser usada con un propósito.
- Integridad: Completitud, totalidad y legibilidad de la información y su característica de no ser cambiada desde un estado anterior.
- Autenticidad: validez, conformidad y genuinidad de la información.
- Confidencialidad: asegurar que la información no pueda ser leída por una parte no autorizada o que la información no sea divulgada sin autorización.
- Posesión: La tenencia, control y capacidad de usar la información.

Todas estas definiciones fundamentales pueden ser vulnerables independientemente, si hay un ataque de negación del servicio afecta la disponibilidad, si un atacante logra modificar un mensaje que está en tránsito se pierde la integridad, si un atacante se hace pasar por un usuario legitimo se pierde la autenticidad, si un atacante descifra la clave usada para proteger una red inalámbrica se pierde la confidencialidad, si un usuario pierde su computador portátil se pierde la posesión de la información. Si se pierde la confidencialidad es posible que se pierda el uso exclusivo de la información y por lo tanto su posesión única. Este es el único caso en el que implícitamente se mezclan dos conceptos.

3.1. Pérdida de disponibilidad

Una pérdida de disponibilidad en una red inalámbrica puede ser causada por dos factores, o interferencia o inundación de datos. La interferencia ocurre cuando un atacante deliberadamente transmite una señal electromagnética que satura las señales de los dispositivos inalámbricos. También puede haber interferencia accidental, causada por otros dispositivos que usan la misma frecuencia, como teléfonos inalámbricos o un horno microondas, la interferencia tiene como consecuencia una interrupción o una pérdida completa de la comunicación, porque la señal no puede ser transmitida correctamente.

Un atacante también puede causar una pérdida en la disponibilidad al provocar una inundación de datos, este tipo de ataque ocurre cuando se transmiten una gran cantidad de paquetes de datos a un punto de acceso u otro dispositivo inalámbrico, teniendo como consecuencia que el dispositivo no pueda responder a todos los paquetes y no tenga una operación normal. Puede haber una inundación de paquetes no intencional, si un usuario monopoliza la capacidad de la red por ejemplo descargando archivos muy grandes. En este tipo de ataque la red puede degradar su rendimiento o incluso fallar completamente.

Estos dos factores, la interferencia y la inundación de paquetes, son difíciles de controlar en una comunicación de radio y en el estándar 802.11 no hay ningún mecanismo de defensa.

3.2. Pérdida de integridad

Tanto en las redes cableadas como en las redes inalámbricas, la integridad de los datos, es algo que normalmente se le deja a las aplicaciones en niveles superiores para que lo verifiquen, pocas veces se hace un control de integridad en niveles inferiores o se hace usando herramientas que pueden ser vulnerables. Las redes inalámbricas 802.11 usan el mecanismo de integridad CRC32, este mecanismo es vulnerable porque se pueden modificar bits sin ser detectados por el CRC32. Esto puede llegar a extremos hipotéticos en los que un atacante pueda modificar un mensaje de correo electrónico sin ser detectado. Para proteger la integridad se recomienda usar 802.11i, que utiliza códigos de integridad del mensaje, estos códigos se cifran y no es posible modificar los datos transmitidos, sin que sea detectado algún cambio en los mismos.

3.3. Pérdida de autenticidad

Un ataque posible en las redes inalámbricas es el de hombre en el medio, en este ataque, un atacante con un equipo básico se hace pasar por un PA legítimo, mientras restringe la disponibilidad o emite su señal más fuertemente que el PA legítimo, de esta forma, las ESTs se conectaran al PA del atacante, este PA recibe los datos de autenticación y simultáneamente puede autenticarse al PA original, actuando como un puente transparente entre las partes, de esta forma el atacante puede recolectar todos los datos que se transmitan, modificarlos, retardarlos, extraviarlos, sin ser detectado, y efectivamente creando pérdida de autenticidad en la información tanto para la EST como para el PA legítimo, puesto que las dos partes si no están bien protegidas no tienen forma de detectar fácilmente este ataque. Todo este ataque se facilita en las redes que usan un conexión anterior a una RSNA, en una RSNA, la autenticidad se protege luego de crear la asociación entre las partes, exigiendo una autenticación mutua, de esta forma el ataque de hombre en el medio no puede ser realizado, a menos de que el atacante tenga los medios para suplantar los certificados y métodos usados para garantizar la autenticidad de las partes.

3.4. Pérdida de confidencialidad

Debido a que las redes inalámbricas utilizan un medio abierto, el cuidado que se debe tener con la confidencialidad de la información debe ser mayor al que se tiene en otros tipos de transmisiones y es más sensible que en una red cableada.

Un atacante que se ubique dentro del radio de alcance de un PA, puede escuchar pasivamente la información que se transmite, sin levantar sospechas, mientras monitorea el tráfico que flota en el aire, puede ver información sensible, como nombres de redes y claves, datos de la configuración de la red e incluso analizando solamente la cantidad de tráfico transmitida en un periodo de tiempo deducir si se está transmitiendo una videoconferencia o una conversación por chat. Este riesgo de ser escuchado sin ser detectado, se debe a que las señales de IEEE 802.11 pueden viajar más allá del radio de servicio previsto, permitiendo que un atacante pueda monitorear la información, incluso si no utiliza una antena especial para ello.

Monitorear el tráfico de una red inalámbrica es sencillo, si se usa una herramienta como un analizador de protocolos o sniffer, esta herramienta permite que alguien pueda recibir el tráfico inalámbrico de las redes que se encuentran a su alcance y es posible porque la mayoría de las redes inalámbricas no están debidamente protegidas o están protegidas con protocolos no seguros, que le permiten a un atacante tener acceso a los datos que se transmiten sin mayor dificultad.

Para proteger la confidencialidad es necesario evitar protocolos poco seguros como WEP y en lo posible usar el estándar IEEE 802.11i en la versión para hogar o empresa dependiendo del caso. Hasta ahora no existe un método algebraico para descifrar la clave que se usa en los casos de CCMP y TKIP, aunque se recomienda CCMP por usar un algoritmo más fuerte, solo se tienen noticias de ataques basados en diccionario, por lo tanto sigue siendo muy importante seleccionar una contraseña lo suficientemente larga y compleja como para que un ataque de diccionario no sea viable.

Qué es un ataque de diccionario? Es un método por el cual, se recorre una serie de palabras o combinaciones de letras, números y símbolos, con el fin de usarlos como palabra clave y generar un texto conocido cifrado, si el resultado que se obtiene es igual a algún texto que se encontraba cifrado, se ha encontrado la llave usada, si es diferente se continua la búsqueda, es posible generar o descargar de internet estos diccionarios, pero no son eficaces ante una contraseña cuidadosamente seleccionada.

3.5. Pérdida de Posesión

Cuando se presenta una pérdida de confidencialidad, potencialmente se pierde posesión exclusiva sobre la información, porque una vez que la confidencialidad ha sido comprometida un atacante puede descifrar todos los datos que se transmiten, leer correos electrónicos, reproducir conversaciones por voz IP, replicar la sesión de navegación web que se esté llevando a cabo, capturar contraseñas y archivos que se transmitan. La pérdida de posesión es potencial porque puede que el atacante guarde toda la información sin revisar su contenido, es ese caso el atacante no ha vulnerado efectivamente la posesión de la información a menos de que elimine los datos originales, en un proceso destructivo de recaudo de datos. Pero además de la pérdida de posesión causada por una pérdida de confidencialidad, también existe el caso en que efectivamente se pierde posesión sobre los dispositivos, un computador portátil, un organizador personal o un PA, además de la información que pueden contener estos dispositivos se pierde la configuración de la WLAN, comprometiendo otros niveles de seguridad, con un organizador personal un atacante puede acceder a una red, haciéndose pasar por un usuario autorizado, o con los datos que se encuentran en un PA puede descifrar la clave usada por la red inalámbrica y luego intentar usarla. La pérdida de posesión física de los equipos se puede prevenir con

alarmas o seguridad física, pero luego de que se pierda la posesión es importante informar sobre la pérdida, para que se niegue el acceso a ese dispositivo y se cambien las claves de red que estén en uso, incluso además de verificar la clave es importante verificar la identidad del usuario. De esta forma aunque se presente una pérdida de posesión, se mitigan futuras pérdidas potenciales. También es importante tener un proceso al momento de retirar dispositivos de la red, botarlos inmediatamente es una mala idea, tanto para puntos de acceso, como para computadores.

4. REDES CON SEGURIDAD ROBUSTA

El estándar 802.11i introduce el concepto de redes con seguridad robusta, en inglés Robust Security Network (RSN), una RSN es una red inalámbrica que solo permite la creación de asociaciones a redes con seguridad robusta, en inglés Robust Security Network Asociations (RSNA). Una RSNA es una conexión lógica entre dos dispositivos 802.11 que se establece a través del esquema de manejo de claves 802.11i, este esquema se llama apretón de manos de cuatro tiempos, que es un protocolo que valida que ambos dispositivos compartan una llave maestra par, en inglés Pairwise Master Key (PMK), que las llaves temporales se sincronicen y confirma la selección y configuración de los protocolos de confidencialidad e integridad. Los dispositivos obtienen la PMK de dos formas, o la PMK está configurada en cada uno, si es así, se llama llave pre-compartida, en inglés Pre-Shared Key (PSK), o se obtuvo como efecto de una autenticación exitosa contra un servidor de autenticación usando el protocolo EAP que es un componente de la especificación 802.1X que sirve para controlar el acceso.

Hay dos componentes en la definición de 802.1X que son usados para la creación de RSNAs, los servidores de autenticación y el control de acceso de 802.1X, el estándar IEEE 802.1X provee un marco de operación para el control de acceso que permiten la existencia de un servicio centralizado de autenticación mutua. Este estándar originalmente fue diseñado para redes cableadas y prevenir el acceso a usuarios no autorizados en ambientes abiertos, como un campus universitario, 802.1X permite bloquear a los usuarios hasta que estos se autentiquen correctamente, de esta forma se controla el acceso a los recursos de la WLAN.

La figura-8 muestra una vista conceptual de IEEE 802.1X, presentando todos los componentes fundamentales de 802.11i: varias EST, un PA y un servidor de autenticación, las estaciones buscan ser autenticadas y se denominan suplicantes y el PA es el que facilita la autenticación por esto se denomina el autenticador. Solamente hasta que haya una autenticación exitosa entre la EST y el servidor de autenticación, las comunicaciones de la EST son desbloqueadas por el PA, como el PA está en la frontera entre la red inalámbrica y la red cableada, esto evita que una EST no autenticada acceda a la red cableada. La técnica usada para bloquear las comunicaciones se conoce como control de acceso basada en el puerto. IEEE 802.1X puede distinguir los flujos de datos de paquetes de autenticación y paquetes normales de datos, solamente deja pasar los paquetes de autenticación por un puerto no controlado del PA, los demás paquetes pasan por un puerto controlado que puede bloquear el acceso. 802.11i extiende estas capacidades para que el PA bloquee la comunicación hasta que las claves estén debidamente utilizadas. Es así que 802.11i solamente permite que un PA no autorizado pueda solo ver datos de autenticación que ya están cifrados.

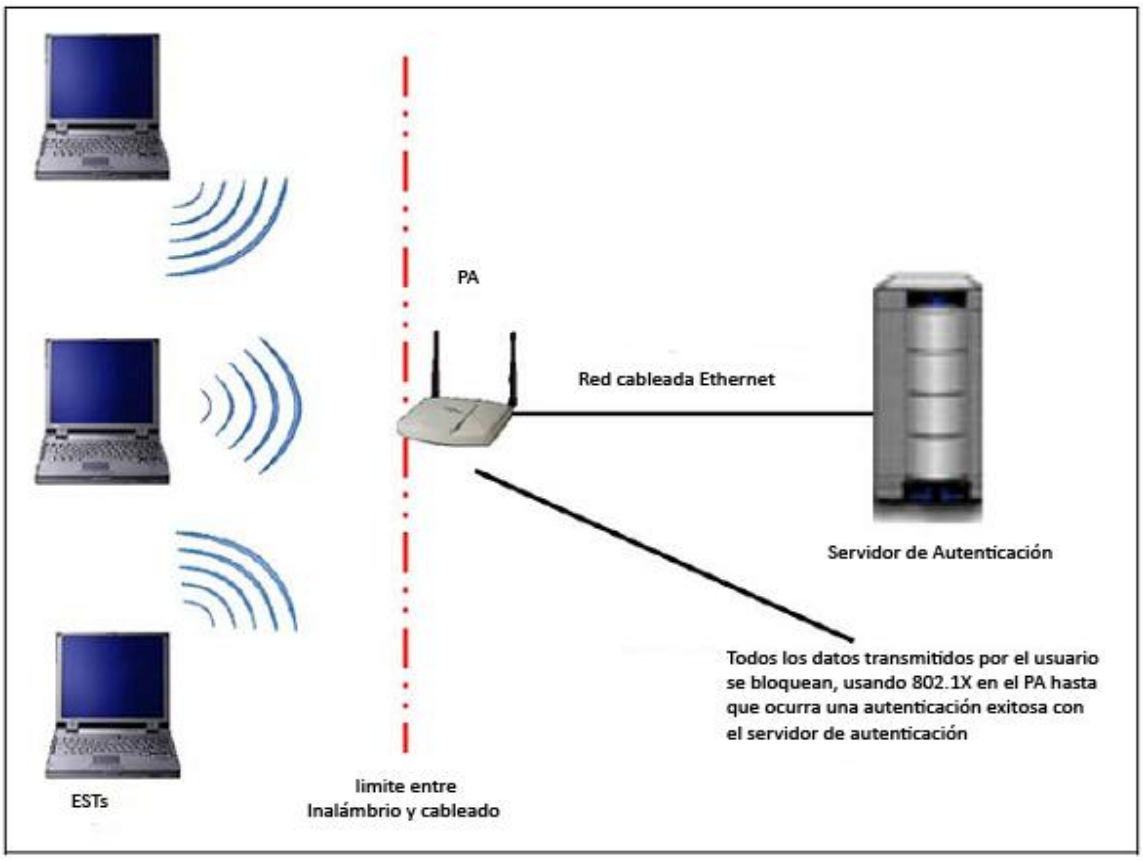

Figura 8 Vista conceptual de IEEE 802.1X (tomada de [3] traducida por el autor)

4.1. CARACTERÍSTICAS DE LAS REDES CON SEGURIDAD ROBUSTA

Luego de la ratificación del estándar 802.11i en 2004, IEEE 802.11 comienza a ofrecer dos clases generales de capacidades en seguridad para las WLAN, la primera clase, es la seguridad anterior a RSN, que incluye las capacidades originalmente ideadas para el estándar IEEE 802.11: autenticación basada en sistema abierto o por clave compartida para validar la identidad de la estación inalámbrica y WEP para proteger la confidencialidad del tráfico. La segunda clase de seguridad incluye mecanismos para crear RSN. Una RSN incluye mejoras en la seguridad para afrontar todas las debilidades conocidas de WEP y provee una protección robusta para el enlace inalámbrico, incluyendo integridad de datos y confidencialidad. [3] La figura-9 presenta una taxonomía de alto nivel de los mecanismos anteriores a RSN y de RSN.

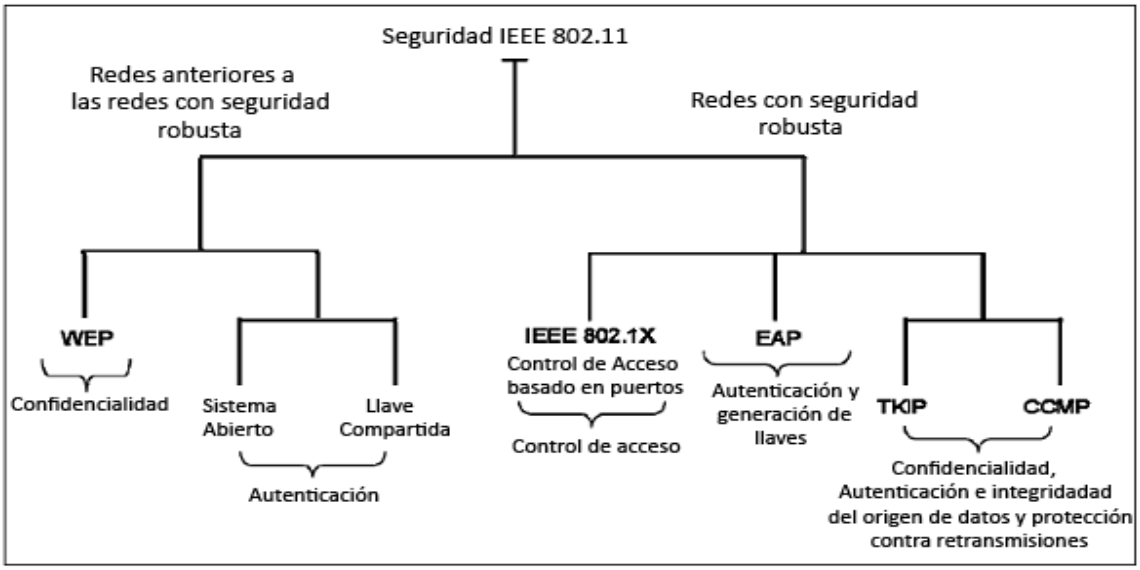

Figura 9 Mecanismos de seguridad usados en pre-RSN y en RSN (tomada de [3] traducida por el autor)

Si se describe desde un nivel alto RSN incluye control de acceso basado en puertos IEEE 802.1X, técnicas de administración de llaves, los protocolos TKIP y CCMP para la confidencialidad y la integridad de los datos, la seguridad RSN se encuentra solamente al nivel de enlace[4], brindando protección al tráfico entre una EST inalámbrica y su PA asociado, o entre una EST inalámbrica y otra EST inalámbrica. No brinda protección de punta a punta, por ejemplo entre una EST inalámbrica y un servidor de correo electrónico, o una EST inalámbrica y un servidor Web, porque estas comunicaciones entre entidades requieren de más de un enlace. Para tener protección de punta a punta, se puede implementar mecanismos a nivel de red como, seguridad en la capa de transporte, en inglés, Transport Layer Security (TLS) o IPSec. [3]

Una RSNA dispone de las siguientes características de seguridad para WLAN 802.11: [3]

- Mecanismos mejorados de autenticación de usuario
- Administración de llaves criptográficas
- Confidencialidad de datos
- Autenticación del origen de datos e integridad
- Protección contra la retransmisión

[4] Un protocolo a nivel de enlace describe las reglas de comunicación entre dos entidades sobre un medio de comunicación en particular, como el aire (redes inalámbricas) o varios tipos de cables (redes cableadas). Define como estas entidades deben ser tratadas, como debe ser usado el medio cuando mas de dos entidades lo están utilizando simultáneamente, y como corregir los errores de transmisión. Los protocolos a nivel de enlace se diferencian de los protocolos a nivel de red porque estos últimos se enfocan principalmente por enrutar los paquetes de datos por diferentes enlaces e incluso por diferentes medios.

Para poder ofrecer la seguridad robusta de una RSNA los diseñadores del estándar 802.11i usaron diversos algoritmos y técnicas criptográficas. En la figura-10 se muestra una taxonomía de los algoritmos criptográficos incluidos en el estándar 802.11i. Estos algoritmos pueden ser categorizados según su uso: Confidencialidad, Integridad o Generación de llaves. Todos los algoritmos usados en este estándar son simétricos, lo que significa que la misma llave criptográfica que usan para cifrar es la misma que usan para descifrar.

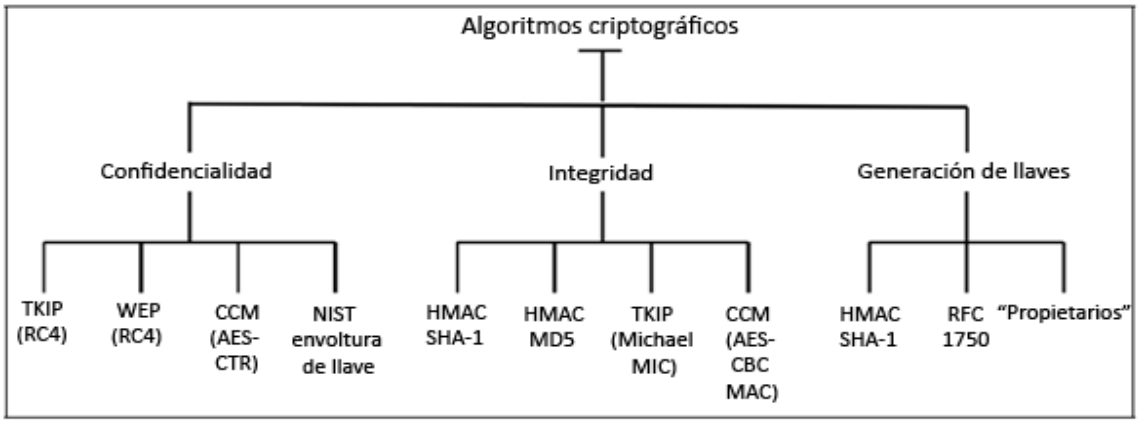

Figura 10 Algoritmos criptográficos incluidos en IEEE 802.11i (tomada de [3] traducida por el autor)

4.2. GENERACIÓN Y ADMINISTRACIÓN DE LLAVES

En todo sistema criptográfico son fundamentales las llaves criptográficas usadas en los procesos de transformación (cifrado – descifrado). Las llaves deben tener las siguientes características: [3]

- Generarse aleatoriamente para reducir la probabilidad de que puedan ser descubiertas por un atacante o de que sean reutilizadas.
- Cambiarse frecuentemente para reducir la posibilidad de ser descubiertas por medio de análisis criptográfico.
- Protegerse mientras se guarden, para evitar que comunicaciones anteriores sean descifradas.
- Protegerse durante la transmisión.
- Borrarse completamente cuando ya no se necesiten.

Estas características se desprenden de la administración de llaves, la administración de llaves se define como: el proceso de manipular y controlar, llaves criptográficas y material relacionado (como valores de

inicialización) durante su ciclo de vida en un sistema criptográfico, incluyendo la ordenación, generación, distribución, almacenamiento, carga, auditoria y destrucción del material. [3]

En las redes anteriores a RSN que usaban WEP no existía la administración de llaves criptográficas, normalmente solo existía una clave o un número pequeño de claves, para todos los dispositivos de la red y no existe un mecanismo estándar para la distribución de las llaves. IEEE 802.11i, define dos jerarquías para las llaves de las RSNAs que especifican las interrelaciones de las llaves. La jerarquía de llave emparejada que se utiliza para la protección de tráfico dirigido y la jerarquía de llave de grupo que se utiliza para proteger el tráfico multi-dirigido o de difusión.

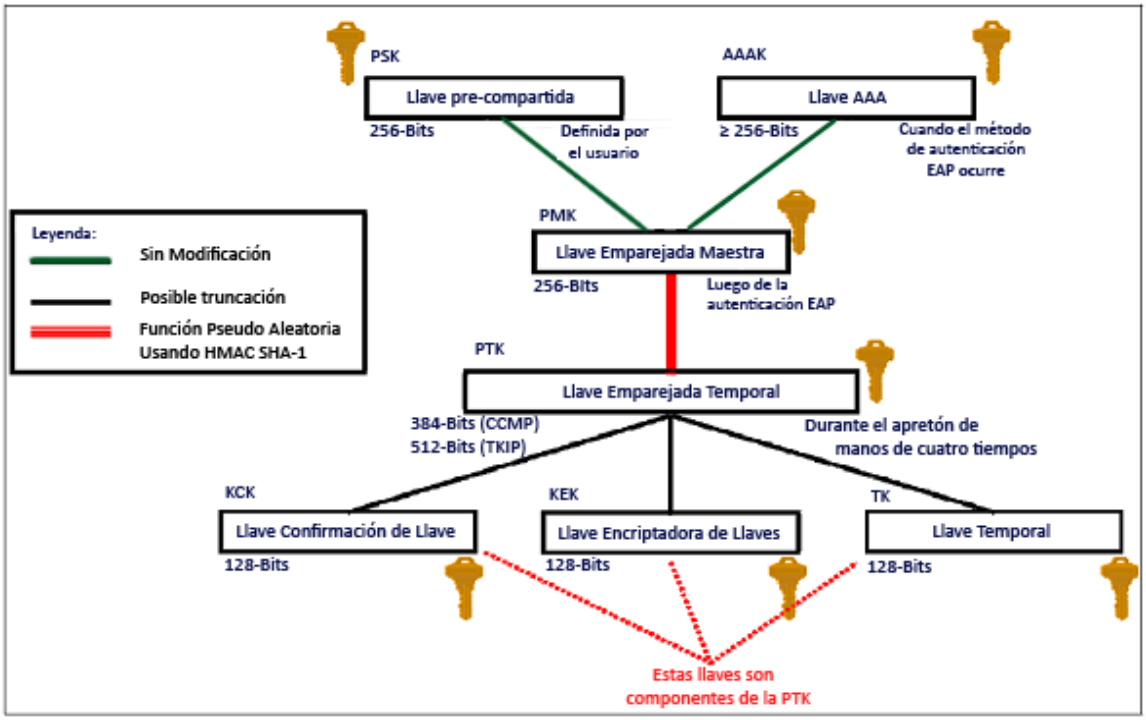

Figura 11 Jerarquías de llaves emparejadas (tomada de [3] traducida por el autor)

4.2.1. **Jerarquía de llave emparejada**, en la figura-11 se muestra la jerarquía de llave emparejada, las dos llaves que se presentan en la parte superior se conocen como llaves raíz, son usadas como base para generar todas las demás claves, las llaves raíz representan el método que se utiliza para instalar las llaves en los dispositivos:

Llave pre-compartida, es una llave estática que se instala en el dispositivo sin utilizar los canales inalámbricos, sino accediendo físicamente al dispositivo, por ejemplo usando un almacenamiento USB, o una palabra clave que luego se transforme en una llave conveniente. Si cualquiera de las PSK instaladas es atacada, debe instalarse una nueva en todos los dispositivos usando el método que se haya seleccionado. Una práctica común es asignar una

misma clave a cada SSID, así un usuario puede recorrer toda la red sin cambiar de conexión, pero esto tiene como consecuencia que un usuario puede descifrar todo el tráfico que se genere en esa WLAN así sea de otro usuario y un atacante externo también lo pueda llegar a hacer.

Llave de autenticación, autorización y control, en inglés Authentication, Authorization and Accountability Key (AAAK), la llave AAAK también se conoce como llave maestra de sesión o MSK, se instala en el PA usando el protocolo extendido de autenticación, en inglés Extensible Authentication Protocol (EAP) mientras se establece la RSNA, cada vez que un usuario se autentica a la red la AAAK cambia, la nueva clave se usa todo el tiempo que dure la sesión del usuario, la cual dura hasta que el usuario se des autentique o hasta que la vida de la llave termine. [3]

En la figura anterior se ve como la clave raíz PSK o AAAK, se utiliza para crear la llave emparejada maestra, en inglés Pairwise Master Key (PMK), PMK es una llave generadora de llaves, y se usa para derivar de ella la llave emparejada temporal, en inglés Pairwise Transiente Key (PTK), junto con la MAC de la EST y del PA, y valores aleatorios generados que cada uno crea durante el proceso de generación de la llave. Usar la MAC de la EST y del PA crea una mayor protección contra el secuestro de la sesión o la suplantación de una de las partes, los valores aleatorios dan una mayor entropía a todo el proceso, la PTK se compone de las siguientes tres llaves:

- EAP sobre red de cobertura local – llave confirmación de llave, en inglés EAP over LAN (EAPOL) Key Confirmation Key (EAPOL-KCK), se usa para soportar la integridad y la autenticidad del origen de los datos de control de la EST al PA durante la instalación operativa de la RSN. También cumple labores control de acceso: prueba que las partes poseen la PMK. Un dispositivo que tenga la PMK puede usar el enlace.

- EAPOL llave cifradora de llaves, en inglés EAPOL Key Encryption Key (EAPOL-KEK), que se usa para proteger la confidencialidad de las llaves y otros datos durante algunos procedimientos de una RSNA.

- Llave temporal, en inglés Temporal Key (TK), es usada para brindar protección del tráfico de usuario.

La figura anterior también presenta la longitud en bits de cada una de las llaves. La PSK es de 256 bits, AAAK es de 256 o mayor, la PTK tiene dos valores dependiendo del protocolo de integridad y confidencialidad usado, 128 bits para CCMP y 256 para TKIP. También se muestra cuando se crea cada llave. Por ejemplo la PMK se crea para cada sesión luego del proceso de autenticación EAP.

4.2.2. **Jerarquía de llave de grupo**, esta jerarquía se presenta en la figura-12, consiste de una sola llave, la llave temporal de grupo, en inglés Group Temporal Key (GTK). A diferencia de la PMK

que se genera usando información de la EST y del PA, la GTK es generada por el PA y transmitida a las EST asociadas con él, no existe una definición precisa sobre cómo se debe generar la GTK, lo único que requiere IEEE 802.11i es que su valor sea computacionalmente indistinguible de un valor aleatorio. [3]

La GTK es un valor de 256 bits para TKIP, de 128 bits para CCMP y 40 o 104 bits para WEP, en la figura también se muestra cuando se genera cada llave.

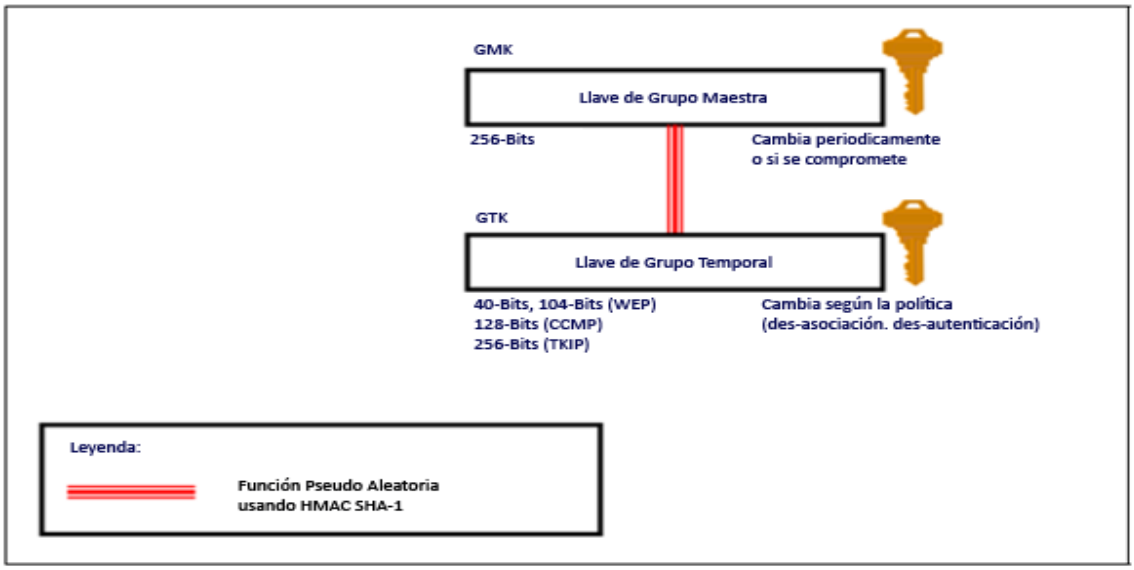

Figura 12 Jerarquía de llave de grupo (tomada de [3] traducida por el autor)

La tabla-4 hace un resumen de las llaves usadas por 802.11, según las especificaciones de 802.11i.

Abreviación	Nombre	Descripción/propósito	Longitud (bits)	Tipo
AAAK	Authentication, Accounting, and Authorization Key	Se usa para producir la PMK, es la misma MSK	>= 256	Llave generadora de llaves, llave raíz
PSK	Pre-Shared Key	Se convierte en la PMK, si se pre-comparte.	256	Llave generadora de llaves, llave raíz
PMK	Pairwise Master Key	Usada con otros datos para generar la PTK	256	Llave generadora de llaves
GMK	Group Master Key	Usada con otros datos para generar la GTK	128	Llave generadora de llaves

PTK	Pairwise Transient Key	Se deriva de la PMK, comprende la EAPOL-KCK, EAPOL-KEK, TK y en TKIP la llave MIC	512(TKIP) 384(CCMP)	Llave compuesta
TK	Temporal Key	Se usa con TKIP o CCMP para brindar confidencialidad e integridad a la información en un tráfico dirigido	256(TKIP) 128(CCMP)	Llave de tráfico
GTK	Group Temporal Key	Se deriva de la GMK, se usa para brindar confidencialidad e integridad a la información en un tráfico multi-dirigido o de difusión.	256(TKIP) 128(CCMP) 40,104 (WEP)	Llave de tráfico
MIC Key	Message Integrity Code Key	La usa TKPI para proveer protección de integridad a los mensajes	64	Llave de integridad de mensajes
EAPOL-KCK	EAPOL-Key Confirmation Key	Se usa para brindar integridad a las llaves distribuidas durante el proceso de apretón manos de 4 tiempos	128	Llave de integridad de mensajes
EAPOL-KEK	EAPOL-Key Encryption Key	Se usa para asegurar la confidencialidad de la GTK y otras llaves durante el proceso de apretón de manos de 4 tiempos	128	Llave de tráfico / llave cifradora de llaves
WEP	Wired Equivalent Privacy	Usada con WEP	40,104	Llave de tráfico.

Tabla 4 Resumen de llaves usadas por 802.11 (adaptada de [3])

4.3. PROTOCOLOS DE CONFIDENCIALIDAD E INTEGRIDAD

802.11i define dos protocolos RSNA para la confidencialidad e integridad de datos. Protocolo de integridad de llave temporal, en inglés Temporal Key Integrity Protocol (TKIP) y Protocolo de modo

contrario con cifrado en bloque encadenando MAC, en inglés Counter Mode with Cypher Block Chaining MAC Protocol (CCMP). TKIP fue creado para permitir que los dispositivos existentes pudieran afrontar las debilidades de WEP. TKIP puede ser implementado a través de una actualización de software, sin requerir cambios en el hardware en los PA o en las ESTs. Sin embargo TKIP usa RC4 (el mismo cifrado de WEP) y el código de integridad de mensaje Michael MIC, que tienen debilidades conocidas. Por esto TKIP no es la mejor alternativa cuando se requiere la mejor protección, en esos casos es mejor usar CCMP. Pero CCMP es un protocolo que computacionalmente es más exigente y no se puede implementar en dispositivos anteriores a RSN. Es obligatorio que todos los dispositivos que soporten RSNA implementen CCMP, TKIP es opcional.

4.3.1. TKIP

TKIP es un protocolo de cifrado que amplía el protocolo WEP en hardware anterior a RSN sin causar una degradación significativa en el desempeño. TKIP ofrece las siguientes características de seguridad para WLAN 802.11:

- Protección de la confidencialidad usando el algoritmo de cifrado RC4. [3]
- Protección contra varios tipos de ataques contra la integridad de los datos, usando un algoritmo que genera un código de integridad para los mensajes (MIC). [3]
- Prevención del reenvio de paquetes de datos, por medio de una técnica que secuencia los paquetes. [3]
- Uso de una nueva llave con cada paquete de datos, para prevenir ataques como Fluhrer-Mantin-Shamir (ataque FMS) que es uno de los principales ataques que compromete la confidencialidad en WEP. [3]
- Implementación de medidas cuando una EST o un PA encuentra un paquete de datos con un error MIC, lo cual es un indicador fuerte de que un ataque puede estar ocurriendo. [3]

4.3.2. CCMP

Al igual que TKIP, CCMP fue diseñado para afrontar las debilidades que tiene WEP, con la diferencia de que CCMP fue diseñado sin pensar que fuera compatible con los dispositivos anteriores a RSN. Se considera que CCMP es la solución a largo plazo para la creación de RSNs para WLANs.

CCMP se basa en CCM que es un modo autenticado genérico de cifrado en bloque de AES (AES es un estándar de cifrado usado mundialmente y de uso obligatorio en las agencias de gobierno de los Estados Unidos, en inglés Advanced Encryption Standard). CCMP protege la integridad de los datos transmitidos y también de los encabezados del paquete de datos usando una TK de 128 bits para proteger el canal.

CCMP tiene las siguientes características de seguridad:

- Una sola llave criptográfica para manejar la confidencialidad y la integridad de los datos, así se minimiza la complejidad y se maximiza el desempeño. [3]
- Protección de la integridad del encabezado del paquete de datos y de los datos, además de la confidencialidad de los datos. [3]
- Computación de algunos parámetros antes de recibir los paquetes y así posibilitar una comparación rápida cuando lleguen, lo que reduce la latencia. [3]
- Computacionalmente liviano, lo que permite que pueda ser implementado en software o en hardware. [3]
- Poca sobrecarga relacionada con la seguridad de los paquetes. [3]
- No hay problemas por patentes pendientes o existentes. [3]

En la tabla-5 se muestra una comparación entre las características de seguridad de WEP, TKIP y CCMP.

Característica	WEP (Pre – RSN)	TKIP (RSN)	CCMP (RSN)
Algoritmo Criptográfico	RC4	RC4	AES
Tamaño de llaves	40 o 104 bits (cifrado)	128 bits (cifrado) 64 bit (protección de integridad)	128 bits (cifrado y protección de integridad)
Llave por paquete	Creada al concatenar la llave WEP y el IV de 24 bits	Creada por el algoritmo de TKIP	No es necesaria, la TK es lo suficientemente fuerte.
Mecanismo de integridad	CRC-32	Michael MIC	CCM
Protección de encabezados	Ninguna	Direcciones de fuente y destino protegidas por Michael MIC	Direcciones de fuente y destino protegidas por Michael CCM
Protección contra retransmisión	Ninguna	Se usa una secuencia en el IV	Se usa una secuencia en el IV
Autenticación	Sistema abierto o clave compartida	Metodo EAP con 802.1X o PSK	Metodo EAP con 802.1X o PSK
Distribución de llaves	Manual	802.1X o Manual	802.1X o Manual

Tabla 5 Comparación entre WEP, TKIP y CCMP (adaptada de [2])

4.4. Fases de operación en una RSN 802.11

Al agrupar los intercambios de paquetes según su función, la operación de una RSN puede pensarse que ocurre en cinco fases distintas: descubrimiento, autenticación, generación y distribución de llaves, transferencia protegida de datos y terminación de la conexión. La figura-13, presenta las fases y las asocia con los componentes de una red.

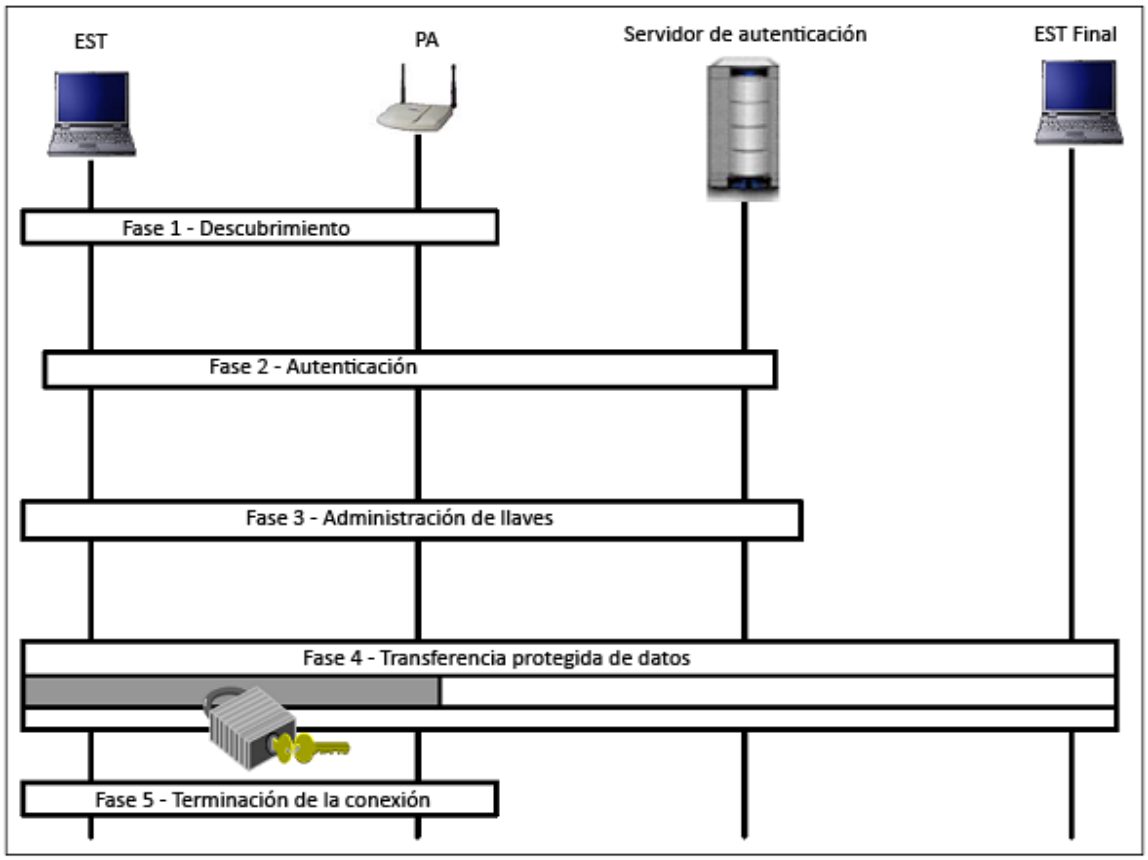

Figura 13 Fases de operación de una RSN 802.11 (tomada de [3] traducida por el autor)

4.4.1. Fase de descubrimiento.

Esta es la primera fase en el proceso de establecer una RSNA. Un PA hace pública su presencia por medio de los paquetes de señal y las respuestas de existencia. Además de su presencia también presenta sus características de seguridad. Una EST usa esos paquetes para identificar un PA de una WLAN con la que se quiere conectar. Un paquete de señal contiene una marca de tiempo, un intervalo de señal e información sobre las capacidades de velocidad y el SSID, el PA comunica las opciones que soporta y solamente los clientes que tengan configuraciones compatibles pueden intentar una conexión.

Durante la fase de descubrimiento las ESTs y los PA negocian los siguientes parámetros: [3]

- Protocolos de confidencialidad e integridad para proteger el tráfico.
- Método de autenticación para la identificación mutua del PA y la EST.
- Método para el manejo de llaves criptográficas.
- Capacidades de pre-autenticación.

El flujo de paquetes durante la fase de descubrimiento se divide en tres partes, en la primera, la estación hace una solicitud de existencia para ubicar los PA en el área, el punto de acceso responde con una respuesta de existencia, donde indica algunos parámetros de seguridad soportados, en la segunda parte la EST solicita una autenticación de sistema abierto, y el PA responde a la solicitud con un mensaje de éxito, la autenticación abierta se realiza solamente para mantener la compatibilidad con IEEE 802.11, en la tercera parte la estación hace una solicitud de asociación con los parámetros de seguridad escogidos, la estación responde con los parámetros de seguridad seleccionados, finalmente la EST usa los parámetros de seguridad, hasta este punto todo el tráfico ha ocurrido entre el PA y la EST usando el protocolo 802.1X. Todo este proceso se puede ver en la figura-14.

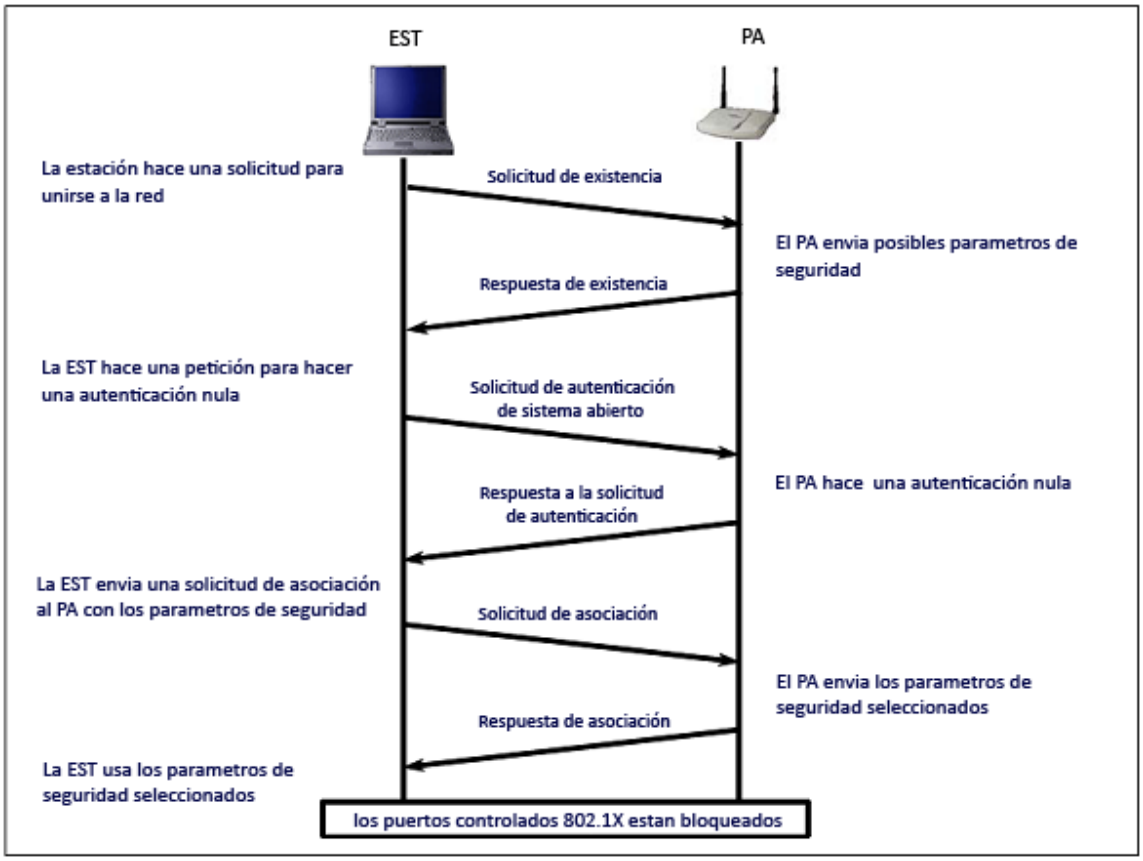

Figura 14 Flujo de paquetes durante la fase de descubrimiento (tomada de [3] traducida por el autor)

También es posible que no sea necesaria la primera parte, porque una estación estaba monitoreando pasivamente el tráfico a la espera de un paquete de señal de algún PA.

Durante esta fase una estación puede declinar comunicarse con un PA u otra EST que no entregue los siguientes datos: características de seguridad en los paquetes de señal o en las respuestas de existencia, un SSID, protocolos autorizados de autenticación y cifrado.

4.4.2. Fase de autenticación.

Al terminar exitosamente la fase de descubrimiento, la EST y el PA entran en la segunda fase para establecer una RSNA, la fase de autenticación. En esta fase la EST se identifica con la WLAN. Este paso es crítico para prevenir el uso no autorizado de los recursos de red. La autenticación mutua hace que la WLAN también se identifique ante la EST, esto le asegura a la EST que se está comunicando con una WLAN genuina. Durante esta fase el PA solo sirve para pasar el tráfico, no interviene de ninguna otra forma.

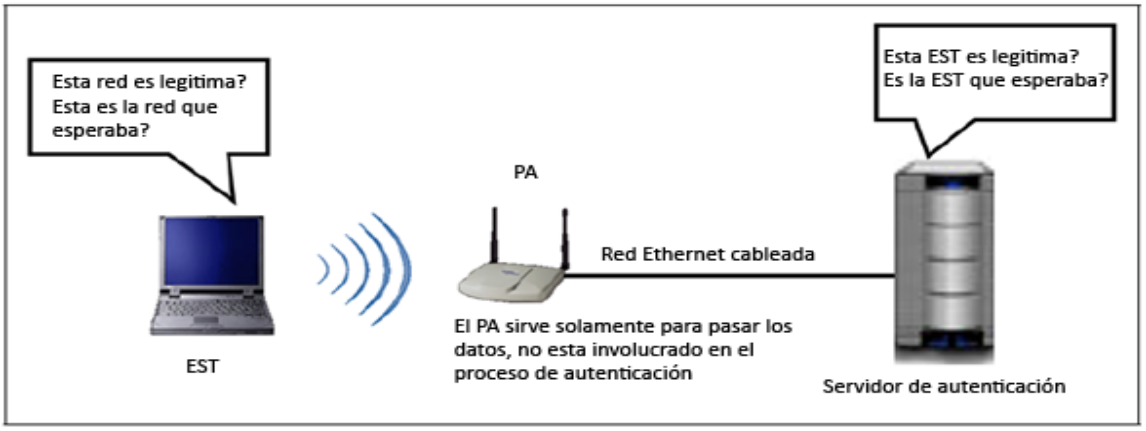

Figura 15 Concepto de autenticación (tomada de [3] traducida por el autor)

En la figura-15, se puede ver el concepto de autenticación que ocurre en esta fase. El proceso solo se lleva a cabo entre la EST y el AS que se localiza en la zona de distribución, el proceso está diseñado para evitar que ninguna de las estaciones pueda usar la red, excepto aquellas que están autorizadas para hacerlo.

Para proveer los servicios de autenticación mutua entre la EST y la WLAN, IEEE 802.11 usa el estándar IEEE 802.1X. Este estándar es un marco de trabajo extensible para la autenticación de usuarios, como mecanismo de autenticación se usa EAP. EAP a su vez es un marco de trabajo que permite usar diversos métodos para lograr la autenticación: claves estáticas, claves dinámicas, y certificados criptográficos de llave pública.

IEEE 802.1X tiene tres componentes principales: un cliente o suplicante, un autenticador y un servidor de autenticación. El autenticador pasa el tráfico entre el cliente y el servidor de autenticación. 802.1X controla el flujo de datos entre la zona de distribución y la EST usando el modelo de puertos controlados y no controlados para el envió de datos. Los datos de autenticación EAP pasan por un puerto no controlado en el autenticador, los datos que no son EAP pasan por un puerto controlado que los bloquea o los deja pasar, dependiendo del éxito o la falla que haya ocurrido al autenticarse.

El proceso para que la autenticación se efectúa es el siguiente: [3]

- El cliente opcionalmente puede comenzar con un mensaje de inicio.
- El intercambio EAP comienza cuando el autenticador hace una solicitud EAP solicitud-Identidad al suplicante.
- El suplicante responde con un paquete de EAP respuesta-identidad, el cual el PA recibe por el puerto no controlado. El paquete se encapsula y se pasa al servidor como un paquete de petición de acceso.
- El servidor replica con un paquete de acceso-desafío, el cual es pasado al suplicante como un paquete de EAP solicitud. Esta solicitud es del tipo apropiado de autenticación y contiene la información necesaria para el desafío.

- El suplicante arma un paquete EAP respuesta y lo envía al autenticador, la respuesta es convertida por el PA en un paquete de petición de acceso, con la respuesta en desafío entre sus datos. Este paso y el anterior pueden ser repetidos múltiples veces dependiendo del método EAP usado.

- El servidor de autenticación finalmente da acceso con un paquete de aceptación. El autenticador le envía al suplicante un paquete EAP éxito. El puerto controlado se autoriza y el usuario puede comenzar a usar la red.

- Durante la fase de terminación, cuando el suplicante termina de usar la red puede enviar un mensaje opcional de terminación para restablecer el puerto controlado a un estado de no autorización

La figura-16, presenta el flujo de paquetes usado durante la autenticación

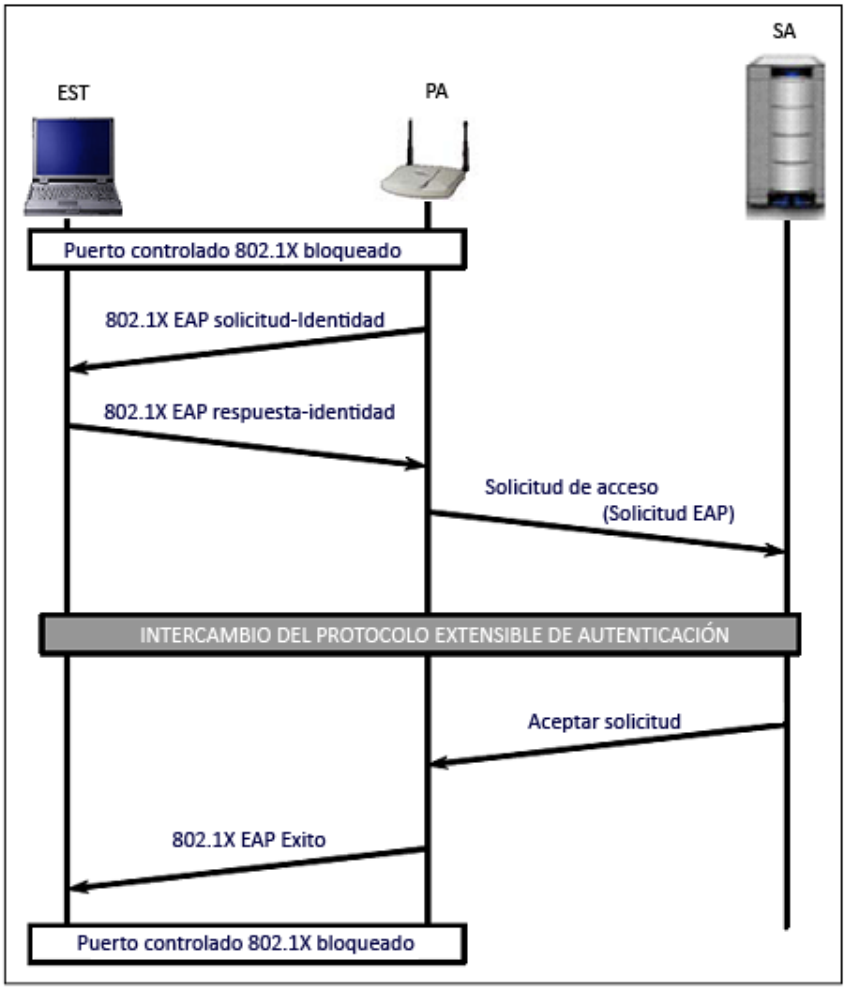

Figura 16 Flujo de paquetes durante la autenticación (tomada de [3] traducida por el autor)

Al completar la autenticación la llave AAAK está instalada en la EST y el AS, como se hablo anteriormente esta llave sirve como llave raíz y generar otras llaves que se usaran para asegurar las comunicaciones entre la EST y el PA.

Todo lo anterior es válido si se hace una autenticación usando AAAK, pero si se usa una llave pre-compartida PSK, la autenticación ya se completó en la fase de descubrimiento, en el momento en que la EST y el PA usaron la PSK, para así verificar mutuamente su identidad. Por lo tanto toda la fase de autenticación se salta, tal como se ve en la figura-17, ya que el uso de la PSK previamente sirvió para autenticarse, sin embargo los puertos controlados continúan bloqueados, previniendo que el tráfico de los usuarios pase a la zona de distribución, hasta que se complete la fase siguiente.

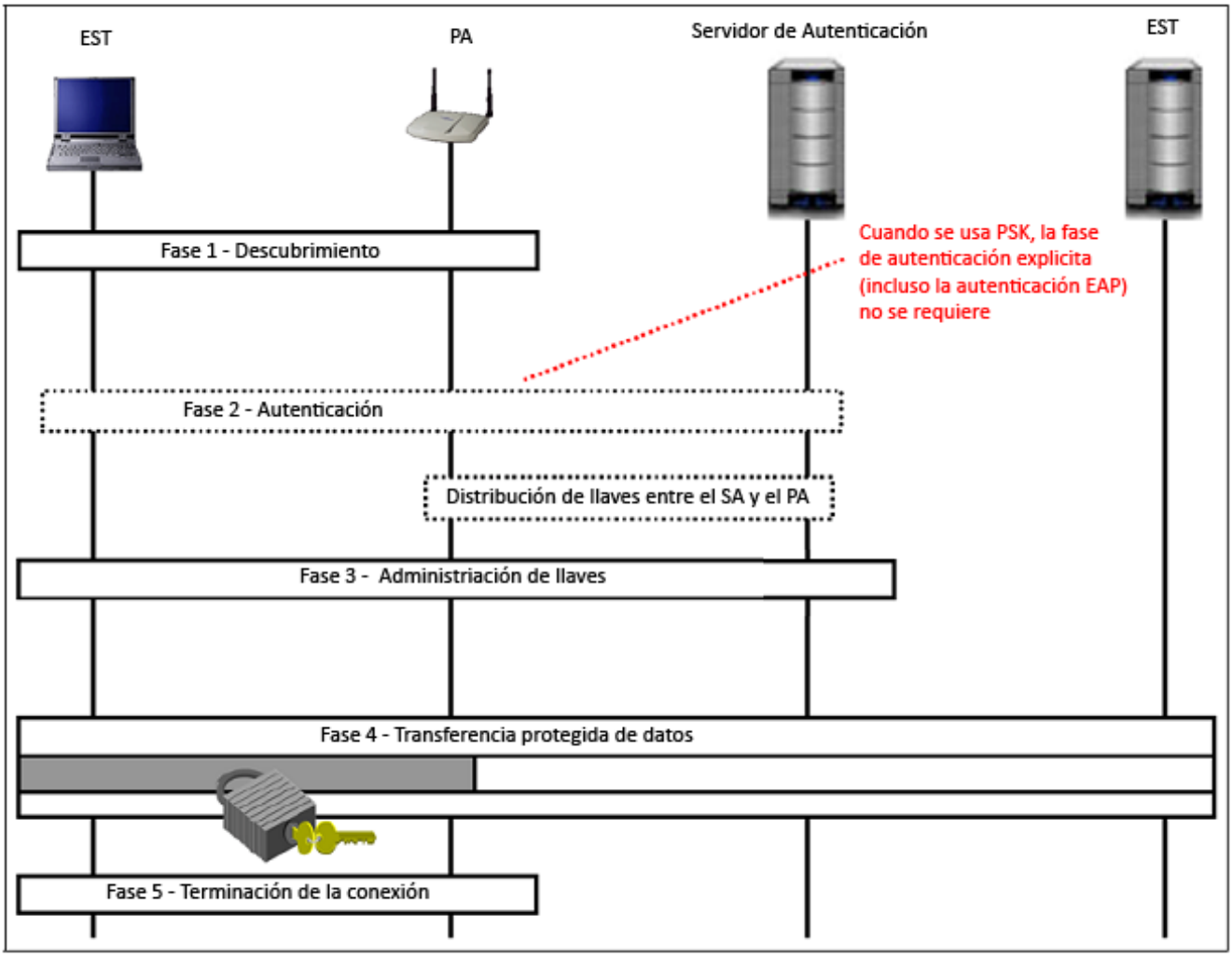

Figura 17 Autenticación cuando se usa PSK (tomada de [3] traducida por el autor)

4.4.3. Fase de generación y distribución de llaves.

Luego de completar satisfactoriamente la fase de autenticación, la EST y el PA realizan una serie de operaciones que activan las llaves criptográficas de las dos partes. Esta fase es la fase de generación y distribución de llaves, en inglés Key Generation and Distribution (KGD), es el último paso antes de que sea posible la transferencia segura de datos. La KGD tiene los siguientes propósitos:

- Confirmar la existencia de la llave emparejada maestra PMK. [3]
- Asegurar que las llaves de asociación son nuevas. [3]
- Derivar y sincronizar la instalación las llaves de tráfico (llaves temporales) en el PA y la EST.
- Distribuir la llave de grupo para tráfico multi-dirigido o de difusión. [3]
- Confirmar la selección de algoritmos de cifrados ya seleccionada.

La fase KGD tiene dos tipos de intercambio de paquetes. El apretón de manos de cuatro tiempos y el apretón de manos grupal, el tipo grupal solo se usa para tráfico multi dirigido o de difusión. Los dos tipos utilizan las siguientes características de seguridad: [3]

- Chequeo de la integridad del mensaje, para proteger contra alteraciones maliciosas y validar la fuente del tráfico
- Cifrado de los mensajes, para proteger contra una revelación no autorizada de los datos.

Como algoritmos de confidencialidad e integridad ambos tipos de apretones de manos pueden usar cualquiera de los siguientes:

- Cifrado RC4 con HMAC-MD5, RC4 es el algoritmo sobre el que se basa WEP. RC4 usa la llave de 128 bits de EAPOL-KEK que se deriva de la PTK
- Envoltura de llave AES con HMAC-SHA-1-128, la envoltura de llave AES fue diseñada para cifrar llaves criptográficas, la envoltura de llave separa los datos en bloques de 64 bits y los envuelve (cifra), este método usa AES en conjunto con la llave EAPOL-KEK

Apretón de manos de cuatro tiempos, La fase de generación y distribución de llaves comienza con el apretón de manos de cuatro tiempos, durante este proceso se intercambian cuatro paquetes entre la estación y el punto de acceso, al completar exitosamente el apretón

de manos el PA y la EST se han autenticado mutuamente. Es en este punto en el que los puertos controlados de IEEE 802.1X se abren para permitir el flujo de paquetes del tráfico de datos de usuario. El apretón de manos de cuatro tiempos se presenta en la figura-18 a continuación

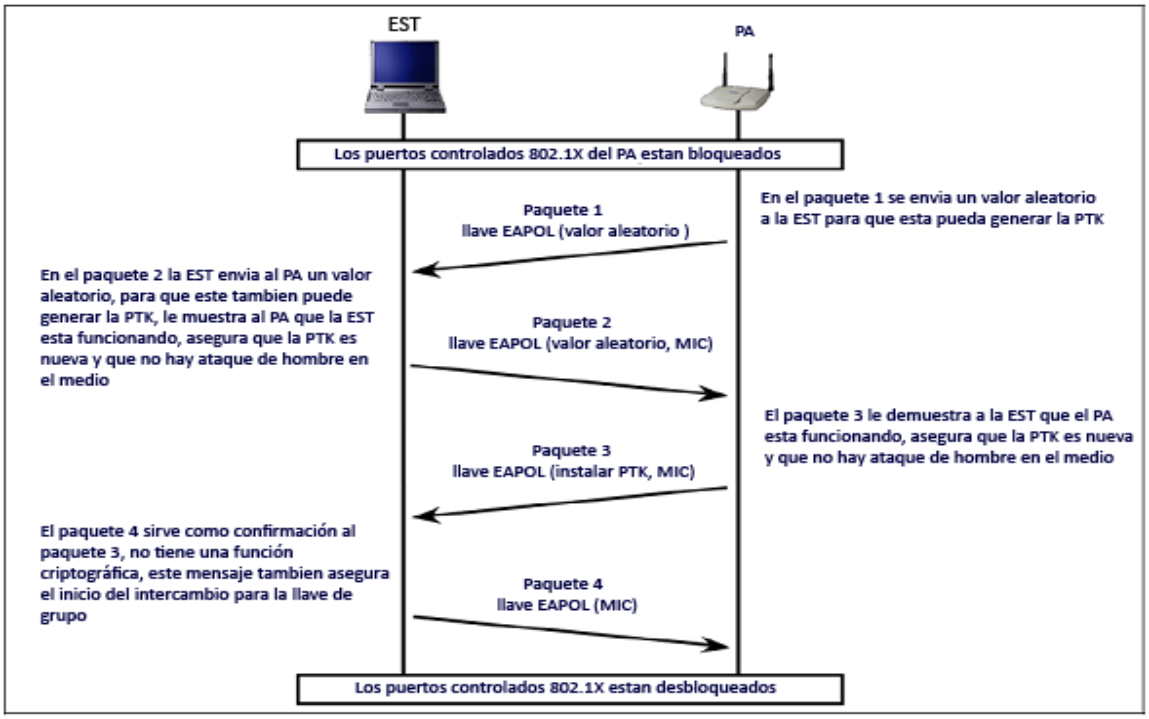

Figura 18 Apretón de manos de cuatro tiempos (tomada de [3] traducida por el autor)

El primer paquete, lo envía el PA a la EST, este contiene, un valor aleatorio, para que la EST pueda generar la PTK. El segundo paquete es de la EST al PA, en este paquete también se envía un valor aleatorio para que el PA también genere la PTK, este paquete le demuestra al PA que la EST está funcionando, sirve para asegurar que la PTK es nueva y que no hay un ataque de hombre en el medio. El tercer paquete le demuestra a la EST que el PA esta funcionando, le asegura que la PTK es nueva y que no hay un ataque de hombre en el medio. El cuarto paquete sirve como una confirmación al paquete 3, No tiene ninguna función criptográfica.

Los paquetes 2, 3 y 4 están protegidos por un código de integridad de mensaje (MIC), esto se hace para proteger los paquetes en su confidencialidad e integridad

Apretón de manos grupal, este mecanismo es usado por el PA para enviar a una EST la GTK, puede ocurrir luego del apretón de manos de cuatro tiempos o luego de la iniciación de la

EST. Es necesario hacerlo para soportar el tráfico multi dirigido o de difusión, se puede ver en la figura-19

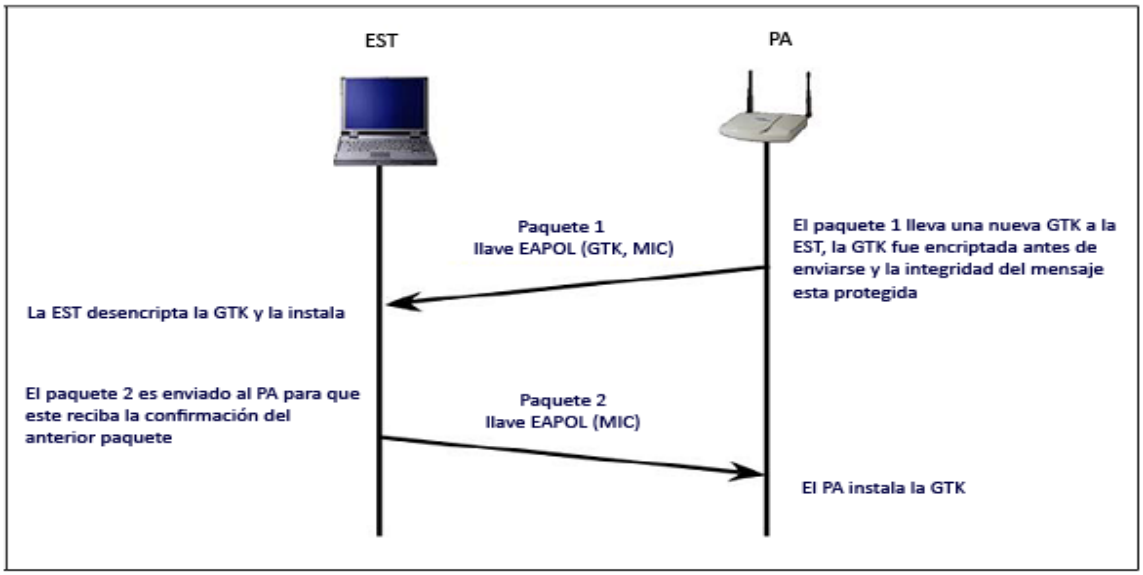

Figura 19 Apretón de manos grupal (tomada de [3] traducida por el autor)

En este caso solo se necesitan dos paquetes, el primero es enviado por el PA a la EST y en él se envía la GTK, la cual antes de ser enviada se ha cifrado, además se protege la integridad de todo el paquete. El segundo paquete es enviado por la EST al PA, y sirve solamente como confirmación para el PA.

Al completar correctamente el apretón de manos grupal el PA y la EST están listos para operar.

4.4.4. Fase de intercambio protegido de datos.

La cuarta fase en la operación de una RSN es la de intercambio protegido de datos, antes de esta fase el PA y la EST han tenido que haber hecho lo siguiente: [3]

- Haberse asociado y negociado los protocolos de autenticación
- Haberse autenticado mutuamente usando EAP
- Haber generado, distribuido y confirmado las llaves de sesión usando el apretón de manos de cuatro tiempos.

- Haber derivado un llave temporal emparejada y desbloquear los puertos controlados de IEEE 802.1X.

Estas acciones han preparado el PA y la EST para que se comuniquen seguramente. El tráfico entre el PA y la EST está protegido porque usa los algoritmos de confidencialidad e integridad de datos seleccionados en la fase de descubrimiento. El estándar IEEE 802.11 soporta tres métodos para la transferencia de datos: dirigido, multi-dirigido y difusión. [3]

El tráfico dirigido es el más utilizado durante esta fase, puede ocurrir cuando existe una sola asociación entre una EST y un PA y se utiliza una llave temporal emparejada para su protección. Los paquetes de este tipo de tráfico están protegidos por estar cifrados, tener protección de integridad, protección contra retransmisión y autenticación del origen de los datos.

Las transferencias multi-dirigidas y de difusión, permiten la transmisión de un dato en particular entre varios dispositivos eficientemente. La comunicación entre el PA y las ESTs se protege usando CCMP. Hay que tener cuidado porque la llave grupal se comparte entre todos los dispositivos, por lo tanto si uno solo es vulnerable, se afectan todos los demás.

4.4.5. Fase de terminación de la conexión.

La quinta fase, es la que termina la conexión, en esta fase se borra la asociación entre el PA y la EST y la conexión inalámbrica se termina. Esta fase es un final organizado de una conexión y la restauración a un estado inicial.

Durante la fase de terminación de la conexión, ocurren lo siguientes eventos: [3]

- El PA des autentica la EST.
- Las asociaciones de seguridad usadas internamente por el PA para seguir el rastro de las asociaciones entre STAs y PA se borran.
- Las llaves temporales usadas para cifrar y proteger la integridad del tráfico de datos, se borran.
- Los puertos controlados IEEE 802.1X vuelven a quedar en un estado bloqueado, para que el tráfico de usuario no pueda pasar.

La fase de terminación puede iniciarse por varios eventos, incluyendo los siguientes:

- La comunicación de radio entre el PA y la EST se pierde.

- El tiempo de validez del apretón de manos de cuatro tiempos o del apretón de manos grupal se vence durante su ejecución.
- El chequeo de los algoritmos de seguridad pactados durante la fase de descubrimiento, falla durante el apretón de manos de cuatro tiempos.
- El usuario apaga la EST o desactiva la tarjeta inalámbrica de red.
- La política de seguridad indica una terminación de la conexión

Al terminar esta fase la EST y el PA quedan en su estado inicial, si se requiere una nueva comunicación, entonces deben comenzar nuevamente todo el proceso.

III PARTE – INSTALACIÓN DE UNA RED INALÁMBRICA DOMÉSTICA

Crear una red inalámbrica doméstica es más fácil de lo que parece, hace un par de años estas redes eran escasas y costosas, pero con la penetración que ha tenido la banda ancha en Colombia y el aumento de computadores portátiles, se han popularizado enormemente. Otro factor que ha influido ha sido la caída en el precio de los equipos necesarios, hace 2 o 3 años los computadores portátiles que venían con una tarjeta de red inalámbrica se anunciaban con bombos y platillos, además de que se cargaban con un valor adicional, adicional a esto los enrutadores inalámbricos podían representar entre un 10 y un 20 por ciento del valor de un computador nuevo, pero ahora un enrutador inalámbrico se puede adquirir a un menor costo, representando un 5 por ciento o menos del valor de un computador nuevo. Pero tal vez el factor que más intimidaba es el factor técnico, en una época en la que algunas personas se intimidan incluso al fijar la hora de un televisor o de un reproductor de DVD, pensar en instalar una red inalámbrica doméstica podía parecer ciencia ficción, algo que solo algunos elegidos podían hacer.

En esta tercera parte se explicará de una forma sencilla y practica como instalar y proteger una red inalámbrica.

1. INSTALACIÓN DE LA RED

Para instalar una red inalámbrica doméstica se requieren al menos tres elementos, una conexión a Internet de banda ancha, un enrutador inalámbrico o punto de acceso, un computador que soporte redes inalámbricas, el proceso se puede resumir así: el punto de acceso se conecta a la conexión a Internet, se configura el punto de acceso para que transmita inalámbricamente y se configura el computador para que se conecte al PA usando la configuración que se hizo previamente. Al completar estos pasos, se tendrá una red inalámbrica doméstica, que brindará todos los beneficios de la comunicación sin cables y de movilidad, pero aún faltará por tratar la seguridad de la nueva red.

1.1. CUÁLES ELEMENTOS SE DEBEN SELECCIONAR

En la mayoría de casos, al pensar en una red inalámbrica, se piensa en acceder a internet, para navegar, revisar el correo, ver videos o escuchar música, todo de forma móvil, tal vez desde el jardín, o desde la cama, en estos casos, lo primero que se debe tener en cuenta al instalar una red inalámbrica doméstica es tener un servicio de acceso a Internet banda ancha. Hay otros casos que pueden ser complementarios al anterior, en el que al pensar en una red inalámbrica se piensa en comunicaciones entre varios computadores de una misma red, con una impresora, un asistente digital, con un servidor de archivos, en esos casos es necesario un enrutador inalámbrico, que además de proporcionar la comunicación inalámbrica, pueda entregar también comunicación cableada con los dispositivos que no tengan la opción inalámbrica, si toda la comunicación es entre los equipos de una misma red y todos tienen capacidades inalámbricas se puede pensar en una red inalámbrica ad-hoc, donde no es necesario

el uso de un enrutador, sino que los equipos se conectan entre sí sin intermediarios. Pero este último caso no es el más común para una red doméstica, para una red doméstica lo normal es que exista una mezcla de equipos inalámbricos con dispositivos cableados por eso se recomienda usar un enrutador inalámbrico, si no existen equipos cableado ni se prevé su uso, también es posible usar un punto de acceso inalámbrico, un punto de acceso inalámbrico solo tiene dos cables, un cable de poder que le da la energía que necesita y un cable a la conexión de internet, el enrutador en cambio, tiene adicionalmente la opción para que se conecten otros dispositivos cableados a él y usen la conexión directamente.

Según esto lo primero que se debe tener entonces es una conexión de banda ancha, esta conexión llega de diferentes formas a las casas o punto finales de la red, pero una vez en estos sitios, desemboca en un dispositivo MODEM. Lo segundo que se debe tener es un enrutador o un punto de acceso inalámbrico, este dispositivo transmitirá las señales que recibe de la conexión a internet o de otros equipos en la red y al mismo tiempo recibirá las señales dirigidas a él y las direccionará según el caso, en el mercado se encuentras estos dispositivos que usan tecnologías como 802.11a, 802.11b, 802.11g y pre 802.11n (pre porque aún no se ha aprobado completamente el estándar 802.11n), de todas esas, es recomendable usar 802.11g por la compatibilidad que tiene y cantidad de productos disponibles o 802.11n por la velocidad de transmisión y alcance que tiene, aunque en este caso es necesario tener precauciones extras con la compatibilidad de los productos, ya que es un estándar nuevo que no está completamente aprobado. Por último, es indispensable tener un computador que tenga un adaptador de red inalámbrico, no importa si es un computador portátil o un computador de escritorio, lo importante es que tenga la capacidad inalámbrica, si no la tiene de fábrica se debe comprar un adaptador inalámbrico que se puede conectar en un puerto USB o en una bahía de expansión del computador.

Si quiere cubrir un área muy grande o por las características físicas del entorno no se logra un buen cubrimiento con un solo punto de acceso, es posible usar varios puntos de acceso que cubran toda el área que se necesita, si se usa más de un punto de acceso, es mejor usar la misma marca de equipos para minimizar problemas que se puedan presentar

En la figura-20, se puede ver una red doméstica con muchos dispositivos conectados simultáneamente, algunos inalámbricamente otros por cables, también se ve un segundo enrutador inalámbrico que aumenta el área de cobertura, como se ve en la figura solo un enrutador inalámbrico está conectado al MODEM y este a su vez a Internet, el enrutador conectado al MODEM es el que coordina todas las conexiones en esa red, incluyendo las cableadas y las inalámbricas, si un computador quiere comunicarse con otro computador en la misma red, es ese enrutador el que direccionará las comunicaciones para que puedan llevarse a cabo, así mismo si un computador quiere conectarse a Internet o desde Internet hay una conexión para la red interna, ese enrutador direccionará las comunicaciones.

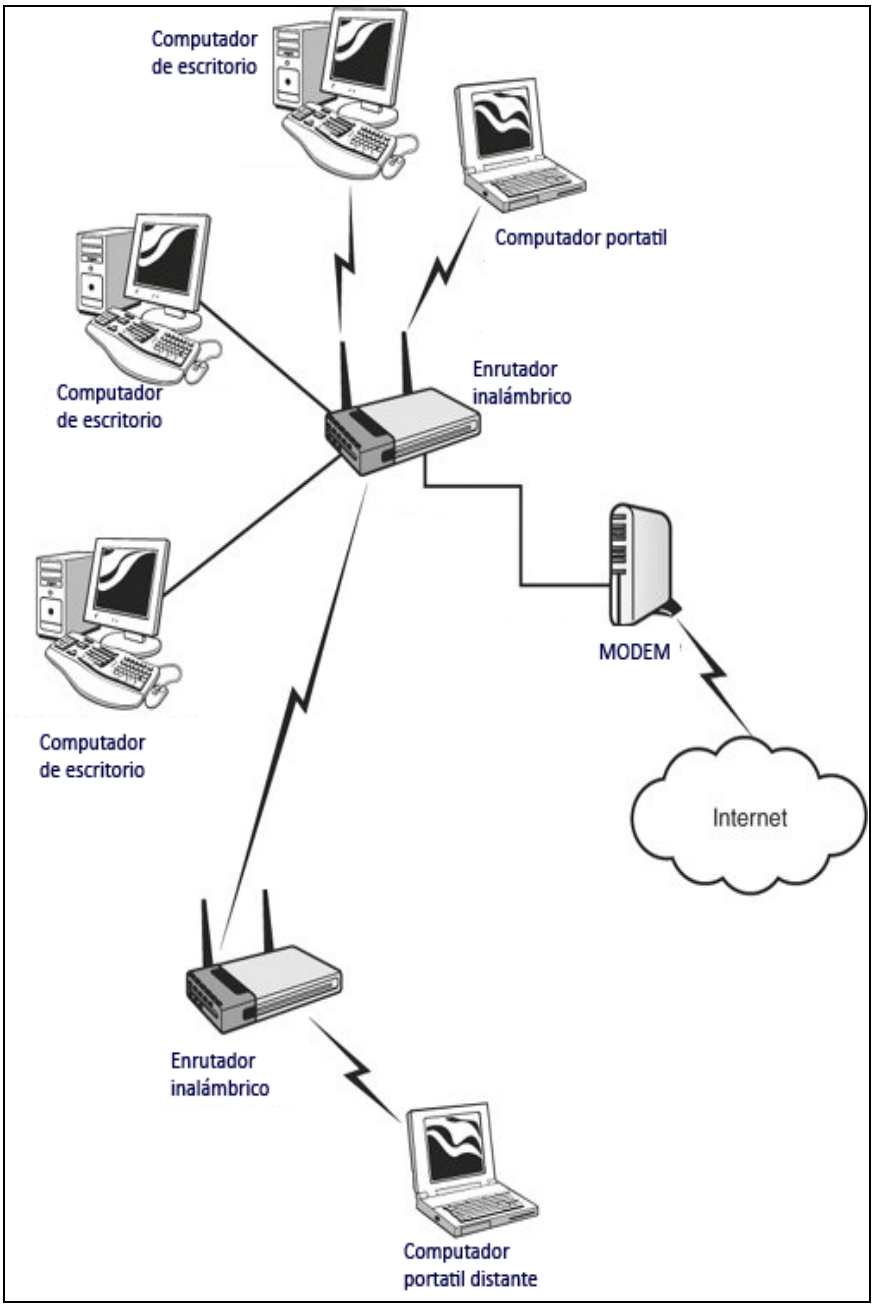

Figura 20 Ejemplo de una red doméstica

1.2. INSTALAR Y CONFIGURAR EL PUNTO DE ACCESO

Una vez se ha adquirido un punto de acceso, hay que decidir en cual parte de la casa se va a ubicar, lo normal es ubicarlo cerca del área de trabajo donde se tenga el computador, pero si hay más dispositivos que se necesiten conectar, lo mejor entonces es ubicar el punto de acceso en una ubicación central, de forma que se tenga un cubrimiento que abarque las áreas necesarias. Al ubicar el punto de acceso hay

que tener en cuenta los obstáculos cercanos, como paredes, techos, libros o cualquier otro obstáculo físico, los puntos de acceso no son elementos decorativos, por eso algunas personas tienden a esconderlos o ubicarlos en estanterías altas para que se vean lo menos posible, pero de esta forma se deteriora la calidad de la señal y el rango de cobertura. Si es necesario disminuir la visibilidad de un punto de acceso, entonces es mejor apuntar su antena alejándose del obstáculo así se asegura que la mayor cantidad de señal sea emitida y no sea absorbida. Una sola pared puede reducir el alcance de 1 a 30 metros. Si se usa un teléfono inalámbrico que funcione en la frecuencia 2.4GHz, hay que ubicar el punto de acceso lo más lejos de la base del teléfono, esta base transmite una señal continuamente aún sin usar el teléfono.

Una vez se ha decidido la ubicación del punto de acceso, el siguiente paso es realizar las conexiones, este es un proceso de 5 pasos:

- Apagar el MODEM, si el equipo no tiene un interruptor de encendido, hay que desconectarlo.
- Conectar el enrutador inalámbrico al MODEM, usando el cable que previamente conectaba el MODEM al computador. Conectar usando el puerto del enrutador inalámbrico marcado como Internet, WAN, WLAN.
- Conectar el computador al enrutador inalámbrico usando alguno de los puertos LAN destinados para ello. Se usará esta conexión para configurar el enrutador inalámbrico.
- Encender el MODEM, espere al menos 30 segundos, para que el MODEM puede iniciar completamente.
- Encender el enrutador

Cuando se completen estos pasos, usaremos el computador para configurar el punto de acceso, se hace de esta forma porque los puntos de accesos vienen de fabrica con el radio inalámbrico apagado, además si se hace una configuración del punto de acceso usando la seguridad que tiene de fabrica es probable que se esté usando una conexión no segura, o una en la que la clave de la red es conocida de antemano por un atacante.

Para realizar la configuración del punto de acceso, se puede usar el cd o dvd de instalación que viene con el equipo o ingresar a un explorador de internet e indicar una de las siguientes direcciones, que son usadas por las marcas más populares

Enrutador	Dirección	Usuario	Contraseña
3COM	http://192.168.1.1	admin	Admin
D-Link	http://192.168.0.1	admin	
Linksys	http://192.168.1.1	admin	Admin

Netgear	http://192.168.0.1	admin	Password

Tabla 6 Datos de configuración de algunos fabricantes (adaptada de [22]

En la figura-21 se ve una pantalla de inicio muy similar a las que se puede encontrar luego de visitar una de las direcciones indicadas arriba

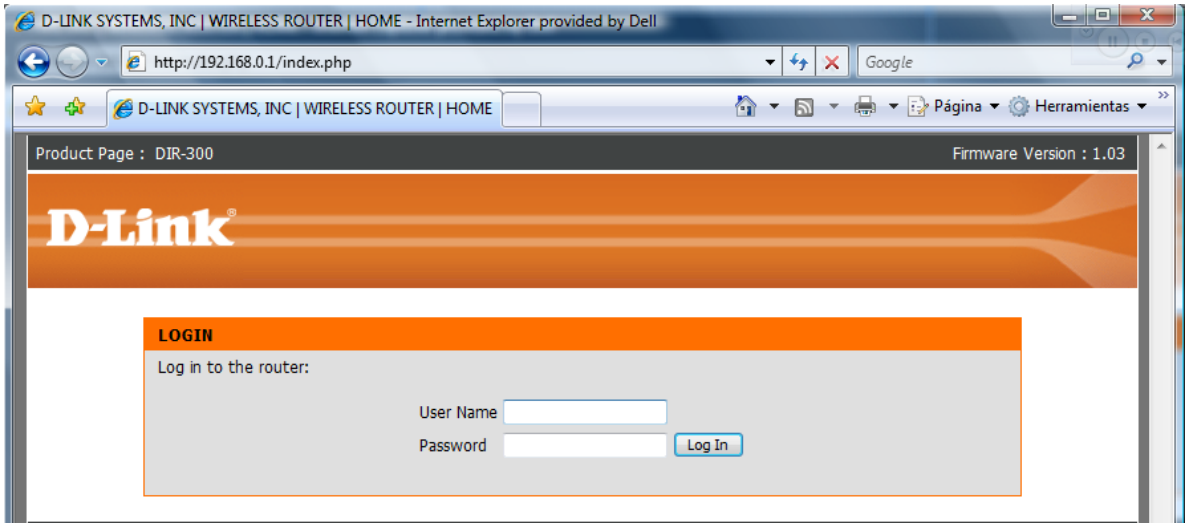

Figura 21 Ventana para iniciar sesión en un enrutador inalámbrico

Tanto en la configuración usando una página web, como al usar el cd o dvd de instalación, se recomienda tener conectado al enrutador inalámbrico el último computador que estuvo conectado a Internet, para que estos equipos puedan tomar la configuración del computador, sin que sea necesario que el usuario tenga que hacer configuraciones manuales. Para esto se usan procedimientos paso a paso, que asisten en la configuración, estos asistentes incluyen pasos como asignar una nueva clave al enrutador inalámbrico (ya vimos que los enrutadores vienen con una clave estándar de fabrica o sin ella, y hay que proteger su configuración), también se configura la conexión a internet del punto de acceso y la hora interna del enrutador, lo cual es útil si alguna vez se registra la bitácora de registros.

Como queremos conectarnos a internet, esa parte del asistente nos interesa, en la figura-22 vemos las distintas opciones que encontramos en el asistente, antes de comenzar la configuración es prudente verificar con el proveedor del servicio de Internet las características de la conexión que se poseen.

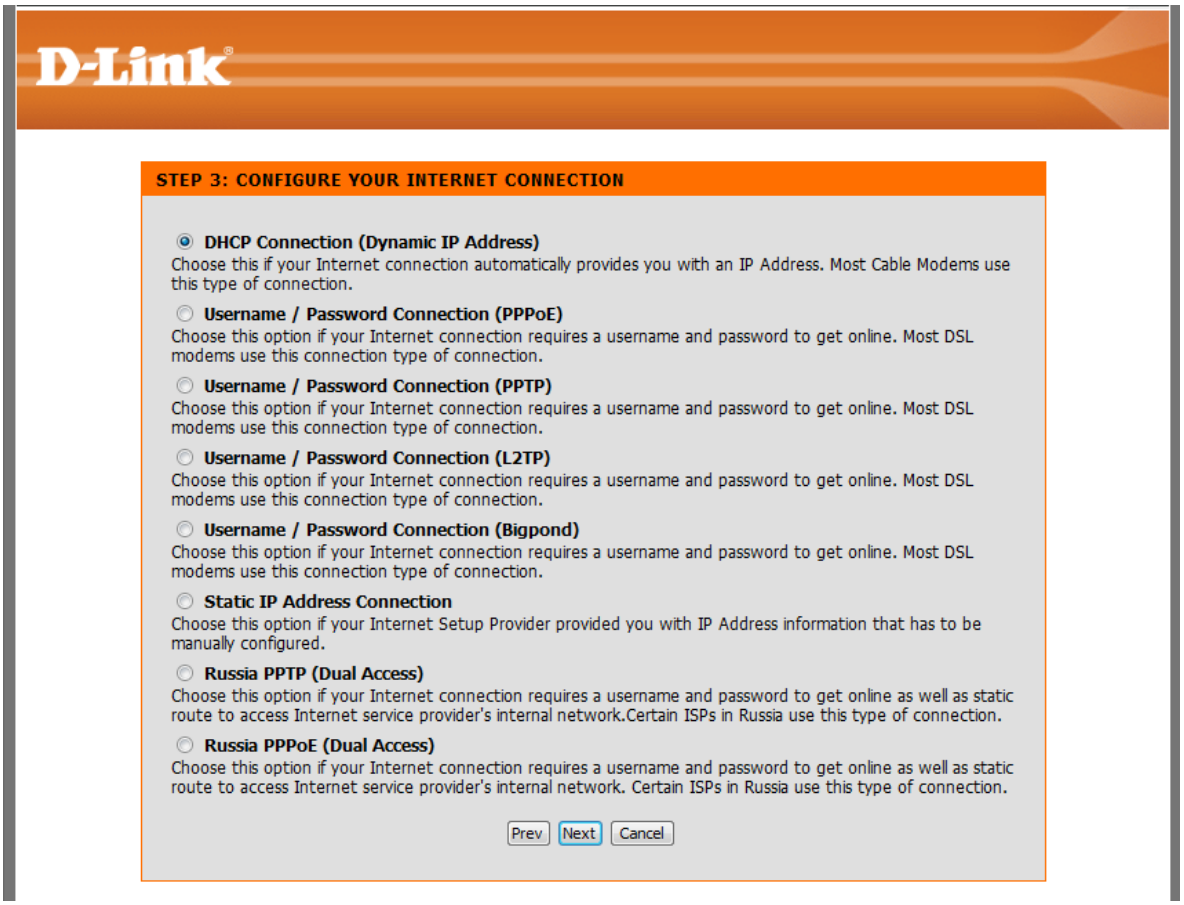

Figura 22 Tipos de conexiones a internet usadas por un punto de acceso

Las conexiones que usan DHCP son muy usadas en Colombia para las conexiones residenciales, este tipo de conexiones asignan dinámicamente una dirección IP al punto de acceso por un lapso de tiempo determinado y se renueva automáticamente, las conexiones DHCP en muchos casos están configurados por el proveedor de servicio para que solo puedan ser utilizadas por un solo computador, por eso el asistente ofrece la posibilidad de tomar la dirección MAC del computador y clonarla, de esta forma el proveedor de servicio piensa que sigue sirviendo al computador que ya tenía registrado, y el usuario se puede conectar a internet desde uno o varios computadores inalámbricamente, en la figura-23 se puede ver este paso. (Los datos aparecen tachados, como medida para proteger la privacidad)

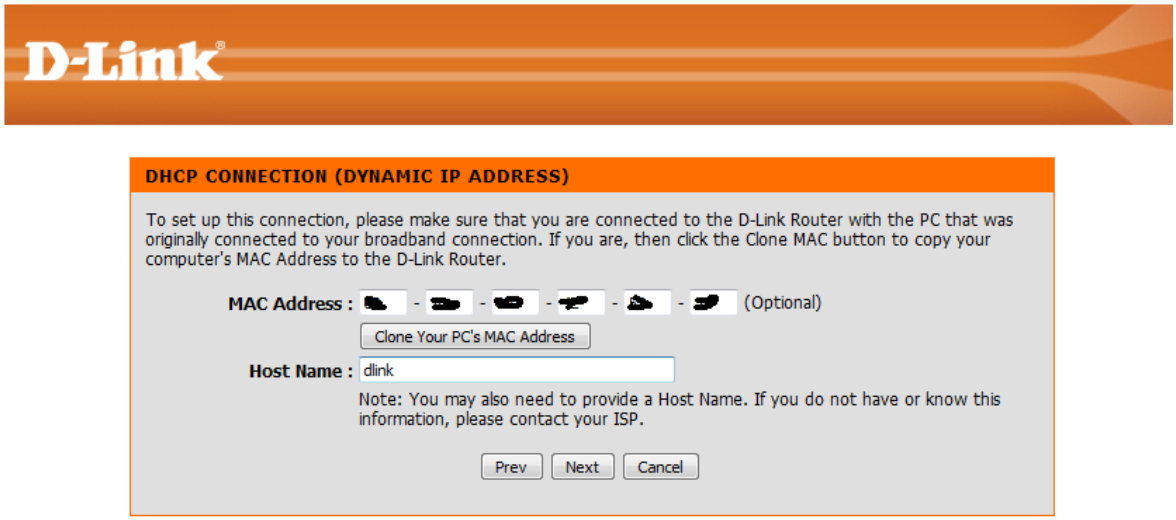

Figura 23 Clonación de una dirección MAC por el punto de acceso

Para cada uno de los métodos de conexión se presentan pasos específicos a ellos y que sirven para que el enrutador inalámbrico se pueda conectar a internet tal como lo hace un computador, hay que recordar que el enrutador inalámbrico ahora sirve como puente de salida y entrada para las conexiones a Internet, o sea que es el enrutador el que está conectado directamente a Internet.

Ahora que el punto de acceso está conectado a internet, hay que activar el radio inalámbrico y configurar la red inalámbrica, para este paso también existe un asistente paso a paso, en el que normalmente se le da un nombre a la red (SSID), se selecciona el nivel de seguridad y se asigna una clave a la red. En la figura-24 se ven algunos aspectos de la configuración.

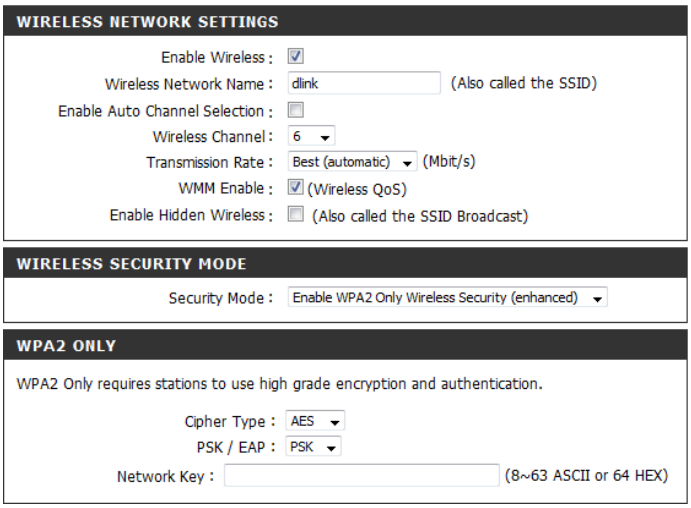

Figura 24 Configuración inalámbrica

Para habilitar la red, se debe tener activada la opción habilitar inalámbrico, sin esto el enrutador inalámbrico solo funcionará con redes cableadas.

El nombre de la red o SSID, es el nombre que identifica la red, es el nombre que transmite periódicamente el enrutador inalámbrico para indicar su existencia, y es el nombre que usan los dispositivos para señalar que se quieren conectar con esa red en particular. Por seguridad se recomienda usar un SSID que no se pueda relacionar con el propietario o el tipo de datos que se transmiten por esa red inalámbrica.

El canal inalámbrico, indica el espacio en el espectro electromagnético que usará el punto de acceso para sus comunicaciones, en América se usan casi siempre tres canales 1,6 y 11, aunque existen 11 o 12 canales para seleccionar, se usan mayoritariamente los canales 1,6 y 11, porque los canales no usan un espectro exclusivo, por ejemplo, si se usa el canal 6, y el vecino usa el canal 5, ambos canales entraran a competir, habrá interferencia mutua y ninguno de los dos tendrá la mejor señal, debe haber al menos 5 canales de diferencia entre redes para evitar interferencias. Pero si se vive en una zona densamente poblada por redes inalámbricas esto se hace más difícil, una opción entonces es dejar que el enrutador inalámbrico seleccione automáticamente el canal a usar o usar algún tipo de herramienta que permita identificar las redes inalámbricas cercanas con los canales que están usando, así se podrá seleccionar un canal poco congestionado, que entregará una mejor señal. Para hacer estas mediciones se puede usar un programa como netstumbler [www.netstumbler.com] o inssider [http://www.metageek.net/products/inssider], en la figura-25 se ve una pantalla del programa inssider funcionando.

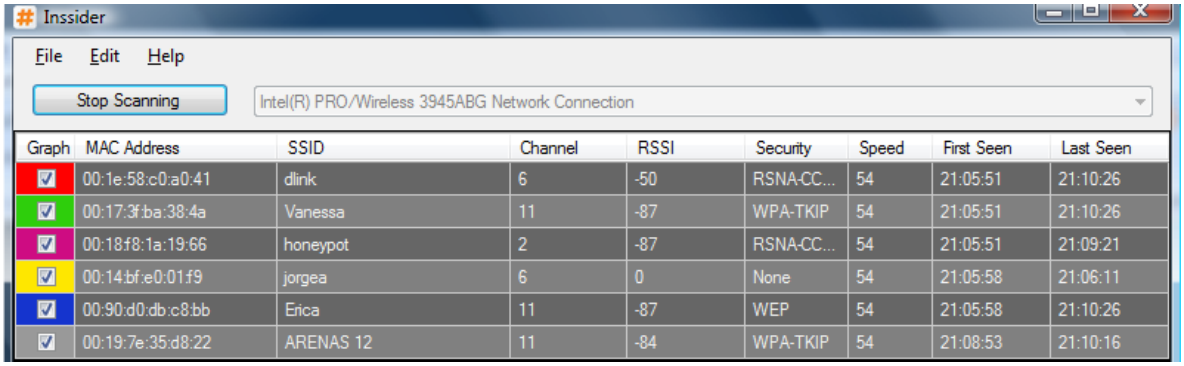

Figura 25 Muestra de los datos presentados por inssider

En la figura-25 se puede ver información interesante sobre las redes que hay alrededor, por ejemplo se ven los canales usados por las redes, con ese dato se puede decir que no es una buena idea usar una red en el canal 11 ya que hay tres redes transmitiendo por ese canal, en el canal 6 aunque hay dos redes, una es la red que se configurando y la otra tiene valor 0 en la columna RSSI (received signal strenght indication) o sea en la fuerza de la señal recibida, un valor de cero indica que no hay señal actualmente en esa red, los valores de fuerza de la señal, se deben interpretar como 100 menos el valor indicado, así un valor de -50, se puede ver como una fuerza de 100-50 o de 50 y un valor de -87 como un valor de 100-87 o sea 13 en la fuerza de la señal. A mayor fuerza de la señal, mejor señal.

La tasa de transmisión también puede ser configurada, con valores desde 1 Mbps hasta la máxima tasa de transmisión del punto de acceso, en este caso 54 Mbps, esto puede ser útil si se configura el punto de acceso para compartir una conexión a Internet abiertamente y no se quiere que el usuario consuma todo el ancho de banda disponible.

Este enrutador inalámbrico tiene la opción de habilitar la opción de QoS inalámbrica, QoS o calidad del servicio por sus siglas en inglés, es un método por el cual se le da prioridad a ciertas transmisiones que así lo requieren, por ejemplo a la voz por internet o el video se le da una mayor prioridad que a la navegación de una página web, de esta forma se intenta garantizar que la voz que se transmite y se escucha o el video que se está viendo, se disfrute con el mínimo de saltos e interrupciones.

Como medida de seguridad este punto de acceso también da la opción de no transmitir periódicamente la señal de existencia de la red inalámbrica, esta es una forma de proteger la red, ya que la red solo será detectada por un equipo que sepa de antemano el nombre de la red o que tenga programas para detectar las redes ocultas.

En el modo de seguridad, existen cinco opciones:

- Deshabilitar la seguridad inalámbrica
- Habilitar la seguridad inalámbrica WEP
- Habilitar solo la seguridad inalámbrica WPA
- Habilitar solo la seguridad inalámbrica WPA2
- Habilitar la seguridad WPA/WPA2

Deshabilitar la seguridad inalámbrica no es una buena idea, porque cualquier persona se puede conectar a la red, y usar o abusar de la red. Habilitar la seguridad WEP, es el nivel mínimo de protección, aunque WEP fue reemplazado por WPA y WPA2, sigue siendo usado, WEP es inseguro y un atacante lo puede vulnerar en poco tiempo. Habilitar WPA es una buena opción si se tiene un computador con más de 2 años, provee un buen nivel de seguridad aunque también tiene sus fallas, WPA2 es el modo más seguro que se ofrece para redes inalámbricas, aunque existen vulnerabilidades teóricas, estas no han sido aprovechadas. Si no sé saben las características del adaptador de red del computador la mejor opción es habilitar WPA/WPA2 que da la mayor interoperabilidad entre equipos.

Si se selecciona WEP, se debe escoger entre autenticación abierta o autenticación por clave compartida (debe existir la misma clave en el enrutador inalámbrico y en el computador que se conecta). La autenticación abierta no ofrece ninguna protección, por eso no se recomienda, en la autenticación por clave compartida, hay varias opciones en el tamaño de la clave, normalmente 64 o 128 Bits, con 64 Bits, se puede usar una clave de letras y números de máximo cinco caracteres, con 128 Bits se puede usar una clave de letras y números de hasta trece caracteres.

Si se selecciona WPA o WPA2, hay que escoger el método de cifrado, TKIP o AES, TKIP es seguro pero puede ser atacado usando un ataque de diccionario, por lo tanto es mejor usar AES que es un método de cifrado más fuerte, como estamos configurando una red inalámbrica doméstica debemos seleccionar

PSK, (pre-shared key) o llave pre compartida, con el cifrado TKIP o AES, se puede seleccionar una clave de 8 a 63 caracteres, la clave puede incluir letras números y símbolos (¡?*&_) y espacios, se aconseja usar una clave larga, que use símbolos, letras y números, de esta forma se minimiza el riesgo de que un atacante pueda obtener la clave.

Una vez se han ingresado los parámetros necesarios, se ha habilitado la red, se ha indicado el canal o se ha señalado que el enrutador inalámbrico seleccionará el mejor canal, que se le ha dado un nombre a la red, se ha escogido un método para proteger la red, y se ha asignado una clave, solo queda salvar los cambios, esperar mientras el punto de acceso reinicia, desconectar el computador al punto de acceso y seguir con el siguiente paso.

1.3. INSTALAR Y USAR EL ADAPTADOR DE RED

Para que un computador se pueda comunicar en una red cableada o inalámbrica, el computador debe tener un adaptador o tarjeta de red, el adaptador de red sirve para conectar el computador al medio de transmisión, los adaptadores de red, también se conocen como tarjetas de red, en este momento todos los computadores portátiles vienen de fábrica con un adaptador de red inalámbrico, o se puede agregar uno al computador al momento de pedirlo por un valor adicional, los fabricantes de procesadores como Intel o AMD han desarrollado procesadores que tienen integrada la funcionalidad inalámbrica, Intel desarrollo el procesador Intel Centrino y AMD el procesador AMD Turion Mobile.

Un computador de escritorio también necesita de un adaptador de red inalámbrico, para ello se puede instalar uno en una bahía de expansión, un proceso que es preferible lo realice un técnico o una persona con conocimientos técnicos en computadores, pero también se puede usar un adaptador de red inalámbrico que se conecte a un puerto USB, en este caso solo se requieren conocimientos técnicos mínimos.

Independiente de si se tiene un adaptador ya instalado de fábrica, uno que se instale en una bahía de expansión o uno que se conecte a un puerto USB, es importante que el adaptador se pueda comunicar con el enrutador inalámbrico, en los equipos nuevos, los adaptadores de red son compatibles con el estándar 802.11 a/b/g lo que los hace prácticamente compatibles con todos los enrutadores inalámbricos. Pero si se usa un enrutador 802.11n es mejor verificar antes que el adaptador de red se pueda conectar y aprovechar las ventajas en velocidad y alcance que ofrezca una red 802.11n. Además es importante verificar que el adaptador de red inalámbrico sea compatible con WPA/WPA2 para poder tener una mejor seguridad.

Cuando se tenga el adaptador de red inalámbrico, si el computador ya lo traía de fabrica no hay que realizar instalación del dispositivo, si es un adaptador nuevo, es casi seguro que luego de conectarlo el computador lo detecte y comience la instalación, usando el software que trae el adaptador. Los computadores portátiles nuevos a veces traen un interruptor físico o lógico para encender el adaptador de red inalámbrico, esto lo hacen los fabricantes para que el computador no esté todo el tiempo buscando señales inalámbricas, como ventaja trae que así se ahorra batería, ya que el adaptador de red inalámbrica solo se enciende cuando es necesario. Se debe verificar con el manual del computador el funcionamiento de dicho interruptor. En la figura-26 se ve un interruptor de los mencionados.

Figura 26 Interruptor que controla la tarjeta de red inalámbrica

Una vez esté instalado el adaptador de red inalámbrico, y se sepa como activar el adaptador, el siguiente paso es configurar el sistema operativo para que establezca una conexión inalámbrica.

1.4. CONFIGURAR EL SISTEMA OPERATIVO

En Windows XP y Windows Vista, una vez se ha activado el adaptador de red inalámbrico, este indica si hay redes inalámbricas dentro de su rango de cobertura, tal como se ve en la figura-27

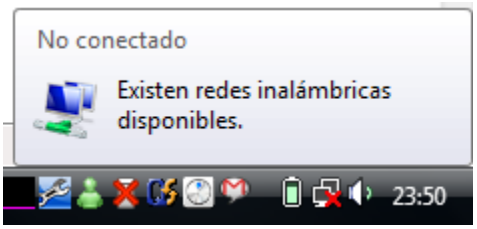

Figura 27 Indicador de redes inalámbricas existentes

Si se da clic derecho sobre este mensaje, aparece la opción para conectarse a una red, tal como se ve en la figura-28

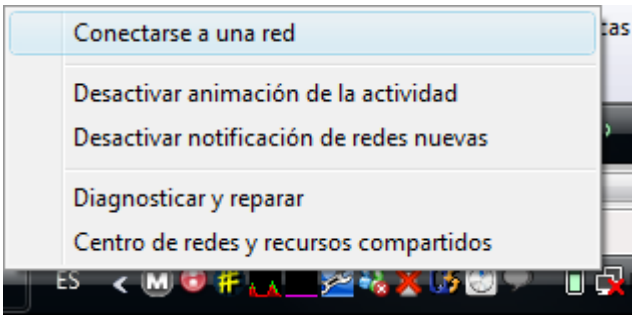

Figura 28 Opción de conectarse a una red inalámbrica

También puede hacerse, al dar clic en el botón inicio y seleccionando la opción “conectar a”, como se ve en la figura-29

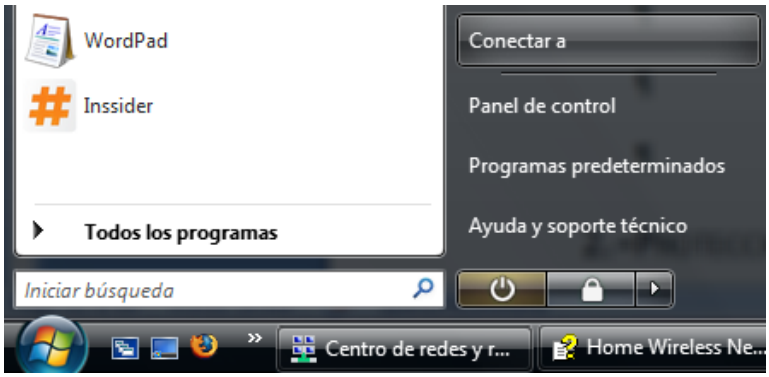

Figura 29 “Conectar a” en Windows vista

Con cualquiera de las anteriores opciones, se abrirá una ventana como la que se presenta en la figura-30

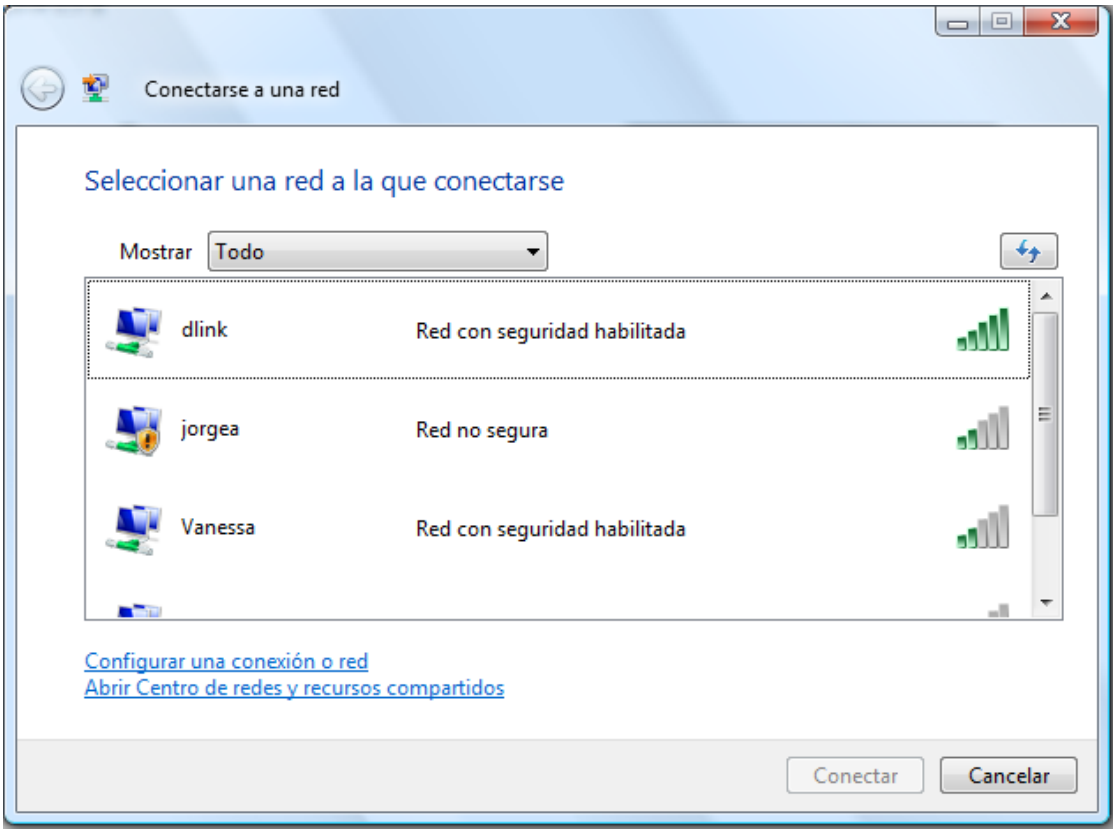

Figura 30 Redes disponibles para conectarse

En la figura-30 se pueden ver varias redes inalámbricas con sus respectivos nombres o SSID, también se puede ver el tipo si las redes tienen seguridad habilitada o si son redes no seguras (sin protección), y la fuerza de la señal que se recibe (entre mas barras, mejor señal), si la red tiene seguridad habilitada, al darle doble clic o un solo clic y luego seleccionar el botón conectar, se ve una pantalla como la de la figura-31

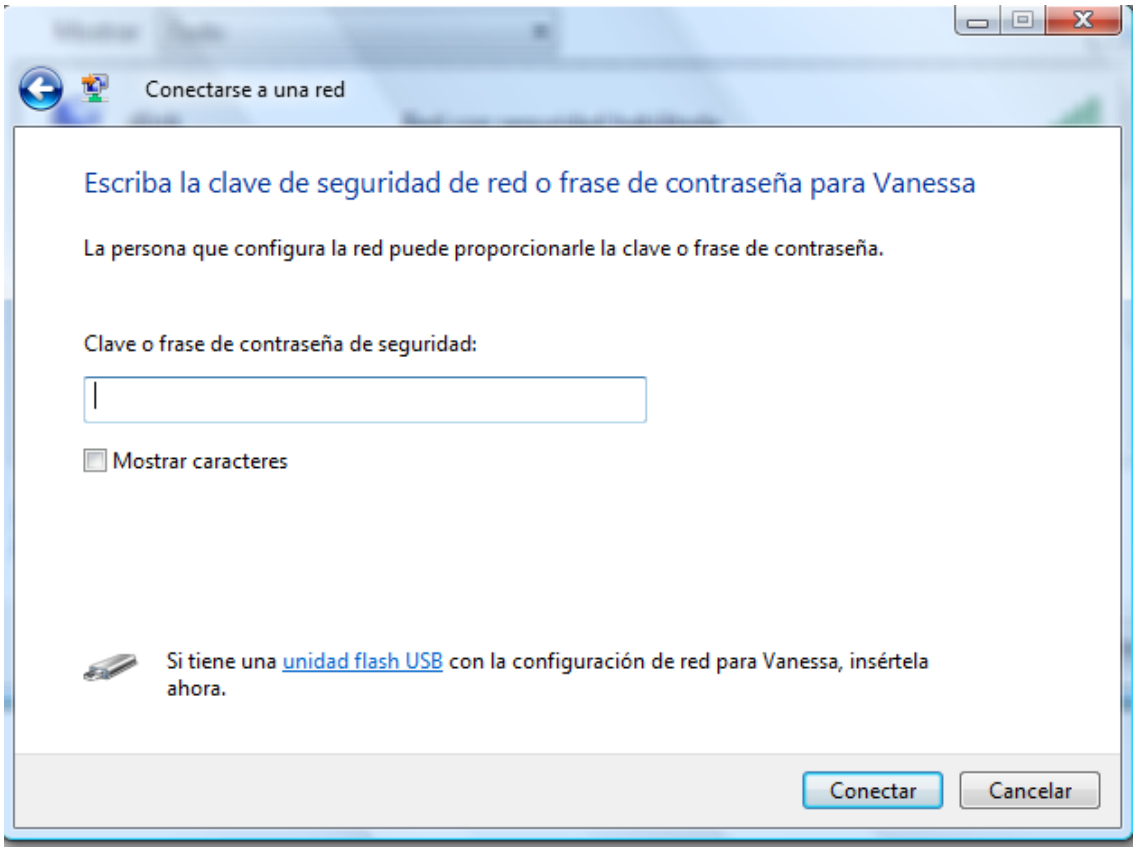

Figura 31 Ingreso de la clave de una red inalámbrica con seguridad habilitada.

En esa ventana se ingresa la clave que se definió para en el enrutador inalámbrico, puede dar clic en la opción para mostrar los caracteres y así ver la clave que se está introduciendo, de lo contrario solo se verán una serie de asteriscos *****, al terminar de ingresar la clave, se da clic en el botón conectar y el computador usando el adaptador de red inalámbrico, intentará establecer una conexión con el enrutador inalámbrico.

Como se pudo ver, al dar la clave para la red, no se indicó si se trataba de una red protegida por WEP, WPA o WPA2, para el usuario en este punto ese asunto es transparente y lo debe solucionar el computador. Si la conexión es exitosa se obtiene una pantalla como la de la figura-32

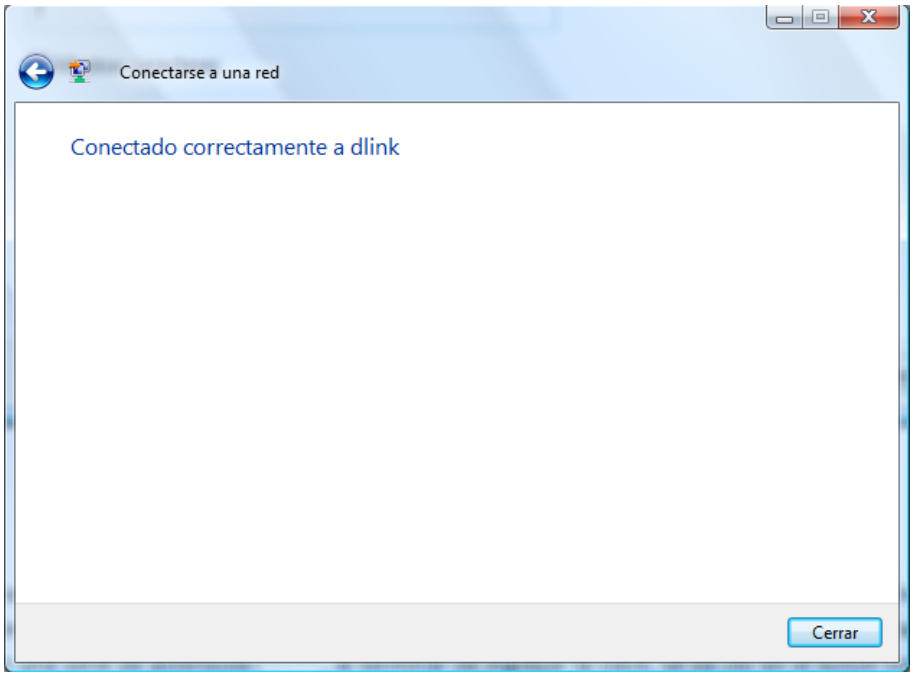

Figura 32 Mensaje de conexión satisfactoria

Si Windows no logra establecer una conexión, se presenta una pantalla como la de la figura-33

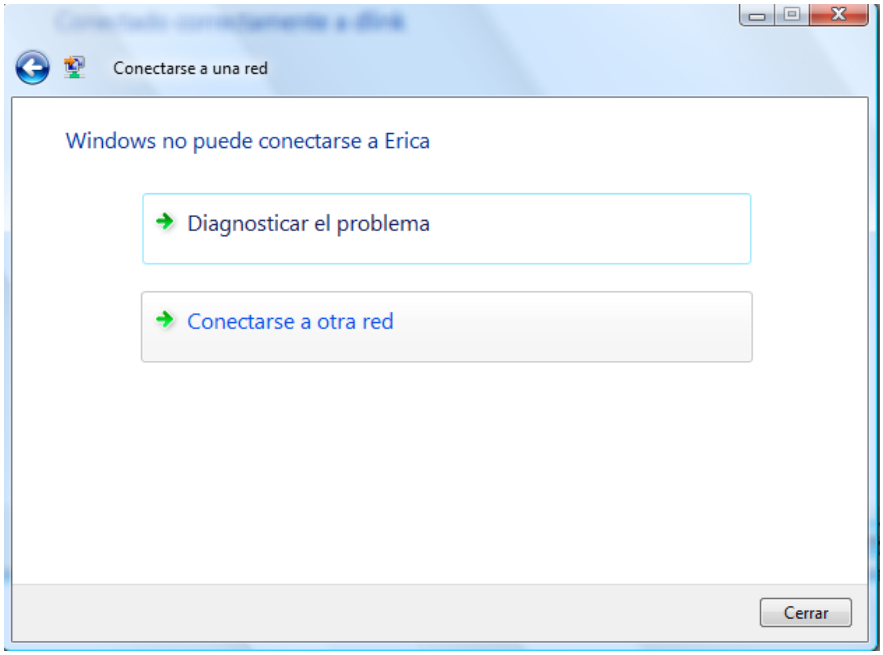

Figura 33 Error al establecer la conexión.

Algunos computadores vienen con software instalado que permite gestionar varias redes inalámbricas, haciendo más fácil conectarse a diferentes redes, sin estar cambiando parámetros o recordando claves, Windows también puede gestionar estas redes, cada que el adaptador de red es encendido este intenta conectarse automáticamente a las redes que tiene grabadas. Esto es práctico porque se obtiene una conexión automática, pero puede ser inseguro, ya que el computador para lograrlo transmite inalámbricamente el nombre de las redes a las cuales se ha conectado anteriormente, esto puede ser aprovechado por una atacante, si este decide hacerse pasar por un punto de acceso que esté en la lista de redes grabadas.

2. PROTECCIÓN DE LA RED

Cuando la red inalámbrica está funcionando uno puede creer que ya no hay nada más que hacer, solo disfrutar de las ventajas de la movilidad y olvidarse por completo de la red inalámbrica que se configuró, pero la seguridad de los datos siempre será importante, así, de la misma forma que es necesario tener un antivirus y un firewall instalado, es necesario proteger los datos que viajan por la red inalámbrica, los datos que se guardan en el computador, y la misma conexión a Internet para que no sea abusada por un atacante, todos estos puntos serán los que se aborden en los siguientes páginas.

2.1. PROTEGER EL COMPUTADOR Y LOS DATOS

Si un computador está conectado a una red es necesario protegerlo, no importa si es una red que no tiene acceso a Internet, porque ya vimos que si un computador está conectado a una red inalámbrica es posible que pueda ser atacado y sus datos sean obtenidos por un atacante, si el computador esta conectado a Internet, los atacantes pueden atacar el computador remotamente, por estas razones es importante que los computadores siempre estén protegidos por un firewall y por un antivirus, esos dos programas son la primera línea de defensa automática contra un potencial atacante.

Para tener una idea de la importancia de la información almacenada en el computador y que puede viajar por la red, se puede hacer una valoración del riesgo latente sobre la información que hay en el computador y decidir si la seguridad que se tiene es adecuada para la información almacenada, por ejemplo si en el computador conectado a la red, se tiene información financiera, legal, médica, laboral, y la pérdida física o la pérdida sobre la confidencialidad de esa información es grave para el usuario del computador, hay que buscar mecanismos más avanzados de protección, como cifrar los archivos o las carpetas donde se guarda la información más sensible, por el contrario si el computador sólo es usado para tareas rutinarias o para navegar y revisar correo esporádicamente, sin almacenar en el computador o visitar por internet sitios donde se tenga depositada información sensible, se puede tener una buena alternativa de protección para estos datos con la seguridad básica, que da la primera línea de defensa.

Además de tener un antivirus y un firewall debidamente instalado y actualizado, existen otras medidas que se deben usar para protegerse, hay que mantener el computador con los últimos parches de seguridad instalados y deshabilitar el uso compartido de carpetas. Si se tienen los parches instalados, se asegura que al menos una parte de los problemas de seguridad que tiene el sistema operativo ya fueron solucionados. Si se comparten carpetas en una red inalámbrica, se corre el riesgo de que un atacante tenga acceso a la red y a las carpetas que están compartidas, ya que estas son las zonas de más fácil acceso.

Realice copias periódicas de la información en su disco duro, los computadores fallan y si ha usado uno por algún tiempo ya lo debe saber de primera mano, además en el caso de un virus que no se pueda erradicar o que dañe los datos, es bueno tener una copia segura de los datos que necesita, para hacer las copias de seguridad hay muchas alternativas, CDs, DVDs, memorias USB, discos duros externos, todas tienen sus ventajas y desventajas, escoja la que mejor se ajuste según su caso.

2.2. ASEGURAR LA RED INALÁMBRICA

Para asegurar la red inalámbrica la primera medida es la **seguridad física**, ya sabemos que por las características de las transmisiones inalámbricas no es posible delimitar exactamente la red, pero si se puede limitar su alcance y hacer más difícil que un atacante la pueda monitorear, para cuidar de la seguridad física, una medida es ubicar el punto de acceso lejos de las ventanas, las antenas de los puntos de acceso son omnidireccionales, esto significa que transmiten formando un patrón como la de la figura-34

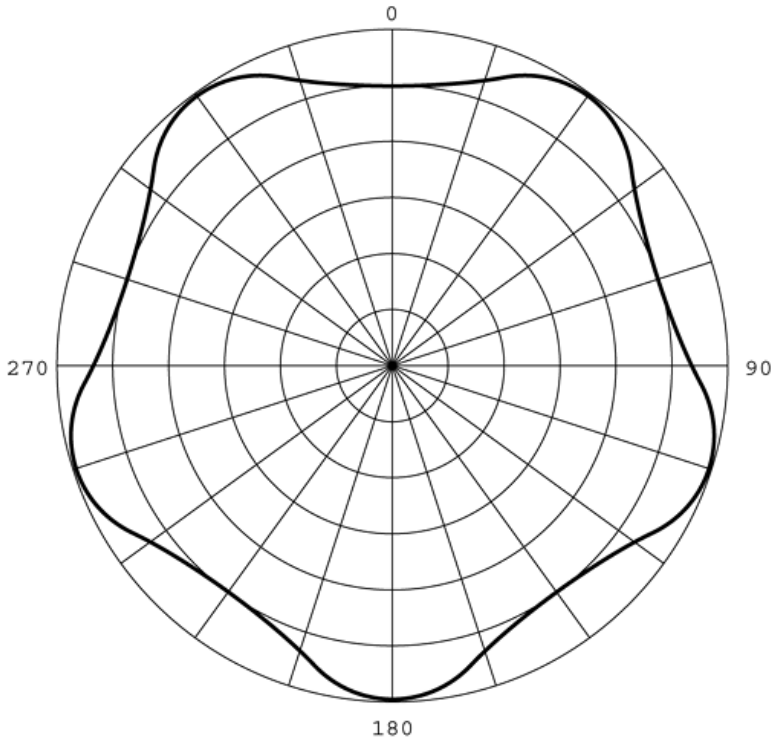

Figura 34 Patrón de radiación de una antena omnidireccional (tomada de [20])

Estas antenas tienen una cobertura de 360 grados omnidireccionalmente, para lograrlo limitan su cobertura vertical, pero esto no significa que si se deja un punto de acceso cerca de una ventana, un atacante no pueda percibir la señal que se emite aún si se encuentra por debajo o por encima, por esto es mejor proteger la señal, poniendo el punto de acceso en una ubicación central.

Agregando a la protección física de la red, se puede hacer una verificación empírica del alcance de la red, para esto, se deja encendido el punto de acceso, mientras se recorre el espacio donde se usará la red inalámbrica con una estación inalámbrica, como un computador portátil o un asistente personal, mientras se hace el recorrido, se debe ir anotando que tan fuerte es la señal, si en todo el espacio se obtiene una señal excelente, se puede pensar en debilitar la señal que transmite el punto de acceso, porque si la señal es excelente o buena en todo el espacio, significa que fuera del espacio la señal es buena o regular, lo que hace que la red este teniendo una cobertura mayor de la deseada. Esta verificación se puede hacer usando un método de prueba y error, hasta que se obtenga una cobertura aceptable en todo el espacio deseado, sin que la red traspase por mucho este espacio.

Complementando la protección física y como última medida en este aspecto, se puede apagar el enrutador inalámbrico cuando no se esté usando, con esto se obtienen dos beneficios, el primero es un beneficio indirecto a la seguridad de la red, y es que se está ahorrando energía mientras el punto de acceso esté apagado. El segundo es un beneficio directo a la seguridad de la red, un punto de acceso que se deje encendido aun cuando no está en uso, transmite continuamente, y puede ser abusado por un atacante, si se suman los dos beneficios, lo mejor es apagar el enrutador inalámbrico mientras no se esté usando.

Además de la protección física que evita que un atacante pueda monitorear la red más fácilmente, existen más formas de proteger la red. Una de ellas se conoce como **seguridad por oscuridad**, este tipo de seguridad lo que hace es ocultar datos que puedan hacer más fácil para un atacante reconocer la red y atacarla. Se hablará de tres formas de proteger la red usando seguridad por oscuridad, la primera: Cambiar el SSID o nombre de la red en el enrutador inalámbrico, para que no sea el mismo que venía de fábrica, esto se hace por una razón simple, el nombre de la red que viene de fabrica, casi siempre es la marca del fabricante, esto ya le indica al atacante un dato valioso, que puede usar para buscar y aprovechar vulnerabilidades especificas que tenga el dispositivo.

La segunda forma: al cambiar el SSID de la red, se debe usar un nombre que no identifique el uso ni el propietario de la misma, hay un gran número de redes que utilizan los apellidos de la familia que usa la red, o el nombre completo, o un teléfono, incluso un numero de apartamento, esto puede ser muy práctico y conveniente al momento de usar la red, también debe haber alguien que está orgulloso de poner esos datos, para mostrar que tiene una red inalámbrica, en redes empresariales casi siempre el nombre de la red es el nombre de la empresa, pero también se ven muchos nombres de dependencias en una empresa, como gerencia general, departamento de cartera, área comercial, todos estos nombres hacen para un atacante mucho más fácil escoger a quien atacar y los métodos que va a utilizar, también hace más fácil para un atacante buscar información sobre el propietario de la red. Por eso como segunda medida de protección por oscuridad, se debe usar un nombre de red que solo el propietario y quien él decida invitar a usar la red, puedan identificar. En la configuración del punto de acceso se puede deshabilitar la transmisión del SSID, si esto se deshabilita, solo se podrá conectar a la red quien posea el dato sobre el nombre, ya que esta es la primera condición para establecer una conexión.

Como tercera medida para proteger la red usando esta forma de seguridad, es posible cambiar la dirección MAC del punto de acceso, la dirección MAC, es un numero que identifica el adaptador de red del dispositivo, estos números son asignados a los fabricantes por una entidad central y en teoría cada número es único, al cambiar la dirección MAC se oculta el fabricante del punto de acceso y se obtienen iguales beneficios que al cambiar el SSID que viene configurado por el fabricante del dispositivo. Si se cambia la dirección MAC es posible que haya que informar del cambio al proveedor de servicio de Internet para que este haga ajustes en la configuración del servicio.

Claves, cambiar las claves, proteger las claves, usar claves complejas, son solo algunas de las formas en las que las claves se deben administrar, para que puedan seguir cumpliendo con sus funciones, en una red inalámbrica, se usan dos claves, una clave para proteger la conexión entre el punto de acceso y una estación, esta clave, protege la confidencialidad y la integridad de los datos, esta clave es la primera que intentará descifrar un atacante, porque una vez tenga esta clave tiene acceso a la red, puede monitorear lo que se transmite, puede intentar acceder al computador que transmite, puede hacerse pasar por un usuario legitimo de la red, y muchas otras cosas más, por eso es importante cambiar periódicamente esta clave, cambiar las claves es una tarea tediosa, tener que recordar una nueva clave también lo es, pero en este caso la clave se cambia en el enrutador inalámbrico y luego en el computador, y no hay que volver a recordarla, esto hace que sea más deseable y práctico usar una clave compleja, que incluya, letras, números, símbolos, espacios, teniendo cuidado de no usar una clave que se pueda encontrar en un diccionario. Se puede programar un recordatorio cada 30 o 60 días, para cambiar la clave, es un procedimiento que no tarda más de un par de minutos y que asegura que si un atacante estaba a punto de descifrar la clave anterior, ahora deberá repetir todo el proceso.

La segunda clave que usan los puntos de acceso, es la clave para la administración del dispositivo, esta clave se debe cambiar para que no se pueda abusar de la red, una persona que conozca la clave administrativa puede configurar el enrutador como mejor le parezca, cambiar sus parámetros, negar el acceso a la red, re direccionar el tráfico de la red, puede hacer lo que quiera con la configuración, como atenuante, para que alguien intente ingresar al punto de acceso con la clave administrativa, debe haber ya ingresado a la red y haber vulnerado la clave que protege la red. Pero si no se modifica esta clave, va a quedar la clave que deja el fabricante, hay sitios en Internet donde se listan las claves y usuarios usados por los fabricantes, haciendo más fácil que se abuse de la red. Esta clave aunque debe ser compleja debe también ser recordada por el usuario, por eso se recomienda una clave que el usuario pueda recordar y que no aparezca en un diccionario, esta clave luego de cambiada una vez, se puede dejar sin cambio por más tiempo que la clave que protege la red inalámbrica, se puede usar como política que la nueva clave administrativa del punto de acceso sea la anterior clave de la red inalámbrica, esto obviamente en el caso de una red residencial, para una red empresarial hay que tomar medidas especiales con ambas claves.

Como aporte final para proteger una red inalámbrica, existe la **seguridad lógica**, que se puede implementar en un enrutador inalámbrico, para este tipo de protección la principal sugerencia, es usar el modo de protección más fuerte que tenga el punto de acceso y que sea compatible con el adaptador de red. Según el estándar IEEE 802.11i el modo de protección más fuerte para una red inalámbrica doméstica se conoce como WPA2, este método, usa un cifrado AES, el cifrado AES está aprobado por varios gobiernos y por ejemplo es de uso obligatorio por las agencias gubernamentales en Estados Unidos, con WPA2 y AES como método de cifrado se tiene una altísima protección de la confidencialidad y la integridad de los datos, pudiéndose usar claves de 8 a 63 caracteres de longitud. En una escala ligeramente inferior en la protección de la red, se encuentra el método TKIP, con este método la red usa una clave diferente para cada paquete que se transmite, haciendo imposible que un atacante use un ataque de diccionario para obtener la clave de la red, sin embargo, el método TKIP es vulnerable al momento en que establecen la asociación inalámbrica el punto de acceso y la estación, porque en ese momento, se está usando la clave original de la red, esta clave puede ser capturada por un atacante, para intentar descifrarla mas tarde (si la clave es larga y compleja se minimiza el riesgo enormemente). En el siguiente peldaño de la escala de los modos para proteger una red inalámbrica, se encuentra el modo WEP, el modo WEP es inseguro desde hace años, da una protección mínima contra un atacante, se puede vulnerar en cuestión de minutos, pero si no es posible tener un modo de protección más fuerte, habrá que usarlo, así su protección sea mínima, al menos sirve para persuadir a un atacante que solo quiera abusar de blancos más sencillos. No se debe utilizar la autenticación abierta o deshabilitar la protección de la red, si se hace esto, la red no tendrá ningún tipo de protección de confidencialidad o integridad sobre los datos.

Cuando un atacante logra acceder a una red inalámbrica, intentará conectarse a ella y obtener una dirección IP, las direcciones IP son direcciones que administra dinámicamente el punto de acceso, y que sirven para identificar la procedencia y destino de los paquetes de datos transmitidos, para controlar las direcciones IP se pueden asignar estáticamente, o sea que cada dispositivo que intente conectarse a la red, se le deberá configurar manualmente los datos de la dirección IP, esto no es practico si son muchos dispositivos o si se desea compartir la red con eventuales visitante, por eso se deja que el enrutador inalámbrico administre esas direcciones, pero hay un punto medio entre tener direcciones IP estáticas y que el punto de acceso administre las direcciones completamente, ese punto medio se logra al usar listas de acceso basadas en la dirección MAC de los dispositivos que se quieran conectar, como ya se explico antes las direcciones MAC son identificadores únicos para los adaptadores de red, al usar una

lista de acceso basada en la dirección MAC, se le está diciendo al enrutador inalámbrico que solo debe asignarle una dirección IP a las estaciones que posean una dirección MAC que esté en su lista de acceso. Suponga que llega un nuevo dispositivo que se quiere conectar a la red inalámbrica, entonces se abre la página administrativa del punto de acceso, en la opción de control de acceso, o MAC Filtering, se puede ver algo parecido a la figura-35

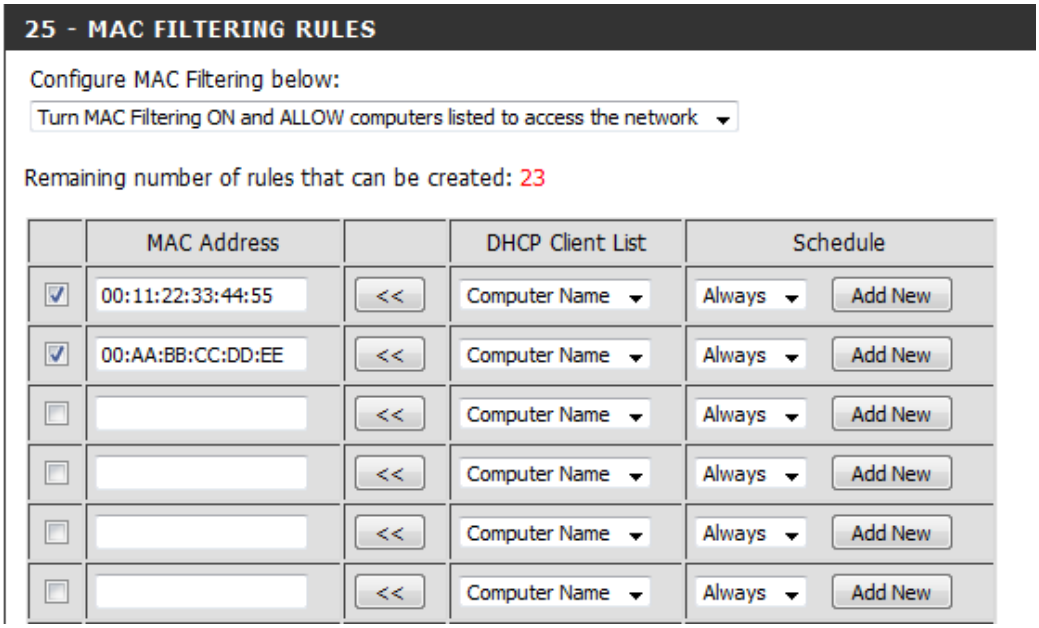

Figura 35 Lista de acceso basada en direcciones MAC

En esta figura se ve que el filtrado por direcciones MAC esta activo y que se permitirá el acceso a la red de los computadores en la lista, también se puede hacer lo contrario, y permitir el acceso a todos los computadores excepto aquellos que se encuentren en la lista.

Para obtener la dirección MAC de un computador lo más fácil es abrir el programa que se llama, símbolo del sistema, que abre una ventana negra, muy conocida para los que llevan años trabajando con un computador y que antes se conocía como ventana D.O.S. en esa ventana se escribe el comando: getmac \v, con esto se obtienen datos como los que se ven a continuación en la figura-36

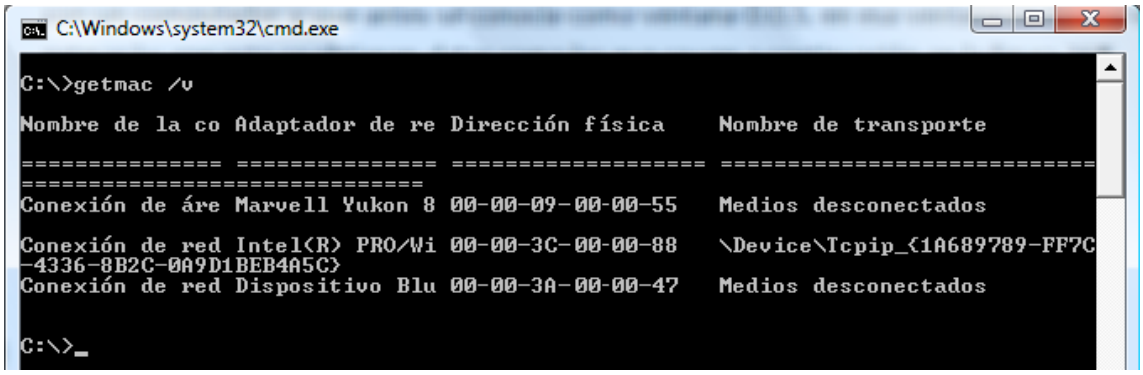

Figura 36 Datos al ejecutar el comando getmac

Para el caso de la figura-36 hay tres direcciones MAC, la primera se refiere al adaptador para redes cableadas, el segundo corresponde al adaptador de red inalámbrico y el tercero al adaptador de red Bluetooth. El valor que interesa es la dirección MAC del adaptador de red inalámbrico, por lo tanto se toman los valores que aparecen allí y se ingresan en la ventana administrativa, usando ":" dos puntos como separados entre cada pareja de valores. Se salvan los cambios. Y el dispositivo nuevo podrá acceder a la red inalámbrica. Esta es una buena protección pero también puede ser vulnerada, un atacante puede observar el tráfico de red durante un periodo prolongado de tiempo y establecer las direcciones MAC que son aceptadas, luego usar una de esas direcciones y acceder a la red. Pero definitivamente hace más difícil el abuso de la red para el atacante.

Una medida que no es preventiva, es la de revisar periódicamente los registros que genera el punto de acceso, esto se puede hacer desde la página de configuración administrativa del enrutador inalámbrico y sirve para detectar comportamientos sospechosos o intentos de ataques a la red, que el usuario no descubrió. En la figura-37 se pueden ver algunos registros.

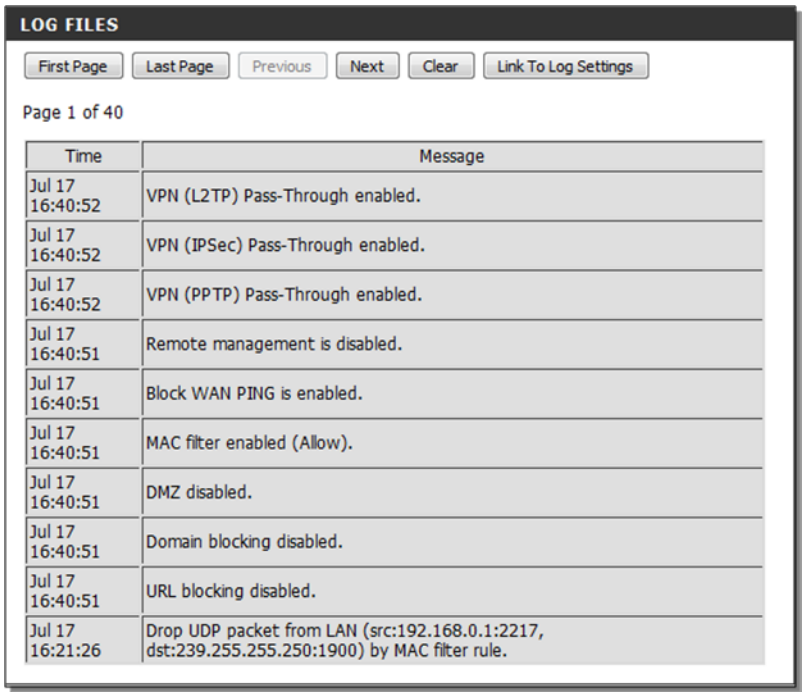

Figura 37 Registros guardados por el punto de acceso

Los registros sirven para verificar el estado del punto de acceso y posibles ataques que haya recibo, en la figura-38 se ve la configuración de los registros.

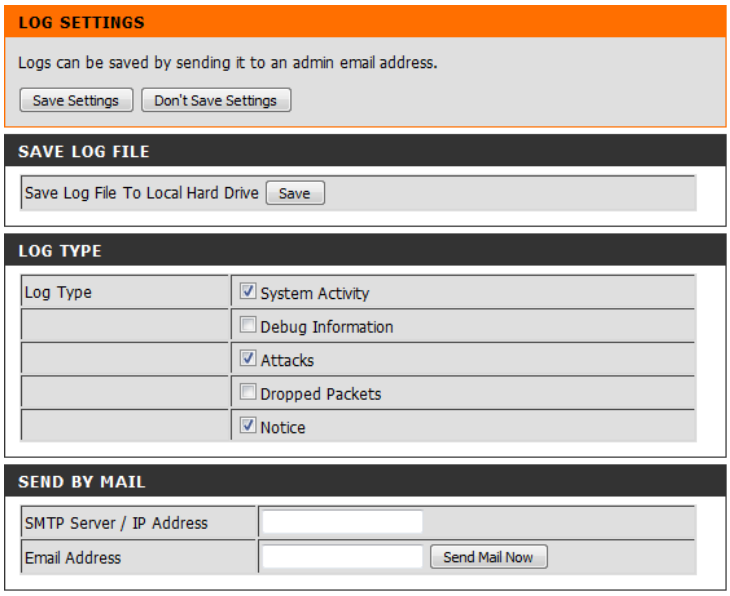

Figura 38 Configuración de los registros

Los registros se pueden configurar para que almacenen los ataques, la actividad del punto de acceso, los paquetes rechazados, y otros avisos, de estos tipos de registros, son interesantes desde un punto de vista de la seguridad, los ataques y los paquetes rechazados, los ataques es obvio porque son importantes, los paquetes rechazados, son importantes porque registran paquetes que llegaron a destiempo, que son repetidos o que no están bien formados, esto puede indicar un ataque sobre la red inalámbrica.

2.3. MONITOREAR LAS CONEXIONES

La red está funcionando, las recomendaciones para proteger la seguridad se llevaron a cabo, pero hay que hacer revisiones periódicas para asegurar que todo esté funcionando correctamente, una de las revisiones que se pueden hacer, es la de revisar las conexiones que hay actualmente en la red inalámbrica, para esto los puntos de acceso tienen una opción en la que se puede ver la actividad en la parte inalámbrica y en la parte cableada, además de las sesiones activas en la red inalámbrica, en la figura-39 se ven las estaciones que están conectadas al enrutador inalámbrico, la duración de la conexión, la dirección MAC del dispositivo conectado y el modo de conexión, en este caso 802.11g

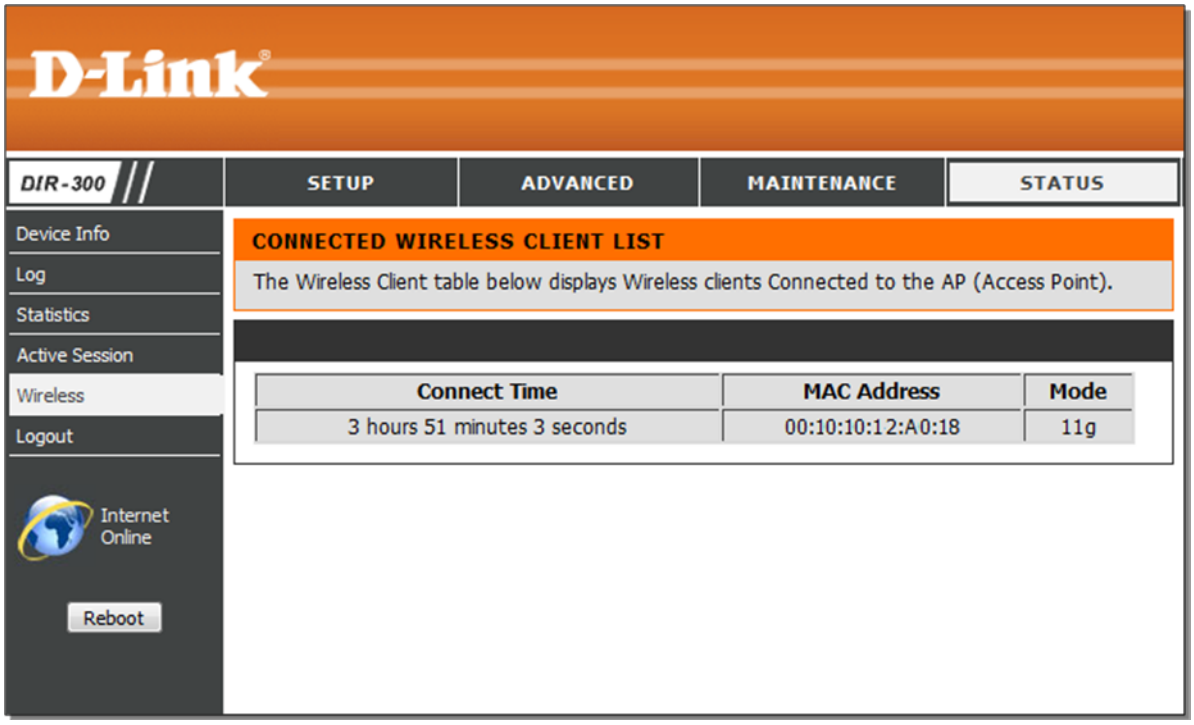

Figura 39 Clientes inalámbricos conectados

Si al revisar las conexiones inalámbricas, detecta mas dispositivos conectados de los que están autorizados, es una señal clarísima de que un atacante esta usando su red, lo mejor, es apagar inmediatamente su adaptador de red inalámbrico y el de los dispositivos inalámbricos autorizados, desconectar el cable que conecta el enrutador inalámbrico a Internet, en ese momento habrá aislado al atacante, si quiere puede conectarse con un cable al enrutador inalámbrico y revisar los registros y todos los datos que pueda recabar del atacante, o si no quiere saber nada del atacante, apagar inmediatamente el punto de acceso y llamar al servicio técnico de su proveedor de Internet, para que le digan cual es el mejor rumbo de acción.

Además de las conexiones inalámbricas, también puede revisar las sesiones activas. Tal como se ve en la figura-40

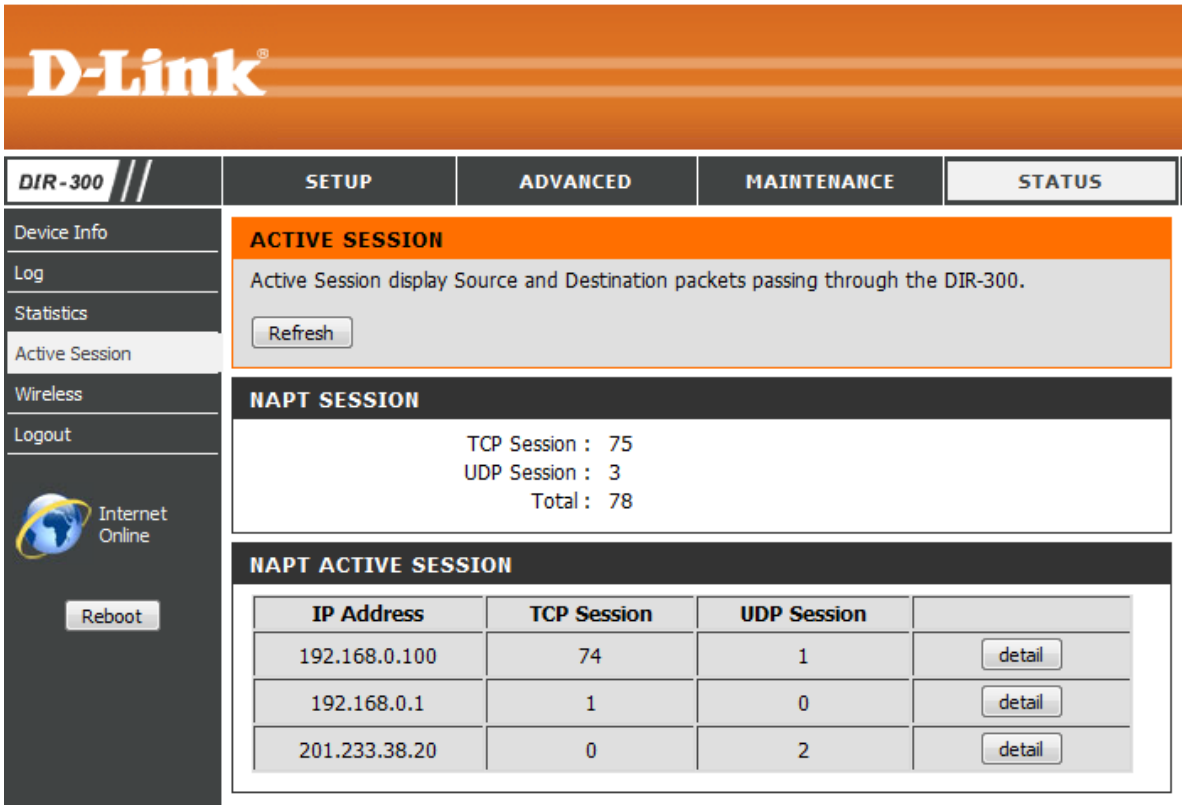

Figura 40 Sesiones activas en el enrutador inalámbrico.

En la figura-40 se ven varias direcciones IP, para saber si esas direcciones son validas se pueden verificar usando un servicio WHOIS como el de el sitio LACNIC [http://lacnic.net/cgi-bin/lacnic/whois] un servicio WHOIS convierte una dirección IP en el nombre de la compañía que dueña de la dirección, LACNIC por su parte, es la compañía que registra las direcciones IP para Latino América y el Caribe.

Intentemos buscar en LACNIC la dirección 192.168.0.100, en la figura-40 se ve el resultado obtenido

Figura 41 Consulta en LACNIC de una dirección IP (tomado de [23])

La consulta dice que la dirección 192.168.0.100 es reservada, esto no es extraño, porque las direcciones IP que comienzan por 192.168 son privadas, en este caso la dirección 192.168.0.100 es la dirección IP que el enrutador inalámbrico le asigno a un computador. La dirección 192.168.0.1 es la dirección que usa el enrutador inalámbrico. Ya se vio que las direcciones que comienzan por 192.168 son privadas, también lo son las direcciones que comienzan por 172.16, desde 172.16.0.0 hasta 172.32.255.255.

Ahora que ocurre al consultar la dirección IP 201.233.38.20. A continuación aparece el resultado de la consulta

```
% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2008-07-17 20:35:16 (BRT -03:00)

inetnum:     201.233.0/17
status:      allocated
owner:       EPM Telecomunicaciones S.A. E.S.P.
ownerid:     CO-EPME1-LACNIC
responsible: Administrador EPMNET
```

```
address:     Carrera 77 39b-16, -, -
address:     940 - Medellin - CO
country:     CO
phone:       +57 4 4152280 []
owner-c:     YGO2
tech-c:      YGO2
abuse-c:     YGO2
inetrev:     201.233.0/17
nserver:     LAUTA.UNE.NET.CO
nsstat:      20080712 AA
nslastaa:    20080712
nserver:     BIRLOCHA.UNE.NET.CO
nsstat:      20080712 AA
nslastaa:    20080712
created:     20060717
changed:     20060717

nic-hdl:     YGO2
person:      Administrador de EPMNET
e-mail:      adminternet@UNE.NET.CO
address:     Carrera 77 No 39b-16, --, --
address:     NA - Medellin - Co
country:     CO
phone:       +57 4 4152281 []
```

En los datos presentados se puede ver que las direcciones que comienzan por 201.233 pertenecen a EPM telecomunicaciones, también aparece la dirección registrada de la compañía, teléfonos, el nombre de algunos servidores, y una dirección de correo electrónico. La información es bastante detallada, y da tranquilidad porque el proveedor de Internet usado en ese momento era precisamente EPM telecomunicaciones, entonces puedo interpretar esa sesión que aparece en el enrutador inalámbrico como una sesión normal entre el proveedor de servicio y mi red.

Si se detecta actividad de otras redes, lo mejor es interrumpir cualquier conexión tomar nota de los datos presentados y apagar el punto de acceso inalámbrico, luego informar al proveedor de servicio sobre los hechos y acoger las recomendaciones que hagan.

IV PARTE – MEDICIONES DE REDES INALÁMBRICAS EN MEDELLÍN

No hay una forma precisa para indicar cuantas redes inalámbricas hay hoy en Medellín, aunque algunos proveedores de Internet, también ofrecen la opción de instalar un punto de acceso inalámbrico, no todas las redes inalámbricas se instalan de esta forma, son muy comunes las redes instaladas personalmente o las redes empresariales, por eso se hicieron varios recorridos por el sector de el Poblado en Medellín, ¿porqué el Poblado? Por la cantidad de empresas en el sector y por la cantidad de viviendas en estratos altos con acceso a una conexión de banda ancha y al poder adquisitivo para instalar una red inalámbrica.

1. METODOLOGÍA

Se Usaron técnicas de wardriving, buscando obtener estadísticas de las redes existentes en el sector de el Poblado en la ciudad de Medellín, específicamente desde la avenida el poblado o carrera 43A hasta la transversal superior o carrera 25 y desde la calle 10 hasta la frontera o calle 20 Sur. Con esta información se obtuvo un panorama de la densidad de redes existentes en un sector específico, el tipo de equipos, la seguridad implantada en la red y otros datos relevantes.

Se hicieron varios recorridos en este sector, durante diferentes horas del día y diferentes días de la semana, para capturar la mayor cantidad de redes, ya que algunas redes funcionan solo durante algunas horas del día.

Al completar el recorrido se guardaron los datos resultantes identificando la fecha del recorrido. Se hicieron recorridos con GPS y sin GPS, en los casos de GPS se adjuntan imágenes de los sectores con mayor densidad de redes y una imagen general de todo el sector.

Al terminar la fase de recaudación de la información, se hizo un análisis estadístico sencillo, como número de redes en el sector, canales utilizados, marcas de puntos de acceso identificadas, método de cifrado aplicado, topología de la red y algunos de los SSID que no se deberían usar en una red inalámbrica.

2. RESULTADOS

2.1. IMÁGENES OBTENIDAS CON EL GPS

Imagen 1 Vista general de las redes encontradas en el sector estudiado

Imagen 2 Avenida el poblado entre la Clínica Medellín y la Aguacatala

Imagen 3 Loma de los Parra entre la Avenida el Poblado y la transversal inferior

Imagen 4 Loma de los Balsos entre transversal intermedia y transversal inferior

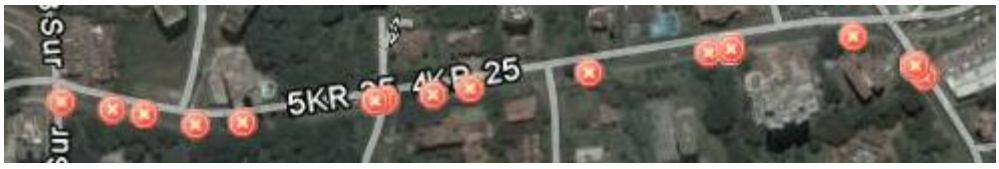

Imagen 5 Transversal superior entre la loma de los Balsos y la loma de los González

Imagen 6 Sector de la frontera entre la avenida el Poblado y la transversal inferior

Imagen 7 Sector analizado, como parte de la ciudad

Todas las Imágenes que se han presentado se obtuvieron usando el programa Google Earth [24], los puntos que representan las redes se obtuvieron al usar el programa vistumbler [7] en conjunto con un GPS y exportar el resultado a un archivo KLM.

2.2. Redes encontradas según el tipo de seguridad asociada al equipo transmisor

El 51,69% de las redes no están protegidas por ningún protocolo de seguridad o tienen cifrado WEP el cual es fácilmente penetrado en pocos minutos.

Canal	Numero de Redes	Porcentaje
RSNA-None	1	0,01%
RSNA-TKIP	85	0,70%
WPA-CCMP	162	1,34%
RSNA-CCMP	365	3,02%
None	2575	21,29%
WEP	3678	30,41%
WPA-TKIP	5230	43,24%
Total	**12096**	**100%**

Tabla 7 Redes encontradas según su protección

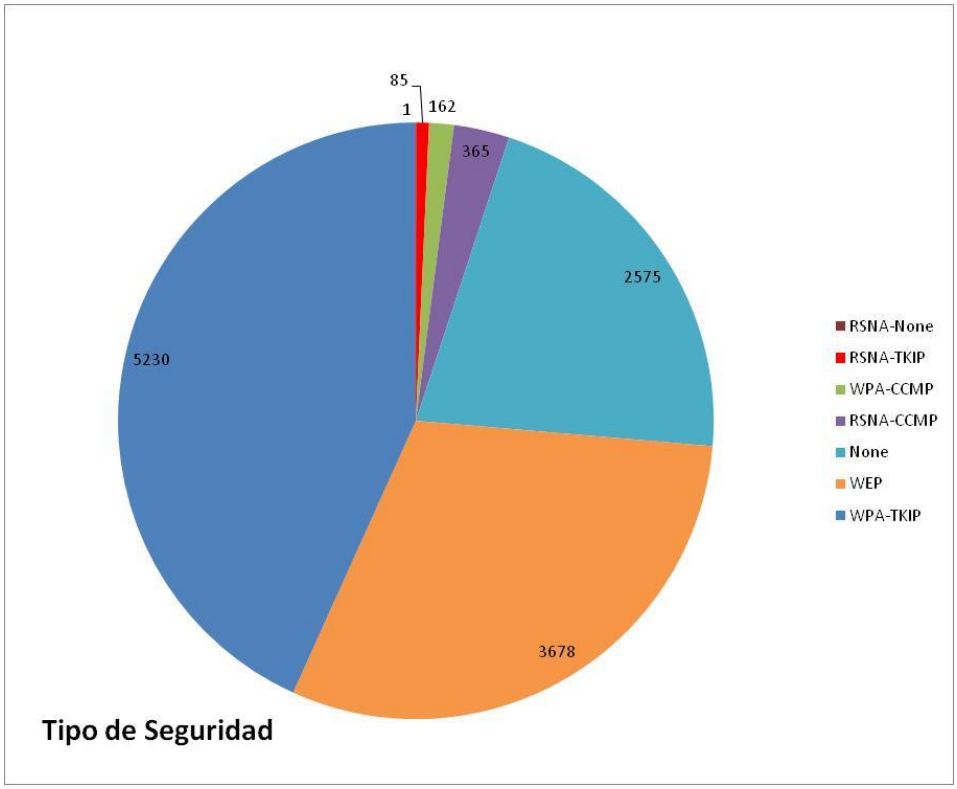

Gráfico 1 Tipo de seguridad utilizada (valores)

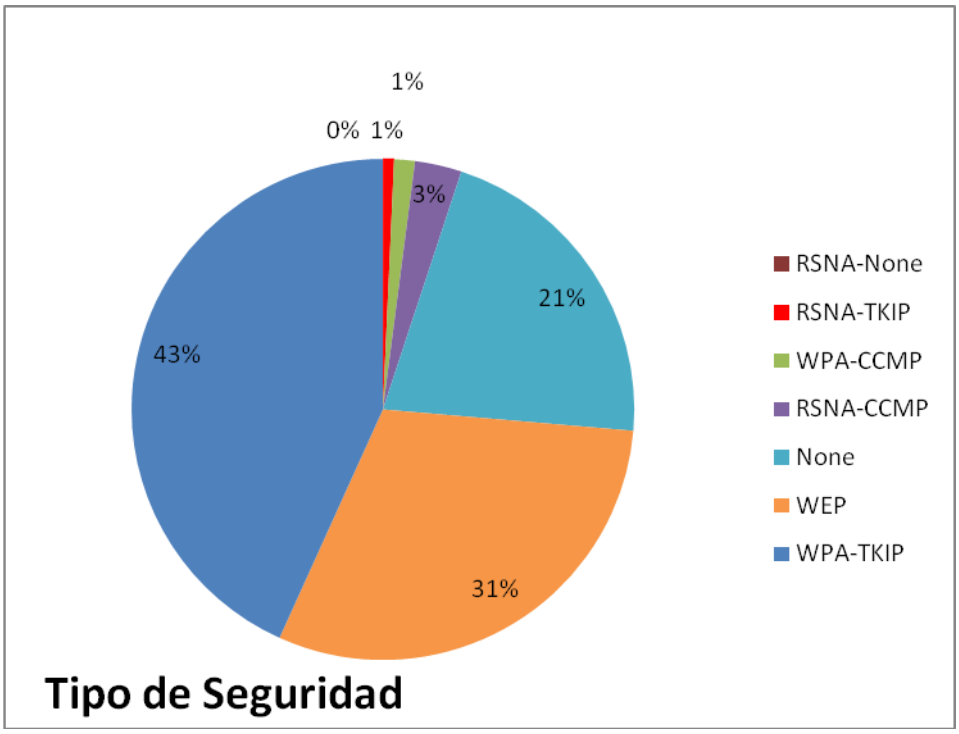

Gráfico 2 Tipo de seguridad utilizada (porcentajes)

2.3. REDES ENCONTRADAS SEGÚN EL CANAL UTILIZADO POR EL EQUIPO TRANSMISOR.

Los más comunes son los canales 1, 6 y 11 que son los canales usados por defecto en las redes 802.11b/g para evitar la superposición de frecuencias, los canales 36 y superiores corresponden al estándar 802.11a, estos canales son usados normalmente cuando se encuentra interferencia en los canales habituales.

Canal	Numero de Redes
40	1
161	2
60	2
157	2
44	12
56	18
52	18
36	33
5	90
2	99
4	102
3	107
8	219
10	226
9	250
7	423
1	1175
6	4290
11	5027
Total	**12096**

Tabla 8 Canales utilizados por las redes

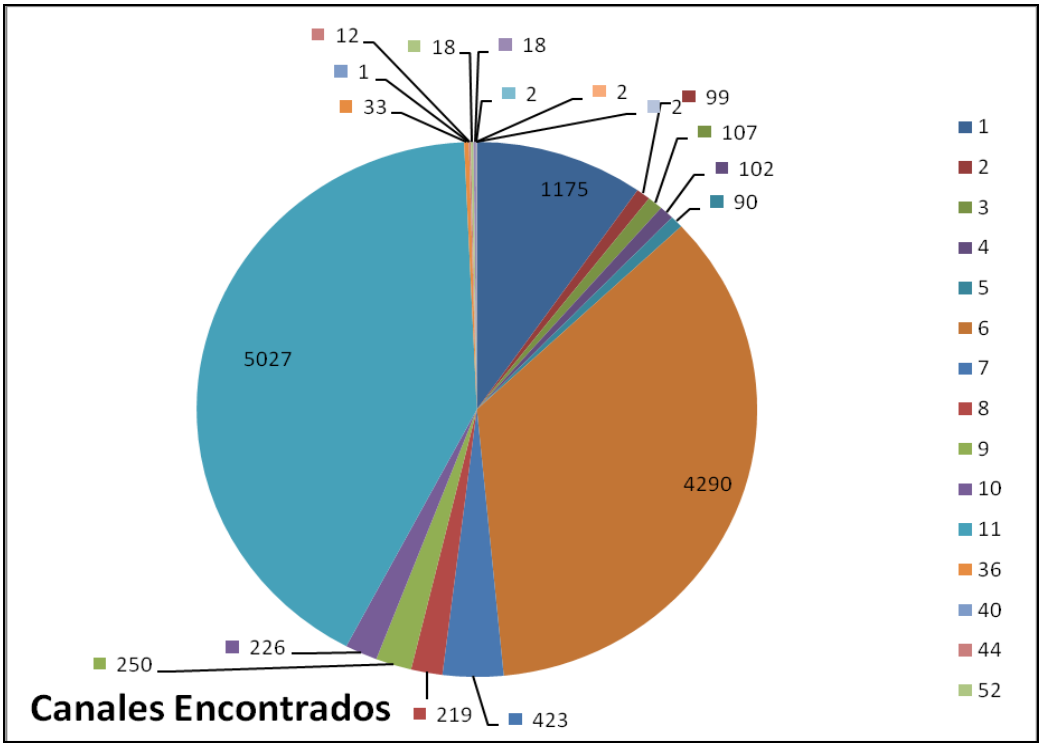

Gráfico 3 Canales utilizados por las redes (valores)

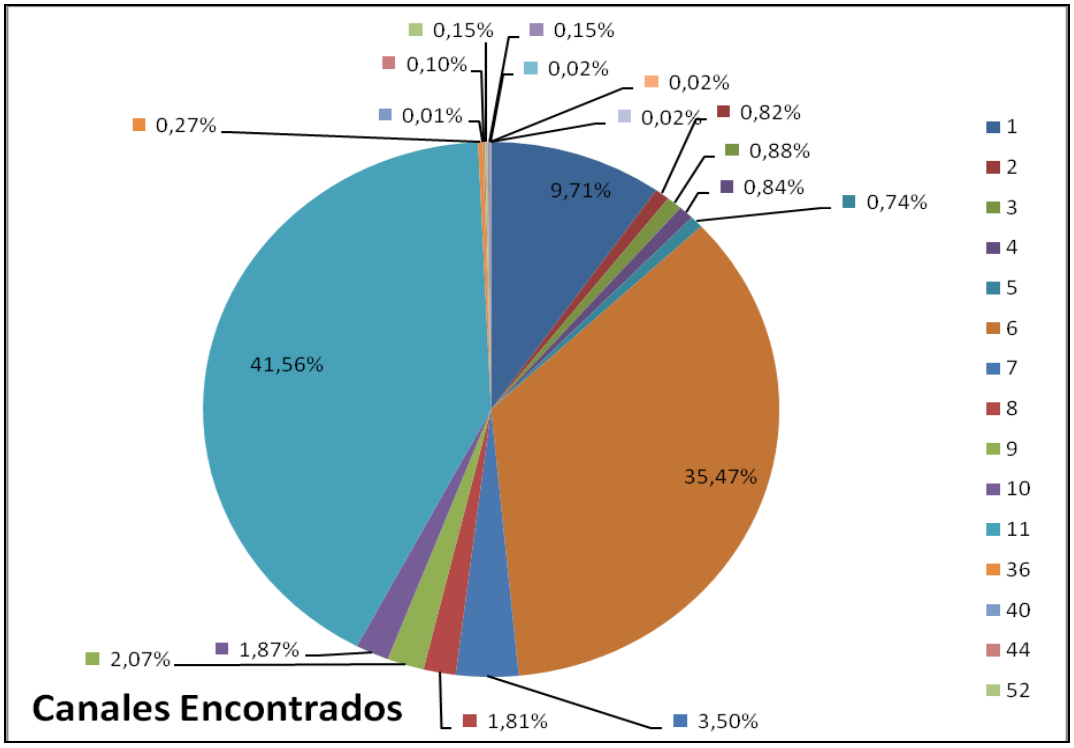

Gráfico 4 Canales utilizados por las redes (porcentajes)

2.4. REDES POR VENDEDOR

Hon-Hai Precision es el mayor vendedor. Hon-Hai es un productor genérico de componentes electrónicos con clientes como Apple, Cisco o Motorola; luego viene D-Link, Cisco Linksys, Netgear, Belkin y Cisco.

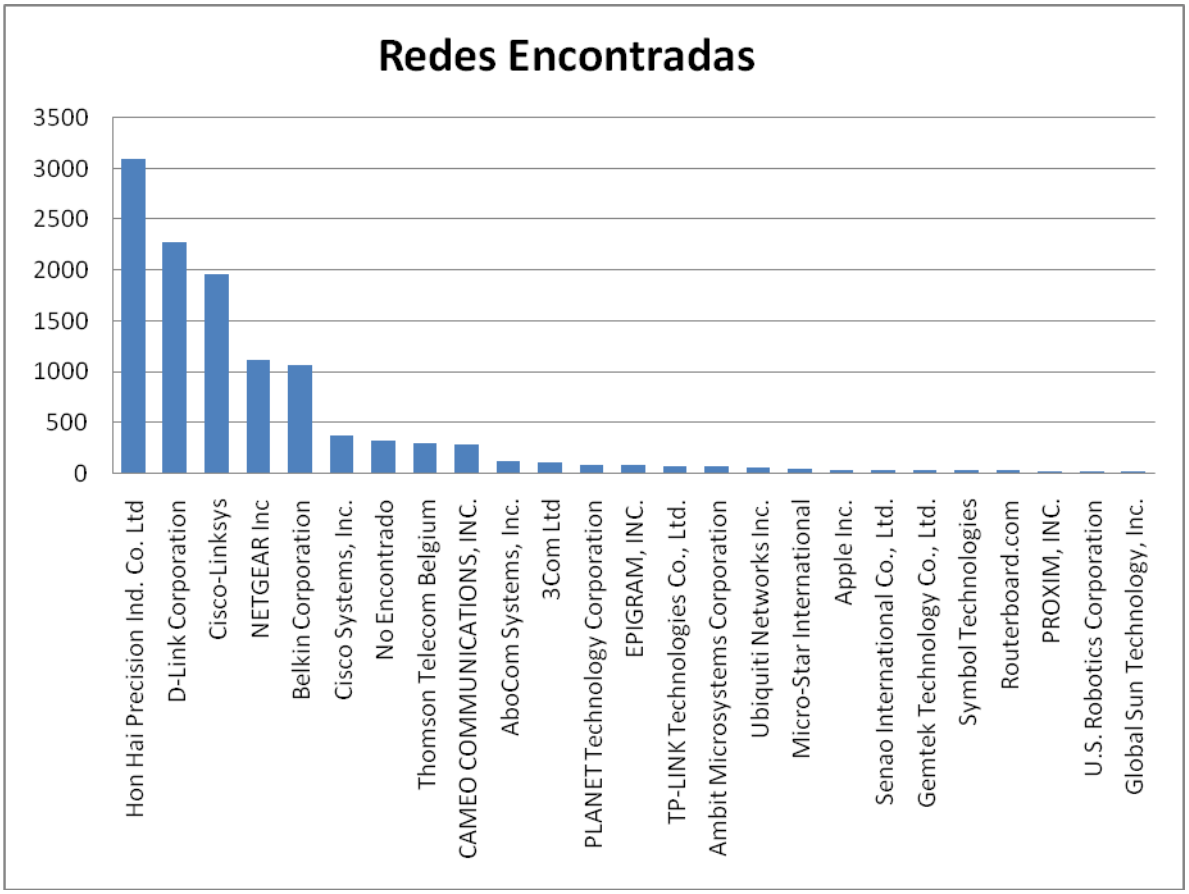

Gráfico 5 25 vendedores con mas redes

Vendedor	Redes
Hon Hai Precision Ind. Co. Ltd	3097
D-Link Corporation	2279
Cisco-Linksys	1968
NETGEAR Inc	1123
Belkin Corporation	1076
Cisco Systems, Inc.	372
No Encontrado	324
Thomson Telecom Belgium	299
CAMEO COMMUNICATIONS, INC.	286
AboCom Systems, Inc.	121
3Com Ltd	119
PLANET Technology Corporation	94
EPIGRAM, INC.	87
TP-LINK Technologies Co., Ltd.	79
Ambit Microsystems Corporation	72
Ubiquiti Networks Inc.	59
Micro-Star International	48
Apple Inc.	44
Senao International Co., Ltd.	39
Gemtek Technology Co., Ltd.	39
Symbol Technologies	33
Routerboard.com	33
PROXIM, INC.	29
U.S. Robotics Corporation	29
Global Sun Technology, Inc.	29
Total	**11778**

Tabla 9 25 principales vendedores.

2.5. VELOCIDADES ENCONTRADAS

El 11,27% o 1363 de las redes encontradas tienen una velocidad de 11Mbps, esto indica que una gran cantidad de redes seguramente funcionan bajo el estándar 802.11b, el 87,81% o 10622 de las redes encontradas transmiten a una velocidad de 54Mbps, o sea la máxima velocidad para las redes 802.11a/g, las demás redes transmiten en fracciones de las anteriores velocidades, tal vez como redes compartidas y así evitar el abuso de los recursos de la red

Velocidad en Mbps	Redes
54	10622
11	1363
36	32
24	21
22	19
6	15
5,5	10
9	10
12	2
2	1
0	1
Total	**12096**

Tabla 10 Velocidades de las redes encontradas

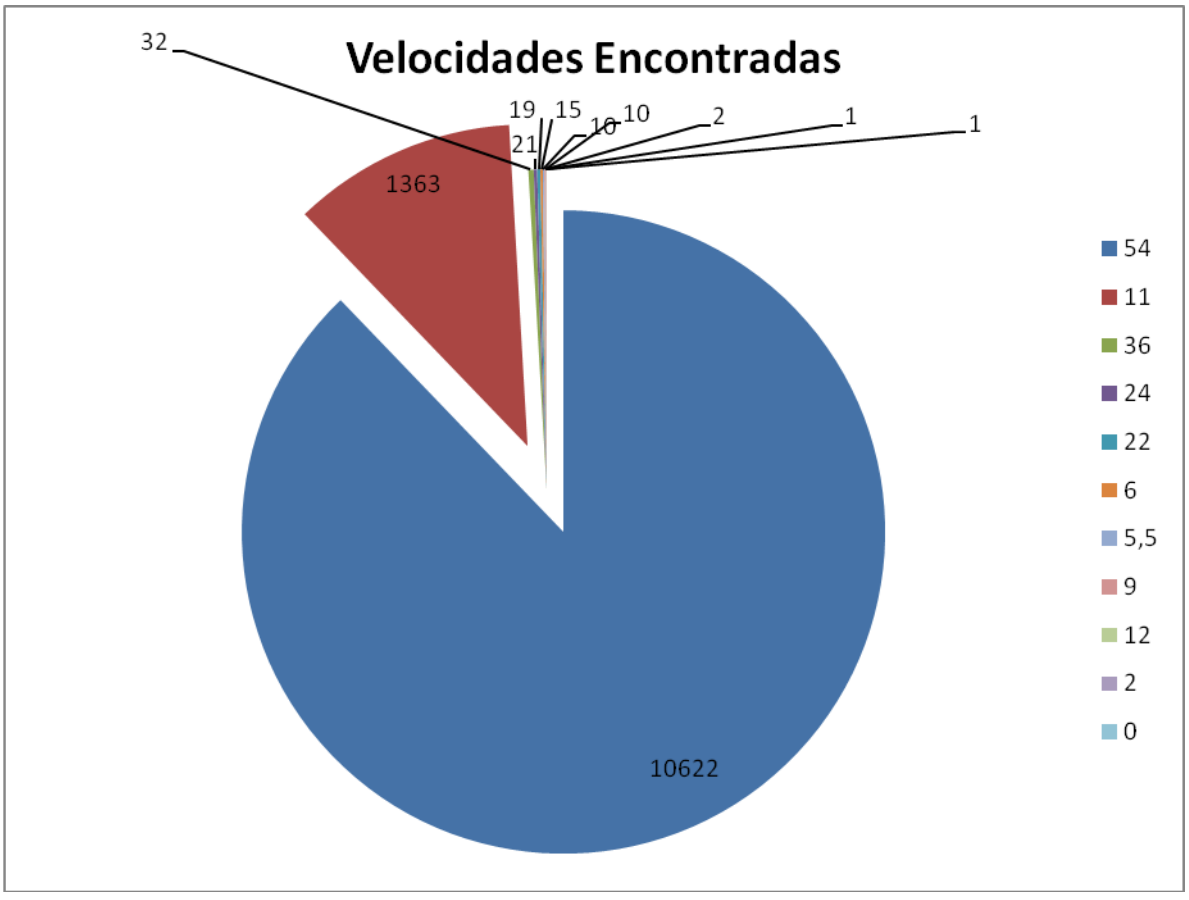

Gráfico 6 Velocidades de las redes encontradas (valores)

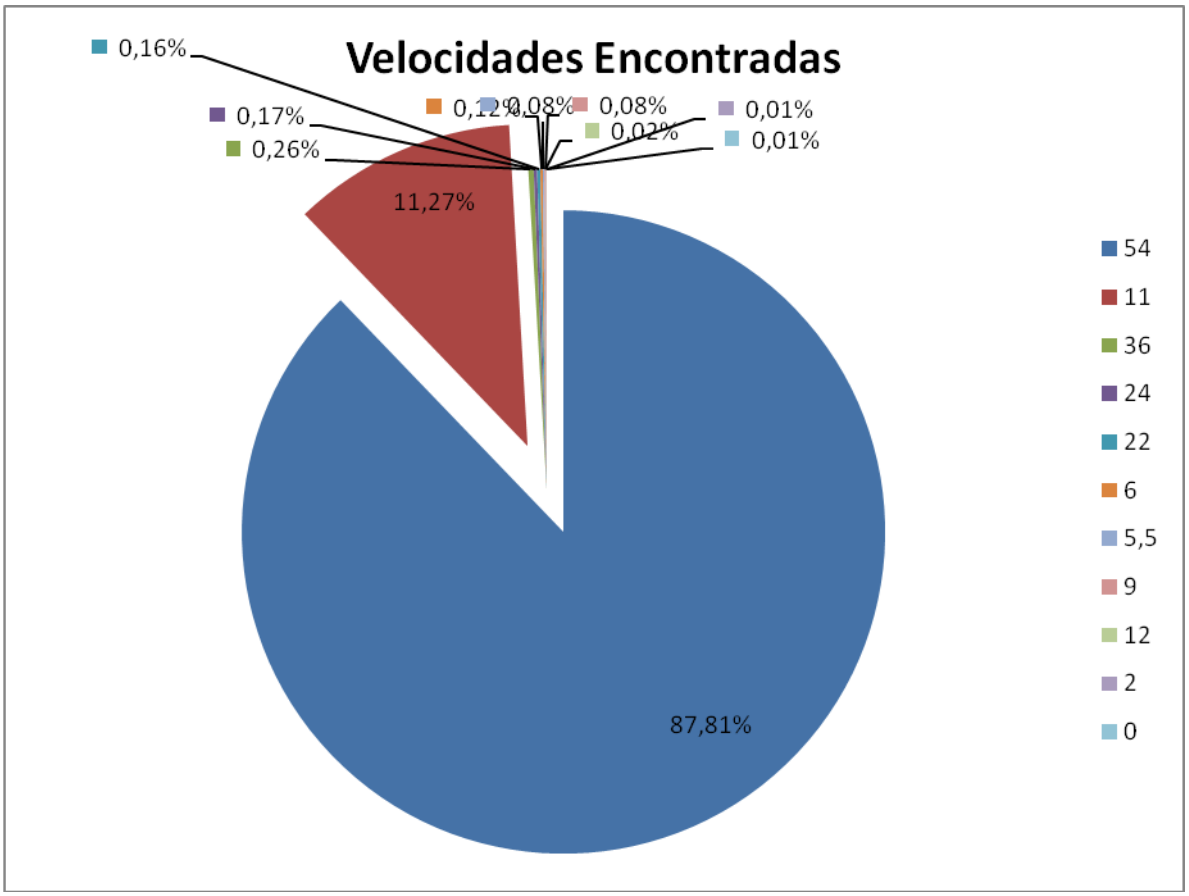

Gráfico 7 Velocidades de las redes encontradas (porcentajes)

2.6. Arquitecturas Encontradas

Las redes inalámbricas según su arquitectura pueden ser redes de infraestructura o redes ad-hoc. En las primeras es necesaria la presencia de un punto de acceso, en las segundas las estaciones configuran la red.

Arquitectura	Redes encontradas
Infraestructura	11951
Ad Hoc	145
Total	**12096**

Tabla 11 Arquitectura de las redes encontradas

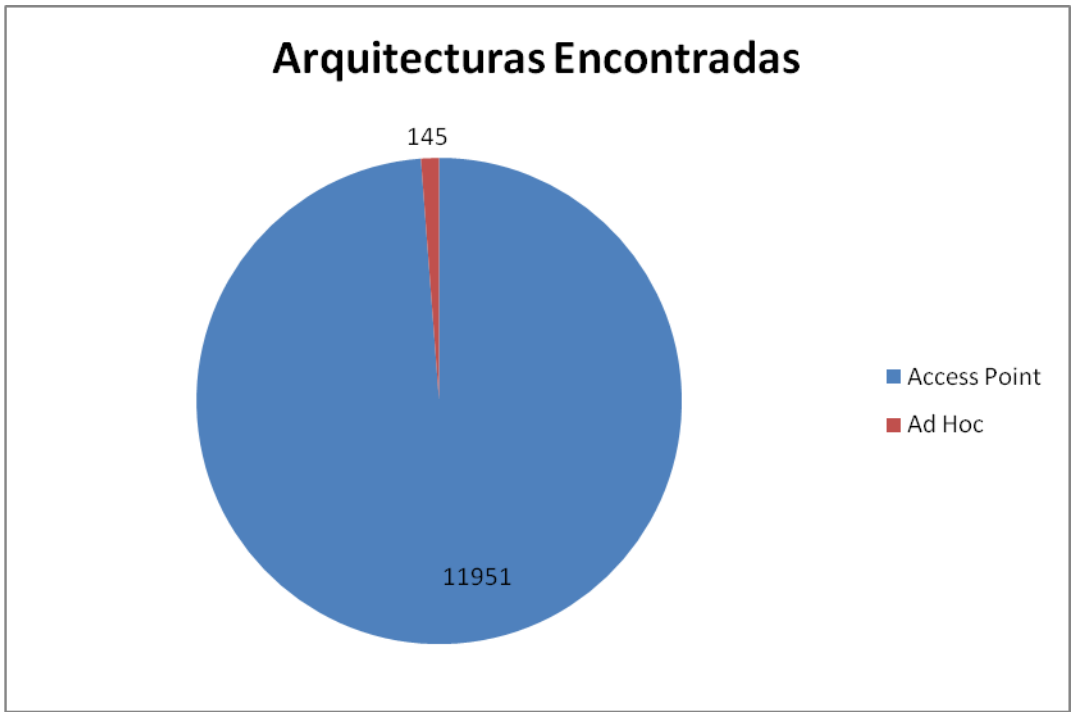

Gráfico 8 Arquitecturas encontradas (valores)

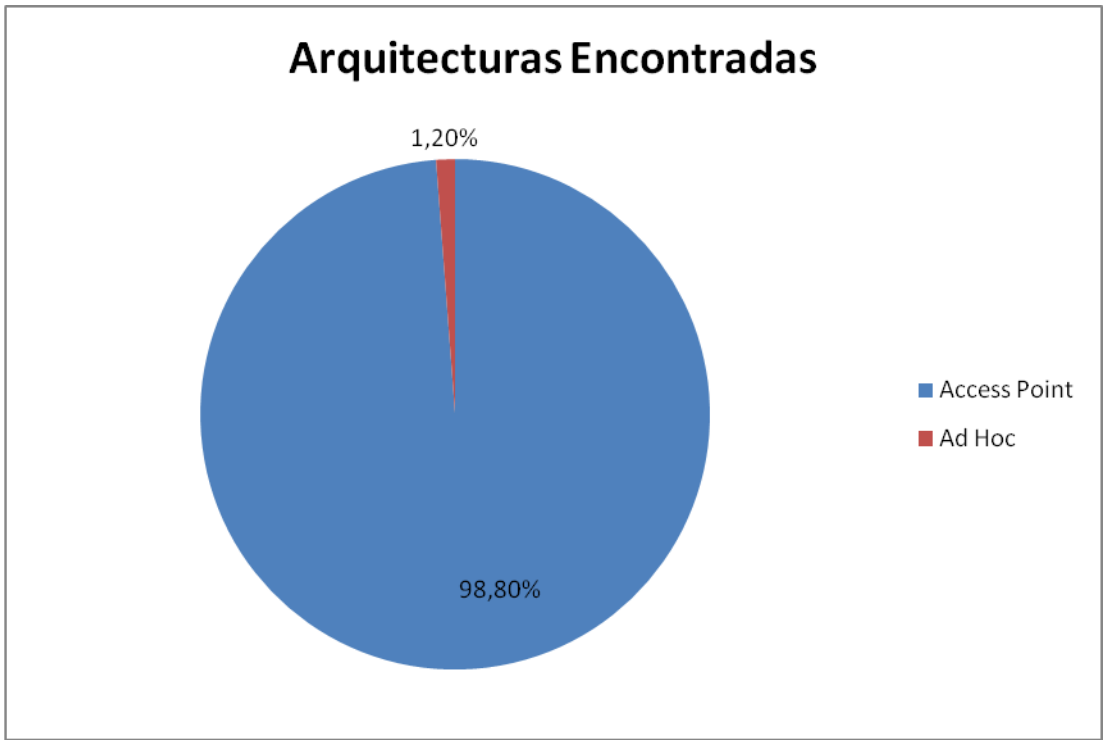

Gráfico 9 Arquitecturas encontradas (Porcentajes)

2.7. NOMBRES DE REDES QUE NO SE DEBERÍAN UTILIZAR

A continuación se listaran algunos nombres de redes que se encontraron durante los recorridos, solo se dará el nombre de la red, para evitar dar más información de la necesaria.

adriana prieto

AgricolasUnidas

Agudelo Ochoa

alarmar_poblado (una empresa de seguridad)

Alejandro Guerra

alvaro123456 (seguramente también es la clave de la red)

apto 1104

Belkin_N_Wireless_C1F99F (fabricante y modelo del equipo)

CasaOrtizRamirez

Departamento Cartera (una red empresarial, que le dice al mundo que departamento hace uso de ella)

Esto seleccionando solo algunos y mirando los datos solo hasta la D. no es buena idea usar un nombre que dé tanta información sobre quién la usa.

3. ANÁLISIS Y CONSIDERACIONES ADICIONALES

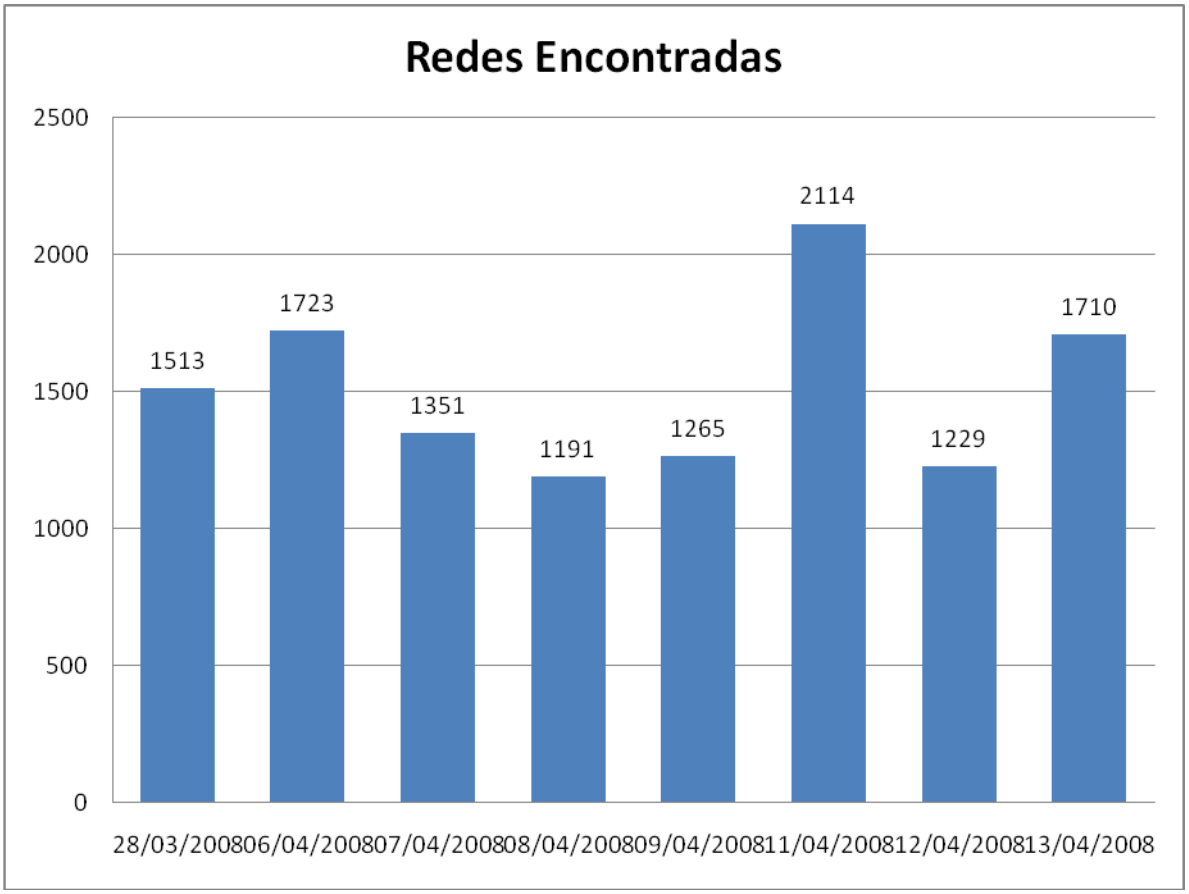

Gráfico 10 Redes encontradas por día de recorrido

El recorrido promedio duró 40 minutos y se realizó entre las 6 pm y las 9pm en diferentes días de la semana, durante los recorridos no se superaron los 40 Kms/h, se evitó al máximo repetir rutas durante un mismo recorrido.

Las velocidades encontradas para el 99% de las redes es de 11 o 54mbps, lo cual es lo habitual para equipos de transmisión 802.11a/b/g, pero en el 1% restante se encuentran fracciones de estas velocidades, lo que indica la presencia de redes configuradas o con el ánimo de compartir parte del ancho de banda o con restricciones hechas al realizar la configuración.

El 99% de las redes encontradas corresponden a puntos de acceso, el 1% restante se explican por redes ad-hoc

Para identificar al vendedor se utiliza la dirección MAC del punto de acceso, los números MAC se entregan a los fabricantes y en teoría son únicos. No se puede determinar el vendedor del equipo en 324 casos, 154 de estos casos son debidos a redes ad-hoc (el total de las conexiones ad-hoc detectadas) en los demás casos se puede presumir que el usuario las cambio por algún motivo, tal vez para proteger las características de su equipo o son Puntos de Acceso configurados con MACs aleatorias (como las que se pueden crear con un punto de acceso por ejemplo desde Linux). Algunos puntos de acceso ofrecen la opción de clonar la MAC de la tarjeta de red del equipo que estaba conectado, esto se hace porque algunos proveedores de Internet, configuran sus dispositivos dando acceso solo a una o dos MAC autorizadas, el punto de acceso al duplicar la MAC del equipo conectado, burla la restricción del proveedor, pero en este proceso es posible que obtenga una MAC de una tarjeta de un fabricante que no respete los números de MAC autorizados y utilice cualquiera de los números disponibles.

4. CONCLUSIONES Y TRABAJOS FUTUROS

Al completar este proyecto, es inevitable sopesar los conocimientos que se tenían sobre el tema antes y después de realizarlo, en este momento los conocimientos sobre las redes inalámbricas, su seguridad, las formas de protegerlas y así mismo de vulnerarlas es mucho mayor que el conocimiento con el que se emprendió este proyecto. Los conocimientos sobre las redes inalámbricas no son completos, hay un largo camino por recorrer, en temas de criptografía, en temas de transmisión electromagnética, y muchos más que complementan las actividades inalámbricas, pero al terminar este trabajo se puede afirmar que se tiene un conocimiento sólido para continuar el aprendizaje.

Así como se aprendió sobre el tema, es preocupante la cantidad de gente que no sabe o no le importa, ver la cantidad de redes inalámbricas sin protección, tan solo en un sector de la ciudad. La cuestión no se limita solo a Medellín, el 7 de julio de 2008, el diario El Tiempo, publico un artículo titulado: “redes inalámbricas de Bogotá son inseguras”, (el artículo se encuentra en esta dirección http://www.eltiempo.com/tecnologia/enter/movilidad/home/redes-wi-fi-en-bogota-son-inseguras_4362972-1).

Las redes inalámbricas se pueden y se deben proteger, una red inalámbrica abierta puede ser abusada muy fácilmente para transmitir contenido peligroso o ilegal, así como también para acceder ilegalmente a equipos de cómputo. Como ya se mostró en este trabajo, proteger una red inalámbrica no es algo necesariamente difícil, tarda un par de minutos y da algo de tranquilidad para con la información que se transmite y se recibe

Como trabajo futuro habría que hacer un mapeo más completo de la ciudad, incluso de los municipios del área metropolitana, recabar información más completa sobre las redes de toda la ciudad, y hacer análisis demográficos sobre las redes, esto se puede hacer con encuestas realizadas al azar, en las que se hagan preguntas abiertas sobre el uso de las redes inalámbricas. También quedan por hacer, manuales de instalación de redes que incluyan otros dispositivos de hardware y sistemas operativos, sin llegar al punto de intentar construir un manual completamente exhaustivo.

Ya a un nivel educativo, los proveedores de Internet deberían dar una capacitación sobre temas inalámbricos y de seguridad, se puede preguntar cuantas llamadas semanales tendrán que responder porque la red comenzó a comportarse extrañamente o porque un virus atacó a un computador, educar siempre será más efectivo que reparar.

BIBLIOGRAFÍA

1. **NIST National Institute of Standars and Technology.** *Wireless Network Security 802.11, Bluetooth and Handheld Devices, Special Publication 800-48.* Gaithersburg : National Institute os Standars and Technology, 2002.

2. —. *Wireless Network Security 802.11, Bluetooth and Handheld Devices, Special Publication 800-48 (draft).* Gaithersburg : s.n., 2007.

3. —. *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, Special Publication 800-97.* Gaithersburg : s.n., 2007.

4. War Driving Tools. *War Drive.* [En línea] [Revisado el: 28 de Julio de 2008.] http://www.wardrive.net/wardriving/tools.

5. Netstumbler Wiki Forums. *Netstumbler Site.* [En línea] [Revisado el: 28 de Julio de 2008.] http://www.netstumbler.org/index.php.

6. IEEE 802.11 Working Group. *IEEE 802.11 Working Group Site.* [En línea] [Revisado el: 28 de Julio de 2008.] http://www.ieee802.org/11/.

7. Vistumbler. *a wireless network scanner for vista.* [En línea] [Revisado el: 28 de Julio de 2008.] http://www.vistumbler.net/.

8. IEEE 802.11i-2004. *Wikipedia.* [En línea] [Revisado el: 28 de Julio de 2008.] http://en.wikipedia.org/wiki/802.11i.

9. Birthday Problem. *Wolfram MathWorld.* [En línea] [Revisado el: 28 de Julio de 2008.] http://mathworld.wolfram.com/BirthdayProblem.html.

10. Fluhrer, Mantin, and Shamir attack. *Wikipedia.* [En línea] [Revisado el: 28 de Julio de 2008.] http://en.wikipedia.org/wiki/Fluhrer,_Mantin,_and_Shamir_attack.

11. Backtrack Remote Exploit. *Backtrack Forums.* [En línea] [Revisado el: 28 de Julio de 2008.] http://forums.remote-exploit.org/.

12. **Beaver, Kevin y Davis, Peter T.** *Hacking Wireless Networks for Dummies.* Hoboken : Wiley Publishing Inc, 2005.

13. Wi-Fi Alliance Home Page. *Wi-Fi Alliance.* [En línea] [Revisado el: 28 de Julio de 2008.] http://www.wi-fi.org.

14. **Tews, Erik, Weinmann, Ralf-Philipp y Pyshkin, Andrei.** Breaking 104 bit WEP in less than 60 seconds. *International Association.* [En línea] 2007. http://eprint.iacr.org/2007/120.pdf.

15. **Habraken, Joe.** *Home Wireless Networking in a Snap .* s.l. : Sams Publishing, 2006.

16. **Carpenter, Tom y Barrett, Joel.** *CWNA, Certified Wireless Network Administrator, Official Study Guide.* New York : McGraw-Hill, 2008.

17. **Heltzel, Paul.** *Complete Home Wireless Networking: Windows® XP Edition.* Upper Saddle River : Prentice Hall PTR, 2003.

18. **Hurley, Chris, y otros.** *WarDriving: Drive, Detect, Defend: A Guide to Wireless Security.* s.l. : Syngress Publishing, 2004.

19. **Hurley, Chris.** *WarDriving & Wireless Penetration Testing.* Rockland : Syngress Publishing, Inc., 2007.

20. **Vladimirov, Andrew A, Gavrilenko, Konstantin V y Mikhailovsky, Andrei A.** *Wi-Foo: The Secrets of Wireless Hacking.* Boston : Pearson Education, Inc., 2004.

21. **Webster's.** *Third New International Dictionary of the English Language.* Springfield : Merriam-Webster, Inc., 2002.

22. 4 steps to set up your home wireless network. *Microsoft.* [En línea] [Revisado el: 2008 de Julio de 2008.] http://www.microsoft.com/athome/moredone/wirelesssetup.mspx.

23. LACNIC - WHOIS. *Latin American and Caribbean Internet Addresses Registry.* [En línea] [Revisado el: 28 de Julio de 2008.] http://lacnic.net/cgi-bin/lacnic/whois?lg=ES.

24. Google Earth. *Google Earth.* [En línea] [Revisado el: 28 de Julio de 2008.] http://earth.google.com/.

25. **Parker, Donn B.** *Fighting Computer Crime: A New Framework for Protecting Information.* Hoboken : John Wiley & Sons, Inc., 1998.