UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA

Desarrollo de una Herramienta que permite Identificar y Monitorear Dispositivos Inalámbricos basados en el Estándar IEEE 802.11

Autor: Ing. CARLOS ALBERTO ROMERO BALZA
Tutor: Prof. WILLIAM POLANCO ROMERO

Barquisimeto, 2006

Universidad Centroccidental
"Lisandro Alvarado"
Decanato de Ciencias y Tecnología
Coordinación de Postgrado

Barquisimeto, Enero 24 de 2006

Profesora: Maritza Bracho de Rodríguez

Coordinadora del Programa Maestría en Ciencias de la Computación

Sirva la presente para notificarle que he aceptado la Tutoría del Trabajo de Grado titulado:

Desarrollo de una Herramienta que permite Identificar y Monitorear Dispositivos Inalámbricos basados en el Estándar IEEE 802.11.

Presentado por el Ciudadano: Carlos Alberto Romero Balza, para optar al título de Magíster Scientiarum en Ciencias de la Computación. Mención: Redes de Computadoras.

Anexo a la presente solicitud, constancia de notas y solvencia administrativa expedida por la Coordinación de Postgrado del Decanato.

Datos del Tutor: Polanco Romero William Ramón

Cédula de Identidad: 7.501.562

Profesión: Ingeniero en Informática

Postgrado: Magíster en Electrónica

Coordinador de la mención de Redes de la Maestría en Ciencias de la Computación del Decanato de Ciencias y Tecnología de la UCLA

_____

Una voz del Pensamiento

Coordinación de Postgrado Decanato de Ciencias y Tecnología Núcleo Obelisco
Teléfonos: 2591712-2591618 Fax: 2591718

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"

DECANATO DE CIENCIAS Y TECNOLOGÍA

MAESTRIA EN CIENCIAS DE LA COMPUTACIÓN

Desarrollo de una Herramienta que permite Identificar y Monitorear Dispositivos Inalámbricos basados en el Estándar IEEE 802.11

Autor: Ing. CARLOS ALBERTO ROMERO BALZA

Tutor: Prof. WILLIAM POLANCO ROMERO

RESUMEN

Este proyecto plantea desarrollar una herramienta de s*oftware* (husmeador), que identifique y monitoree los dispositivos y las conexiones inalámbricas en una red de área local (WLAN – *Wíreless Local Area Network*) bajo el estándar de la IEEE 802.11, aprovechando elementos y capacidades de las redes inalámbricas del laboratorio de redes del DCyT de la UCLA. Realizando las siguientes actividades: a) Diagnosticar si existen en el mercado herramientas similares que permitan supervisar, identificar y monitorear estaciones y dispositivos inalámbricos conectados, no autorizados en la WLAN basada en el estándar 802.11, sin restricciones de tiempo de uso, ni de identificación de una sola marca de componentes, b) Recolectar, analizar y evaluar información pertinente al estándar IEEE 802.11, c) Investigar como desarrollar un software tipo herramienta capaz de identificar y monitorear redes Wlan, haciendo clasificación de la información por dispositivo y conexión, d) Desarrollar la herramienta, e) Evaluar la herramienta verificando que la información arrojada coincida con valores reales de los parámetros estudiados. La importancia del proyecto radica en descubrir todos los dispositivos inalámbricos que estén activos en una WLAN, permitiendo detectar posibles intrusos. Basados en el estándar 802.11, así como medir la distancia aproximada, potencia de la señal. También se obtendrán los parámetros de cada uno de los dispositivos (Dirección IP, *Mac Address*). Herramientas similares tienen limitaciones de tiempo de uso, de marca específica, así como altos costos. Esta herramienta no tendrá ninguna de estas limitaciones, brindando soporte en cuanto a diseño y desarrollo, por lo cual se recomienda para futuros proyectos similares que necesiten de las herramientas aquí utilizadas.

Palabras Clave: Monitor, *Sniffer*, Detección, WLAN, 802.11.

INTRODUCCIÓN

El desarrollo de la tecnología Inalámbrica WLAN ha permitido que este tipo de redes comience a imponerse sobre las redes cableadas de uso común. En sus inicios las WLAN eran costosas, lentas e inseguras; pero hoy en día se cuenta con precios accesibles, velocidades mejoradas bastante aceptables y en continua evolución, además de altos niveles de seguridad.

La identificación y monitoreo de conexiones inalámbricas en una red es esencial para los administradores de redes (debido a que pueden supervisar sus conexiones, observando el tráfico, estimando así la calidad del servicio ofrecido a sus clientes finales), y para quienes son los usuarios finales de los enlaces, puesto que la confiabilidad de sus datos está en juego.

El objetivo principal de este trabajo es el de generar un *software* para la identificación y monitoreo de dispositivos inalámbricos en forma general, basados en el estándar IEEE 802.11, que permita observar las direcciones físicas, las direcciones IP de los diferentes dispositivos que se encuentren en una red de área local inalámbrica.

La presente investigación se sitúa en la modalidad de estudios de proyectos, estructurado como se detalla a continuación:

Capítulo I: Comprende el planteamiento del problema, objetivos, justificación e importancia.

Capítulo II: Se refiere al marco teórico, donde se recopilan los antecedentes del trabajo. También cuenta con la información bibliográfica y analítica que permitió elaborar las bases teóricas que sustentan el estudio.

Capítulo III: Corresponde al marco metodológico, especificando el tipo de investigación, las fases de la metodología de investigación y el plan de trabajo.

Capítulo IV: Corresponde a la propuesta del estudio, especificando la descripción de la propuesta, los requerimientos para el desarrollo y la manera como se llevo a cabo el desarrollo.

Capítulo V: Ofrece un conjunto de Conclusiones y Recomendaciones obtenidas del estudio y desarrollo, enfocadas en la tecnología de redes inalámbricas basadas en el estándar IEEE 802.11.

Estos cinco capítulos descritos definen las herramientas, parámetros, metodología, información y ayudas necesarias para la consecución de los objetivos del presente trabajo.

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

El desarrollo y evolución de los sistemas computacionales, trae consigo inmensa cantidad de mejoras y beneficios, que permiten ser cada día más eficientes en la prestación de servicios. Las conexiones inalámbricas se han convertido en un estándar permanente el cual evoluciona de manera rápida, precisa y eficiente. Se plantea el desarrollo de una herramienta (*software*) capaz de identificar y monitorear los dispositivos inalámbricos que puedan existir (tarjetas, *access point*, *routers*) y que estén en funcionamiento en una red de área local inalámbrica.

Desde que se iniciaron y aún hoy en día, la mayoría de sistemas informáticos son inmovibles, destinados a un escritorio o sitio fijo. En los comienzos de las redes informáticas, en 1969, cuando se creó la primera de esas redes de la historia "Arpanet" estaba basada en la conexión de puntos fijos, como siempre han existido y existirán visionarios, tal como *Scott McNealy*, directivo de la empresa "*Sun*", él hablaba a finales del siglo pasado de la importancia de la movilidad y del trabajo en red en el futuro *McNealy* (1969). Era el paso para acercar las telecomunicaciones al mundo de la computarización en movilidad, algo que ya muchos profesionales y expertos en el área andaban buscando sin cesar.

La movilidad trae consigo el concepto de inalámbrico o su vocablo en ingles "*Wíreless*", concepto que IBM ya había experimentado hace años con su PCjr (1984), aparato dotado de un teclado sin cable, y un puerto de rayos infrarrojos para

comunicarse. Para ese entonces se tenía claro que desde un nivel de conectividad de corta distancia, se tenía que pasar a otros niveles superiores y largas distancias. Debía ser la superación del cable como vía de conexión para pasar a redes inalámbricas que dieran servicio a empresas, organizaciones y entornos que por su carácter de necesaria movilidad de sus usuarios pudiesen solventar sus expectativas de conectividad para sus redes internas así como la utilización de Internet desde puntos móviles.

Muchas personas ven en esta tecnología el valor agregado que necesitan las empresas para estar a la vanguardia de la industria que avanza tecnológicamente. El Instituto de Ingenieros Eléctricos y Electrónicos (*Institute Electrical Electronics Engineers*, Inc. "IEEE") ha establecido los estándares y los parámetros para trabajar y hacer desarrollos en ambientes inalámbricos como lo es el estándar 802.11.

Pocos expertos en la comunicación y profesores universitarios hubiesen podido imaginar hace unos años que se fuera a producir la popularización de un estándar que responde a la definición numérica 802.11. En pleno inicio de la revolución hacia la sociedad-red y con unos procesos de digitalización bastante avanzados en muchas empresas, una tecnología bautizada con el nombre de Wireless Fidelity o Wi-Fi empieza a popularizarse y ganar adeptos entre las comunidades de informáticos, hackers (piratas informáticos) y usuarios de cualquier sistema operativo tal como Linux. Las predicciones llegan incluso más lejos de lo que muchos se podían imaginar; las palabras de Larry Birenbaum Birenbaum (2002), directivo de Cisco Systems, ha dejado una gran reflexión: "creemos que la tecnología inalámbrica tendrá el mismo impacto que la llegada del computador personal - *Personal Computer* (PC)".

Todo empezó con el impulso de la Alianza para: La Compatibilidad del Protocolo Ethernet Inalámbrico - *Wireless Ethernet Compatibility Alliance* (WECA),

donde están empresas tan importantes como IBM, Cisco y Microsoft, son ellas las que venden el hardware y el software que van a utilizar, adaptar y copiar las comunidades wireless. Pero la evolución y mejoras es un impulso natural en el ser humano, ya hoy en día, también existen nuevas empresas, nuevos hardware y nuevos sistemas operativos, conllevando una evolución, crecimiento y desarrollo en el área.

Cuando millones de usuarios disfrutan ya en todo el mundo del éxito que ha supuesto la popularización de la telefonía móvil. Sistema Global para Móviles - *Global System for Mobile* o Grupo Móvil Especial - *Groupe Special Mobile* (GSM), por el gran uso de los mensajes Servicio de Mensajes Cortos - *Short Message Service* (SMS), por el impulso que se le ha dado al lenguaje de marcas - *Wireless Markup Language* (WML) y por tener tres de las grandes empresas globales constructoras de equipos de telefonía: Nokia, Ericsson y Siemens, los expertos se preguntan hacia dónde se encaminan los usuarios en los diferentes niveles de wireless

Red de Área Personal - *Personal Área Network* (PAN), Red de área local - *Local Area Network* (LAN), Red de Área Metropolitana - *Metropolitan Area Network* (MAN), Red de Área Mundial - *World Wide Area Network* (WAN)).

La conexión inalámbrica va desde el contacto milimétrico hasta el campo de los satélites. Definidas como: tecnologías fijas que son los teléfonos y portátiles en comunicación inalámbrica (WLAN – "*Wíreles Local Area Network*" – Redes Inalámbricas de Área Local), tecnologías móviles (WWAN) con costos asociados por tráfico y las sedentarias (WPAN) que se conectan a menos de 10 metros. Las WLAN y las WWAN son las que más pueden revolucionar el panorama dentro del campo de las redes inalámbricas. Tanto en los hogares, como en las empresas para realizar enlaces entre edificios, en sitios públicos de alta concentración (espacios universitarios, estaciones de autobuses, medios de comunicación, ...), las

posibilidades de utilizar las tecnologías inalámbricas son inmensas por no tener que usar cables.

Las WLANs creadas con el estándar 802.11b el cual es un poco más avanzado, son producto de una tecnología madura, de bajo costo y ya experimentadas suficientemente. Basta con que el usuario tenga un computador portátil con tarjeta inalámbrica, la cual alcanza con su antena 150 metros aproximadamente, para que empiece la experiencia de entrada sin cables en la Red. También los obstáculos tales como edificios, montañas, árboles; influyen en el alcance de la tarjeta. Una vez conectados el computador con el software adecuado, se tendrá comunicación con el nodo más cercano, el cual admite hasta 10 computadores conectados a un mismo tiempo. De esta forma, el usuario se conecta al nodo o computador central desde el cual por medio de una conexión de tecnología de línea de subscriptor digital-DSL-Digital Sucriber Line (ADSL) es posible llegar a Internet. Desde la movilidad que da un portátil se puede entrar en la red con lo cual el mundo de los profesionales de la comunicación y de las comunidades de vecinos se pueden acercar más hacia los hábitos-red que cada vez irán apareciendo en diferentes ámbitos de la sociedad.

En Estados Unidos, por unos pocos dólares se podía tener acceso a 750 puntos de conexión Wi-Fi en lugares estratégicos como estaciones de autobús, aeropuertos, hoteles, cafés y restaurantes a principios del año 2002. Los sitios públicos de alta concentración en EEUU aumentan cada día más, y los sitios web de referencia que sirven para buscarlos son muy visitados. Ya en Venezuela, se cuenta con servicios similares.

El crear una herramienta que permita identificar y monitorear los dispositivos inalámbricos que conforman y se conectan a una WLAN, así como poder identificar los dispositivos inalámbricos que tratan de conectarse o se conectan en forma no autorizada, es beneficioso para elevar los niveles de seguridad. Aun contando con servicios tal como la de un Protocolo de Configuración Dinámica de Servidores –

Dinamic Host Configuration Protocol (DHCP) el cual asigna direcciones IP de forma automática en función de las máquinas registradas con sus *MAC ADDRESS*. Podrían conectarse equipos no autorizados y causar daños dentro de la red. Esta herramienta aumenta los niveles de confiabilidad de la red al realizar análisis de las direcciones de Control de Acceso al Medio – *Médium Access Control* (MAC); calcular la distancia aproximada de una estación móvil, dar conocer la potencia de la señal.

A muchas aplicaciones existentes de este tipo a nivel mundial se les define y se les da el nombre de programa tipo *Sniffer* (Husmeador). Aplicaciones similares a esta capaces de hacer los análisis e identificaciones antes descritos han sido desarrolladas por varias empresas y grupos fuera de Venezuela, pero con limitaciones tales como: no informan la forma y metodología de cómo desarrollar este tipo de aplicación, solo pueden identificar una sola marca tipo o modelo de componentes en específico, solo pueden ejecutar ciertas funciones elementales tal como identificar solamente el nombre o identificar solo la dirección IP; la consecución de uso de una gran mayoría de estas aplicaciones es por tiempo limitado (máximo 30 días) y los costos muy altos. Todas estas limitaciones conforman un gran estímulo en la investigación, estudio y desarrollo de cómo lograr la elaboración de esta herramienta para la consecución de los objetivos aquí planteados.

Todo lo antes expuesto lleva a considerar las siguientes interrogantes:

¿Existe en el mercado local una herramienta que permita supervisar, identificar y monitorear estaciones y dispositivos inalámbricos conectados en la WLAN basada en el estándar 802.11?

¿Existen parámetros en el estándar 802.11 que permitan detectar estaciones y dispositivos inalámbricos conectados a una WLAN?

¿Es posible desarrollar esta herramienta usando componentes de software reutilizables que faciliten el manejo de la interfaz gráfica y de las conexiones inalámbricas?

¿Solucionará el problema de detectar intrusos, sirviendo de apoyo al administrador de la red como herramienta de supervisión y monitoreo de redes en un área de WLAN?

¿Esta herramienta será funcional en cualquier área donde exista una WLAN con dispositivos inalámbricos conectados?

Objetivos

Objetivo General:

- Desarrollar una herramienta de *software* que permita identificar y monitorear los dispositivos inalámbricos (estaciones, *access point, routers*) que se encuentren activos en una red inalámbrica local, basada en el estándar IEEE 802.11.

Objetivos Específicos:

1 Determinar si existe una herramienta en el mercado local que permita supervisar, identificar y monitorear estaciones y dispositivos inalámbricos conectados, en la WLAN basada en el estándar 802.11?

2 Identificar los parámetros operativos de una WLAN bajo los estándares 802.11

3 Desarrollar una herramienta gráfica que permita observar y monitorear comparativamente los dispositivos inalámbricos en una red local basados en el estándar 802.11.

4 Evaluar la herramienta programada, comparando los cálculos de los parámetros generados con los valores de los parámetros reales, tales como dispositivos y conexiones activas, potencia de la señal, distancia aproximada, velocidad de transmisión y revisando si se logra detectar dispositivos inalámbricos no autorizados.

Justificación e Importancia

El objetivo del proyecto es crear una herramienta que permita a sus usuarios (administradores) observar las direcciones físicas, las direcciones IP y las tramas transmitidas y recibidas de los diferentes dispositivos (estaciones inalámbricas, puntos de acceso inalámbricos) que se encuentren en una red de área local inalámbrica, lo cual brinda un mejor grado de seguridad al permitir identificar conexiones no autorizadas manteniendo una evaluación permanente de las direcciones MAC.

La implantación de este tipo de herramienta traerá beneficios significativos debido a que los administradores de las redes podrán acceder a la información de dispositivos conectados a una WLAN, permitiendo el análisis, evaluación, control y seguridad. En este sentido las conexiones no autorizadas podrán ser deshabilitadas, por el administrador.

La importancia de la presente aplicación es que formaría parte de una corriente técnica muy poco conocida a nivel de desarrollo lo cual requiere de expertos e investigadores que estudien, manejen, dominen y controlen las herramientas, los métodos, las normas y procedimientos existentes y que están por desarrollar, logrando hacer de ella algo sencillo y de fácil uso. Con las visiones ya establecidas, el concepto *wíreless* continuará en desarrollo y evolución, es una tecnología que a cada momento se arraiga más como uso normal y cotidiano. La mayoría de los equipos eléctricos que

existen de uso común en cualquier oficina, casa o habitación contarán en un futuro próximo con este tipo de tecnología.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes de la Investigación

Identificar y Monitorear dispositivos inalámbricos es una inquietud constante en el ánimo de todos los técnicos, profesionales y personas inmiscuidas en esta área. Saber cuales y como son las conexiones inalámbricas que se encuentran en el entorno de red, puede proveer de controles, para permitir su libre funcionamiento o detener la conexión si esta es desconocida y no esta autorizada. Los diferentes estudios y desarrollos sobre WLAN son incontables. A continuación se presentan algunas herramientas y estudios con el propósito de dar soporte a este trabajo.

El trabajo de Vélez (2005) plantea metodología de diseño de sistemas digitales para telecomunicaciones basada en c/c++: aplicación a WLAN 802.11a; con esta idea, se propone una metodología de trabajo basada en una nueva herramienta denominada HarBest. Este entorno de desarrollo trata de responder a las necesidades de los grupos de diseño, aunando la etapa de descripción funcional y arquitectural en una única y acelerando la verificación del sistema, mediante la reutilización de los vectores de prueba empleados. HarBest está basado en el lenguaje C/C++, se le ha dotado de una interfaz gráfica. Además, HarBest requiere únicamente de herramientas no propietarias, con la consecuente reducción en costos.

Castro (2005), hace uso de redes Neuronales, para estimar la ubicación en áreas tipo vecindarios de computadoras móviles. El problema de la localización de usuarios, ha sido abordado en los últimos años por varios grupos de investigación, de

donde han surgido varios enfoques. De particular interés son los sistemas de localización donde se usan las señales de radiofrecuencia (RF) para estimar la posición, ya que hacen uso de la infraestructura de red inalámbrica existente.

El trabajo de Mendoza (2005), brinda un buen soporte al presente desarrollo, haciendo un estudio de aplicaciones tipo *Sniffer*, acerca de la forma como se debe desarrollar y utilizar esta herramienta. Concluyendo y basando su justificación en la parte de seguridad. Emite el siguiente concepto: "En otras palabras, la detección de *Sniffers* inalámbricos que usen adaptadores configurados con el modo de monitoreo puede ser análoga a la forma en que se detecta a una persona sintonizando una estación de radio, es decir, no existe"

El trabajo de Varea (2004), hace un buen resumen de los aspectos básicos del estándar 802.11, para lograr la implementación de redes inalámbricas seguras. Hace un estudio de la capa física, las direcciones MAC, comparación de redes Ad hoc y de Infraestructura, la asociación (mapeo) y autentificación, aspectos de seguridad WLAN, limitación propagación de radio frecuencia. Y otra buena cantidad de aspectos que conllevan a la instauración de redes inalámbricas seguras. Este escrito brinda un buen soporte al presente desarrollo, el cual al igual que el trabajo de Varea (2004) permitirá observar y monitorear comparativamente los dispositivos inalámbricos de una WLAN.

Todos estos autores sientan importantes bases para el presente desarrollo, ya cada uno de ellos suministra información que servirá de base; Vélez (2005) un desarrollo que da parámetros para hacer desarrollos independientes autónomos proveyendo una de las posibles herramientas que sirve para elaborar el presente desarrollo, Castro (2005) ayuda a reducir el tiempo de investigación al proveer fórmulas para lograr determinar la forma de ubicar computadoras móviles, Mendoza (2005) provee información y capacidades similares al presente proyecto, brindando

una descripción muy precisa de los pasos a seguir descritos en la descripción de la propuesta, Varea (2004) provee información a nivel de la capa física y de la capa MAC haciendo una identificación precisa de cada uno de los aspectos que conforman una WLAN lo cual puntualiza la importancia de este proyecto. Ya en la UCLA, como en otro gran número de instituciones se han desarrollado una gran cantidad de trabajos para controlar, analizar, monitorear el tráfico y conexiones de redes cableadas. Son desarrollos que requieren de profundos conocimientos en el área de redes: protocolos, tráfico, modulación, administración. En el área de redes inalámbricas, los desarrollos que permitan Identificar y Monitorear redes y conexiones, así como el envío de mensajes a dispositivos inalámbricos son pocos. La mayoría de estos desarrollos dependen de terceros (empresas de telecomunicaciones o redes privadas con capacidades inalámbricas tales como antenas, repetidores, satélites) hay que contratar sus servicios para lograr la implantación y puesta en marcha de esos proyectos.

Algunas de las herramientas similares a la de este desarrollo son: *NetStumble (*Stumbler, 2005*), Lycos* WLAN *Sniffer (Lycos*, 2005*), Airfart (Airfart*, 2003*), CommView for* Wifi (*CommView*, 2005), las características de todas ellas son muy similares: identifican conexiones activas, obtienen direcciones IP y direcciones MAC. La aplicación de este desarrollo será similar a la de todas estas herramientas, elaboradas en su mayoría por instituciones, organizaciones y empresas (desarrollos en grupos). Esta aplicación permitirá que sean incluidas manualmente las direcciones MAC de los equipos autorizados a conectarse a la red donde se este ejecutando dicha aplicación. Proveyendo adicionalmente la información de cómo hacer el desarrollo lo cual será de mucha ayuda y respaldo en el aspecto técnico, así como en el aprendizaje, para trabajos futuros.

El estándar IEEE 802.11 es de arquitectura nativa para redes WLAN el cual permite transmisión por Secuencia Directa (DS) y Transmisión de Espectro

Expandido por Salto de Frecuencia (FH) a nivel de la capa física., logrando que un adaptador de red opere como una estación (STA) en forma de infraestructura o como un *Access Point*. A medida que avanza el tiempo avanza también la evolución de nuevos estándares: 802.11a, 802.11b, 802.11g y su evolución y desarrollo se mantiene de forma constante ya se habla del 802.11e, 802.11i, 802.11h, 802.11n y otros.

Bases Teóricas

La historia de la comunicaciones por radio (inalámbricas) data de aproximadamente 150 años, constituyendo la base de las comunicaciones por medio de redes inalámbricas. El físico teórico escocés James C. Maxwell y el físico alemán Heinrich Hertz fueron los principales pioneros y realizaron los descubrimientos científicos sobre la transmisión de ondas electromagnéticas, y de RF (radio-frecuencia) en la segunda mitad del siglo XIX. Luego Guglielmo Marconi, en los comienzos del siglo XX, desarrollo en los Estados Unidos una introducción a las comunicaciones inalámbricas lo cual provocó una actividad febril de innovaciones tecnológicas, a personas tales como Thomas Edison, Nicola Tesla, David Sarnoff. Estas innovaciones resultaron en una serie de nuevos productos militares, profesionales y de consumo tales como comunicación de radio bi-direccionales (usada por primera vez durante la Segunda Guerra Mundial), la radio (AM y después FM) y eventualmente la televisión (blanco y negro y después a color). La tecnología inalámbrica denominada en sus inicios como espectro disperso (expandido) fue depurada en los años 40 en vísperas de la Segunda Guerra Mundial, para proteger comunicaciones militares (Baradello, 2005). El espectro disperso es una tecnología inalámbrica que trabaja en la frecuencia de 902- 928 MHz, 2450-2483.5 MHz y transmite información en bandas de espectro libre y que no requieren autorización

para su uso. Técnica que actualmente es la más utilizada en las redes LAN inalámbricas (Ciberhábitat, 2001).

La IEEE (O'Hara, 1999), ratificó el estándar 802.11 de 2.4 Giga Hertz (Ghz) en el año 1997, manejando velocidades de transmisión de 2 Mega bits por segundo (Mbps), para el año 1999 aprobó los estándares 802.11a de 5Ghz con una velocidad de hasta 54Mbps y el 802.11b de 2.4Ghz con velocidad de hasta 11Mbps; en Junio del 2003 ratifica el estándar 802.11g, capaz de transmitir hasta 54Mbps, el cual además proporciona compatibilidad con el estándar 802.11b.

El estándar IEEE 802.11 representó muchos años de trabajo para un equipo global de ingenieros. Unos de los cambios en el desarrollo del estándar 802.11 fue, unir a expertos en dos disciplinas diferentes. En el "diseño analógico de radio" y en el "diseño de protocolos de red". El IEEE 802.11 se inicia a partir de la introducción en el *Framework* (Armazón) de la IEEE 802, lo cual hace que el estándar inalámbrico sea compatible con las redes tradicionales que han estado en funcionamiento en los últimos 25 años.

Hay dos componentes principales de las redes WLAN descritos por IEEE 802.11, las estaciones móviles y los puntos de acceso (access point). Los cuales han ido mucho más allá de lo que otros estándares han hecho en el pasado. Las dos diferencias más resaltantes entre las redes cableadas y las redes inalámbricas son: Primero la conexión a través del aire en donde se despliegan de manera voluntaria las propagaciones electromagnéticas y segundo la movilidad la cual permite que el usuario no este atado a conexiones situadas en las paredes o sitios fijos.

El estándar IEEE 802.11 define una sub capa de "Control de Acceso al Medio" (MAC), manejando los protocolos, los servicios y tres capas físicas (PHY), las tres capas PHY del estándar son: Banda Base Infrarrojo (IR) PHY, frecuencia de espectro

de radio (FHSS) PHY y una secuencia directa de espectro de radio (DSS) PHY. Las tres capas describen operaciones que se encuentran en el rango de 1 y 2 Mbps. Los otros estándares son IEEE 802.11a, el cual es un dominio de multiplexación de radio frecuencia ortogonal (OFDM) PHY de 54 Mbps, el IEEE 802.11b, es una extensión para (DSSS) PHY de 11 Mbps y la IEEE 802.11g, la cual es una extensión de la 802.11b. Actualmente el desarrollo de protocolos continua en evolución, ya existen dispositivos inalámbricos capaces de operar a 108 Mbps en frecuencias de 2.4 y 2.48 Mhz. También se esta desarrollando la IEEE 802.11n la cual se espera que alcance los 500 Mbps. Una de las características más resaltantes y de gran trascendencia de las redes WLAN es la alta capacidad de la tolerancia a fallos en todos los equipos, eliminando y controlando la posibilidad de cualquier cuello de botella.

La arquitectura de la IEEE 802.11 puede parecer compleja, sin embargo esta aparente complejidad provee a la IEEE 802.11 WLAN de robustez y flexibilidad. La arquitectura envuelve un nivel de conducta oblicua para las direcciones, la cual no se había manejado en redes LAN, permitiendo el paseo de las estaciones móviles a través de una WLAN, aparentando ser estaciones inmóviles para el control de acceso al medio (MAC), el cual no maneja el concepto de movilidad. Este manejo ejecutado por la IEEE 802.11, permite a todos los protocolos de red existentes que conforman el ámbito inalámbrico, ejecutar sobre una WLAN sin tener consideraciones especiales.

Tabla 1. Comparación estándares inalámbricos.
Fuente: Redes Inalámbricas, Varela y Domínguez, Universidad Valladolid 2002

Estándar	Tasa Transferencia	Banda Frecuencia
802.11	**2 Mbit/s**	**2.4Ghz**
802.11b	**11 Mbit/s**	**2.4Ghz**
802.11ª	**54 Mbit/s**	**5 Ghz**
802.11g	**54 Mbit/s**	**2.4Ghz**

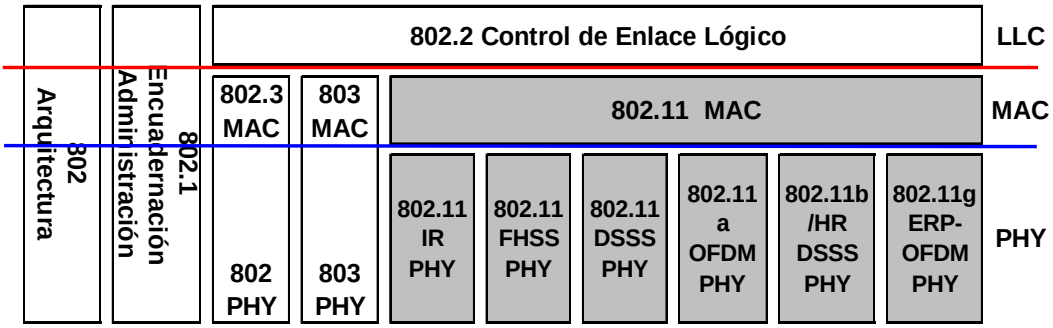

Figura 1. Arquitectura IEEE 802.11

Fuente: *Wíreless Lan Location System, Johnny Shih, University of Queensland 2003*

Formato de la Trama General:

Según los análisis realizados y de acuerdo con los estudios y desarrollos de los estándares ejecutados por la IEEE. Este formato que se muestra a continuación en la figura 2, es mucho más complejo que la mayoría de los formatos de los protocolos usados en redes cableadas de área local (LAN). Durante el desarrollo de este estándar, surgieron múltiples discusiones acerca del formato de la trama, el formato final resultante es considerado el mejor diseño balanceado entre la eficiencia y la funcionalidad.

La trama comienza con un encabezado MAC. El inicio del encabezado es el campo control de la trama (*Frame Control*). Un Campo que contiene la información de la duración para el NAV (*Network allocation* Vector, "Vector de asignación de red") seguido de una pequeña identificación. Este primer elemento es un campo de 16 bits el cual esta representado en la figura 2; le sigue el pequeño identificador y tres campos de direcciones. El próximo campo contiene información de la secuencia de la trama, el último campo del encabezado MAC es la cuarta dirección del campo. Cuando se describe de manera gráfica el formato de la trama, pareciera que el

encabezado MAC es muy largo, sin embargo no todos estos campos son usados en el paquete.

A continuación del encabezado MAC esta el cuerpo de la trama, el cual contiene la MSDU (Unidad de Servicio de Datos MAC), desde la capa de protocolos más alta. El último campo en la trama MAC, es la secuencia de chequeo de la trama (*Frame Check Sequence* "FCS"). Cada uno de estos campos que componen la trama serán descritos a continuación de manera detallada.

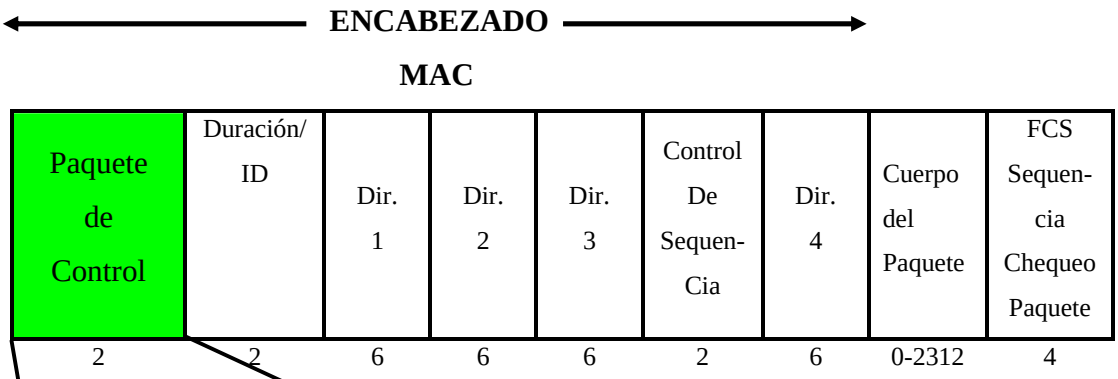

Figura 2. Formato General del paquete IEEE 802.11

Fuente: *IEEE 802.11 Handbook, Bob O'Hara and Al Petrick, IEEE Press*

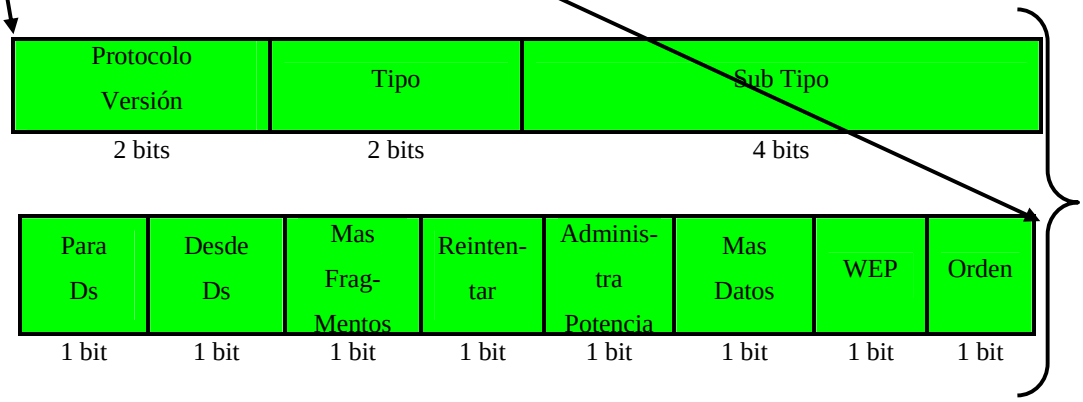

Figura 3. Formato Paquete de Control, primera parte del formato general.

Fuente: *IEEE 802.11 Handbook, Bob O'Hara and Al Petrick, IEEE Press*

El campo de la trama de control representado en la figura 2, esta formado por 16 bits, comprende la información que es requerida por MAC para interpretar todos los campos que se encuentra a continuación del encabezado.

Protocolo Versión: campo con dos bits de longitud, usado para identificar la versión del protocolo MAC IEEE 802.11, usado para construir el paquete. Este campo toma el valor de 0 en la versión estándar normal. Todos los otros valores son reservados, la operación intentada de este sub campo, es permitir a la estación recibir un paquete para determinar si esta fue construida por una versión del protocolo de la IEEE 802.11 MAC, el cual la estación no comprende. La estación debe descartar el paquete y no generar cualquier respuesta en el medio o cualquier indicación de protocolos de capas superiores de que el paquete fue recibido.

Paquete Tipo y Sub Tipo: El paquete de los campos tipo y sub tipo identifican la función del paquete y cual otro campo de encabezado MAC son representados en el paquete. Hay tres tipos de paquetes: Control, Datos y Manejo. El cuarto tipo de paquete esta normalmente reservado. Dentro de cada tipo de paquete hay algunos sub tipos. La tabla 2 provee una lista completa de los tipos de paquetes y sub tipos de combinaciones.

Tabla 2. Paquete de Tipo y Sub Tipo
Fuente: *IEEE 802.11 Handbook, Bob O'Hara and Al Petrick, IEEE Press*

Tipo Valor b3 b2	Tipo Descripción	Sub Tipo Valor b7 b6 b5 b4	Sub Tipo Descripción
00	**Administración**	**0000**	**Pedido Asociación**
00	**Administración**	**0001**	**Respuesta Asociación**
00	**Administración**	**0010**	**Pedido Reasociación**

00	**Administración**	**0011**	**Respuesta Reasociación**
00	**Administración**	**0100**	**Pedido Prueba**
00	**Administración**	**0101**	**Respuesta Prueba**
00	**Administración**	**0110-0111**	**Reservado**
00	**Administración**	**1000**	**Luz Aviso**
00	**Administración**	**1001**	**Mensaje indicación Anuncio Trafico (ATIM)**
00	**Administración**	**1010**	**Disociación**
00	**Administración**	**1011**	**Autenticación**
00	**Administración**	**1100**	**Desautenticación**
00	**Administración**	**1101-1111**	**Reservado**
01	**Control**	**0000-1001**	**Reservado**
01	**Control**	**1010**	**Ahorrar Potencia (PS)**
01	**Control**	**1011**	**Pedido Enviar (RTS)**
01	**Control**	**1100**	**Limpiar Enviar (CTS)**
01	**Control**	**1101**	**Conocimientos (ACK)**
01	**Control**	**1110**	**Conexión Libre (CF)-END**
01	**Control**	**1111**	**CF-End + CF-ACK**
10	**Datos**	**0000**	**Datos**
10	**Datos**	**0001**	**Datos + CF – ACK**
10	**Datos**	**0010**	**Datos + CF – Poll**
10	**Datos**	**0011**	***Datos + CF-ACK +CF-Poll***
10	**Datos**	**0100**	**Función Nula (Sin Datos)**
10	**Datos**	**0101**	**CF-ACK (Sin Datos)**
10	**Datos**	**0110**	**CF-Poll (Sin Datos)**
10	**Datos**	**0111**	**CF-ACK+CF-Poll (Sin Dato)**
10	**Datos**	**1000-1111**	**Reservado**
11	**Reservado**	**0000-1111**	**Reservado**

Sub campos Para DS y Desde DS ("DS" Sistema de Distribución): Para DS su longitud es 1 bit. Se usa solo en paquetes de tipo datos, indicando que el paquete esta destinado para el DS. Esto se pondrá en cada paquete de datos enviado desde una estación móvil a un punto de acceso. Este *bit* es cero en todos los otros paquetes.

El sub campo Desde DS: su longitud es 1 *bit*, utilizado solo en paquetes de tipo datos, para indicar que el paquete esta siendo enviado desde el DS. Este *bit* será puesto en cada paquete enviado desde un punto de acceso a una estación móvil, su valor es cero en todos los otros tipos de paquetes de datos. Hay cuatro combinaciones posibles para estos dos sub campos. Cuando ambos son cero, el paquete es una comunicación directa entre dos estaciones móviles. Cuando el sub campo Para DS es uno y Desde DS es cero, el paquete es una transmisión desde una estación móvil a un punto de acceso. Cuando Para Ds es cero y Desde Ds es uno, el paquete es una transmisión desde un punto de acceso a una estación móvil. Finalmente cuando ambos sub campos tienen uno como valor, se usa como un caso especial, donde una WLAN IEEE 802.11, esta siendo usada como el DS, este caso se refiere como un DS inalámbrico.

La razón para este caso especial de DS inalámbrico es permitir al DS ocupar el mismo medio como el BSS. (Conjunto Servicios Básicos – *Basic Service Set* (BSS)) . Si este caso no existe, allí podría haber una confusión acerca de la dirección del paquete. Cuando ambos sub campos son uno, el paquete esta siendo enviado (distribuido) desde un punto de acceso a otro, sobre un medio inalámbrico.

Sub Campo Más Fragmentos: 1 bit de longitud, es usado para indicar que este paquete no es el último fragmento de un dato o el paquete de administración que ha sido fragmentado. Este sub campo es cero en el último fragmento de un dato o de un paquete de administración que ha sido fragmentado en todo el paquete de control y en cualquier dato o administración de paquetes que no este fragmentado.

Sub campo Reintentar: 1 bit de longitud, es usado para indicar donde un dato o paquete de administración está siendo transmitido por primera vez o si esto es una retransmisión. Cuando su valor es cero, el paquete está siendo enviado por primera vez. Cuando el valor es uno, el paquete está siendo retransmitido. El MAC receptor, para permitir al filtro quitar los paquetes recibidos, usa este sub campo, todo el tiempo en combinación con el sub campo número de secuencia.

Sub campo Administrar Potencia: 1 *bit* de longitud. Una estación móvil usa este sub campo para anunciar su estado administrado de potencia. El valor del sub campo indica el estado administrado de la potencia con la que la estación entrará cuando un intercambio de paquetes sea completado exitosamente. Un cero indica que la estación está en modo activo y estará disponible para comunicaciones futuras. Un uno indica que la estación estará entrando al modo administrado de potencia y no estará disponible para comunicaciones futuras. Este sub campo debe contener el mismo valor para todos los paquetes transmitidos por la estación durante un intercambio simple de información. La estación puede no cambiar su estado administrado de potencia hasta que este intercambio de paquetes haya sido completado exitosamente. Un intercambio exitoso de paquetes es el completado de dos formas o con un apretón de manos entre paquetes de cuatro formas, incluyendo la recepción correcta de un reconocimiento.

Sub campo Más Datos: 1 *bit* de longitud, el punto de acceso usa este sub campo para indicar a una estación móvil que allí esta al menos un paquete guardado en el punto de acceso para la estación móvil. Cuando su valor es uno, allí está al menos un paquete guardado en el punto de acceso para la estación móvil. Cuando es cero, allí no hay paquetes guardados en el punto de acceso para la estación móvil. Una estación móvil que es sondeada por el PC durante un CFP (Período de contienda libre – *Contention-Free period* (CFP)), también puede usar este sub campo para indicar al PC que allí esta al menos uno o más paquetes guardados en la estación

móvil, para ser enviados a un PC. En paquetes múltiples, el punto de acceso puede también configurar este sub campo para indicar que hay múltiples paquetes guardados en el punto de acceso.

Sub campo WEP: 1 *bit* de longitud, cuando es uno indica que el cuerpo del paquete del MAC, ha sido encriptado usando un algoritmo WEP. Este sub campo, puede ser configurado, para uno solamente en paquetes de datos y administrar paquetes de autenticación de subtipo. Es cero en todos los otros tipos de paquetes y subtipos.

Sub campo Orden: 1 *bit* de longitud, cuando vale 1, indica que el contenido del paquete de datos fue proporcionado para el MAC con un pedido para el servicio ordenado estrictamente. Este sub campo provee información a el punto de acceso y al sistema distribuido (DS) para permitir que estos servicios sean entregados.

Campo Duración/ID: 16 bits de longitud. Alternamente contiene información de la duración para actualizar el NAV o un ID corto, llamada la asociación ID (AID), usada por una estación móvil para recuperar paquetes que están guardados por este en el punto de acceso. Solamente revisar el ahorro de potencia (PS-Poll) de los paquetes que contienen el AID. En estos paquetes, el AID es alineado en el menos significante de 14 bits del campo. Los dos bits más significantes son puestos en uno en el paquete del PS-POLL. Porque de otras limitaciones en el protocolo, el valor máximo permitido para el AID es 2007. Todos los valores mayores a 2007 son reservados.

Cuando el *bit* número 15 de la estructura del campo esta en cero, el valor en los bits 14-0, representan el resto de la duración de un cambio de paquetes. Este valor es usado para actualizar el NAV, previendo que una estación reciba este campo desde el inicio de la transmisión, lo cual debe causar corrupción de la transmisión progresiva.

El valor del campo Duración/ID es puesto en 32.768 (ejemplo: el *bit* 15 tiene valor de uno y el resto es cero), en todos los paquetes transmitidos durante el CFP. Este valor es escogido para permitir a la estación que no reciba del CFP para reconocer que el CFP es progresivo y configurar este NAV con un valor bastante grande para que no interfiera con el CFP. Otra forma en que el AID valoriza, es cuando los bits 15 y 14 asumen el valor uno, el resto de los valores en este campo son reservados.

Campos de Direcciones: El formato del paquete MAC, contiene cuatro campos de direcciones. Cualquier tipo de paquete puede contener una, dos, tres o cuatro campos de direcciones. En el estándar IEEE 802.111 de 1997, el formato de la dirección es familiar a la dirección IEEE de 48 bits, normalmente usado para identificar la fuente y el destino de la dirección MAC contenida en el paquete, tal como en el IEEE 802.3. Adicionalmente a la dirección fuente (SA *Source Address*) y a la dirección destino (DA *Destination Address*), el estándar IEEE 802.11 de 1997, defines tres tipos de direcciones: dirección del transmisor (TA), dirección del receptor (RA) y la identificación BSS (BSSID). Este tipo de direcciones adicionales son usadas en el estándar IEEE 802.11 de 1997, para permitir movilidad transparente y para proveer un mecanismo para filtrar paquetes multiformes. La posición de la dirección en el campo dirección determina su función.

Control de Secuencia: Su longitud total es de 16 bits, conteniendo dos sub campos que se utilizan de la siguiente manera, el primer sub campo de 4 bits que maneja el número de fragmentos y el segundo es un número de 12 bits consecutivos. En total este campo es usado para permitir recibir estaciones y eliminar paquetes recibidos que estén duplicados.

Campo Cuerpo del Paquete: Este campo contiene la información específica para la información particular o paquetes administrados. Este campo es de longitud

variable. Puede ser de 2304 *bytes*, sin encriptación WEP, o de 2312 bytes cuando el campo es encriptado usando WEP. El valor de 2304 *bytes* como longitud máxima de este campo, fue escogido para permitir a una aplicación enviar piezas de información de 2048 bytes, la cual puede ser encapsulada como muchos protocolos de 256 bytes de encabezado documental de la capa superior.

Campo Secuencia de chequeo del Paquete: Tiene una longitud de 32 bits. Contiene el resultado de aplicar el polinomio CCITT CRC-32, para el encabezado MAC y el cuerpo del paquete. El polinomio CRC-32 es representado por la siguiente ecuación:

$$\mathbf{G(x) = x^{32} + x^{26} + x^{23} x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1}$$

Este es el mismo polinomio usado en las otras redes estándar IEEE 802 LAN. La secuencia de chequeo del paquete en una IEEE 802.11, el paquete es generado en la misma forma que se realiza en el estándar IEEE 802.3.

Redes Locales Inalámbricas (WLAN) IEEE 802.11:

Este estándar especifica los parámetros de la capa física y de la capa de enlace incluyendo el control de acceso al medio (MAC), para redes locales inalámbricas. Los dispositivos conectados a una red inalámbrica son fácilmente integrables a una red *Ethernet* cableada a través de un puente (punto de acceso) el cual permite la unión de ambas redes.

Ventajas de las redes inalámbricas:

- Movilidad: Ofrecen a los usuarios acceso a la información en tiempo real en cualquier lugar de la organización.

- Instalación sencilla: Evita tender cables a través de paredes y techos.
- Reducción de Gastos: En entornos dinámicos que requieren mudanzas y cambios frecuentes.
- Escalabilidad: Estos sistemas se pueden configurar con diversos tipos de topologías para satisfacer las necesidades de aplicaciones e instalaciones específicas. Encontrándose en permanente evolución y desarrollo con un alto nivel de compatibilidad.

Desventajas de las redes inalámbricas:

- Interferencias: La red estará sometida a interferencias debidas al entorno radioeléctrico e incluso podría producir interferencias en otros dispositivos de su entorno.
- Privacidad: Las transmisiones se propagan en el espacio sin límites definidos, por lo cual pueden ser captados por terceros y permitir ser espiadas si no se habilitan los sistemas adecuados para mantener la privacidad de las transmisiones.

Capa Física:

Las redes inalámbricas se diferencian del resto de las redes de manera principal, en la capa física y en la capa de enlace de datos según el modelo de referencia OSI ya que sustituyen al cable típico por métodos de transmisión inalámbrica: Transmisión por radiofrecuencia y la transmisión por luz infrarroja. La capa física puede usar enlaces por radio frecuencia (FHSS y DSSS) o enlaces infrarrojos por posición del pulso. Los sistemas de transmisión de radiofrecuencia son normalmente los más habituales y se basan en transmisión de espectro disperso o extendido (*spread spectrum*).

Existen dos técnicas de modulación cuando se hace uso de la tecnología de espectro disperso:

- Salto de frecuencia: (*FHSS, Frecuency-Hopping Spread Spectrum*). Los dispositivos saltan de una frecuencia a otra de manera sincronizada según un patrón determinado. Solamente los dispositivos sincronizados pueden acceder a la información.

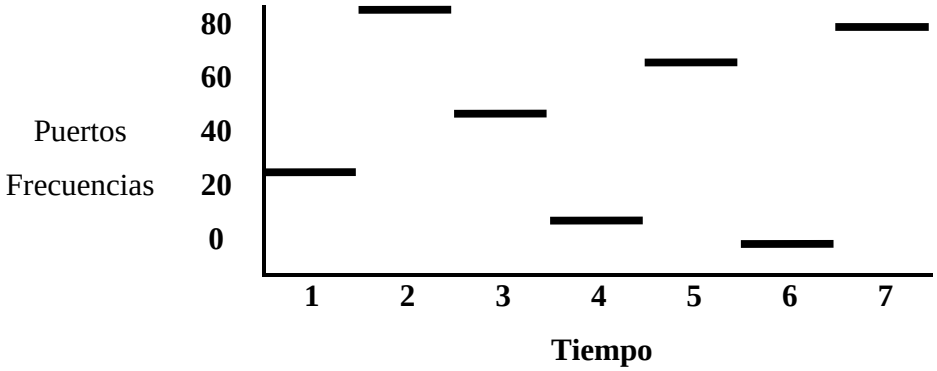

Figura 4. Salto de frecuencia.

Fuente: Redes, Universidad de Oviedo, Ingeniería Sistemas y Automática, Capítulo 3.

- Secuencia Directa: (DSSS, *Direct-Sequence Spread Spectrum*). La información a transmitir se mezcla con un patrón seudo aleatorio de bits para extender los datos antes de que se transmitan. Cada *bit* transmitido se modula por medio de la secuencia de bits del patrón de referencia, extendiendo su ancho de banda. Sólo el receptor que tenga el mismo código de extensión será capaz de regenerar la información original, mientras que cualquier otro receptor es ruido de baja potencia que resulta ignorado. Esta técnica permite corregir algunos de los errores que se puedan producir en la transmisión y requiere de un procesador digital de señales (DSP) para correlacionar la señal de entrada.

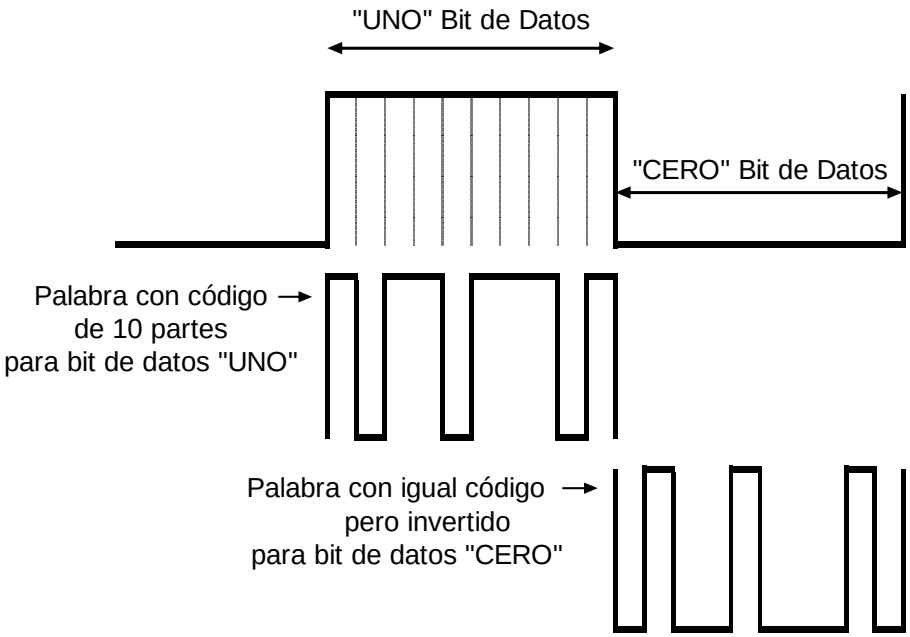

Figura 5. Conformación del Bit de Datos.

Fuente: Redes, Universidad de Oviedo, Ingeniería Sistemas y Automática, Capítulo 3.

Capa Enlace:

La capa de enlace incluye el mecanismo CSMA/CA (*Carrier Sense Multiple Access Collision Avoidance* – Percepción de la Portadora Multiple Evita el Choque de Acceso), donde un nodo se asegura de que el canal este libre antes de transmitir. El mecanismo de detección de colisiones usado en CSMA/CD no puede utilizarse en este caso debido a que un nodo no puede transmitir y escuchar el canal para detectar si otra estación lo hace al mismo tiempo. El mecanismo CSMA/CA no elimina las colisiones completamente, solo minimiza su probabilidad.

Cuando un paquete está listo para transmitir y el canal esta vació, en el nodo emite un paquete RTS (*Ready to Send* – Listo para Enviar) y espera que el receptor le

envíe un paquete CTS (*Clear to Send* – Vacio para Enviar). Tras este intercambio de paquetes el emisor envía su trama y si no hubo errores (utilizando en un mecanismo basado en el uso de CRC), el receptor envía un paquete ACK. Este mecanismo ayuda a controlar los nodos ocultos.

Seguridad de la Red Inalámbrica:

Para mantener la privacidad en las transmisiones, se ha desarrollado un algoritmo de codificación denominado WEP (*Wired Equivalent Privacy* – Privacidad Equivalente a la Cableada). Sistema que ha presentado ciertas deficiencias en su sistema de claves simétricas de 64 y 128 Bits, basado en el algoritmo RC4, al capturar una gran cantidad de paquetes, es posible descubrir la clave utilizada para el sistema.

Para mantener la privacidad es recomendable cambiar periódicamente las claves del punto de acceso y de los computadores de la red. También se puede limitar el acceso a los equipos con direcciones de red conocidas. Utilizando el sistema Radius (*Remote Autentication Dial In User Service*, Marcado Remoto de Autenticación en el Servicio de Usuario), para la autenticación de los usuarios que acceden a la red inalámbrica o también se puede usar la alternativa WPA (Wi-Fi Protected Access – Red Inalámbrica Acceso Protegido).

Otro problema es que las redes inalámbricas pueden causar un problema de seguridad para redes cableadas. Si un usuario instala por su cuenta y riesgo un punto de acceso conectado a la red cableada sin conocimientos del administrador de la red, pone en peligro la privacidad de toda la red. Es conveniente que el administrador utilice un equipo con tarjeta de red inalámbrica para revisar la red periódicamente en busca de puntos de acceso no controlados.

CAPÍTULO III

MARCO METODOLÓGICO

Tipo de Investigación

El presente estudio está enmarcado bajo la modalidad de Estudios de Proyectos, puesto que es una creación tangible sustentada en un modelo viable, susceptible de ser utilizada como herramienta de solución a problemas prácticos que se plantean, tendentes a satisfacer necesidades institucionales o sociales y se pueden referir a la formulación de políticas, programas, tecnología, métodos y procesos. Este tipo de estudio puede apoyarse tanto en la investigación de campo como en la investigación monográfica documental. Toda la descripción anterior se soporta en el: “Manual Para La Presentación Del Trabajo Conducente Al Grado Académico De Maestría”, UCLA (2002).

Fases del Estudio

A continuación se explican cada una de las diferentes fases requeridas para el desarrollo del presente proyecto.

Fase 1. Diagnóstica:

Tiene como finalidad determinar si existe en el mercado local una herramienta que permita supervisar, identificar y monitorear estaciones y dispositivos inalámbricos conectados, no autorizados en la WLAN basada en el estándar 802.11., la cual no debe presentar restricciones de tiempo de uso, ni de hacer

identificaciones de una sola arca de componentes, permitiendo controlar la identificación y monitoreo en las conexiones y enlaces que se ejecutan en redes inalámbricas tales como la del Laboratorio de Redes del DCyT de la UCLA.

Fase 2. Documentación Bibliográfica:

Se recolectará toda la información pertinente al estándar 802.11 así como también a la forma y manera de desarrollar un software capaz de Identificar y Monitorear redes WLAN, basadas en este estándar.

Fase 3. Elaboración de la Herramienta:

En función de los datos obtenidos y las identificaciones realizadas en la fase anterior, se desarrollará una herramienta que permita identificar y monitorear las conexiones inalámbricas en un entorno WLAN.

Fase 4. Evaluación de la Herramienta:

La evaluación permitirá verificar que la información arrojada por la herramienta coincide con los valores reales de los parámetros estudiados.

Fase 5. Elaboración de Conclusiones y Recomendaciones:

Se presentaran las conclusiones acerca de esta aplicación y desarrollo, donde se plantearan los aportes suministrados por el trabajo, así como las recomendaciones para investigaciones y desarrollos futuros.

CAPÍTULO IV

PROPUESTA DEL ESTUDIO

En este capítulo se describen de una forma precisa y objetiva los puntos concernientes a la realización de la propuesta planteada en el estudio. De igual forma se detallan las funcionalidades de la aplicación desarrollada, para garantizar un uso adecuado por parte de todo aquel que necesite o desee hacer uso de esta herramienta.

Descripción de la Propuesta

El presente desarrollo es una herramienta que provee de muchas ventajas y beneficios a los administradores de redes que hacen uso de tecnología inalámbrica. El nombre asignado a la herramienta es “IMCI” (Identificar y Monitorear Conexiones Inalámbricas), de las funciones ejecutadas por este tipo de desarrollo se puede definir como una aplicación tipo *Sniffer* (Husmeador).

La herramienta corresponde a un conjunto de módulos e interfaces que son presentados al usuario, los cuales ofrecen la posibilidad de identificar el tipo de red y de los dispositivos, detalles y localización de estos dentro de la WLAN. Adicionalmente la aplicación provee la capacidad de capturar paquetes que se transmiten entre los diferentes equipos conectados a la WLAN, permitiendo hacer un análisis más completo de todas las funciones que se ejecutan dentro de la misma. Además es importante resaltar que la aplicabilidad, bajo la cual se enfoca la herramienta es permitir satisfacer las necesidades de

información para profesores, alumnos, administradores de red de la UCLA mientras están conectados a la WLAN. De este modo la herramienta permite informar a través de sus módulos (sin ningún costo, sin limitaciones de tiempo y sin limitaciones de marca).

Requerimientos para el Desarrollo

Los requerimientos para lograr el desarrollo comprenden varios elementos de investigación, análisis y estudio los cuales una vez identificados y evaluados permitieron dar inicio al desarrollo, dichos requerimientos se encuentran planteados de la siguiente manera primero en un área física (*Hardware*) y segundo un área lógica (*Software*).

Área Física (*Hardware*):

Esta área requiere de estaciones (computadoras) fijas o móviles que conformen parte de la WLAN las cuales deben contar con una tarjeta de red de tipo inalámbrica, también se puede contar con *Access Point* y *Routers* inalámbricos. Dichas tarjetas y equipos deben estar basados en alguno de los siguientes estándares 802.11, 802.11a, 802.11b, 802.11g, definidos por la IEEE. Todos estos elementos y equipos serán analizados y reconocidos por esta aplicación.

Área Lógica (*Software*):

Se puede definir como el área de mayor importancia en la consecución del presente desarrollo. Está conformada por elementos tales como: Sistema Operativo en

el cual se ejecuta, Herramienta - Lenguaje de Programación, Librerías que Contengan los Estándares y Parámetros Requeridos.

Sistema Operativo: El sistema operativo en el cual se ejecuta la presente aplicación es *Windows*, en sus versiones *Windows* 2000, *Windows* XP (*Home* y *Professional Edition* con *Service Pack*) y *Server* 2003 (preferiblemente con *Service Pack* I). En sistemas operativos anteriores a las versiones antes descritas no se debe ejecutar esta aplicación ya que según los requerimientos de las librerías, no garantizan que los resultados obtenidos sean correctos. A medida que transcurre el tiempo los desarrolladores de este tipo de librerías van depurando y haciendo mejoras que se adapten a cada elemento nuevo de hardware que es creado.

Herramienta – Lenguaje de Programación: La herramienta de Programación utilizada para el presente desarrollo es *Visual Studio .Net* 2005, Lenguaje utilizado: *Visual Basic* y C++. Esta herramienta es la última versión que ha salido al mercado y en la cual ya se incluyen funciones que permiten hacer reconocimientos y manejos de dispositivos inalámbricos a diferencias de versiones anteriores que no contaban con estas cualidades.

Librerías y Estándares:

- Librería SDK (Paquete de Desarrollo de *Software – Software Development Kit*), contiene una buena cantidad de ejemplos con las fuentes disponibles en C++ y C#, viene anexa a la librería DDK.
- Librería DDK (*Driver Development Kit* - Paquete de Desarrollo de Controladores), esta librería debe ser adquirida a través de la empresa *Microsoft* la cual provee todas las funciones necesarias para la consecución del presente desarrollo, todo aquel que trabaje desarrollando hardware y desee implantarlo en ambiente Windows se le recomienda hacer uso de esta librería, con lo cual se logra la aprobación con firma digital.

- Librería NDIS (*Network Driver Interface Specification* - Especificación de Interfases para Dispositivos de Red), es la librería destinada de manera precisa a funciones de chequeo bajo nivel para redes, lo que quiere decir que al ser instalada se incluye en los directorios de *drivers* del sistema operativo, permitiendo hacer análisis de los hardware de red que se estén manejando.
- Librería PCausa.Rawether .NET., librería desarrollada por la empresa PCausa, a través de la cual debe ser adquirida, maneja todas las funciones y parámetros de la librería DDK, la ventaja es que no limita hacer uso solo de lenguaje C++ o C#, permite ser usada en varios tipos de lenguajes de programación, gracias a ello se pudo desarrollar utilizando el lenguaje de programación Visual Basic .Net 2005.

Desarrollo de la Herramienta

El desarrollo de la herramienta estuvo enmarcado en un profundo estudio y análisis de las herramientas requeridas, lo cual condujo a la previa instalación de las librerías a ser utilizadas, la librería DDK es el estándar mas adecuado para realizar este tipo de desarrollo tal como se describe en la figura 6, este es un proceso previo, independiente y complejo, la cual se debe manejar con lenguaje C++, esta es una librería que presenta una complejidad muy extrema, se manejan mas 17.000 clases y funciones, lo que quiere decir que requiere de tiempo de estudio para lograr desarrollar aplicaciones. Se realizaron suficientes pruebas para confirmar la ejecución adecuada de los módulos del sistema, llegando a la conclusión de hacer uso de la librería *PCausa.Rawether*, la cual está gráficamente detallada en la figura 7, brinda una ventaja adicional de permitir que las mismas librerías y funciones utilizadas bajo DDK, sean utilizadas haciendo uso del lenguaje de programación Visual Basic .Net 2005, cuyo lenguaje de programación también es bastante complejo e incluye muchas nuevas clases y funciones para el uso, manejo e identificación de redes inalámbricas.

Un concepto importante que se debe manejar en el ámbito de las WLAN es: El *Media Sense* (Canal de Percepción), en teoría es por donde van pasando los paquetes que se transmiten a través de la WLAN, normalmente es soportado por los *drivers* de minipuertos IEEE 802.11 NDIS cuando se encuentra en modo de infraestructura. Si el NIC (*Network Interface Card* – Tarjeta de Interfase de Red) es asociado con un AP (*Access Point* – Punto de Acceso*)* un evento conectado es generado. Cuando el NIC no es asociado con un AP un evento de canal desconectado es generado. Cuando se cambia de un AP a otro no se debe generar un evento de canal desconectado. El evento del canal de percepción conectado se genera llamando a la función *NdisMIndicateStatus* usando como argumento la función *NDIS_STATUS_MEDIA_CONNECT*, de forma similar un evento de canal de percepción desconectado es generado llamando a *NdisMIndicateStatus* usando como argumento la función *NDIS_STATUS_MEDIA_DISCONNECT*.

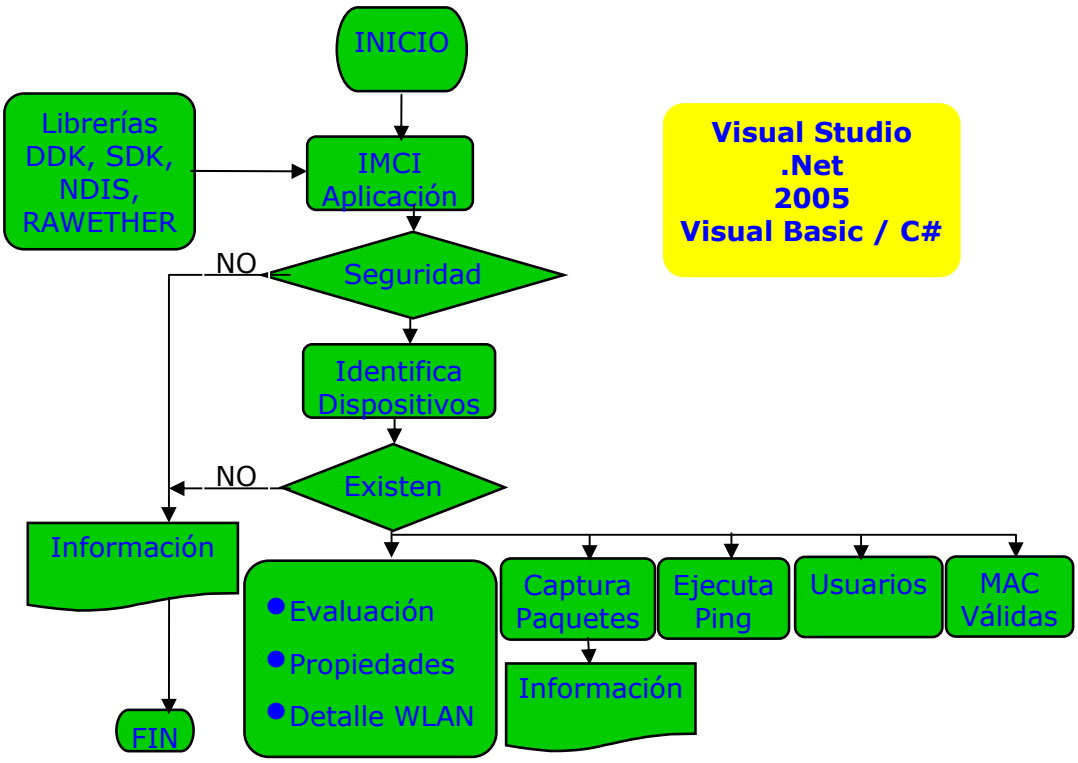

Figura 6. Diagrama Estructura.

Fuente: El autor.

El *Rawether* para componentes de *Windows* en tiempo de ejecución, incluye dos archivos DLL (*Dynamic Link Library* - Biblioteca de vínculos dinámicos), la librería W32N55.DLL - para sistemas operativos Windows 32-bit y la librería W64N55a64.DLL para el sistema extendido de Windows 64-bit (AMD64) y además de un total de ocho protocolos de *drivers* NDIS. Estas son las librerías que contienen la gran cantidad de clases y funciones las cuales suministran la alta capacidad de ir desarrollando cada una de las funciones que se ejecutan dentro de la aplicación. Para el presente desarrollo se hizo uso de la librería W32N55.DLL.

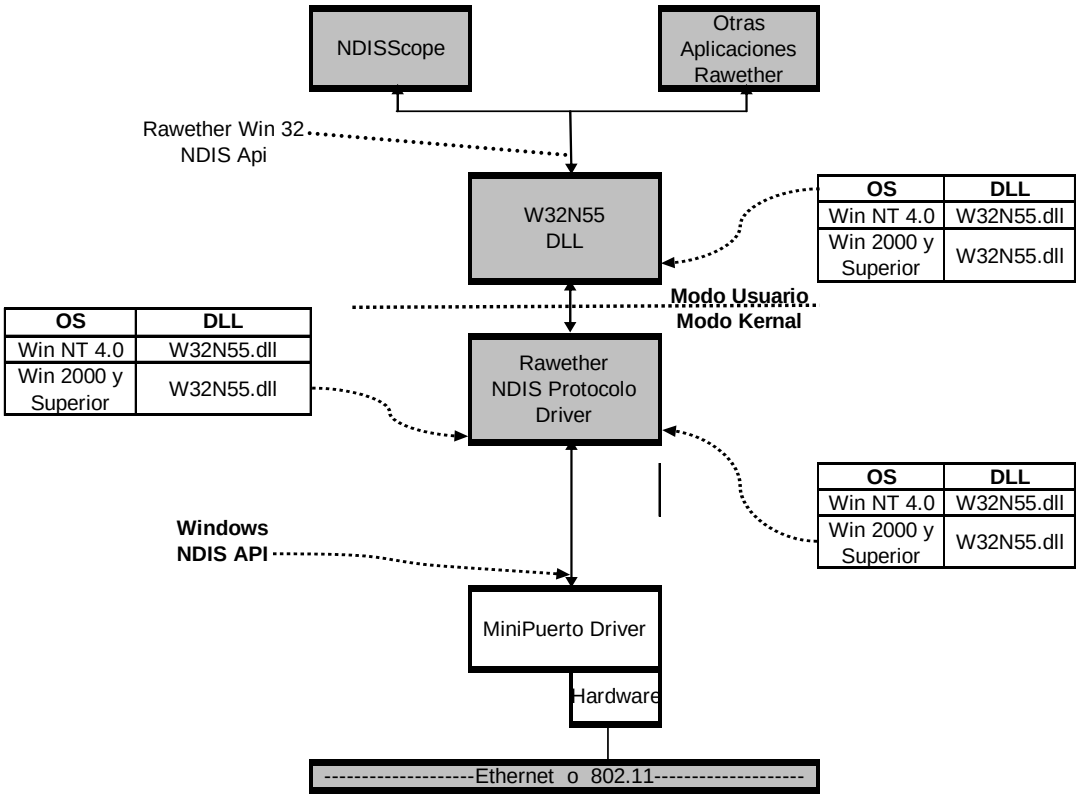

Figura 7. Arquitectura del Software.

Fuente: Manual PCAUSA NDIScope Help V5.5.

Funcionalidad de la Herramienta (Manual de Usuario)

Cuando se inicia la aplicación el primer módulo que se ejecuta presenta en pantalla la figura 8, opción de control de acceso el cual permite establecer cierto nivel de seguridad, se le pide al usuario que incluya el nombre usuario y la contraseña, lo cual evitará que personas no autorizadas puedan ejecutar la aplicación.

Figura 8. Seguridad Control de Acceso.

Fuente: El autor

Al dar inicio a la aplicación se presentan cuatro opciones, mostradas en la figura 9; Actualizar Dispositivos, Bandeja, Ayuda y Salir. "Actualizar Dispositivos" se presenta con un color de fondo diferente (azul) el cual trata de hacer resaltar esta opción se puede presionar click o se pueden usar las teclas Alt-D de forma simultanea, dando inicio a la ejecución de las funciones, una vez iniciada esta opción la aplicación hará la selección de forma automática, de la tarjeta de red inalámbrica que se encuentre instalada en el equipo donde se esta ejecutando esta aplicación. La opción "Bandeja" permite minimizar la ejecución de la aplicación colocándola como un icono en la barra de herramientas el cual al ser seleccionado con un click permite maximizar de nuevo la ejecución de la aplicación. La opción "Ayuda", suministra

información para el usuario de cómo hacer uso de esta aplicación y de los parámetros utilizados. Por último se consigue la opción “Salir”, usada para salir de la aplicación de forma segura.

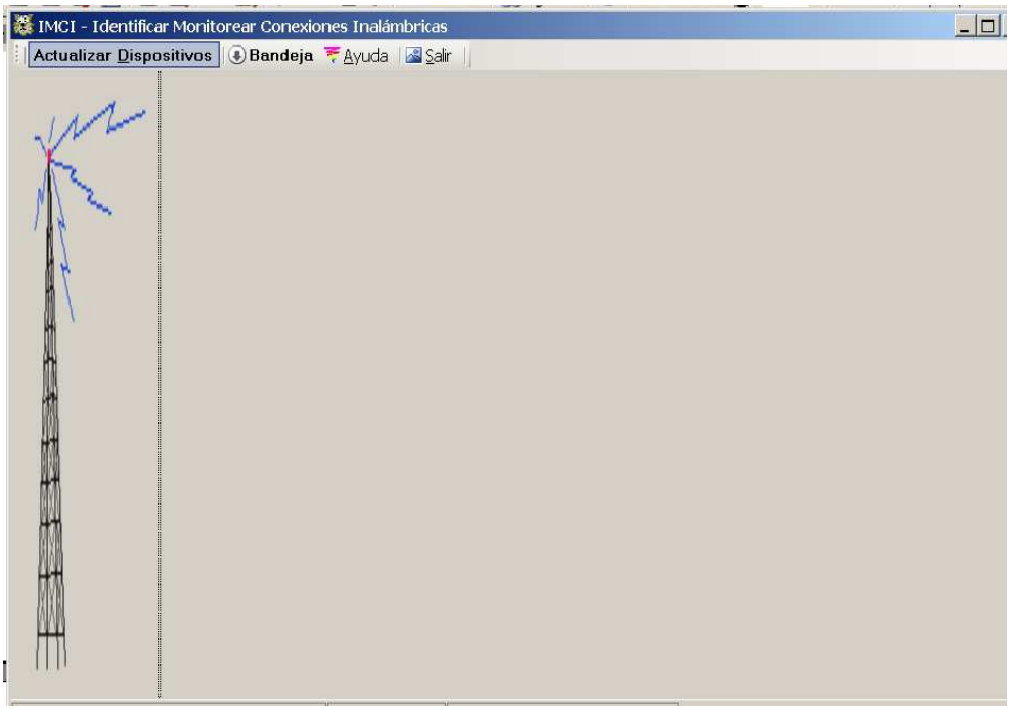

Figura 9. Pantalla de Inicio.

Fuente: El autor

Al iniciarse la ejecución de la herramienta ella hace una revisión de las tarjetas de red que se encuentran instaladas en el equipo donde se este ejecutando la aplicación, automáticamente ejecuta un rápido análisis y selecciona la tarjeta de red inalámbrica con mayor grado de potencia en su señal. Si no encuentra una tarjeta inalámbrica el sistema arranca sin hacer ningún análisis, y no permitirá que se ejecute

ninguno de sus módulos o funciones ya que es indispensable la existencia de una tarjeta de red o de algún dispositivo inalámbrico que se conecte a la WLAN.

La aplicación muestra mensaje de iniciación correcta e inmediatamente muestra una interfaz gráfica de iniciación presentada en la figura 10, mostrando en movimiento el nombre del equipo *host* (equipo local) donde se ejecuta la aplicación, se sugiere se ejecute Detalles WLAN para su correcta carga de información y los parámetros de la tarjeta de red seleccionada. Aun no se ha evaluado cuantos AP o *Routers* se encuentran conectados. Se debe salir de esta interfaz gráfica presionado la tecla ENTER o la tecla ESC o dando un click en el icono “Cerrar”.

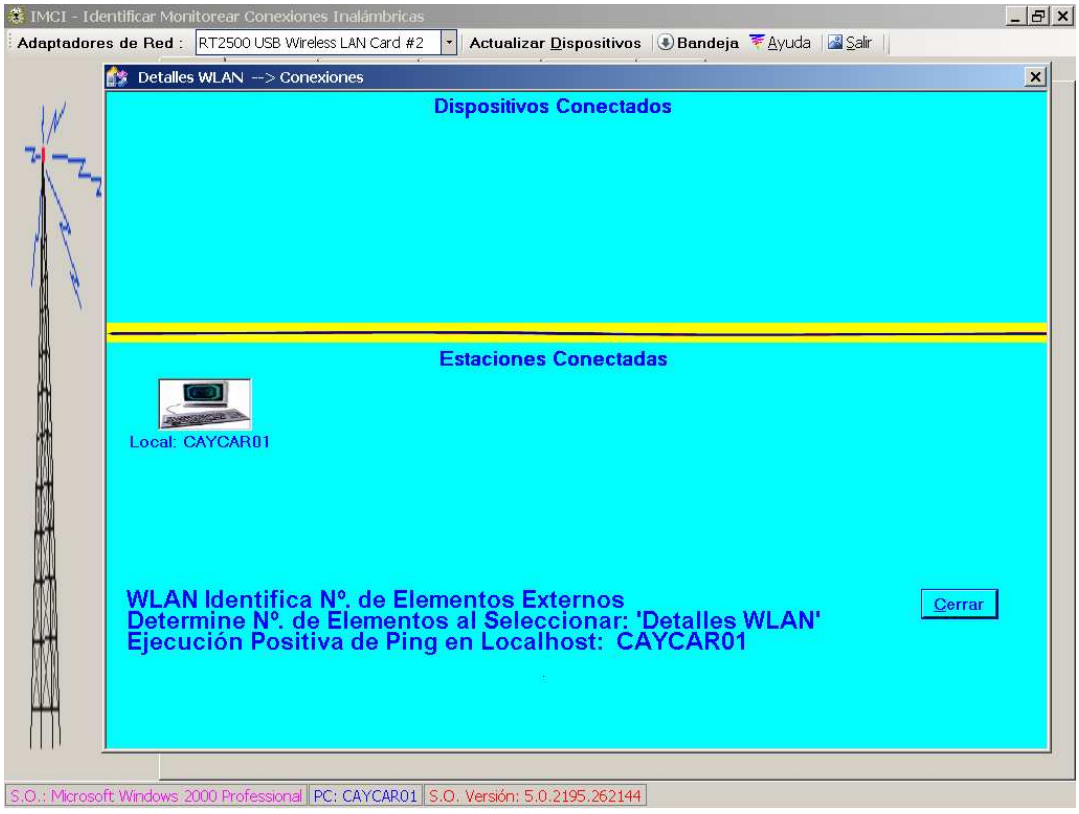

Figura 10. Primera interfaz gráfica de Inicio.

Fuente: El autor

De la opción gráfica inicial se puede seleccionar: la opción General definida en la figura 11, la cual provee información de la tarjeta de red, la dirección MAC, su dirección IP, el estándar utilizado, el estado de la conexión y el tipo de Medio Físico; del Access Point o Routers se obtiene el nombre asignado a la WLAN y características tales como su dirección MAC y la graficación dinámica de la potencia de la señal. Se puede definir como pantalla principal, la cual permite la selección del resto de módulos que conforman esta aplicación.

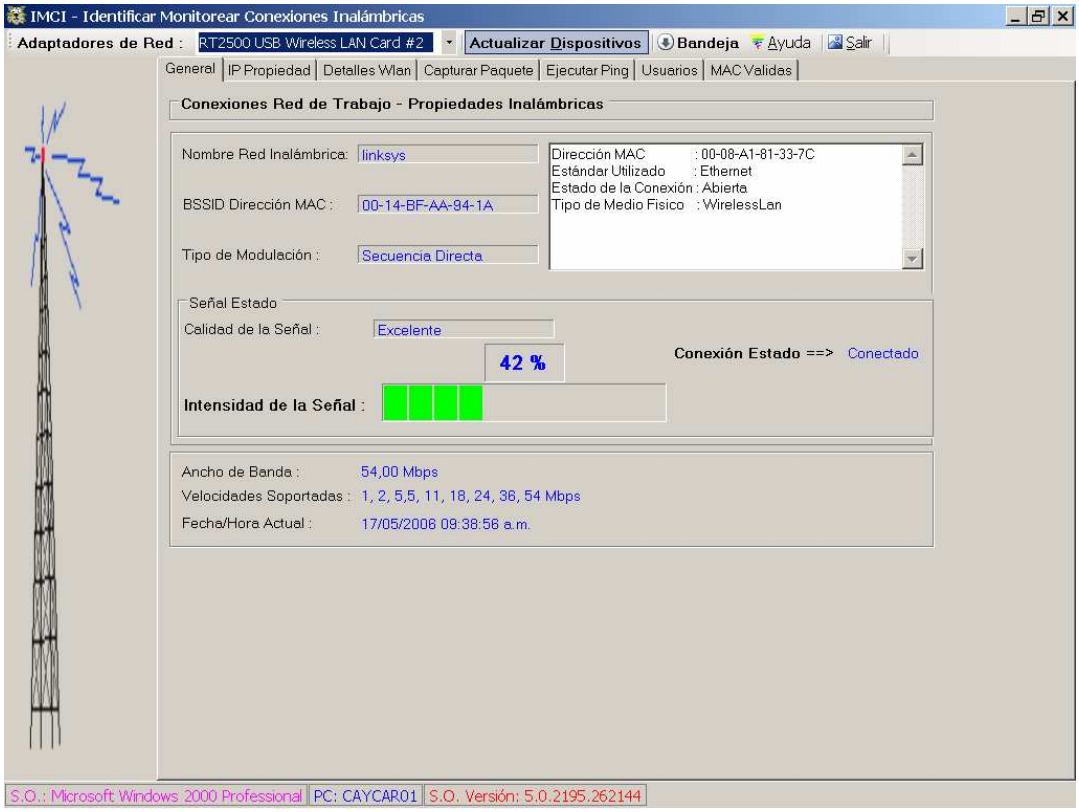

Figura 11. Pantalla de Inicio Correcto Ejecutado.

Fuente: El autor

- La opción IP Propiedad: Figura 12, presenta los detalles de la conexión de red, los cuales son la dirección MAC, nombre del adatador (en hexadecimal), descripción la cual es el nombre de la red, canal de adaptador activado, dirección IP del *host* local, submáscara de red y dirección broadcast.

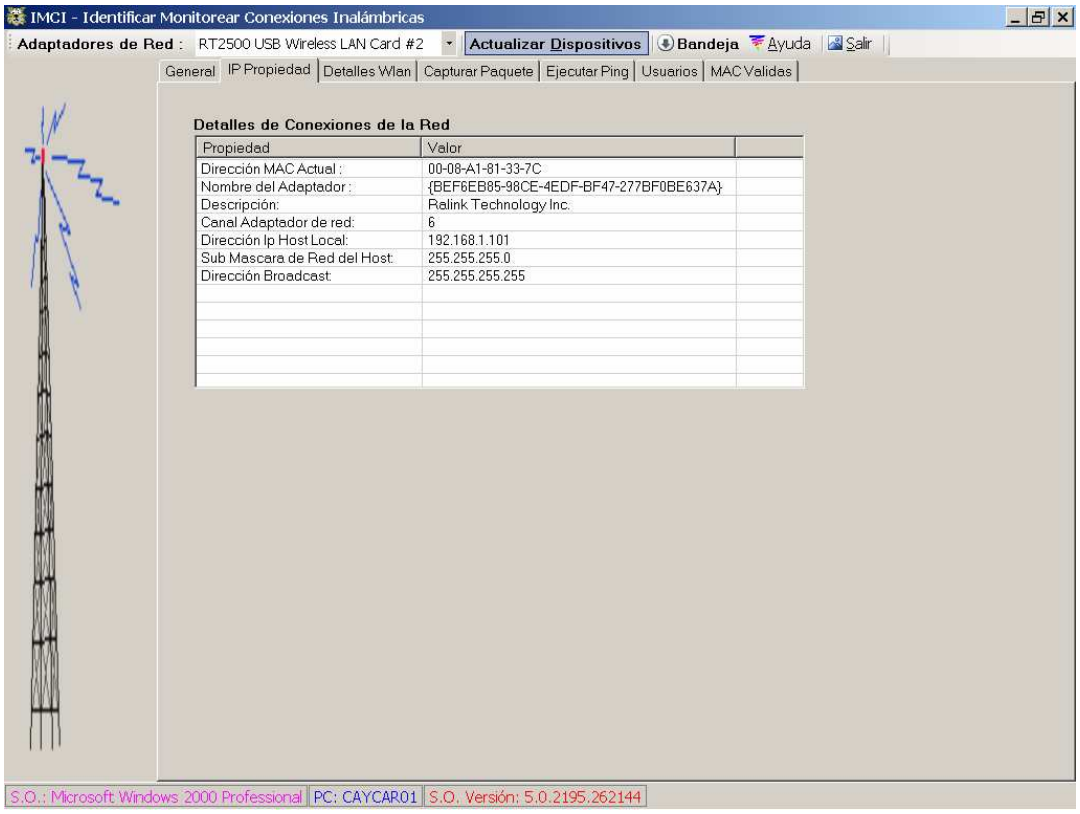

Figura 12. Pantalla de IP Propiedad.

Fuente: El autor

La opción Detalles Wlan: Figura 13, provee de la información descriptiva de cada uno de los componentes (AP, Routers y Estaciones) que se encuentren conectados a la WLAN. Cuando se hace la selección inicial de entrar al módulo se debe seleccionar el icono actualizar, el cual presenta en primera instancia la pantalla gráfica cargada anteriormente al haber iniciado el sistema por primera vez, pero

conteniendo todos los componentes activos más el *host* local, los cuales son representados por iconos gráficos dividiendo la pantalla en dos partes la superior muestra los componentes y la inferior las estaciones. Si se hace *click* sobre uno de estos iconos se presentará la información de la dirección IP, el nombre y la dirección MAC de ese componente. Los componentes conectados no autorizados cuyas direcciones MAC no se hayan almacenado como conexiones autorizadas, presentaran un icono en movimiento representando la conexión no autorizada. Al cerrar la pantalla gráfica haciendo *click* en el icono cerrar o presionando la tecla ESC, se cierra la pantalla gráfica y se presenta un cuadro que contiene la misma información de la pantalla anterior pero de manera escrita y detalla tal como se muestra en la figura 14.

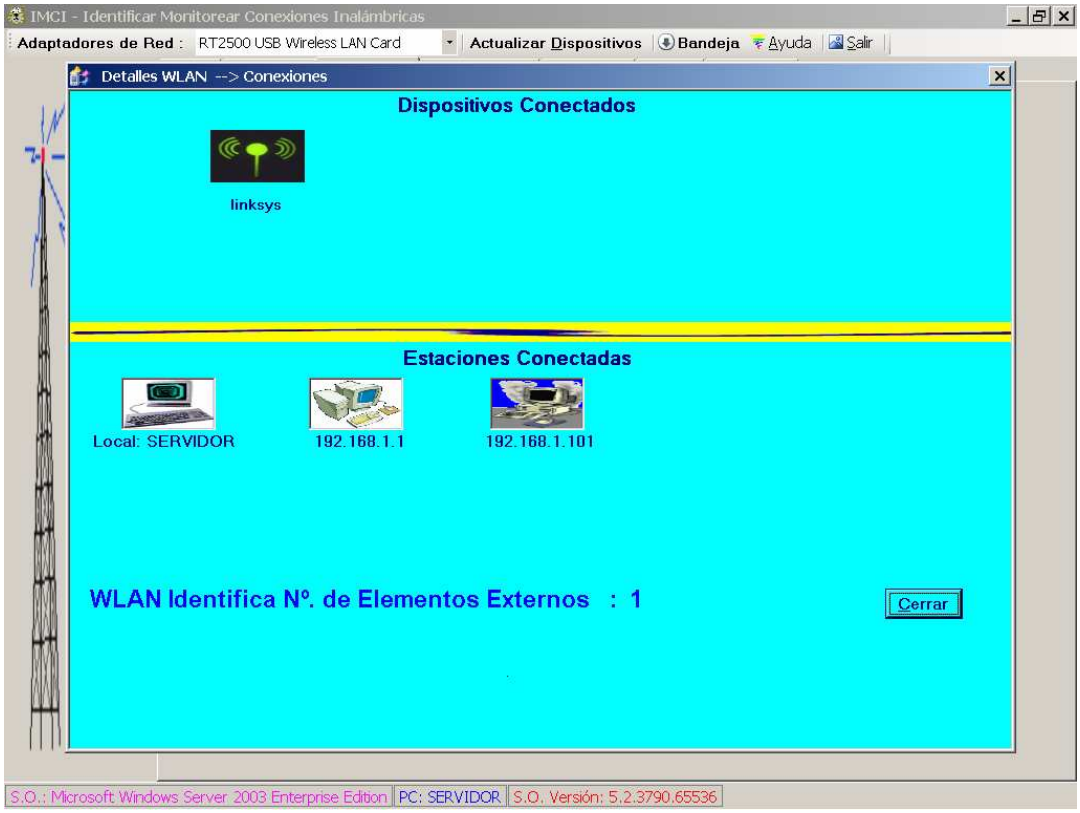

Figura 13. Pantalla Gráfica Detalles WLAN.

Fuente: El autor

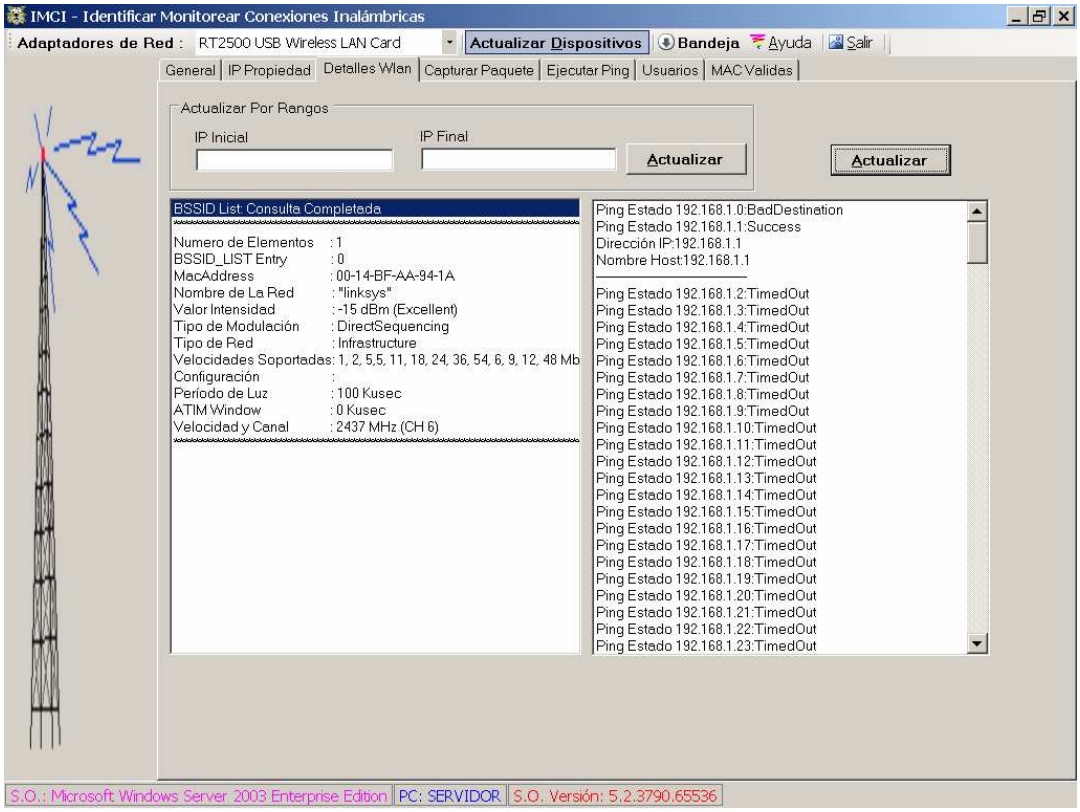

Figura 14. Pantalla Detalles WLAN.

Fuente: El autor

- La opción Capturar Paquete: Permite guardar y grabar en un archivo los paquetes que se transmiten entre los diferentes componentes de la WLAN. Se debe seleccionar la opción Iniciar Captura, para comenzar a ejecutar el análisis y grabación de paquetes. Al mismo tiempo se da inicio a una interfaz gráfica la cual indica que se está llevando a cabo la ejecución de esta opción. Después de cierto tiempo y cuando se hayan tratado de hacer la mayor cantidad de conexiones posibles se puede seleccionar la opción de Analizar Captura, la cual llenará todos los cuadros que se presentan en pantalla. Estos paquetes de presentar información relevante pueden ser guardados en un archivo de texto, el cual puede ser abierto con cualquier editor. Esta

transmisión y control de paquetes también permite que las direcciones MAC de cada uno de los dispositivos conectados a la red sean guardados y revisados, todo lo anteriormente descrito se muestra en la figura 15.

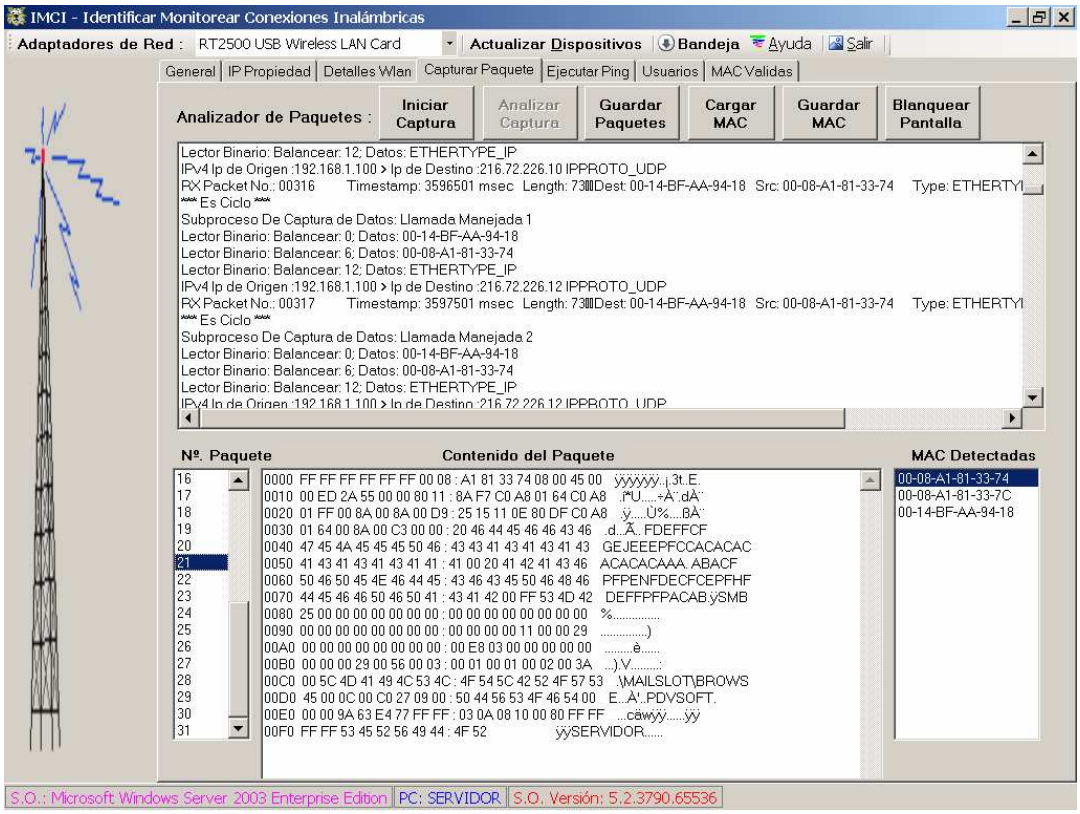

Figura 15. Pantalla Capturar Paquete.

Fuente: El autor

Opción Ejecutar Ping: Módulo que al ser seleccionado permite ejecutar la opción de hacer ping a la dirección individual que se necesite validar, mostrando los detalles de la ejecución de dicha opción para saber si fue exitosa o fallo, función mostrada en la figura 16.

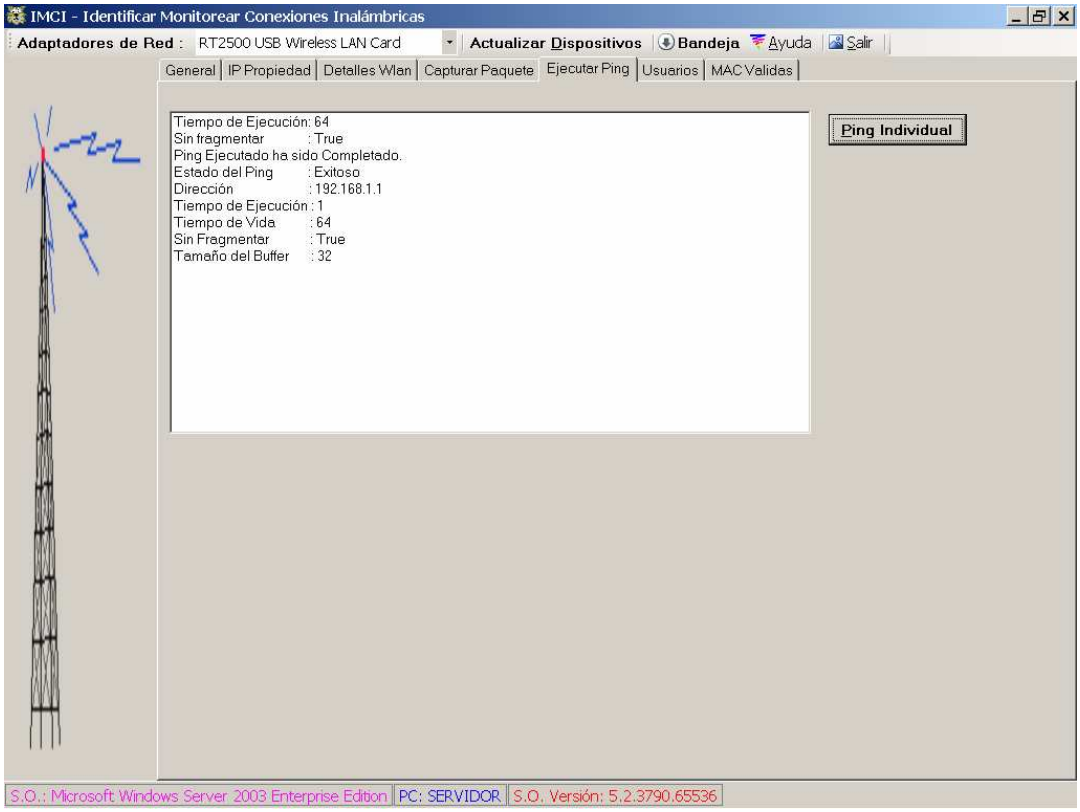

Figura 16. Pantalla Ejecutar Ping.

Fuente: El autor

La opción Usuarios: mostrada en la figura 17, permite manejar y controlar los usuarios que pueden hacer uso de la presente aplicación. Permite incluir, buscar, modificar y eliminar usuarios, los cuales son definidos en dos niveles: Usuario normal y Administrador, para limitar el uso de los módulos de manera ilimitada.

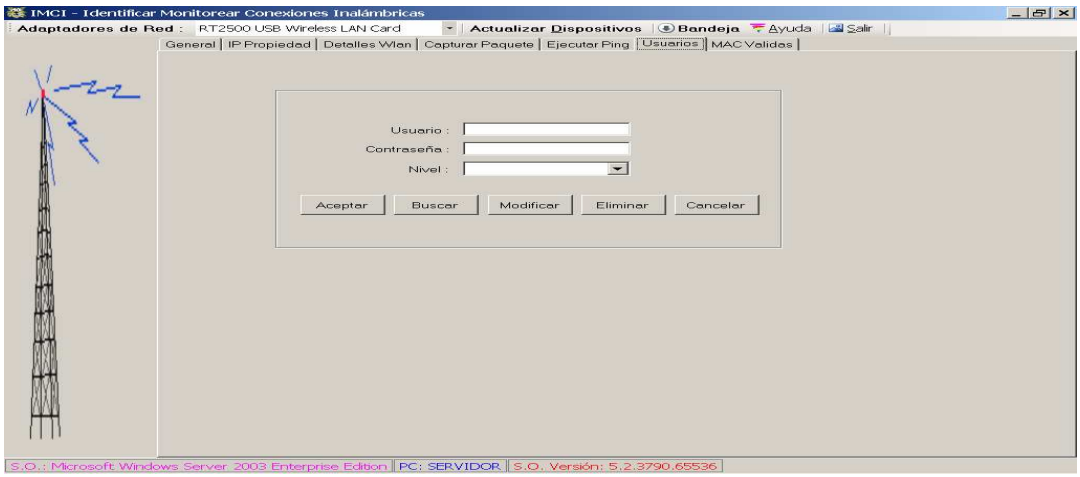

Figura 17. Pantalla Usuarios.

Fuente: El autor

La opción MAC Válidas: figura 18, permite grabar en un archivo tipo texto las direcciones MAC autorizadas de la WLAN.

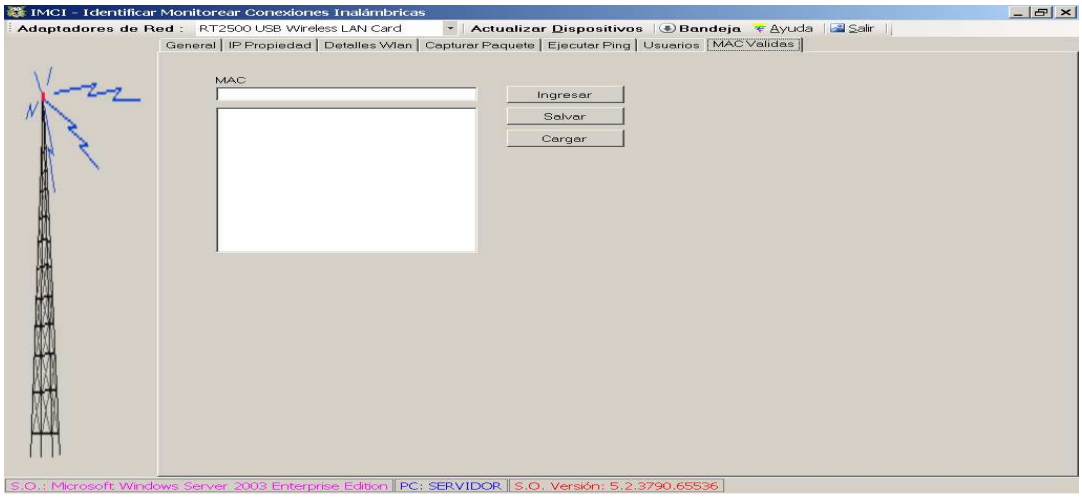

Figura 18. Pantalla MAC Validas.

Fuente: El autor

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Después de realizar el desarrollo de la aplicación que permite identificar y monitorear dispositivos inalámbricos basados en el estándar IEEE 802.11 se emiten las siguientes conclusiones que dan respuesta a las interrogantes planteadas:

- Al evaluar la aplicación generada se pudo determinar que no existen en el mercado local herramientas similares a la de este desarrollo, las cuales permitan capturar paquetes, capturar y grabar las direcciones MAC todo lo cual permite efectuar un mejor análisis, supervisar, identificar y monitorear estaciones y dispositivos inalámbricos que se encuentren conectados a la WLAN sin estar autorizados, todo lo antes expuesto basados en los estándares 802.11.

- Si existen parámetros en el estándar 802.11 que permiten detectar estaciones y dispositivos inalámbricos conectados a una WLAN, tales como la dirección MAC y el algoritmo de codificación denominado WEP (Wired Equivalent Privacy – Privacidad Equivalente a la Cableada), utilizados por la herramienta permanentemente.

- El parámetro para el cálculo de la distancia se debe revisar analizando otras de las fórmulas existentes las cuales también permiten determinar distancias, puesto que presenta variaciones permanentes en los resultados obtenidos.

- Si ha sido posible desarrollar esta herramienta utilizando componentes de software reutilizables los cuales han dado más facilidad en el manejo de la interfaz gráfica y de las conexiones inalámbricas. El componente utilizado ha sido el Visual Studio .Net 2005, la cual es una herramienta de última generación que provee muchas nuevas ventajas para el manejo, desarrollo y control de redes WLAN. Ventajas que anteriormente no existían en las herramientas de programación antiguas. Así mismo se pudo determinar el uso y manejo de librerías desarrolladas específicamente para la elaboración de herramientas similares, tales como NDIS, DDK, PCausa Rawether.

- El problema de la detección de intrusos queda resuelto con la presente aplicación y al realizar las pruebas de evaluación de la herramienta se ha determinado de forma muy técnica y amena que si presta apoyo al administrador de la red para que ejecute supervisión y monitoreo de redes WLAN.

- El hecho de lograr identificar y grabar las direcciones MAC de todos los dispositivos inalámbricos conectados a la WLAN, para el control y seguridad, la provee de un alto grado de funcionalidad en cualquier red inalámbrica donde pueda ser ejecutada esta herramienta.

Recomendaciones

Tomando en cuenta las conclusiones emitidas permiten plantear las siguientes recomendaciones:

- Desarrollar nuevas aplicaciones similares a la actual pero dando al desarrollador la sugerencia de utilizar las herramientas que se ejecutan en la presente aplicación, lo cual ahorrara una gran cantidad de tiempo, logrando que las aplicaciones cumplan con todos los requerimientos planteados.

- Hacer un análisis exhaustivo de cada uno de los grupos de clases y funciones que se manejan en las librerías del presente desarrollo.

- Realizar un profundo análisis del *software* de instalación y configuración de todos los componentes de hardware para *wíreles* de los cuales se tenga disposición.

- Sugerir proveer presente la información de cómo lograr este tipo de desarrollo a nivel de aula de clase para las nuevas cohortes.

- Las librerías en uso en el presente desarrollo bajo ambiente Windows se deben ir estudiando, evaluando e instalando para ser utilizadas en otros sistemas operativos.

- Sería importante sugerir a los desarrolladores de proyectos futuros que hagan una previa preparación en lenguaje C++, ya que es la herramienta que provee mejor uso de los parámetros a bajo nivel.

REFERENCIAS BIBLIOGRAFICAS

McNealy, 1969. Redes Wireless, MiC PAC 3 – Grup F.R.A.J. consulta: 30/12/2003 URL: http://biruji.org/wireless/cap1.shtml

O'Hara, 1999. IEEE 802.11 Handbook A Designer´s Companion. Bob O'Hara, Al Petrick, 1999. Editorial Standards Information Network IEEE Press.

Ciberhábitat, 2001. Tecnología Espectro, consulta 15/11/2005 URL: http://ciberhabitat.com.mx/museo/cerquita/textos/texto_ethernet.htm

Birenbaum Larry, 2002. Revista Ariadn@, Abril / 2002

Varea, 2004. Introducción Wlan. Redes WLAN 802.11, consulta 16/11/2005, URL: http://www.ilustrados.com/publicaciones/EpZFAAlZFpAqGQaqIx.php

Baradello, 2005. Carlos Baradello, Redes Wifi, 802.11 b/g/a, consulta 16/11/2005 URL: http://www.icamericas.net/Cases_Reports/Wi-FiBriefs/WiFi2_Spanish.pdf

Vélez, 2005. Sistemas digitales telecomunicaciones c/c++: WLAN 802.11, consulta 16/11/2005, URL: http://www1.ceit.es/Tesis/orden/electronica/electro31.htm

Mendoza, 2005. Implementación Sistema Captura Paquetes redes Inalámbricas, consulta 16/11/2005, URL: http://jupiter.utm.mx/~tesis_dig/9583.pdf

Luis Castro, Ubicación Móviles, consulta 18/11/2005 URL: http://usuario.cicese.mx/~quiroa/quiroa-thesis-final.pdf

Airfart, 2003. *Sniffer* de prueba, consulta 18/11/2005 URL: http://airfart.sourceforge.net/

Stumbler, 2005. *Sniffer* de prueba, consulta 16/08/2005 URL: http://www.stumbler.net/

CommView, 2005. *Sniffer* de prueba, consulta 18/09/2005 URL: http://www.tamos.com/products/commwifi/

Lycos, 2005. *Sniffer* de prueba, consulta 18/11/2005 URL: http://wlan.lycos.de/