



**UNIVERSIDAD AMERICANA DE ACAPULCO  
EXCELENCIA PARA EL DESARROLLO**

**FACULTAD DE INGENIERIA**

**INGENIERIA EN TELECOMUNICACIONES**

**INCORPORADA A LA**

**UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO  
CON CLAVE DE INCORPORACION: 8852 – 58**

**“PROPUESTA DE UNA RED INALÁMBRICA PARA UN  
CONJUNTO HABITACIONAL”**

**T E S I S**

**QUE PARA OBTENER EL TITULO DE:**

**INGENIERO EN TELECOMUNICACIONES**

**P R E S E N T A:**

**MANUEL GILES CALLEJA**

**DIRIGIDA POR:**

**ING. ALFREDO RICARDO ZARATE VALENCIA**

**2007**



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

## Agradecimientos

Esta tesis, si bien ha requerido de esfuerzo y mucha dedicación por parte del autor y su director de tesis, no hubiese sido posible su finalización sin la cooperación desinteresada de todas y cada una de las personas que a continuación citaré y muchas de las cuales han sido un soporte muy fuerte en momentos de angustia y desesperación.

Primero que nada, dar gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mis Padres, que estuvieron conmigo todo el tiempo, desde mi niñez hasta mi hombría, desde el preescolar hasta esta etapa de hoy que soy un profesionista y con orgullo comparto con ellos.

A mi Padre Félix Manuel Giles Loza que se esfuerza día con día trabajando y trayendo el dinero suficiente para mantener a la familia y así pagar un patrimonio y mi carrera profesional que por fin concluí.

A mi Madre que siempre estaba y aun lo hace apoyándome en estos momentos difíciles, todo acerca de superarme profesionalmente, siempre atrás de mí encaminándome por el camino del estudio para llegar a ser un profesionista y sus esfuerzos, deseos se realizan hoy al concluir esta tesis para hacerme un profesionista de bien.

A mi director, amigo y asesor de tesis el Ingeniero Alfredo Zarate Valencia, que gracias a su apoyo fue posible la finalización de esta tesis, ya que me guío por el camino de la investigación para hacer posible la elaboración de la misma.

A mi hermano que entre risas y travesuras siempre ha estado conmigo en todo momento importante en el paso del tiempo.

A mis profesores de la carrera, que estuvieron ahí aportando sus conocimientos para que nosotros que fuimos alumnos darnos una guía, apoyo y encaminarnos por el camino profesional para desempeñar un papel en la vida para que hoy día seamos profesionistas.

A mis padrinos Mr. Harry Leonard Singh & Mrs. Mercedes Olivera de Singh, que para darles las gracias se necesita un minuto, pero recordar sus amabilidades y apoyo serán recordados por mucho tiempo.

A mis amigos de la preparatoria, que desde aquellos días de bachillerato, cuando fuimos adolescentes, haciendo travesuras, paseos, aventuras y anécdotas siempre estuvimos juntos apoyándonos en cada momento de nuestras vidas de estudiantes y hoy en día lo seguimos haciendo, reuniéndonos cada temporada de vacaciones, días festivos, etcétera, contándonos como nos fue, que hemos logrado y hasta donde queremos llegar y desde entonces seguimos haciéndolo y espero que sea por mucho tiempo mas ya que el mundo da vueltas y nuestras vidas cambiaran de un momento a otro y no se sabe si seguiremos haciéndolo, pero esos momentos los llevaremos muy orgulloso y con mucho cariño con nosotros a donde quiera que estemos.

A mis compañeros de la carrera, que aunque no estuvimos siempre juntos, siempre estuvimos ahí apoyándonos en los estudios, proyectos y cosas que estuvieron a nuestro paso en nuestra época de estudiantes universitarios, espero y tengan éxito en sus vidas profesionales ya que fue un camino duro de bajas de compañeros y conforme íbamos avanzando se hacia mas duro el camino para seguir adelante y que con ahínco llegamos a la meta de terminar nuestra carrera.

# CONTENIDO

|   |    |
|---|----|
| <b>Introducción</b> .....                                   | 7  |
| <b>CAPITULO I</b>   |    |
| <b>INTRODUCCIÓN A LAS REDES INALÁMBRICAS</b> .....          | 13 |
| Redes Inalámbricas.....                                     | 13 |
| Descripción general de IEEE 802.11 .....                    | 13 |
| Protocolos.....   | 15 |
| • 802.11.....   | 15 |
| • 802.11b.....  | 15 |
| • 802.11 a.....   | 15 |
| • 802.11g.....  | 16 |
| • 802.11n.....  | 17 |
| • 802.11e.....  | 17 |
| Protocolo propietario .....                                 | 18 |
| • 802.11 Súper G .....                                      | 18 |
| Modo de infraestructura .....                               | 18 |
| Redes de Área Local (LAN) .....                             | 20 |
| Redes infrarroja.....                                       | 20 |
| Redes de Radio Frecuencia.....                              | 22 |
| WI – FI (Wireless Fidelity) Fidelidad Inalámbrica.....      | 23 |
| WLAN ( <i>Wireless Local Area Network</i> ) .....           | 24 |
| Origen de la WLAN .....                                     | 25 |
| Características de la WLAN .....                            | 26 |
| Principios de las redes WLAN.....                           | 26 |
| Configuraciones de red para radiofrecuencia .....           | 27 |
| Seguridad inalámbrica.....                                  | 30 |
| Cifrado .....   | 31 |
| WEP-WPA .....   | 31 |
| WEP (Wired Equivalent Privacy).....                         | 32 |
| Características del protocolo WEP .....                     | 32 |
| Problemas .....   | 33 |
| Solución del problema.....                                  | 33 |
| WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi).....  | 33 |
| WPA 2 .....   | 35 |
| Servidor .....  | 35 |
| Administrador de red de área local .....                    | 35 |
| Arquitectura Cliente – Servidor .....                       | 36 |
| Servidor de archivos .....                                  | 37 |
| SERVIDORES RADIUS (Remote Access Dial-In User Server) ..... | 37 |
| Protocolo 802.1x .....                                      | 40 |
| Funcionamiento de el Protocolo 802.1X .....                 | 41 |

|   |           |
|---|-----------|
| <b>CAPITULO II</b>  |           |
| <b>PLANEANDO LA RED INALÁMBRICA .....</b>                         | <b>43</b> |
| Introducción .....  | 43        |
| Escogiendo red cableada o inalámbrica .....                       | 43        |
| Escogiendo la tecnología inalámbrica .....                        | 44        |
| Factores que afectan fuerza de la señal .....                     | 47        |
| Interferencia RF .....  | 48        |
| Obstáculos de señal .....   | 48        |
| Tabla de atenuación relativa de obstáculos de RF .....            | 49        |
| Conectar a Internet .....   | 50        |
| Planeando la seguridad .....                                      | 52        |
| <br>  |           |
| <b>CAPITULO III</b>   |           |
| <b>INSTALACIÓN INALAMBRICA DEL PUNTO DE ACCESO (ACCESS POINT)</b> |           |
| .....   | 54        |
| Introducción .....  | 54        |
| Punto de acceso (Access point) .....                              | 54        |
| Preparando instalar el punto de acceso (AP) .....                 | 54        |
| Instalando el Punto de Acceso (AP) .....                          | 56        |
| Configurar los parámetros del AP .....                            | 59        |
| <br>  |           |
| <b>CAPITULO IV</b>  |           |
| <b>COMPARTIENDO LA CONEXIÓN DE INTERNET POR MEDIO DE NUESTRA</b>  |           |
| <b>RED INALÁMBRICA .....</b>                                      | <b>62</b> |
| Introducción .....  | 62        |
| Decidiendo como compartir el Internet .....                       | 62        |
| Compartiendo la conexión .....                                    | 63        |
| Routers y Puertas de enlace (Gateways) .....                      | 63        |
| Compartiendo conexión a Internet por marcado telefónico .....     | 65        |
| Obteniendo una dirección IP automáticamente .....                 | 66        |
| Configuración y compartir la conexión de Internet .....           | 68        |
| <br>  |           |
| <b>CAPITULO V</b>   |           |
| <b>SEGURIDAD EN LA RED INALÁMBRICA .....</b>                      | <b>72</b> |
| Introducción .....  | 72        |
| Asegurando la red inalámbrica .....                               | 73        |
| Longitud de la llave (WEP Key) .....                              | 73        |
| Librando los valores que están por default .....                  | 74        |
| Habilitando WEP .....   | 75        |
| Seguridad Radius .....  | 76        |

|   |            |
|---|------------|
| <b>CAPITULO VI</b>  |            |
| <b>CONFIGURANDO EL SERVIDOR .....</b>   | <b>79</b>  |
| Introducción .....  | 79         |
| ➤ Configuraciones   |            |
| 1.- Ejecutar el DCPROMO (convertir en un dominio independiente) .....                 | 79         |
| 2.- Instalar las utilerías (DHCP, DNS, IAS, IIS, CA, RRA) .....                       | 86         |
| 3.- Configurar DHCP .....   | 89         |
| 4.- Configurar Certificado Servidor y Cliente Certificado Servidor .....              | 96         |
| 5.- Configurar Access Point .....   | 117        |
| 6.- Configurando el Radius .....  | 119        |
| 7.- Configuración del de Servicio Activo (Active Directory Service) Windows 2003..... | 131        |
| 8.- Configurando Router y Acceso Remote (Routing and Remote Access) .....             | 131        |
| <b>CONCLUSIONES .....</b>   | <b>134</b> |
| <b>BIBLIOGRAFÍA .....</b>   | <b>136</b> |

## Titulo de Tesis

“Propuesta de un red inalámbrica para un conjunto habitacional”

Caso: conjunto habitacional la marquesa 2da etapa

## Planteamiento del problema

En la actualidad la tecnología ha avanzado conforme el tiempo, hoy en día mas y mas usuarios tienen la oportunidad de adquirir un equipo de computo ya sea un equipo fijo de escritorio como un equipo móvil y se adentran al mundo de Internet ya sea para diversión como para realizar una investigación como son los casos de empresarios, estudiantes u otro usuario que tenga su equipo y estos requieran de comodidad al no recurrir a la conexión clásica que se obtiene por medio de una línea telefónica y dejar libre la línea para su uso, además tener una velocidad de transmisión aceptable y fácil acceso a red.

El estudio que se planteara es el de implementar una red inalámbrica para el conjunto habitacional la marquesa 2da etapa, que se localiza en cayaco – puerto Márquez, llano largo, su propietario es GEO Guerrero S.A. de C.V.

El proyecto se resolverá mediante un estudio de campo para recaudar datos sobre el área de cobertura para así proporcionar y dar paso a la implementación del equipo y la tecnología necesaria para resolver el problema de la propuesta y así mismo proveer el servicio de Internet inalámbrico y dar paso siguiente para acceder a Internet con un ancho de banda aceptable y disfrutar de sus beneficios.

La problemática es que se quiere proveer un servicio de Internet que se lo suficientemente veloz, fácil acceso a la red, y sin la necesidad de estar conectado a una línea telefónica o utilizar cables de cualquier índole, se esta hablando mas que nada de una red inalámbrica que puede ser proveída a un conjunto habitacional ya mencionado anteriormente para así facilitar a los habitantes el libre acceso, trabajo, investigación y diversión en cualquier parte



del hogar o fuera de el como lo será todo el conjunto habitacional siempre y cuando el usuario este dentro de la cobertura estipulada.

## Objetivos

Diseñar, implementar y proveer el servicio de una red inalámbrica para un conjunto habitacional con velocidad de transmisión aceptable y fácil acceso.

Se realizara un estudio en el área para proveer un servicio de Internet inalámbrico para los habitantes, el cual será muy útil y no requiera de una línea telefónica para acceder a la red, esto conlleva a que todo usuario que este dentro del área de cobertura dispondrá de Internet inalámbrico para su equipo ya sea fijo o móvil en cualquier parte de su domicilio.

Los usuarios requieren cada vez de más movilidad y los que cuenten con un equipo de cómputo móvil se vuelven un candidato evidente y factible para una red inalámbrica. Esto permitirá al usuario moverse a distintas ubicaciones como lo es su sala, pasillos, habitaciones, el jardín o área de descanso del hogar siempre y cuando este en el área de cobertura y aún tener acceso a los datos en red.

Para lograrlo se estudiarán los estándares, protocolos y la tecnología suficiente, necesaria y que satisfaga los requerimientos principales para la implementación, el diseño y el servicio que proveerá al conjunto habitacional de acceder a la red. Estos requerimientos principales nos trataran de ayudar a resolver el problema.

La tecnología inalámbrica permitirá a los usuarios enviar y recibir datos en recintos cerrados y abiertos, es decir, en cualquier punto del alcance de una estación base inalámbrica.

## Hipótesis

Se podrá diseñar e implementar la tecnología inalámbrica para el conjunto habitacional, esto permitirá que trabajadores, empresarios, estudiantes u otros usuarios que estén dentro de la zona cobertura y que dispongan de un equipo de cómputo sin importar que sea fijo o móvil tengan la facilidad de acceder a la red a una velocidad de transmisión aceptable, que facilitara la operación en lugares donde la computadora no puede permanecer en un solo lugar.

Esto ofrece ventajas evidentes, ya que no será necesaria la instalación de cableado. La tecnología de transmisión por una red inalámbrica puede completar la operabilidad de trabajo para aquel usuario necesite de alta velocidad y confiabilidad, ya que la conectividad inalámbrica le permite mantener su productividad y conectarse durante sus desplazamientos. Al trabajar sin cables, rosetas de teléfono podrá acceder de forma segura, investigar en Internet o colaborar al instante con los miembros de su equipo si es el caso de que algún usuario sea empresario desde el despacho de casa. Y todo esto significa que el tiempo que pase desplazándose dejará de ser sinónimo de tiempo de inactividad.

## Justificación

La realización de la propuesta es factible ya que todo usuario puede adquirir un equipo y acceder a Internet para trabajo, investigación o diversión, ya sea estos casos, el usuario requiere de una conexión a Internet que no requiera el uso de cableado y tenga movilidad en cualquier punto, siempre y cuando este dentro del área de cobertura, el caso es que el usuario disponga aparte de no utilizar el cableado pueda disponer de una red y un servicio de Internet con una velocidad aceptable para cualquier uso que el usuario disponga, eso da paso a que el usuario pueda recibir o transmitir datos en poco tiempo ya que se le puede proporcionar un ancho de banda aceptable para su fin y propósito del usuario.

La disponibilidad de la tecnología inalámbrica y de las redes (LAN) inalámbricas puede ampliar la libertad del usuario que este en la red, se puede resolver distintos problemas asociados con redes de cableado físico.

La propuesta nos mostrara y que el estudio será factible y necesario ya que las redes inalámbricas de alta velocidad pueden proporcionar beneficios de conectividad y acceso a la red sin las restricciones de estar ligadas a una ubicación específica o conectadas por cables.

La conexión inalámbrica en el conjunto habitacional puede ampliar o reemplazar una infraestructura cableada dependiendo el tipo de conexión que este usando el usuario en su domicilio. Las redes inalámbricas son una alternativa importante para que todo usuario que este dentro del área de cobertura disponga de su conectividad a la red.

El acceder a Internet en los sitios que cuentan con esta facilidad y comodidad de una red inalámbrica como en lugares públicos ya sea el caso de aeropuertos, restaurantes y áreas comunes en donde se pueda contar con este servicio nos conlleva a que también puede disfrutar de esta comodidad y facilidad sin salir de su hogar, con esta propuesta se soluciona una problemática de acceso a la red que no tiene suficiente velocidad de transmisión, estar en un solo lugar específico, buscar un punto de red para acceder a Internet y sin pasar por alto el cableado.

En esta parte los fundamentos, motivaciones y razones para realizar esta propuesta es que hoy en día mas y mas personas se adentran a la red al menos realizar tareas sencillas como revisión de correo electrónico o estar en contacto con otro usuario por medio de la misma red, aquí lo principal es dar un servicio de movilidad, sin recurrir a líneas telefónicas y que el servicio que se brindara sea lo suficientemente veloz para la transmisión o recepción de información deseada por el usuario sin salir de su domicilio.

## Alcance

El alcance de la propuesta a realizar es una investigación y estudio del área en el conjunto habitacional para proveer un servicio de Internet inalámbrico.

Lo que se realizara será la implementación de esta tecnología inalámbrica para el conjunto habitacional, esto permitirá que trabajadores, empresarios, estudiantes u otros usuarios que estén dentro de la zona cobertura y que dispongan de un equipo de cómputo sin importar que sea fijo o móvil tengan la facilidad de acceder a la red a una velocidad de transmisión aceptable.

La propuesta ayudara a diseñar, implementar y proveer un servicio para acceder a la red sin la necesidad de utilizar cableado, fácil y comodidad de movimiento dentro del área de cobertura, que es este caso será un domicilio particular.

Lo que se pondrá en práctica será un estudio y recurrir a la tecnología que satisfaga, apoye y resuelva el problema planteado.

Para la recopilación de información con respecto a la propuesta es investigar en el conjunto habitacional por medio de encuestas, si les agradaría acceder a Internet sin la necesidad de ocupar su línea telefónica, o cables de cualquier índole.

Al hacer el estudio de encuestas se podría pasar a estudiar el área en el cual se situara la red inalámbrica.

La metodología que se requerirá para esta propuesta será el conocimiento de protocolos y estándares que se necesitan para el estudio de la propuesta a realizar.

Uno de los principales puntos es saber que tecnología se usara para la ayuda de este problema a resolver. La tecnología requerida para el estudio de la

investigación para hacer pruebas es la que llene los requisitos, satisfaga y resuelva la problemática.

Para empezar a recaudar datos, la tecnología requerida es por lo pronto una conexión a Internet, un hub o switch que conmute los datos de nuestra red fija, puntos de acceso (Access point) que se encargaran de dar cobertura de radio a los usuarios y que se podrán conectar al switch, y tarjetas adaptadoras para los equipos fijos así como los móviles que hoy en día no requieren estos adaptadores, todo equipo que se vaya a conectar a la red. Si se requiere de un área de cobertura muy grande se requerirá de mas puntos de acceso (Access points) para cubrir mas el área deseada y así no perder la conectividad.

Al recaudar datos de cobertura es ahí cuando tiene inicio la propuesta del proyecto, que a plan futuro todo habitante del conjunto habitacional pueda obtener un servicio de Internet inalámbrico el cual le permitirá realizar trabajos, investigaciones, transmisión o recepción de información, diversión, etcétera a una velocidad aceptable para su fin.

La propuesta dará un alcance y nos mostrara que el estudio será factible y necesario ya que las redes inalámbricas de alta velocidad pueden proporcionar beneficios de conectividad y acceso a la red sin las restricciones de estar ligadas a una ubicación específica o conectada por cables.

La tecnología de transmisión por una red inalámbrica puede completar la operabilidad de trabajo para aquel usuario necesite de alta velocidad y confiabilidad.

Hasta donde se llegara será de proveer un servicio y una innovación a la comunidad para que todo aquel futuro usuario que disponga de un equipo de computo y permanezca dentro del área de cobertura podrá disponer de acceder a la red y realizar operaciones que el disponga con un ancho de banda y una velocidad proporcional que no ofrecen las conexiones a Internet comunes.

# CAPITULO I

## INTRODUCCIÓN

### **Redes Inalámbricas**

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica.

La utilidad de las redes inalámbricas en el hogar y las pequeñas empresas ofrece ventajas evidentes. Con una red inalámbrica no es necesario instalar cables para conectar los distintos equipos entre sí y los equipos portátiles pueden trasladarse de un lado a otro de la casa o la pequeña oficina y mantener su conexión a la red.

Aunque existen varias tecnologías para crear redes inalámbricas, se describirá el uso de los estándares 802.11 del IEEE (Instituto de ingenieros eléctricos y electrónicos).

### **Descripción general de IEEE 802.11**

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

IEEE 802.11 constituye un conjunto de estándares del sector para tecnologías de red de área local inalámbrica (WLAN) compartidas, de los cuales el que se utiliza con mayor frecuencia es IEEE 802.11b, también denominado Wi-Fi. IEEE 802.11b transmite datos a 1, 2, 5,5 u 11 mega bits por segundo (Mbps) en el intervalo de frecuencias ISM (industrial, científico y médico) de banda S es de 2,4 a 2,5 giga hercios (GHz). Otros dispositivos inalámbricos, como teléfonos inalámbricos, videocámaras inalámbricas y dispositivos que utilizan otra tecnología inalámbrica denominada Bluetooth, también utilizan ISM de banda S.

En condiciones ideales, en situación de proximidad y sin fuentes de atenuación o interferencias, IEEE 802.11b funciona a 11 Mbps, una tasa de bits mayor que Ethernet con cables a 10 Mbps. En condiciones no tan ideales, se utilizan velocidades inferiores de 5,5 Mbps, 2 Mbps y 1 Mbps.

El estándar IEEE 802.11a tiene una tasa de bits máxima de 54 Mbps y utiliza frecuencias del intervalo de 5 GHz, incluida la banda de frecuencias ISM de banda C de 5,725 a 5,875 GHz. Esta tecnología de velocidad mayor permite que las redes locales inalámbricas tengan un mejor rendimiento para aplicaciones de vídeo y de conferencia. Debido a que no se encuentra en las mismas frecuencias que Bluetooth o los hornos microondas, IEEE 802.11a proporciona una mayor tasa de datos y una señal más nítida.

El estándar IEEE 802.11g tiene una tasa de bits máxima de 54 Mbps y utiliza ISM de banda S. Todas las instrucciones de este artículo para configurar los nodos inalámbricos se aplican a las redes inalámbricas basadas en IEEE 802.11b, 802.11a y 802.11g.

## Protocolos

### 802.11

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 mega bits por segundo (Mbits/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

### 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

### 802.11a

En 1997 la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) crea el Estándar 802.11 con velocidades de transmisión de 2Mbps. En 1999, el IEEE aprobó ambos estándares: el 802.11a y el 802.11b. En 2001 hizo su aparición en el mercado los productos del estándar 802.11a.



La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s.

La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede ínter operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2.4 Ghz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

Transmisión Exteriores Valor Máximo A 30 metros 54 Mbps Valor Mínimo A 300 metros 6 Mbps Interiores Valor Máximo A 12 metros 54 Mbps Valor Mínimo A 90 metros 6 Mbps

### **802.11g**

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño

del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias hasta medio vatio, que permite hacer comunicaciones de hasta 50 Km. con antenas parabólicas apropiadas.

### **802.11n**

En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. la velocidad real de transmisión podría llegar a los 500 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b.

También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que no es hasta principios de 2007 que no se acabe el segundo boceto.

No obstante ya hay dispositivos que se han adelantado al protocolo y ofrecen de forma no oficial éste estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo esté implantado)

### **802.11e**

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS)

proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access y
- (HCCA) Controlled Channel Access.

## **Protocolo propietario**

### **802.11 Súper G**

Hoy en día el estándar 802.11 Súper G, con una banda de 2.4 Ghz y 5 Ghz, con una velocidad de transferencia de 108 Mbps.

## **Modo de infraestructura**

Los estándares IEEE 802.11 especifican dos modos de funcionamiento: infraestructura y ad hoc.

El modo de infraestructura se utiliza para conectar equipos con adaptadores de red inalámbricos, también denominados clientes inalámbricos, a una red con cables existente. Por ejemplo, una oficina doméstica o de pequeña empresa puede tener una red Ethernet existente. Con el modo de infraestructura, los equipos portátiles u otros equipos de escritorio que no dispongan de una conexión con cables Ethernet pueden conectarse de forma eficaz a la red existente. Se utiliza un nodo de red, denominado punto de acceso inalámbrico (PA), como puente entre las redes con cables e inalámbricas. En la siguiente figura se muestra una red inalámbrica en modo de infraestructura.

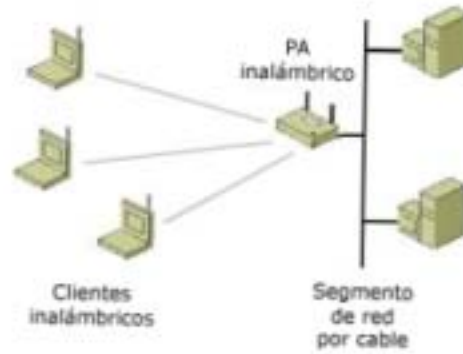


Figura 1.1 Red inalámbrica en modo de infraestructura

En el modo de infraestructura, los datos enviados entre un cliente inalámbrico y otros clientes inalámbricos y los nodos del segmento de la red con cables se envían primero al punto de acceso inalámbrico, que reenvía los datos al destino adecuado.

Modo ad hoc

El modo ad hoc se utiliza para conectar clientes inalámbricos directamente entre sí, sin necesidad de un punto de acceso inalámbrico o una conexión a una red con cables existente. Una red ad hoc consta de un máximo de 9 clientes inalámbricos, que se envían los datos directamente entre sí. En la siguiente figura se muestra una red inalámbrica en modo ad hoc.



Figura 1.2 Red inalámbrica en modo ad hoc

## **Redes de Área Local (LAN).**

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

## **Redes Infrarroja**

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

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

El mismo principio se usa para la comunicación de Redes, se utiliza un "*transreceptor*" que envía un haz de Luz Infrarroja, hacia otro que la recibe. La transmisión de luz se codifica y decodifica en el envío y recepción en un

protocolo de red existente. Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un "Transreceptor Infrarrojo".

Los primeros transreceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transreceptor recibía la señal. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transreceptor.

La siguiente figura muestra un transreceptor. En la actualidad Photonics ha desarrollado una versión AppleTalk/LocalTalk del transreceptor que opera a 230 Kbps. El sistema tiene un rango de 200 mts. Además la tecnología se ha mejorado utilizando un transreceptor que difunde el haz en todo el cuarto y es recogido mediante otros transreceptores. El grupo de trabajo de Red Inalámbrica IEEE 802.11 está trabajando en una capa estándar MAC para Redes Infrarrojas.

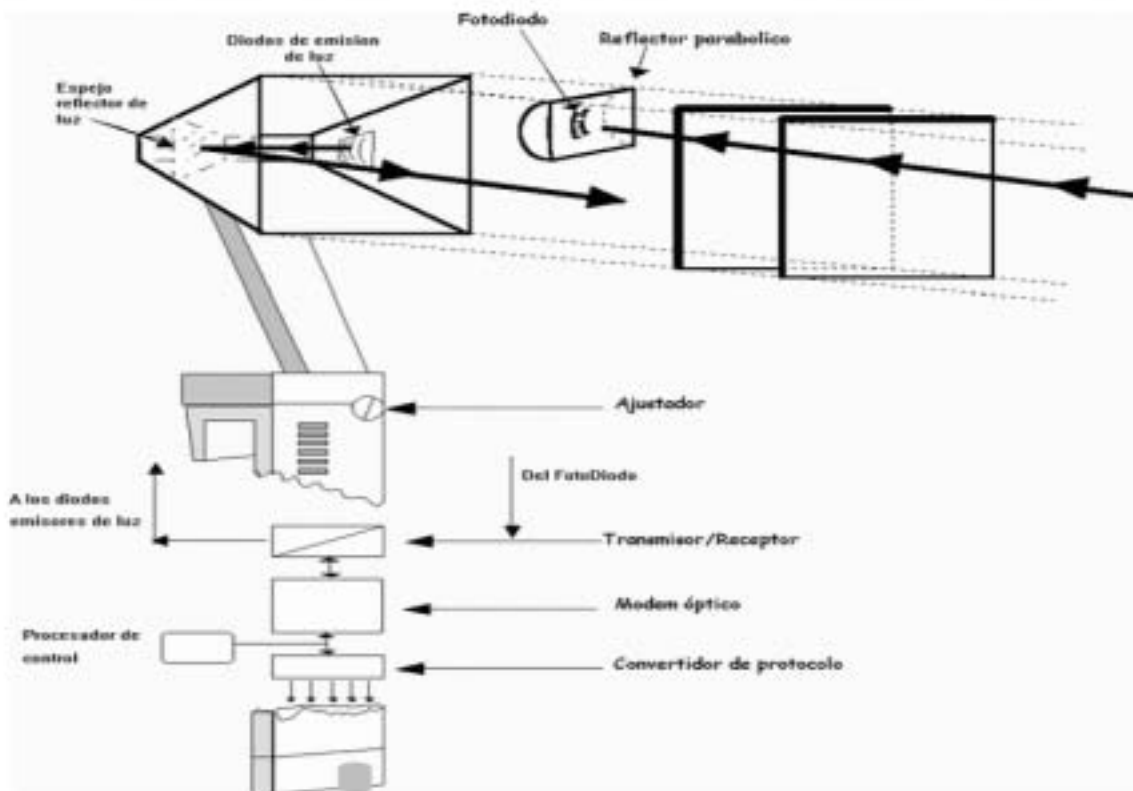


Figura 1.3 Transreceptor

## Redes de Radio Frecuencia

Por el otro lado para las Redes Inalámbricas de Radiofrecuencia, la FCC permitió la operación sin licencia de dispositivos que utilizan 1 Watt de energía o menos, en tres bandas de frecuencia: 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 Mhz. Estas bandas de frecuencia, llamadas bandas ISM, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales.

Esta banda, a diferencia de la ARDIS y MOBITEX, está abierta para cualquiera. Para minimizar la interferencia, las regulaciones de FCC estipulan que una técnica de señal de transmisión llamada *spread-spectrum modulation*, la cual tiene potencia de transmisión máxima de 1 Watt. Deberá ser utilizada en la banda ISM.

Esta técnica ha sido utilizada en aplicaciones militares. La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia.

Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente:

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

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

### **WI – FI (*Wireless Fidelity*)**

La expresión Wi-Fi (*Wireless Fidelity*) se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, *Wireless Local Área Networks*).

En un principio, la expresión Wi-Fi era utilizada únicamente para los aparatos con tecnología 802.11b, el estándar dominante en el desarrollo de las redes inalámbricas, de aceptación prácticamente universal, que funciona en una banda de frecuencias de 2,4 GHz y permite la transmisión de datos a una velocidad de hasta 11Mbps (aunque la velocidad real de transmisión depende en última instancia del número de usuarios conectados a un punto de acceso).

Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término Wi-Fi se extendió a todos los aparatos provistos con tecnología 802.11 (802.11a, 802.11b, 802.11g, 802.11i, 802.11h, 802.11e, con diferentes frecuencias y velocidades de transmisión).

Wi - Fi es todavía una tecnología novedosa y que han empezado a utilizar, en hogares o empresas, sólo los pioneros tecnológicos (*early-adopters*). Antes de



consolidarse definitivamente, deberá resolver una serie de incógnitas que penden en la actualidad sobre su viabilidad:

- ❖ **Seguridad:** una de las mayores tareas pendientes, a la espera de estándares que garanticen la seguridad de las transmisiones inalámbricas.
- ❖ **Provecho:** mejorar la experiencia del usuario final, incidir en las ventajas o aplicaciones para éste, conseguir en definitiva que la tecnología se convierta en una *commodity*.
- ❖ **Flexibilidad:** dado el gran número de aplicaciones y tecnologías emergentes, el usuario final debe contar con la posibilidad de actualizar ambas, de modo que pueda planear a medio y largo plazo, más que limitarse a las necesidades inmediatas.
- ❖ **Educación:** actualmente, la Wi-Fi Alliance ejerce el papel de principal difusor de las tecnologías inalámbricas y valedor de sus ventajas. A medida que el mercado crezca y se segmente, así como las necesidades particulares del usuario final, otros agentes deberán hacerse cargo de este papel o colaborar en la tarea.

### **WLAN** (*Wireless Local Area Network*)

**WLAN** (*Wireless Local Area Network*) es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufacturación, en los que se transmite la información en tiempo real a una Terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

## Origen de la WLAN

En 1990 se formó en Estados Unidos el grupo de trabajo IEEE 802.11 para el estudio y desarrollo de estándares de redes WLAN. Su principal tarea fue el desarrollo de un estándar mundial para equipos y redes inalámbricas que trabajasen en la banda de frecuencias ISM (Industry, Science and Medicine), alrededor de 2,4 GHz y con tasas de transmisión de 1 a 2 Mbit/s. En cierto modo, con este estándar se pretendía unificar el mercado WLAN, bastante confuso y repleto de soluciones propietarias. La especificación original permitía tres tipos diferentes de técnicas de transmisión: espectro ensanchado por secuencia directa (DSSS), espectro ensanchado por salto de frecuencia (FHSS), e infrarrojos, si bien el mayor desarrollo se ha realizado para DSSS.

El estándar IEEE 802.11 fue adoptado finalmente en 1997. Todos los equipos que implementan esta tecnología (tarjetas de red, puntos de acceso, etc.) se basan en una estructura de capas de acuerdo con el modelo de referencia OSI. La primera capa es el medio de transmisión o nivel físico. Por otro lado, la siguiente capa (nivel de enlace) define el control de acceso al medio (MAC) y el control de enlace lógico (LLC). Este último está definido por el estándar IEEE 802.2, por lo que para las capas superiores una red 802.11 es equivalente a una red Ethernet, facilitándose de este modo la interconexión entre redes heterogéneas basadas en distintos estándares del IEEE. Las tasas de transmisión que permite el estándar IEEE 802.11 son de 1 y 2 Mbit/s. El esquema de modulación propuesto para velocidades de 1 Mbit/s es BPSK, mientras que para 2 Mbit/s es QPSK. Sin embargo, estas velocidades significativamente inferiores a las de las redes de área local cableadas (10 y 100 Mbit/s) redujeron inicialmente el interés por estos sistemas.

## Características de la WLAN

- ❖ **Movilidad:** permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.
- ❖ **Facilidad de instalación:** al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la habitabilidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.
- ❖ **Flexibilidad:** puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas.

## Principios de las redes WLAN

### Cómo trabajan



Figura 1.4 Punto de Acceso WiFi

Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado.

El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena.

La naturaleza de la conexión sin cable es transparente a la capa del cliente.

### **Configuraciones de red para radiofrecuencia**

Pueden ser de muy diversos tipos y tan simples o complejas como sea necesario. La más básica se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual (peer to peer). Cada cliente tendría únicamente acceso a los recursos del otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.

Instalando un Punto de Acceso se puede doblar la distancia a la cuál los dispositivos pueden comunicarse, ya que estos actúan como repetidores. Desde que el punto de acceso se conecta a la red cableada cualquier cliente tiene acceso a los recursos del servidor y además gestionan el tráfico de la red entre los terminales más próximos. Cada punto de acceso puede servir a varias máquinas, según el tipo y el número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con un rango de 15 a 50 dispositivos cliente con un solo punto de acceso.

Los puntos de acceso tienen un alcance finito, del orden de 150 m en lugares cerrados y 300 m en zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso, esto es llamado roaming.

Para resolver problemas particulares de topologías, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso. Los puntos de extensión funcionan como su nombre indica: extienden el alcance de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un puente entre ambos.

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: si se quiere una Lan sin cable a otro edificio a 1 km de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cuál permite una conexión sin cable en esta aplicación.

Las redes de área local inalámbricas (WLANs) constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones inalámbricas de banda ancha. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado.

Las redes WLAN fueron diseñadas para el ámbito empresarial. Sin embargo, en la actualidad han encontrado una gran variedad de escenarios de aplicación, tanto públicos como privados: entornos residenciales y del hogar, grandes redes corporativas, PYMES, zonas industriales, campus universitarios, entornos hospitalarios, ciber-cafés, hoteles, aeropuertos, medios públicos de transporte, entornos rurales, etc. Incluso son ya varias las ciudades en donde se han instalado redes inalámbricas libres para acceso a Internet.

Básicamente, una red WLAN permite reemplazar por conexiones inalámbricas los cables que conectan a la red los PCS, portátiles u otro tipo de dispositivos, dotando a los usuarios de movilidad.

Un esquema típico de WLAN se muestra en la figura siguiente, donde se puede observar la existencia de diferentes zonas de cobertura alrededor de cada uno de los puntos de acceso, los cuales se encuentran interconectados entre sí y con otros dispositivos o servidores de la red cableada. Entre los componentes que permiten configurar una WLAN se pueden mencionar los siguientes: terminales de usuario o Clientes (dotados de una tarjeta interfaz de red que integra un transceptor de radiofrecuencia y una antena), puntos de acceso y controladores de puntos de acceso, que incorporan funciones de seguridad, como autorización y autenticación de usuarios, firewall, etc.

El futuro de la tecnología WLAN pasa necesariamente por la resolución de cuestiones muy importantes sobre seguridad e interoperabilidad, en donde se centran actualmente la mayor parte de los esfuerzos. Sin embargo, desde el punto de vista de los usuarios, también es importante reducir la actual confusión motivada por la gran variedad de estándares existentes.

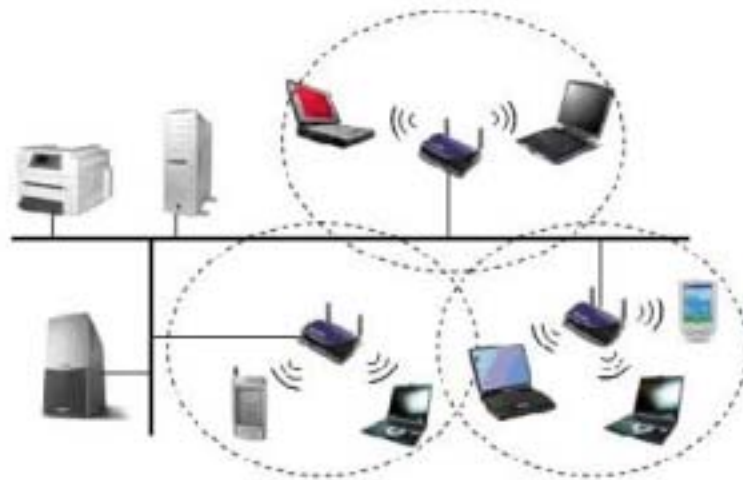


Figura 1.5 Arquitectura básica de una red WLAN

## Seguridad inalámbrica

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad, ya que cualquier persona con una Terminal inalámbrica podría comunicarse con un punto de acceso privado si no se disponen de las medidas de seguridad adecuadas. Un muy elevado porcentaje de redes son instaladas por administradores de sistemas y redes por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de seguridad de datos específicos para los protocolos Wi-Fi como el cifrado WEP y WPA que se encargan de autenticación, integridad y confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) y el conjunto de protocolos IEEE 802.1X, proporcionados por otros dispositivos de la red de datos y de reconocida eficacia a lo largo de años de experiencia.

Actualmente existe el protocolo de seguridad llamado WPA2, que es una mejora relativa a WPA, es el mejor protocolo de seguridad para Wi-Fi en este

momento. Para su utilización en PCS con Windows XP se requiere el Service Pack 2 y una actualización adicional.

La seguridad de IEEE 802.11 consta de cifrado y de autenticación. El cifrado se utiliza para cifrar o codificar, los datos de las tramas inalámbricas antes de que se envíen a la red inalámbrica. Con la autenticación se requiere que los clientes inalámbricos se autenticquen antes de que se les permita unirse a la red inalámbrica.

## **Cifrado**

Están disponibles los siguientes tipos de cifrado para su uso con las redes 802.11:

- WEP
  
- WAP
  
- WAP 2

## **WEP – WPA**

WEP (privacidad equivalente por cable) se definió como parte del estándar de red inalámbrica 802.11 del instituto Institute for Electrical Engineers (IEEE) de 1999 para proporcionar un nivel de protección equivalente a un sistema con cables. WEP básica (o estática) proporciona codificación y control de acceso para el tráfico inalámbrico en función de una clave precompartida. Se ha demostrado que WEP adolece de varias vulnerabilidades que pueden permitir que un atacante eluda este control de seguridad 802.11 nativo.

El sector de WLAN ha respondido a las vulnerabilidades de WEP mediante la oferta de una solución de seguridad más robusta denominada WPA. WPA incrementa el nivel de protección de datos y el control de acceso de los sistemas WLAM mediante una especificación de seguridad basada en



estándares e interoperabilidad. WPA es un subconjunto inicial del estándar 802.11i y se prevé que mantenga la compatibilidad en el futuro. Actualmente está previsto que 802.11i se publique como WPA 2.0.

WPA proporciona un mayor nivel de seguridad que WEP dinámica, esta última todavía constituye una solución viable hasta que todo el hardware se pueda actualizar para ser compatible con WPA.

### **WEP (Wired Equivalent Privacy)**

WEP (Wired Equivalent Privacy – Privacia Equivalente por Cableado) es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de inicialización *IV*), de 128 bits (104 bits más 24 bits del *IV*).

### **Características del protocolo WEP**

El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

El cifrado RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla o "seed" para generar una secuencia de números pseudos aleatorios de mayor tamaño. Esta secuencia de números pseudos aleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar el mismo seed para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes.

Para evitar esto, WEP especifica un vector de inicialización (*IV*) de 24 bits que se modifica regularmente y se concatena (encadenan) a la contraseña (a través de esta concatenación se genera el seed que sirve de entrada al algoritmo

RC4) para evitar secuencias iguales; de esta manera se crean seeds nuevos cada vez que varía.

## **Problemas**

El principal problema con la implementación del algoritmo anteriormente descrito es el tamaño de los vectores de inicialización. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso (AP Access Point) es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de inicialización, y por lo tanto sea fácil hacerse con la clave. Por lo tanto es inseguro debido a su implementación.

WEP es fácil de configurar y cualquier sistema que cuente con el estándar 802.11 lo aceptara y podrá soportarlo, no se puede decir que ocurra lo mismo con el cifrado WPA; por ejemplo con WPA, muchas máquinas hardware utilizan WPA y por ello el hardware más moderno pasará a utilizar el nivel de seguridad del anterior hardware para poder interactuar con él.

## **Solución del Problema**

Hoy en día hay sistemas de cifrado mucho mejor para redes WiFi, como el WPA o WPA2, surgidos para solucionar los problemas de seguridad que son mencionados del WEP.

## **WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi)**

*WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi)* es un sistema para proteger las redes inalámbricas Wi-Fi; creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente por Cableado). Se han encontrado varias debilidades en el cifrado WEP como la reutilización del vector de inicialización (IV).

WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

WPA fue diseñado para utilizar un servidor de autenticación, normalmente un servidor RADIUS, que distribuye claves diferentes a cada usuario a través del protocolo 802.1x; sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK - Pre-Shared Key) para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece, con una clave de 128 bits y un vector de inicialización de 48 bits.

Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado.

Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

WPA también mejora la integridad de la información cifrada. El chequeo de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - *Message Integrity Code*). WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

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

## **WPA2**

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

El estándar 802.11i fue ratificado en Junio de 2004. La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

## **Servidor**

Servidor es una computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos. Internet es en último término un conjunto de servidores que proporcionan servicios de transferencia de ficheros, correo electrónico o páginas WEB, entre otros. En ocasiones se utiliza el término servidor para referirse al *software* que permite que se pueda compartir la información.

## **Administrador de red de área local**

Es la persona encargada del diseño o mantenimiento de una red de área local. Entre sus funciones están dar permisos de utilización de los recursos a los distintos usuarios, instalar nuevas aplicaciones o nuevas versiones de las que están instaladas y gestionar el almacenamiento y las copias de seguridad de los datos. También comparte esta denominación un software que permite interconectar computadoras que trabajan con diversos sistemas operativos en un entorno de red, y autoriza a los usuarios a compartir archivos y recursos del sistema, por ejemplo discos duros e impresoras. Asimismo, ofrece la posibilidad de ejecutar aplicaciones distribuidas usando arquitecturas cliente/servidor.

## **Arquitectura Cliente – Servidor**

Arquitectura hardware y software adecuada para el proceso distribuido, en el que la comunicación se establece de uno a varios. Un proceso es un programa en ejecución. Proceso cliente es el que solicita un servicio. Proceso servidor es el capaz de proporcionar un servicio. Un proceso cliente se puede comunicar con varios procesos servidores y un servidor se puede comunicar con varios clientes.

Los procesos pueden ejecutarse en la misma máquina o en distintas máquinas comunicadas a través de una red. Por lo general, la parte de la aplicación correspondiente al cliente se optimiza para la interacción con el usuario, ejecutándose en su propia máquina, a la que se denomina Terminal o cliente, mientras que la parte correspondiente al servidor proporciona la funcionalidad multiusuario centralizada y se ejecuta en una máquina remota, denominada de forma abreviada, simplemente, servidor.

Los servidores hardware tienen fundamentalmente dos funciones, bien “servidores de aplicaciones”, que alojan distintos tipos de programas que pueden llamarse desde y ejecutarse en los terminales, bien “servidores de bases de datos”, que alojan archivos con datos que pueden ser consultados y/o editados y modificados en las máquinas terminales o clientes; también pueden ser servidores de ambos tipos simultáneamente.

Si se trata de una red de área local, la interconexión entre el o los servidores y los clientes es directa, mediante un sistema de cable o red inalámbrica; si es una red corporativa distribuida o a través de Internet, la interconexión es indirecta, y la alternativa más común es mediante un módem y vía telefónica. Una aplicación cliente/servidor típica es un servidor de base de datos al que varios usuarios realizan consultas simultáneamente.

El proceso cliente realiza una consulta, el proceso servidor le envía las tablas resultantes de la consulta y el proceso cliente las interpreta y muestra el

resultado en pantalla. Los sistemas distribuidos pueden consistir en diversos servidores que alojen datos, de forma que el cliente no tiene por qué conocer exactamente dónde se encuentran, simplemente hace una petición de servicio, y es el sistema servidor el encargado de localizarlos y proporcionar el resultado de la consulta al usuario que hizo la petición.

### **Servidor de archivos**

Es un dispositivo de almacenamiento de archivos en una red de área local, o en Internet, al que los distintos usuarios de la red pueden acceder, en función de los privilegios que les hayan sido dados por parte del administrador.

A diferencia de un servidor de disco, que aparece ante el usuario como una unidad de disco remota, un servidor de archivos es un dispositivo más complejo que no sólo almacena archivos sino que también los administra y los mantiene en orden a medida que los usuarios de la red los solicitan y los modifican. Para gestionar las tareas de manejo de varias solicitudes y a veces simultáneas, un servidor de archivos cuenta con un procesador y software de control, así como una unidad de disco para el almacenamiento.

Un servidor de archivos suele ser un ordenador o computadora de altas prestaciones, con gran capacidad de almacenamiento, que está dedicado exclusivamente a las funciones de administración de archivos compartidos.

### **SERVIDORES RADIUS (Remote Access Dial-In User Server)**

RADIUS es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Radius utiliza el puerto 1812 UDP para establecer sus conexiones.

Un servidor RADIUS centraliza una base de datos de usuarios y passwords y espera que equipos como access servers le pregunten si cierto usuario con cierto password tiene acceso. El servidor RADIUS recibe no solo usuario y password sino una multitud de atributos, como el puerto del access server a

donde el usuario se esta conectando y su numero de telefono, y debe responder por si o por no si se le permite al usuario conectarse, junto con una serie de atributos que pueden ir desde la dirección IP a asignarle al usuario, protocolos a utilizar o reglas de filtrado de paquetes.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red) *sobre el protocolo PPP, quien dirige la petición a un servidor RADIUS sobre el protocolo RADIUS.*

*El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.*

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores de Acceso a la Red (NAS), más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto.

Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes). RADIUS es extensible; la mayoría de fabricantes de software y hardware RADIUS implementan sus propios dialectos.

Un servidor RADIUS puede realizar consultas en una base de datos de autenticación local si ello es adecuado para el escenario. O bien, la solicitud puede transmitirse a otro servidor para su validación. Cuando RADIUS decide que se puede autorizar el equipo en esta red, vuelve a enviar el mensaje al punto de acceso y éste permite que el tráfico de datos fluya hacia la misma.

**Un ejemplo real sería el siguiente:**

- Cuando un usuario enciende su equipo portátil y activa su WLAN, con tarjeta 802.11, en un aeropuerto.
- El equipo portátil detecta la existencia de redes inalámbricas disponibles, elige la óptima y se asocia a ella.
- El equipo envía las credenciales de usuario al punto de acceso para verificar que tiene permiso en esta red.
- El usuario es manuel@shura.com. Shura ha adquirido acceso inalámbrico para todos sus usuarios en todos los aeropuertos del mundo.
- El servidor RADIUS, que recibe la solicitud desde el punto de acceso, comprueba el paquete y descubre que procede de un usuario de Shura.
- RADIUS pide a un servidor de shura que determine si esta persona (manuel) es un usuario real y si le conceden acceso.
- Si el servidor de Shura responde afirmativamente, se indica al punto de acceso que permita el flujo del tráfico.



Microsoft incluye una implementación del cliente 802.1X en Windows XP y mejora el servidor RADIUS de Windows, el servidor de autenticación de Internet (IAS), para admitir la autenticación de dispositivos inalámbricos.

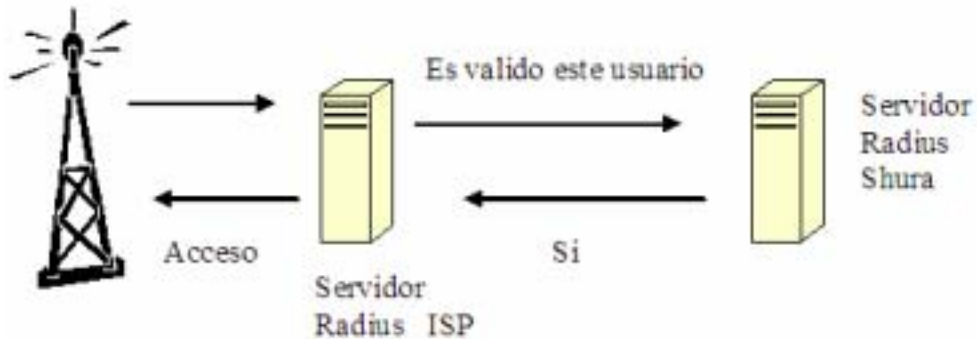


Figura 1.6 Acceso Publico

## Protocolo 802.1x

IEEE 802.1X es una norma creada por la IEEE para el control de admisión de red basada en puertos. Esta norma permite la autenticación de los dispositivos que se encuentran conectados a un puerto LAN, y esta establece una conexión punto a punto. Se es utilizado en algunos puntos de acceso inalámbricos (AP Access Point) y es basada en el protocolo de autenticación extensible (EAP – RFC 2284) el cual ha sido declarado obsoleto por el RFC 3748.

802.1X son utilizados en el punto de acceso el cual se utiliza como punto de acceso cerrado, para corregir fallas de seguridad de WEP. La autenticación es realizada por el servidor RADIUS, que permitirá la autenticación de un usuario o más apropiadamente, también abra una autenticación más fuerte al utilizarlo con los protocolos EAP – TLS.

La norma IEEE 802.1X ya que permite la autenticación del usuario, tal y como un proceso de variación dinámica de claves, que son ajustados al protocolo EAP. Esto permite a todo usuario que este empleando la red, este se encuentra autenticado y con solo una clave única, y esta se va a ir modificando

automáticamente y es tratada por el servidor y el cliente de una manera transparente para el usuario.

### **Funcionamiento de el Protocolo 802.1X**

- El cliente, que quiere conectarse a la red, manda un mensaje de inicio de EAP que da lugar al proceso de autenticación.

Por ejemplo, una persona que pertenece y quiere acceder a un edificio de oficinas resguardado pediría acceso al guardia de seguridad de la puerta del edificio.

- El punto de acceso a la red respondería con una solicitud de autenticación EAP.

El guardia le solicitara el nombre y el apellido de la persona, así como su huella digital si es el caso. El guardia de seguridad le diría una contraseña a la persona, para que éste sepa que realmente es un guardia de seguridad.

- El cliente responde al punto de acceso con un mensaje EAP que contendrá los datos de autenticación.

La persona le daría el nombre y los apellidos al guardia de seguridad además de su huella digital'.

- El servidor de autenticación verifica los datos suministrados por el cliente mediante algoritmos, y otorga acceso a la red en caso de validarse.

El sistema del edificio verificaría la huella digital, y el guardia validaría que este corresponde a la persona autorizada para ingresar al edificio.

- El punto de acceso suministra un mensaje EAP de aceptación o rechazo, dejando que el cliente se conecte o rechazándolo.

Para finalizar el guardia le permitirá entrar o no al edificio, esto en función de la verificación a la persona que pertenece al edificio.

- Una vez autenticado, el servidor acepta al cliente, por lo que el punto de acceso establecerá el puerto del cliente en un estado autorizado.

La persona ya autenticada podrá entrar y tendrá acceso al edificio.

El protocolo 802.1x provee una manera efectiva de autenticar, se implementen o no claves de autenticación WEP. De todas formas, la mayoría de las instalaciones 802.1x otorgan cambios automáticos de claves de encriptación usadas solo para la sesión con el cliente, no dejando el tiempo necesario para que ningún sniffer sea capaz de obtener la clave.

802.1X esta a convertirse en un estándar como la solución la red inalámbrica.

## **CAPITULO II**

### **PLANEANDO LA RED INALÁMBRICA**

#### **Introducción**

Este capítulo nos explicará cómo planear una red, desde seleccionar una tecnología inalámbrica a decidir qué otros hardware conectar, donde podrás conectarlos y lo principal compartir el Internet y tener una seguridad en tu red inalámbrica.

Cuando se decida el número de computadoras que se desea conectar a la red, se podrá dar respuesta para contar con las computadoras y dispositivos de la propiedad de cada uno de los usuarios a conectar a la red.

#### **Escogiendo red cableada o inalámbrica**

Se debe decidir si se conectará cada computadora o dispositivo inalámbricamente a la red o tal vez conectar una o más por una conexión cableada.

Los dispositivos de la red inalámbrica o cableada pueden ser usados en la misma red. Pero obviamente cuando estamos hablando de una red inalámbrica, es el deseo de eliminar el cableado.

La figura 2.1 nos muestra una red que conecta una red de computadora inalámbrica y una computadora cableada a través de dos dispositivos de red; un Access point AP y un hub or switch.

Esto nos muestra que una red puede usar ambas conexiones, cableadas e inalámbricas.

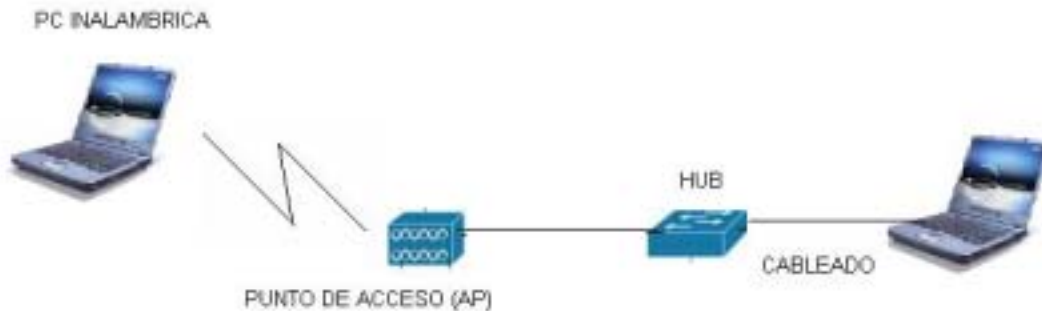


Figura 2.1

## Escogiendo la tecnología inalámbrica

Las tecnologías inalámbricas usadas para conectar una computadora a una red inalámbrica son referido a sus nombres técnicos: Institute of Electrical and Electronics Engineers (IEEE), IEEE 802.11a, IEEE 802.11b e IEEE 802.11g.

Para usuarios caseros, los tres más importantes diferencias prácticas entre IEEE 802.11a, IEEE 802.11b e IEEE 802.11g:

- ✓ IEEE 802.11a el equipo es típicamente de mas alto costo que IEEE 802.11b, pero es al menos cinco veces más rápido.
- ✓ IEEE 802.11g es tan rápido como IEEE 802.11a pero es también de menor costo como IEEE 802.11b.
- ✓ IEEE 802.11a e IEEE 802.11b no son compatibles.
- ✓ IEEE 802.11b e IEEE 802.11g son compatibles.

802.11g es compatible con 802.11b, un AP que incluya 802.11g debe trabajar con cualquier dispositivo 802.11b también (a la más baja, 11Mbps de velocidad de 802.11b). Así, uno no tiene que buscar un AP modo dual 802.11b y 802.11g.

Si la razón primaria es establecer que las computaras compartan el Internet, IEEE 802.11 es más rápida por que su conexión excederá probablemente 11Mbps.

Access Point AP puede manejar los estándares de la tecnología de IEEE 802.11a y de IEEE 802.11b/g. Linksys, NETGEAR, el D-Link, y varios otros fabricantes principales de equipo inalámbrico ofrecen ya el dual-mode (modo dual) de a/b/g, dispositivos inalámbricos tri – estándares.

El más importante y la mayoría del dispositivo costoso en una red inalámbrica es típicamente el punto de acceso (Access point AP). Un AP actúa como una pequeña central telefónica inalámbrica que conecta los dispositivos inalámbricos en la red el uno al otro y al resto de la red conectada con cable; esto es requerido para crear una red casera inalámbrica. La figura 2.2 representa tres computadoras conectadas inalámbricamente el uno al otro con un AP.

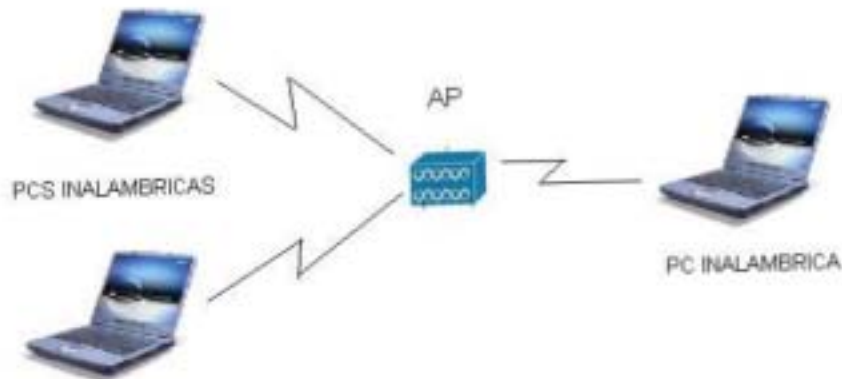


Figura 2.2

**Elegir un AP que realiza varios servicios orientados a la red adicionales puede también ser más económico para usted. El AP más popular para el uso en las redes caseras son los que pueden hacer uno o más de lo siguiente:**

- **Computadoras conectadas por cable**

Un interruptor (switch) es una versión realizada de un hub que funciona más eficientemente y rápidamente que un hub simple. Construyendo un switch dentro del AP, usted puede utilizar el único dispositivo para conectar las computadoras con su red usando los adaptadores cableados o los adaptadores inalámbricos.

- **Asigne las direcciones de red**

Cada computadora en una red o en el Internet tiene su propia dirección: su dirección del Protocolo de Internet (IP). Las computadoras en el Internet se comunican, e-mail, las páginas Web, y los similares - enviando datos hacia adelante y hacia atrás de la IP address a otra IP address. Un servidor dinámico (Dynamic Host Configuration Protocol DHCP) asigna dinámicamente direcciones privadas del IP a las computadoras en su red casera de modo que puedan comunicarse.

- **Conecte a Internet**

Con una línea del suscriptor de cable/digital (DSL) se puede rutear entre un módem de banda ancha y su red casera, todas las computadoras en la red pueden tener acceso al Internet directamente. Un AP combinado con un DHCP y un router de cable/DSL a veces se llamada una entrada a Internet inalámbrico.

- **Proporcione la seguridad firewall**

Un firewall es un dispositivo que guarda básicamente a malos individuos de su red y fuera de sus computadoras. Un firewall se puede incluir en su punto de acceso para proporcionar seguridad de la red.

## Factores que afectan fuerza de la señal

Muchas variables afectan si usted consigue una señal adecuada en cualquier punto dado en su casa, incluyendo los factores siguientes:

### ❖ **Distancia del AP**

El más lejano del AP, la más débil es la señal. Los estándares Wi-Fi 802.11b, por ejemplo, prometen un rango de operación máximo de 100 pies a 11 Mbps a 300 pies 1 Mbps. Dentro, una gama realista en 11 Mbps es cerca de 60 pies. Cuando las redes 802.11a y 802.11g llegan a ser más frecuentes, su gama máxima puede variar.

### ❖ **La energía del transmisor**

El Wi-Fi AP transmite en una salida de energía menos de 30 dBm (un watt).

### ❖ **La directividad o el aumento de las antenas unidas al AP y a los adaptadores inalámbricos de la red**

Diversas antenas se diseñan para proporcionar diversos patrones de radiación. Ésa es una manera de lujo de decir que diseñan algo para enviar las ondas de radio en todas las direcciones igualmente, todavía otras concentran su fuerza en ciertas direcciones.

### ❖ **Los materiales de construcción usados en las paredes, los pisos, y los techos**

Algunos materiales de construcción son relativamente transparentes a las señales de radio, pero otros materiales, tales como mármol, ladrillo, agua, papel, cristal a prueba de balas, concreto, y especialmente metal, tienden para reflejar algo de la señal, así reduciendo fuerza de la señal.



### ❖ **Localizaciones del cliente**

La distancia del AP a los cuartos en su casa afecta a la recepción en donde alguien necesitará el acceso de red inalámbrico.

### ❖ **Access Points APs**

La interferencia puede también ser causada por la presencia del otro AP. Es decir si se tiene una casa grande (demasiado grande para que un solo AP la cubra), usted tiene que tener presente que en las partes de la casa, usted encontrará que las ondas de radio de cada AP pueden interferir con el otro.

## Interferencia RF

Hoy en día, muchos dispositivos que requirieron una vez el cableado ahora son radio, y están llegando a ser más frecuentes todo el tiempo. Algunos dispositivos inalámbricos utilizan la tecnología infrarroja, incluyendo la red inalámbrica, se comunican usando ondas de la radiofrecuencia (RF). Por consiguiente, la red se puede interrumpir por interferencia de RF de otros dispositivos que comparten las mismas frecuencias usadas por su red inalámbrica.

Entre los dispositivos muy probablemente a interferir con las redes de IEEE 802.11b y de IEEE 802.11g están los hornos de microondas y los teléfonos sin cordón que utilizan de 2.4 gigahertz de banda. La mejor manera de evitar esta interferencia es colocar el AP y las computadoras con los adaptadores inalámbricos por lo menos seis pies lejos del microondas y de la estación baja de cualquier teléfono portable que utilice 2.4 gigahertz de banda.

## Obstáculos de señal

Las tecnologías inalámbricas son susceptibles a los obstáculos físicos. Cuando se decide donde colocar el AP, refiera a la tabla siguiente, que enumera los obstáculos que pueden afectar la fuerza de sus señales inalámbricas. La tabla enumera obstáculos comunes de la casa (aunque está pasado por alto a menudo) así como el grado para el cual el obstáculo es un obstáculo a sus señales de red inalámbrico.

**Tabla de atenuación relativa de obstáculos de RF**

| Tabla de Atenuación Relativa de Obstáculos de RF |                     |                                   |
|--|---------------------|-----------------------------------|
| Obstrucción                                      | Grado de Atenuación | Ejemplo                           |
| Espacio abierto                                  | Bajo                | Patio                             |
| Madera   | Bajo                | Pared interior, puerta, piso      |
| Yeso   | Bajo                | Pared interior                    |
| Materiales sintéticos                            | Bajo                | Particiones                       |
| Bloque de ceniza                                 | Bajo                | Pared interior, pared externa     |
| Asbestos   | Bajo                | Edificios viejos                  |
| Vidrio   |                     | Ventana                           |
| Maya en vidrio                                   | Medio               | Puerta, ventana                   |
| Vidrio pintado de pintura metálica               | Medio               | Ventana pintada                   |
| Cuerpo humano                                    | Medio               | Grupo de gente                    |
| Agua   | Medio               | Acuario, contenedores de agua     |
| Ladrillos  | Medio               | Pared interior, exterior y pisos  |
| Mármol   | Medio               | Pared, pisos                      |
| Cerámica   | Alto                | Teja, piso                        |
| Papel  | Alto                | Papel apilado, pilas de periódico |
| Concreto   | Alto                | Pisos, paredes                    |
| Plateados  | Muy alto            | Espejos                           |
| Metal  | Muy alto            | Paredes, gabinetes                |

## **Conectar a Internet**

Una red inalámbrica (o cualquier red casera) proporciona un elemento dominante. Utiliza un NAT Router, para proporcionar el acceso del Internet a los dispositivos múltiples sobre una sola conexión de Internet que viene en el hogar. Con un NAT Router (que sea construida típicamente en su punto de acceso o en un router de red casera separada), usted no puede conectar solamente más de una computadora con el Internet, sino que usted puede conectar simultáneamente las computadoras múltiples (y otros dispositivos como las consolas del juego) con el Internet sobre una sola conexión. La NAT Router tiene los cerebros para resolver de qué página del Web o E-mail o información en línea del juego va a qué cliente (PC/device) en la red.

No sorpresivamente, para aprovecharse de esto Internet, cualquier lugar de acceso en su hogar, usted necesitará una cierta clase de servicio y de módem del Internet. No vamos a conseguir en el gran detalle sobre este asunto, sino que deseamos cerciorarnos de que usted lo tenga presente cuando usted planea su red.

La mayoría de la gente tiene acceso al Internet de un ordenador personal de estas maneras:

- ✓ Conexión de marcado telefónico
- ✓ Línea de suscriptor digital (DSL)
- ✓ Internet por cable
- ✓ Satélite de banda ancha

## **Hay dos maneras de compartir una conexión a Internet en una red:**

### ➤ **Software-basado en compartir la conexión de Internet**

Windows 98 (y versiones más actualizadas de Windows) y Mac OS X permite compartir de una conexión de Internet. Cada computadora en la red

se debe fijar hasta conectar con el Internet a través de la computadora que está conectada con el módem de banda ancha. La desventaja con este sistema es que usted no puede apagar o quitar a la computadora que está conectada con el módem sin desconectar todas las computadoras del Internet. Es decir la computadora que está conectada con el módem debe estar encendida para que otras computadoras networked tengan acceso al Internet a través de ella.

➤ **Router Cable/DSL**

Conectando un router de cable/DSL entre el módem de banda ancha y su red casera, todas las computadoras en la red pueden tener acceso al Internet sin pasar a través de otra computadora. La conexión del Internet depende no más de largo de cualquier computadora en la red. Los routers de Cable/DSL son también servidores de DHCP e incluyen típicamente los interruptores (switches). De hecho, el AP y/o el módem pueden también incluir un router incorporado que proporcione el Internet inmediato que comparte todos en un dispositivo.

Ambos software basados en compartir la conexión de Internet y los routers de cable/DSL permiten a todas las computadoras en su red compartir la misma dirección de la red (IP) en el Internet. Esta capacidad utiliza la conversión de dirección de red (network address translation NAT). Un dispositivo que utiliza la característica NAT a menudo se llama NAT Router. La característica NAT es que se comunica con cada computadora en la red usando un IP address privado asignado a esa computadora local, pero el router usa un solo IP address público en los datos que envía a las computadoras en el Internet. Es decir no importa cómo cuantas computadoras se tienen en casa o en el lugar donde se instalara la red inalámbrica que comparte el Internet, parecen solamente una computadora a el resto de computadoras en el Internet.

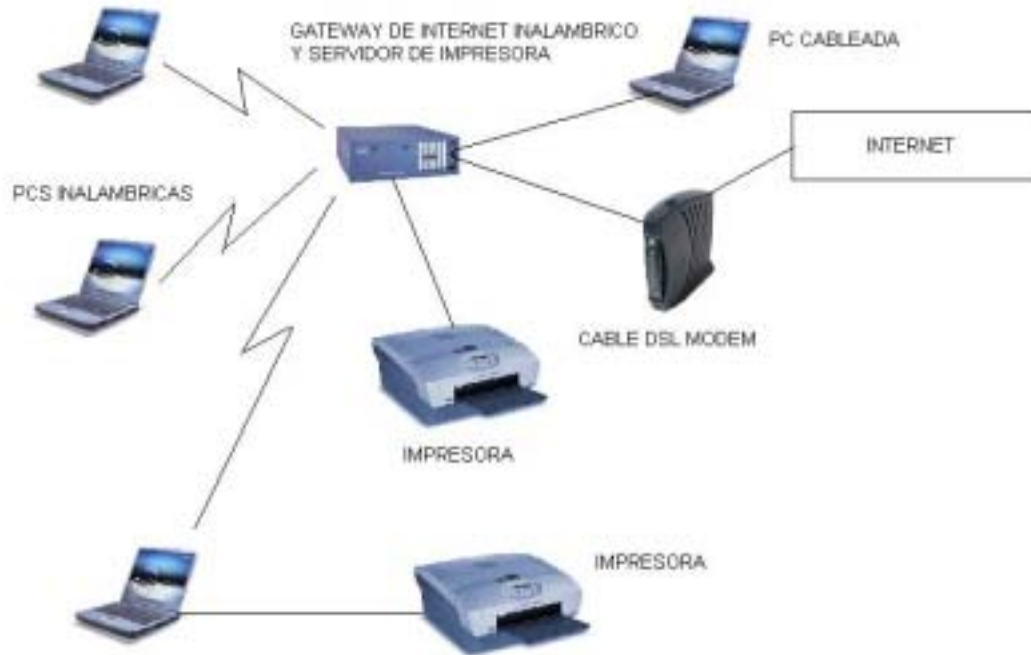


Figura 2.3 Ir por una red inalámbrica gateway que combina AP, DHCP, NAT, servidor de impresora y funciones de switched hub.



Figura 2.4 Red cableada con un AP y una estación de red inalámbrica

## Planeando la seguridad

Cualquier red puede ser atacada por un hacker persistente, pero una red bien-defendida desalentará a la mayoría de los hackers suficientemente para mantener sus datos seguros. Sin embargo, es más fácil que un hacker acceda a una red inalámbrica a través del aire que al acceso físico del aumento a una

red cableada, haciendo redes inalámbricas más vulnerables al ataque, incluso redes caseras. Porque una señal Wi-Fi es una señal de radio, mantiene el ir y el ir y el ir, hasta que golpea algo bastante sólido para pararlo. Cualquier persona con una PC portable, un adaptador inalámbrico de red, puede tener acceso a su red inalámbrica.

- **Seguridad de Internet**

Cualquier conexión de Internet, especialmente siempre-en conexiones de banda ancha, pero conexiones del dial up, también pueden ser vulnerable a los ataques que llegan del Internet. Para mantener sus PC seguras usted debe encender cualquier firewall disponible en su AP o router. Algunos APs o routers más incluye una clase altamente eficaz de firewalls (un solemne paquete de inspección (Stateful Packet Inspection SPI) ). Usted debe también considerar el instalar de software del antivirus así como software personal del cortafuego en cada PC o mac en su red para un nivel adicional de la protección.

- **Seguridad de Airlink**

Ésta es una necesidad especial de una red inalámbrica. En el mundo inalámbrico, la seguridad física es imposible, así que usted necesita poner seguridad del airlink en ejecución. Usted no puede mantener las ondas de radio de salir de la casa, sino que usted puede hacerla muy dura para que alguien haga cualquier cosa con ellas (como lea los datos que contienen). Semejantemente, usted puede utilizar seguridad del airlink para guardar otras de conseguir sobre su punto de acceso y de freeloading en su conexión del Internet. Los medios primarios de proporcionar seguridad del airlink y los nuevos avances están en la manera es WEP.

## CAPITULO III

### INSTALACIÓN INALAMBRICA DEL PUNTO DE ACCESO (ACCESS POINT)

#### Introducción

En este capítulo, se describe la instalación y configuración de un dispositivo importante requerido para nuestra red inalámbrica, es el Access point. Se explicara como configurar el Access point listo para comunicar con cualquier y todos los dispositivos inalámbricos en tu red inalámbrica.

#### Punto de acceso (Access point)

Antes de que se instale un adaptador de interfaz inalámbrico de red en una de las computadoras, usted debe primero instalar el punto de acceso inalámbrico (también a veces llamado una estación base) que facilitará la comunicación entre los varios dispositivos inalámbricos en su red.

#### Preparando instalar el punto de acceso (AP)

Por que tener una red hace fácil compartir una conexión del Internet, el mejor tiempo de instalar el AP para ese propósito está durante la disposición inicial. En términos de instalación, una conexión compartida de Internet, se tendrá ya una computadora conectada por cable en su conexión de banda ancha (cable o la línea digital del suscriptor [DSL]) o de dial-up (marcación por telefonía) de Internet. Esto es muy provechoso como para comenzar la mayoría de las instalaciones del AP porque la mayoría de la información que se necesita para instalar el AP, está ya disponible en su computadora. Si usted no tiene una computadora conectada en conexión de Internet, esto es, que si es la primera computadora que se esta conectando, primero se tiene recopilar cualquier información, esto es como un nombre de usuario (username) o una contraseña

(password) que su proveedor de servicio de Internet (Internet service provider ISP) le haya dado para usar a su servicio.

- **Asegúrese de que su computadora tenga una conexión atada con alambre estándar de Ethernet.**

La mayoría de las configuraciones del AP requieren el acceso cableado para su disposición inicial. Un puerto de Ethernet se encuentra normalmente en la parte posterior de la computadora; este puerto parece un jack típico de teléfono, solamente un poco más ancho. Si usted no tiene un adaptador de Ethernet, se debe comprar uno e instalarlo la computadora. Alternativamente, si la computadora tiene un puerto serial universal bus (USB) (preferiblemente USB 2.0), se puede comprar un AP que conecta con el puerto del USB.

- **Recopila información acerca de tu ISP**

Lo que se necesita saber para la instalación es lo siguiente:

- **Dirección del Protocolo de Internet (IP address)**

Este es el equivalente del número telefónico de la red. El IP identifica tu red en Internet y habilita las comunicaciones

- **Puerta de enlace (gateway)**

Este es el IP del dispositivo de la red que conecta los dispositivos adjuntos a la red de Internet.

- **Mascara de subred**

Red de área local (LAN), la red usa esto para definir la locación de las computadoras con la red y a las que estas conectadas a Internet.

- **Sistema de nombres de dominio (domain name system DNS)**



Esta es una computadora especial con la red ISP que traslada el IP dentro de los nombres del host. Los nombres host son el plano de los nombres para las computadoras adjuntadas a Internet. Por ejemplo manuel.com parte de www.manuel.com es el nombre del host del servidor WEB.

- **Si el ISP esta enviando todo esto a la vía del protocolo de configuración del host dinámico (dynamic host configuration protocol DHCP)**

En todos los casos, el servicio de Internet que se tiene en casa usa DHCP, el cual significa que un servidor o computadora automáticamente provee una red ISP.

- **Colectar la dirección física de la tarjeta de red usada en la computadora, solo si ya esta listo para conectar.**

Muchos ISP usan la dirección física como una seguridad para asegurar que la computadora conecta a su red, y que sea la única que paga por el servicio. Muchos de los AP y dispositivos de accesos a Internet permiten cambiar la dirección física (control de acceso a medio (media Access control MAC)) para unir la dirección física de la tarjeta de red existente, eliminando la necesidad de tener el proveedor de servicio para ajustar tu cuenta.

### Instalando el Punto de Acceso (AP)

Si se esta conectando la primera computadora con un ISP, el ISP debe haber proveído toda la información que se enlista en sección de procedimiento excepto por la dirección física de la tarjeta de red el cual no es necesario si no se esta ya conectado.

Ya que los sistemas operativos han ido actualizándose conforme el paso del tiempo, hoy en día los usuarios usan un sistema operativo XP.

## **1. obtener la información necesaria para instalar el punto de acceso (AP)**

Para iniciar y visualizar la información que se requiere para la instalación del punto de acceso se debe realizar lo siguiente.

- a. Ir a inicio (start), programas (programs), accesorios (accessories), símbolo del sistema (command prompt)

Esto abrirá una ventana similar a la pantalla DOS.

- b. Escribir IPCONFIG / ALL y presionar enter

La información que se despliega en pantalla se debe tener a la mano, ya que contiene la información para configurar el AP (dirección física, dirección IP, puerta de enlace gateway, máscara de subred, DNS servers y DHCP).

## **2. software del AP**

El software probablemente iniciara al momento de insertar el disco. En muchos casos el software detectara la configuración de Internet, el cual lo hace en muchos casos más fácil para configurar el AP para compartir Internet y configurar la primera computadora a la red.

- 3. cuando el indicador de comandos (prompted) del software para conectar el AP, se desconecta el cable de red que conecta la banda ancha del MODEM a la computadora del puerto de ethernet de la computadora y conecta este cable en el puerto ethernet que esta marcado WAN o MODEM en el cable/DSL router de la red o la puerta de enlace de Internet (gateway).**

Si se esta usando un Internet o gateway inalámbrico, corre un cable Cat 5e de una de sus puertos de ethernet a la computadora sobre el cual se esta corriendo el software de instalación.

Si no se necesita conectar el cable Cat 5e entre el AP y uno de los puertos de ethernet de los routers entonces se conecta otro cable de otro puerto de ethernet de los routers para la computadora sobre el cual se esta corriendo el software de instalación.

**4. Completa la instalación del software y cuando enliste los comandos, inserta la información que se recopiló en el paso 1 (esto se tiene que tener a la mano).**

**5. Registra los siguientes parámetros del AP**

La siguiente lista cubre los parámetros del AP que se encontraran y necesitara para configurar.

- ✓ Identificador de servicio (SSID)
- ✓ Canal
- ✓ WEP Keys
- ✓ Password / contraseña
- ✓ MAC Address / Dirección MAC
- ✓ WAN / IP Address
- ✓ Local IP address / dirección IP local
- ✓ Mascara de sub red / subnet mask
- ✓ PPPoE (point to point protocol over ethernet) / protocolo punto a punto sobre Ethernet

**6. Completa la instalación del software y habrá finalizado.**

## Configurar los parámetros del AP

En esta sección se puede ver los parámetros mas a fondo del punto numero 5.

### ✓ Identificador de servicio (SSID)

El SSID puede ser cualquier cadena alfa numérica. El AP puede que tenga un set SSID por default, pero se deben cambiar estas configuraciones. Asignar un único SSID no realmente agrega mucha seguridad, sin embargo, establecer un identificador que es diferente al que viene de fábrica lo hace un poco más difícil para los intrusos acceder a la red inalámbrica.

### ✓ Canal

Este es el canal de radio sobre el cual el AP comunicara. Si se desea usar mas de un AP en su red, se debe asignar un canal diferente (sobre el cual el AP comunicara) por cada AP para evitar interferencia de la señal. Si la red usa los protocolos IEEE 802.11b o IEEE 802.11g, 11 canales, el cual están en los intervalos de 5 MHz están disponibles, esto es en USA. Como sea, a causa de que las señales de radio usadas por IEEE 802.11b rebasan 22 MHz de espectro, se debe usar tres canales, típicamente 1, 6 y 11.

Si se esta instalando un AP 802.11a, se tiene 11 canales de el cual escoger. Pero por que estos canales son de 20 MHz y no superpone, realmente se tiene 11 canales con el cual trabajar, comparado con 3 con IEEE 802.11b o 802.11g. Si opera solo un AP, todo los demás realmente importa, eso es que la red debe estar puesta en el mismo canal. Si se opera más AP, se les da mucho más frecuencia de separación para reducir la probabilidad de una interferencia mutua.

A continuación podemos observar una tabla de estándares de canales de frecuencia para redes inalámbricas.

**TABLA**

| Tabla de Frecuencias para Redes Inalámbricas |                        |       |                 |
|--|------------------------|-------|-----------------|
| Canal  | 2.4 GHz (802.11 b / g) | Canal | 5 GHz (802.11a) |
|  | GHZ                    |       | GHZ             |
| 1  | 2.412                  | 36    | 5.18            |
| 2  | 2.417                  | 40    | 5.2             |
| 3  | 2.422                  | 44    | 5.22            |
| 4  | 2.427                  | 48    | 5.24            |
| 5  | 2.432                  | 52    | 5.26            |
| 6  | 2.437                  | 56    | 5.28            |
| 7  | 2.442                  | 60    | 5.3             |
| 8  | 2.447                  | 64    | 5.32            |
| 9  | 2.452                  |       |                 |
| 10   | 2.457                  |       |                 |
| 11   | 2.462                  |       |                 |
| 12   | 2.467                  |       |                 |
| 13   | 2.472                  |       |                 |
| 14   | 2.477                  |       |                 |

## ✓ WEP Keys

Se debe siempre utilizar WEP. Solo un intruso determinado, puede irrumpir en tu red de trabajo y molestar a otros usuarios que se encuentren conectados en la red inalámbrica y tener acceso a Internet sin que este sea invitado.

## ✓ Password / contraseña

La configuración del software quizás requiera de una contraseña, para hacer cambios al AP. Algunos AP traen una contraseña por default. Se usa la contraseña por default cuando primero abres las páginas de configuración y entonces inmediatamente cambia la contraseña para evitar el rompimiento de la seguridad.

## ✓ MAC Address / Dirección MAC

Es la dirección física del AP. Se debe encontrar este número impreso en una etiqueta adjunta al dispositivo. El ethernet (RJ-45) de la conexión del AP

también tiene un MAC address que es diferente a la MAC address de el radio del AP.

✓ WAN / IP Address

Si la red es conectada a Internet, debe tener una dirección IP asignado por el ISP. El ISP asignara esta dirección. El router o la puerta de enlace a Internet (gateway) podrían ser configurados para aceptar una IP dinámicamente asignado por un servidor DHCP. Eso es posible, aunque el ISP requerirá una dirección IP estática.

✓ Local IP address / dirección IP local

La dirección física (MAC address), el AP también tendrá su propia dirección IP. Se necesita saber este IP para acceder a la configuración usando un Web browser.

✓ Mascara de subred / subnet mask

En muchos casos, esto se valuara a 255.255.255.0. Si se esta usando un esquema IP de el tipo descrito en el procedimiento, 255.255.255.0 es el numero correcto para usarse. Este número junto con la dirección IP, establece la subred sobre el cual el AP reside. Los dispositivos de red con direcciones sobre la misma subred pueden comunicar directamente sin la ayuda del router.

✓ PPPoE (point to point protocol over ethernet) / protocolo punto a punto sobre Ethernet.

Muchos DSL ISP usan PPPoE. Los valores que se necesita recordar es el nombre de usuario (username / user ID) y la contraseña (password).

## **CAPITULO IV**

### **COMPARTIENDO LA CONEXIÓN DE INTERNET POR MEDIO DE NUESTRA RED INALÁMBRICA.**

#### Introducción

Uno de los más populares usos de las redes, que este caso es una red inalámbrica para el conjunto habitacional, será el compartir la conexión a Internet. En este capítulo demuestra el uso de una red incluyendo una red inalámbrica, para compartir una conexión de Internet de varias computadoras en una sola red inalámbrica.

También se describirá como obtener una dirección IP automáticamente, usar un router o puerta de enlace de Internet (gateway), y en adición compartir el Internet.

#### Decidiendo como compartir el Internet

Si se ha instalado una red inalámbrica o se esta usando algún tipo de dispositivo inalámbrico para crear una red, no debe haber duda que los equipos de cómputo puedan acceder a Internet y compartir la misma conexión.

Hay dos maneras de compartir nuestra conexión a Internet en nuestra red:

- ❖ **Compartiendo la conexión**

Todos los usuarios de la misma red acceden a Internet vía una computadora que es específicamente instalada para hacer eso, que los usuarios compartan la conexión.

- ❖ **Un Router o puerta de enlace de Internet (gateway)**

Un Router maneja el tráfico para habilitar a todos los usuarios de la red acceder a Internet. Un gateway es un MODEM con banda ancha con un router incluido. Un gateway de Internet de la red inalámbrica se le agrega o se le suma un Access point (AP).

## Compartiendo la conexión

Las versiones de Windows disponen de compartir la conexión a Internet. Cuando se usa este método para compartir una conexión a Internet, cada computadora en la red ya sea que tenga una conexión cableada o inalámbrica es montada para conectar a Internet por medio de una computadora que es conectada al MODEM que esta conectada a Internet.

La desventaja es que no se puede apagar ni remover la computadora que esta conectada al MODEM que provee Internet a los demás equipos.

## Routers y Puertas de enlace (Gateways)

Para conectar un router entre el MODEM de banda ancha y la red, todas las computadoras que están en red pueden acceder a Internet sin pasar por otra computadora. La conexión a Internet no depende de cualquier otra computadora en la red.

Los tipos de routers usados en este tipo de casos para una red inalámbrica para le hogar son a menudo los router cable/DSL. Estos dispositivos son servidores DHCP y también incluyen un servicio de traslación de dirección de red "NAT" (network address translation). De los más populares tipos de dispositivos para compartir la conexión de Internet, a menudo descrito como un gateway inalámbrico, combina las características de un router, un servidor DHCP, un servidor NAT, y la compatibilidad con un Access Point (AP).



Para la conectividad inalámbrica, más de estos dispositivos cuentan con puertos ethernet para conectar computadoras con cable, dando la flexibilidad de adherir dispositivos cableados y expandir tu conexión de red. Cada computadora se conecta al gateway inalámbrico, el dispositivo gateway inalámbrico se conecta al MODEM de banda ancha (DSL o cable) y el MODEM conecta a Internet.

La naturaleza de Internet y el protocolo control de transmisión/ protocolo de Internet (transmission control protocol TCP/ Internet protocol IP) requiere que cada computadora o dispositivo tenga una única dirección IP, para información de obtener su propio destino, cada pieza de información contiene la dirección IP que viene de y la dirección IP que va de un punto a otro.

Un servidor NAT permite para la conversión de una dirección IP a una o más direcciones IP. Esto significa que todo un grupo de computadoras pudiere verse como solo una computadora para el resto de Internet.

Si se tiene una computadora, obtener una dirección IP asignado a tu computadora por que el dispositivo de MODEM entrega la dirección IP para la computadora, y la computadora usa esa dirección para conectar a Internet. Si se tiene más de una computadora se tiene que compartir la dirección IP. NAT un direccionamiento interno usando uno de los rangos de direcciones IP reservados que el Internet no usa. (192.168.x.x es una de las dos redes clase B que son usados internamente para redes de casa u oficina usando NAT).

Los routers cable / DSL usan este rango de dirección en las redes. En muchos casos, eso es dado que las direcciones IP de el router cable/ DSL será 192.169.1.1 o 192.168.2.1, dependiendo sobre cual dirección NAT es configurado para usar.

Después de la dirección de traslación esta en posición, un servidor DHCP asigna las direcciones IP locales para todos los dispositivos conectados dentro de la red. La función de NAT del gateway de Internet habilita a todas las

computadoras a acceder a Internet a través del dispositivo gateway de Internet para compartir la misma dirección IP en Internet.

La figura 4.1 describe una red inalámbrica que utilice un gateway de Internet que provee NAT y DHCP para compartir el acceso a Internet a tres computadoras con conexión inalámbrica y dos con conexión cableada.

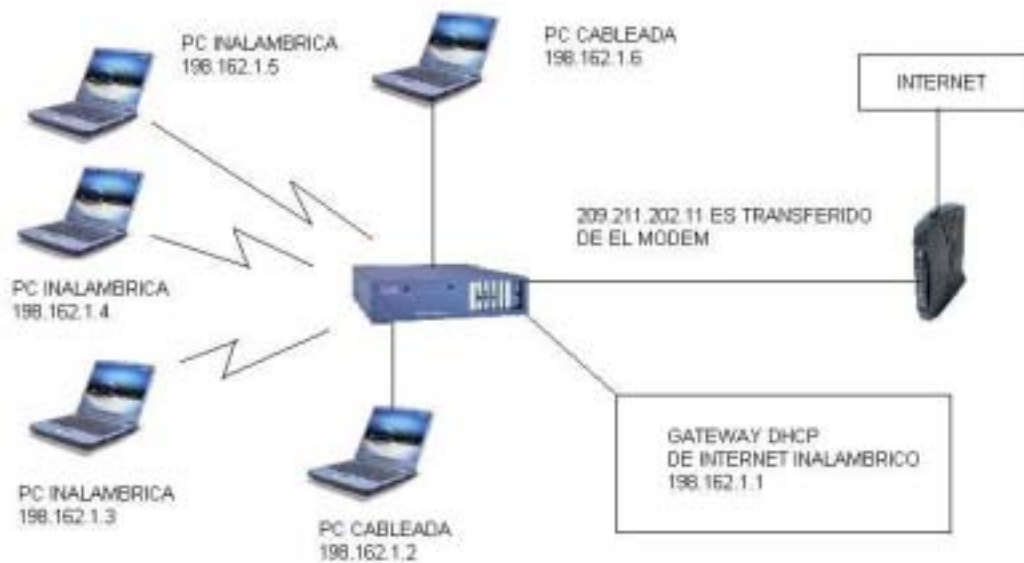


Figura 4.1

### Compartiendo conexión a Internet por marcado telefónico

Se puede compartir la conexión de Internet si es que se tiene una conexión por marcado telefónico. Esto podría ser especialmente práctico si se tiene una línea telefónica con el cual se accede a Internet por medio del mismo. Similarmente si se adquiere un gateway de Internet que incluye un MODEM por marcado, se puede compartir la conexión. Se puede conectar el gateway a Internet usando el MODEM de marcado telefónico y entonces usar la característica de router del gateway para compartir la conexión con todas las computadoras. Algunos gateways de Internet combinan ambos, un MODEM de banda ancha DSL y un MODEM de marcado telefónico como un sistema de soporte si la conexión de banda ancha se cae.

## Obteniendo una dirección IP automáticamente

Para las computadoras que están en red y que puedan comunicarse efectivamente con otra, si están conectadas a la red por medio de cableado o ya sea inalámbricamente, todas deben tener una dirección IP, sobre la misma subred. Por ejemplo la dirección IP local 192.168.0.1 y 192.168.0.55 son de la misma subred, pero la dirección 192.168.0.1 y 192.168.1.55 no lo es. Se nota que número después del segundo punto debe ser el mismo para la dirección para que sea en la misma subred. Todas deben tener la misma máscara de subred, el cual es típicamente 255.255.255.0.

Una subred es simplemente una porción de una red que ha estado dividida y agrupada junta como una sencilla unidad. Cuando se usa un gateway de Internet inalámbrico, todas las computadoras están ubicadas dentro de la misma subred. La sencilla dirección IP asignada al MODEM puede proveer acceso a Internet a todas las computadoras en la subred. Los números actuales usados para identificar la subred están en la máscara de subred. Como ya se menciona previamente, típicamente se usará 255.255.255.0 como máscara de subred. Lo importante es asegurar que todas las computadoras y dispositivos conectados a la red inalámbrica tengan la misma máscara de subred asignada a ellos, de otra manera no conectarán a Internet.

Hoy en día las computadoras corren con el sistema operativo más actual, en este caso para obtenerla, se siguen los siguientes pasos para la obtención automática de la dirección IP de un servidor DHCP:

1. Elije conexiones de red

Esto es menú inicio, panel de control, conexiones de red, aparecerá una ventana como se muestra a continuación (figura 4.2)



Figura 4.2

2. En LAN o Internet de alta velocidad que aparece en sección de la ventana, están los adaptadores que se desea configurar.
3. De la conexiones de redes inalámbrica, elije propiedades
4. En la pantalla, de la pestaña general, elije (TCP/IP), entonces da un clic en propiedades, eso se vera como la siguiente ventana (figura 4.3).

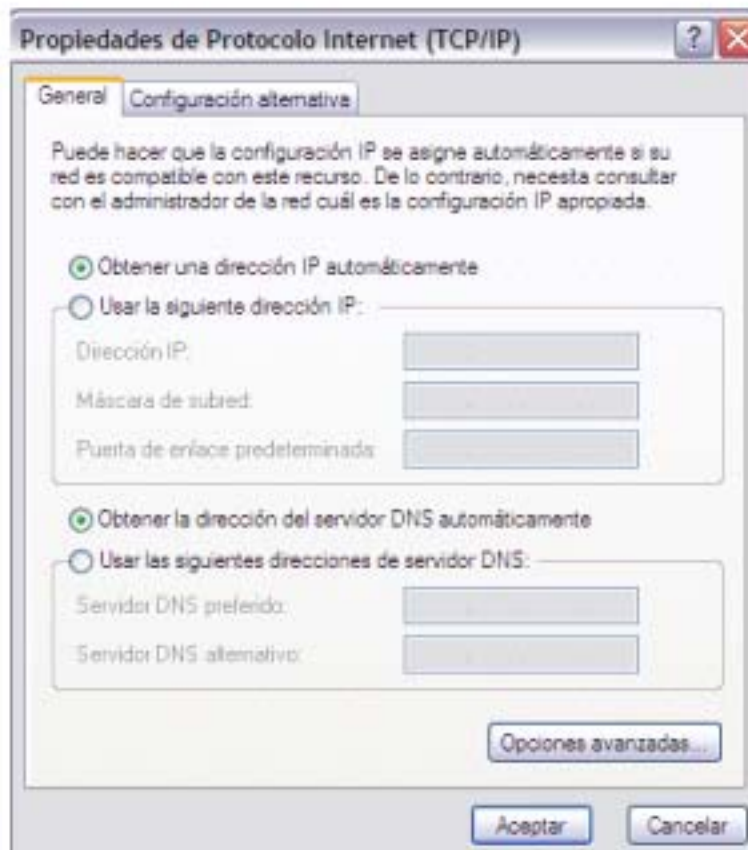


Figura 4.3

5. En la pestaña general, selecciona ambos, obtener una dirección IP automáticamente y obtener la dirección del servidor DNS automáticamente.

6. Después da un clic en aceptar para retornar a la ventana conexiones de red, entonces cierra esa ventana.

Windows aplicara el cambio y obtendrás una dirección IP para el adaptador de red del servidor DHCP de la red inalámbrica.

## Configuración y compartir la conexión de Internet

Las puertas de enlace de Internet (gateways) y los routers cable/DSL son ciertamente la manera mas fácil para completar nuestra conexión para compartir el Internet. Todas las versiones de Windows proveen un software basado en la solución para compartir una conexión de Internet en una red de

área local (LAN). Esta opción es viable si se esta usando una red cableada, inalámbrica o la combinación de las dos.

Cuando se instala un software de Windows basado para compartir la conexión de Internet, se debe seleccionar una computadoras para que sea el host de la conexión de Internet, la computadora que esta siempre encendida y conectada a Internet, así cualquier otra computadora que este cerca del área de cobertura de la red pueda acceder a Internet por medio de esa computadora. Esa computadora host también debe tener dos adaptadores de red: uno que conecta a Internet y otro que comunica con la red de área local (LAN). La conexión a Internet puede ser a través de un MODEM de marcado telefónico, un MODEM de banda ancha o una conexión de red mas grande que conecta a Internet. Después completar con el asistente de configuración, Windows regresa al servidor de conexión de Internet dentro de ambos; un servidor DHCP y la puerta de enlace (gateway) a la conexión de banda ancha y a Internet.

Al usar el software de compartir la conexión de Internet es equivalente adherir un router cable/DSL a la red. Por ejemplo el Access Point (AP), al adjuntarlo a la computadora vía un puerto ethernet, todas las computadoras inalámbricas que estén dentro de la cobertura de Internet, podrán acceder a Internet por medio del punto de acceso (AP).

La figura 4.4 describe una red inalámbrica que usa la conexión compartida de Internet mediante Windows para proveer Internet a todas las computadoras inalámbricas que se encuentren cerca dentro del área de cobertura de Internet.

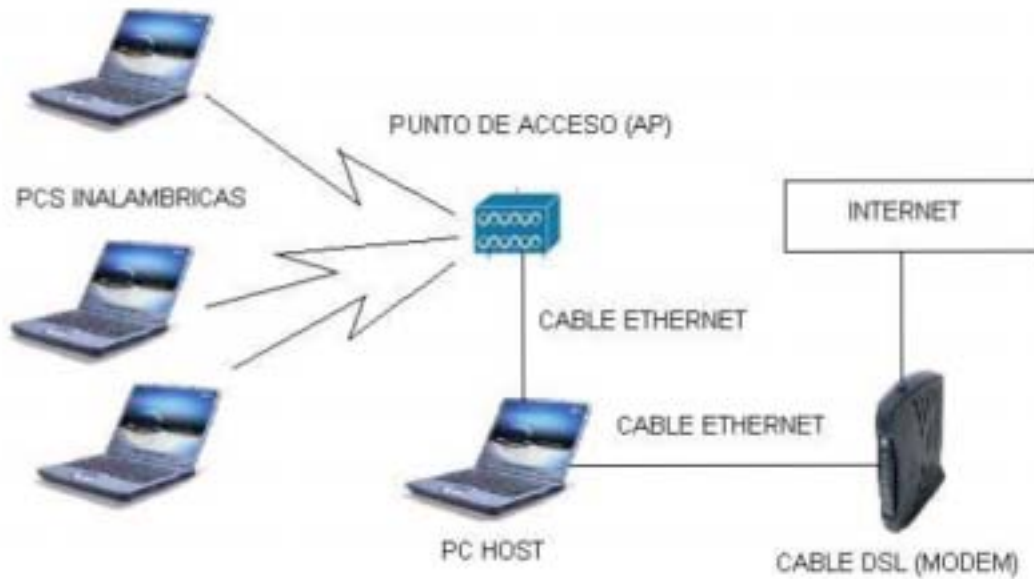


Figura 4.4

Cuando se usa la conexión compartida de Internet mediante Windows, la computadora host debe siempre estar encendida, con la computadora encendida y corriendo, otras computadoras que estén en la red y cerca del área de cobertura pueden acceder a Internet. Cada computadora que este en la red debe ser configurada para obtener una dirección IP automáticamente, el cual se describió anteriormente.

Para configurar la conexión compartida de Internet en Windows se realizan los siguientes pasos:

1. Se va a el menú inicio, panel de control
2. después a conexiones de red
3. En LAN o Internet de alta velocidad que aparece en sección de la ventana, están los adaptadores que se desea configurar.  
En propiedades de conexión de área local.

4. en la pestaña de avanzado, selecciona permitir a otros usuarios conectarse a través de la conexión de este equipo como se muestra en la siguiente figura (figura 4.5).

Por default, el permitir a otros usuarios controlar o deshabilitar la conexión compartida de Internet del cuadro es seleccionada. A menos de que se desee que otros usuarios en la red se disponga a habilitar o deshabilitar la conexión compartida.

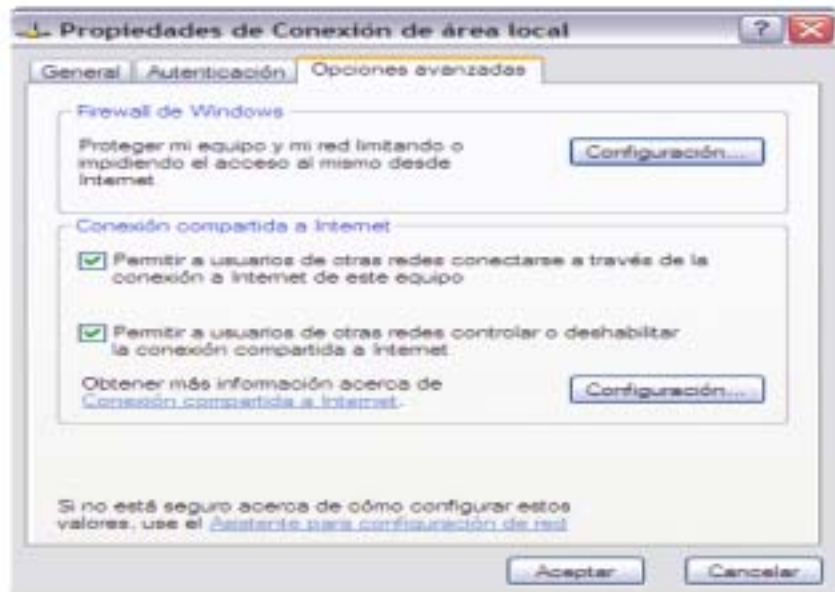


Figura 4.5



## **CAPITULO V**

### **SEGURIDAD EN LA RED INALÁMBRICA**

#### Introducción

En este capítulo, describe acerca de la seguridad de nuestra red inalámbrica, riesgos etcétera. También se describe como hacer la red mas segura para que intrusos o cualquier otro usuario que no se desee que este en nuestra red irrumpa dentro de la red o trate de utilizar la conexión de Internet.

La mayoría del equipo de redes inalámbricas (Access points, tarjetas de red, etcétera) no son seguras del todo. Algunos Access points están ahí para que cualquier usuario que se encuentre dentro de la cobertura de red inalámbrica pueda acceder a la red. Hoy en día esto es una mala opción, configurar la red inalámbrica y habilitar las características de seguridad es una muy buena opción. Un gran numero de Access points están completamente abiertos al publico, esto es que arriba del 60 % de los Access points no tienen métodos de seguridad del todo. Es por eso que si se desea que tenga un acceso restringido es necesario asegurar la red inalámbrica.

Ningún sistema de seguridad de una red es absolutamente seguro, es lo que se describe en este capítulo. Las redes Wi – Fi tienen algún defecto en sus sistemas de seguridad, el cual significa que incluso si implementa completamente el sistema de seguridad en Wi – Fi (WEP), un individuo o usuario determinado podrían obtener y acceder a la red.

También se retomaran los conceptos vistos en el capítulo I para dar un enfoque mas claro del uso del Servidor Radius ya que se cuenta con el para asegurar la seguridad del acceso inalámbrico de la red.

## Asegurando la red inalámbrica

Se puede discutir en esta parte algunos de los pasos de las llaves (WEP Key) que pueden tomarse para asegurar la red inalámbrica de los usuarios no deseados o intrusos por así decirlo. Esto es requerido si es que se desea asegurar la red inalámbrica para que no pueda acceder cualquier usuario, de lo contrario es como si se dejara abierta la señal de acceso a Internet.

Para asegurar las llaves (WEP Keys) se siguen los siguientes pasos:

- 1) Cambiar todos los valores que están por default en la red.
- 2) Habilitar WEP
- 3) Cerrar la red para los usuarios extraños

## Longitud de la llave (WEP Key)

Los primeros 24 bits de la llave son actualmente llamadas un vector de inicialización, y el resto de los bits comprende e incluye la llave misma. Por tanto, las llaves de 128 bits son solo realmente 104 bits de tamaño, y 64 bits son solo 40 bits. Así que cuando se entra a la llave de 128 bits (matemáticamente), se puede ver que solo hay 26 caracteres alfa numéricos o dígitos para el usuario al entrar a la llave (WEP Key) esto es 4 bits por dígito ( $26 \times 4 = 104$  bits).

Muchos Access points (AP) también tienen algunas conexiones cableadas disponibles. Los puertos de ethernet que se pueden usar para conectar las computadora al Access point (AP). Se puede usar esta conexión cableada para

correr el software de configuración del Access point. Cuando se esta configurando la seguridad, se recomienda hacer una conexión cableada y hacer toda la configuración del Access point de este modo. De esa manera se puede evitar bloquear accidentalmente los Access points cuando se esta configurando.

### Librando los valores que están por default

Cuando se inicia la seguridad de la red, lo primero que se debe hacer es cambiar todos los valores que se encuentren por default en los Access points. A un mínimo, se debe cambiar lo siguiente

- El SSID que esta por default
- La contraseña administrativa que esta por default

Si se quiere tener la seguridad necesaria, se debe cambiar la contraseña por que alguien que tenga acceso a la red puede adivinar la contraseña y al final puede cambiar toda la configuración en el Access point sin saberlo. Así el usuario puede bloquear el Access point hasta que se tenga que reiniciar y volver a configurar todo de nuevo. Las contraseñas que están por default la mayoría son conocidas, ya que vienen en las páginas del vendedor del equipo o la marca de dicho Access point, así alguien podría bajar una copia o guía disponible y cambiar la configuración.

Cuando se cambia el SSID que esta por default en el Access point, se necesita cambiar la configuración SSID de cualquier computadora u otro dispositivo que se quiera conectar a la red (LAN).

## Habilitando WEP

Después de que se eliminan los riesgos de seguridad causados por dejar todas las configuraciones por default, es debido hacer la encriptación. Cada Access point tiene su propio sistema para configurar WEP.

Para habilitar WEP en la red inalámbrica se realizan los siguientes pasos:

1. abrir la pantalla de configuración del Access point
2. ir a redes inalámbricas, seguridad, o a la pestaña de encriptación o sección
3. seleccionar el botón de radio o revisar el cuadro de habilitar WEP o habilitar encriptación o configurar WEP
4. seleccionar la casilla o presionar el menú para la apropiada longitud de la llave WEP (WEP Key) para la red

Se recomienda la llave de 128 bits si es que el equipo de la red puede soportar la configuración

5. después se puede crear una propia llave si se desea (es preferible que el programa haga una propia)
6. escribe una frase de pase (pass phrase) dentro del cuadro (pass phrase)
7. se da clic en el botón generar llaves

Se puede observar en la siguiente figura 5.1 como debe de verse la ventana de configuración.



Figura 5.1

Se debe recordar la frase de pase (pass phrase) si es que se quiere volver a configurar una computadora a este Access point. Algunos Access point no muestran la contraseña.

8. para finalizar se da clic en OK para cerrar la configuración de WEP.

Con esto esta configurada la seguridad de la red inalámbrica.

## Seguridad Radius

Un servidor RADIUS centraliza una base de datos de usuarios y passwords y espera que equipos como Access Server le pregunten si cierto usuario con cierto password tiene acceso. El servidor RADIUS recibe no solo usuario y password sino una multitud de atributos, como el puerto del Access Server a donde el usuario se esta conectando y su numero de teléfono, y debe responder por si o por no si se le permite al usuario conectarse, junto con una serie de atributos que pueden ir desde la dirección IP a asignarle al usuario, protocolos a utilizar o reglas de filtrado de paquetes.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red) *sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS.*

*El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.*

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

Un servidor RADIUS puede realizar consultas en una base de datos de autenticación local si ello es adecuado para el escenario. O bien, la solicitud puede transmitirse a otro servidor para su validación. Cuando RADIUS decide que se puede autorizar el equipo en esta red, vuelve a enviar el mensaje al punto de acceso y éste permite que el tráfico de datos fluya hacia la misma.

**Ejemplo:**

- Cuando un usuario enciende su equipo portátil y activa su WLAN, con tarjeta 802.11, en un aeropuerto.
- El equipo portátil detecta la existencia de redes inalámbricas disponibles, elige la óptima y se asocia a ella.
- El equipo envía las credenciales de usuario al punto de acceso para verificar que tiene permiso en esta red.

- El usuario es manuel@shura.com. Shura ha adquirido acceso inalámbrico para todos sus usuarios en todos los aeropuertos del mundo.
- El servidor RADIUS, que recibe la solicitud desde el punto de acceso, comprueba el paquete y descubre que procede de un usuario de Shura.
- RADIUS pide a un servidor de shura que determine si esta persona (manuel) es un usuario real y si le conceden acceso.
- Si el servidor de Shura responde afirmativamente, se indica al punto de acceso que permita el flujo del tráfico.

Microsoft incluye una implementación del cliente 802.1X en Windows XP y mejora el servidor RADIUS de Windows, el servidor de autenticación de Internet (IAS), para admitir la autenticación de dispositivos inalámbricos.

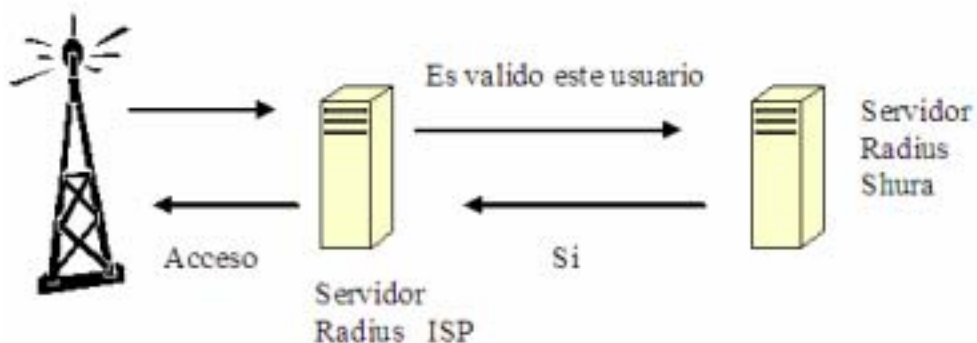


Figura 5.2 Acceso Publico

## CAPITULO VI

### CONFIGURANDO EL SERVIDOR

#### Introducción

En este capítulo se explicará cómo se debe instalar las utilidades, dispositivos y cómo configurar los mismos para el funcionamiento del servidor. Es muy importante tener a la mano el disco del servidor en este caso Windows 2003 ya que en algunos campos de la configuración e instalación se requerirá de él para la instalación de los mismos.

Nota: Las imágenes que se presentan en este capítulo son para el caso de la Universidad Americana de Acapulco, así que en los campos de las imágenes se explicará profesionalmente lo que representa y representará para dicha configuración en futuras configuraciones del servidor.

#### 1.- Ejecutar el DCPROMO (convertir en un dominio independiente)

Dependiendo del idioma del sistema operativo:

Inicio (start), ejecutar (run), dcpromo. Siguiendo las pantallas se configurará lo necesario para realizarlo.









**Active Directory Installation Wizard**

**New Domain Name**  
Specify a name for the new domain.

Type the full DNS name for the new domain  
(for example: headquarters.example.microsoft.com).

Full DNS name for new domain:  
wifiserver.net

< Back   Next >   Cancel

**Active Directory Installation Wizard**

**NetBIOS Domain Name**  
Specify a NetBIOS name for the new domain.

This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.

Domain NetBIOS name: wifiserver

< Back   Next >   Cancel

**Active Directory Installation Wizard**

**Database and Log Folders**  
Specify the folders to contain the Active Directory database and log files.

For best performance and recoverability, store the database and the log on separate hard disks.

Where do you want to store the Active Directory database?

Database folder:

Where do you want to store the Active Directory log?

Log folder:

**Active Directory Installation Wizard**

**Shared System Volume**  
Specify the folder to be shared as the system volume.

The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.

The SYSVOL folder must be located on an NTFS volume.

Enter a location for the SYSVOL folder.

Folder location:



**Active Directory Installation Wizard**

**Directory Services Restore Mode Administrator Password**  
 This password is used when you start the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.  
 The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

Restore Mode Password:

Confirm password:

For more information about Directory Services Restore Mode, see [Active Directory Help](#).

< Back   Next >   Cancel

En esta ventana se ingresa un clave si el administrador de la red así lo desea.

**Active Directory Installation Wizard**

**Summary**  
 Review and confirm the options you selected.

You chose to:

Configure this server as the first domain controller in a new forest of domain trees.

The new domain name is wif.server.net. This is also the name of the new forest.

The NetBIOS name of the domain is WIFISERVER

Database folder: C:\WINDOWS\NTDS  
 Log file folder: C:\WINDOWS\NTDS  
 SYSVOL folder: C:\WINDOWS\SYSVOL

The password of the new domain administrator will be the same as the password of the administrator of this computer.

To change an option, click Back. To begin the operation, click Next.

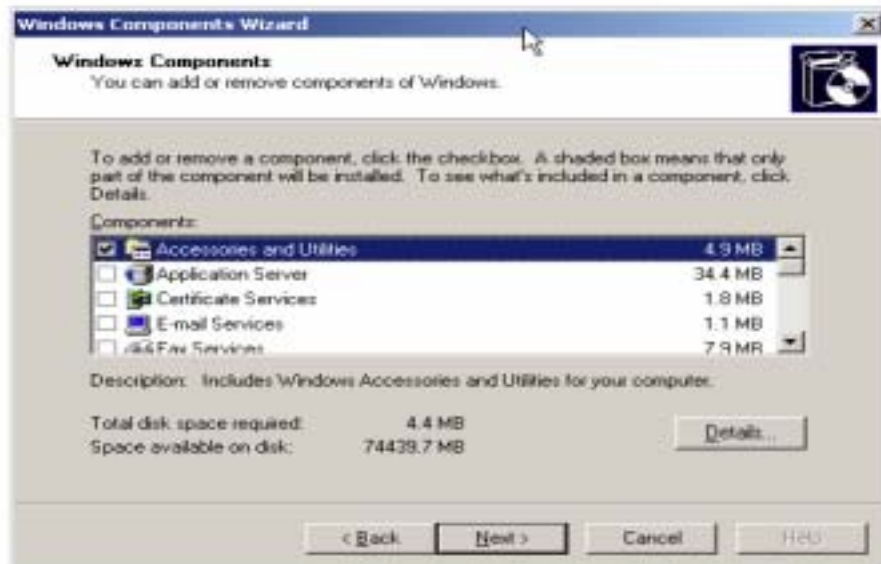
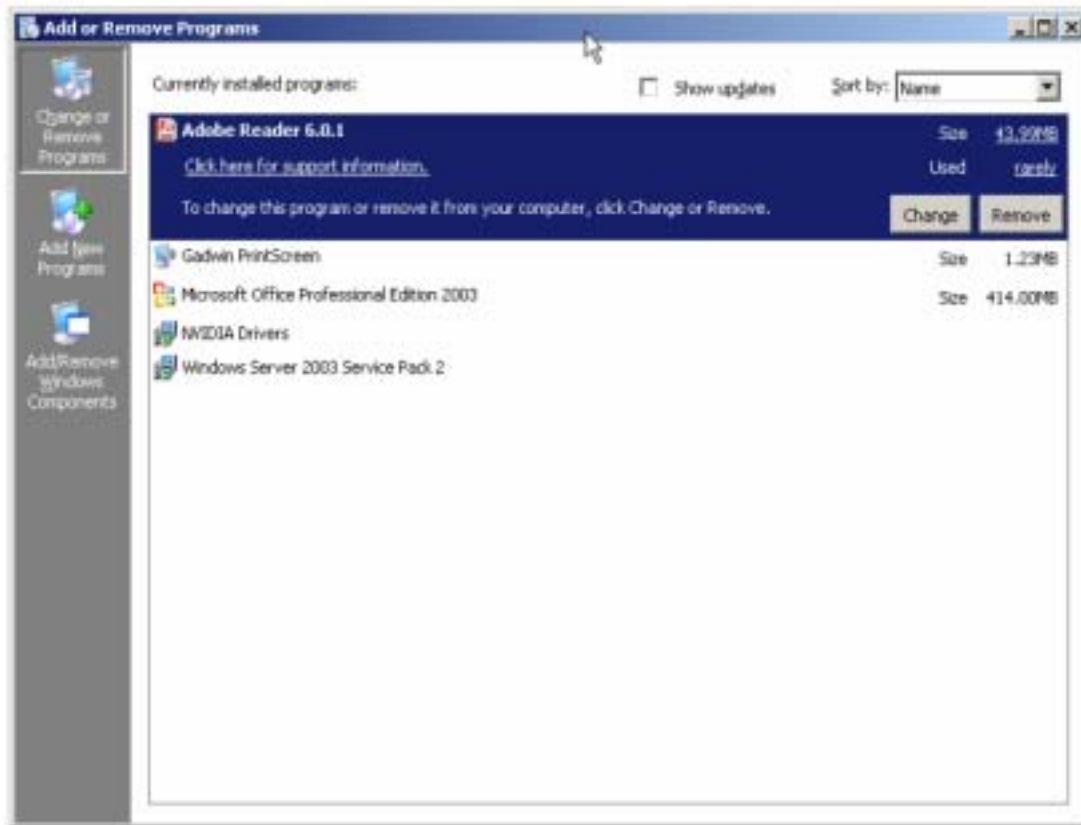
< Back   Next >   Cancel



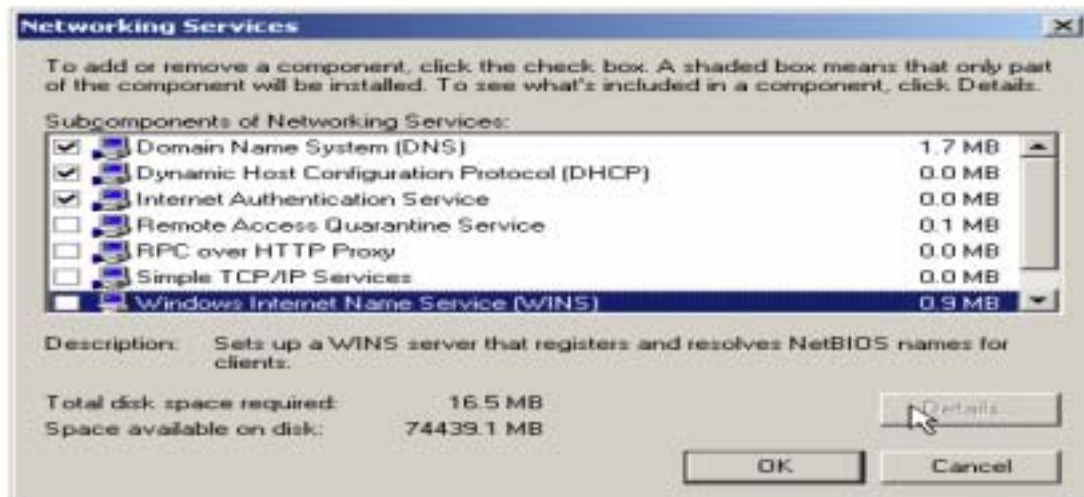
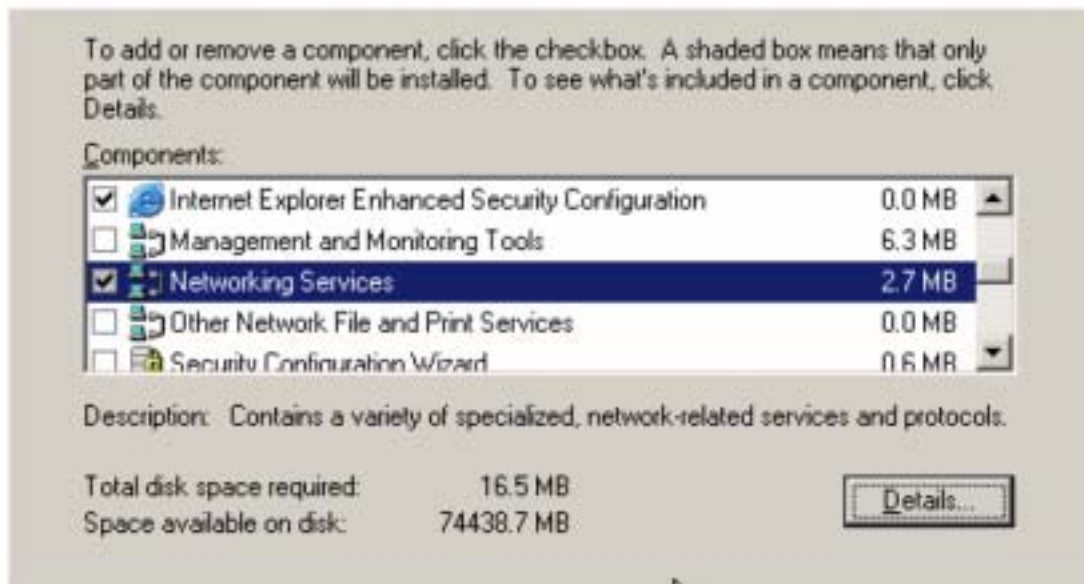
En esta parte finaliza la instalación y es necesario reiniciar para que queden establecidas las configuraciones.

## 2.- Instalar las utilerías (DHCP, DNS, IAS, IIS, CA, RRA)

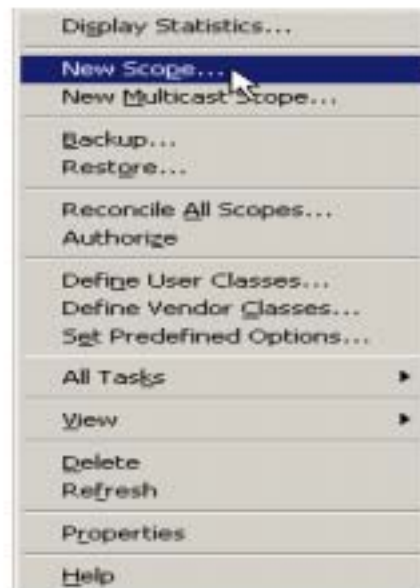
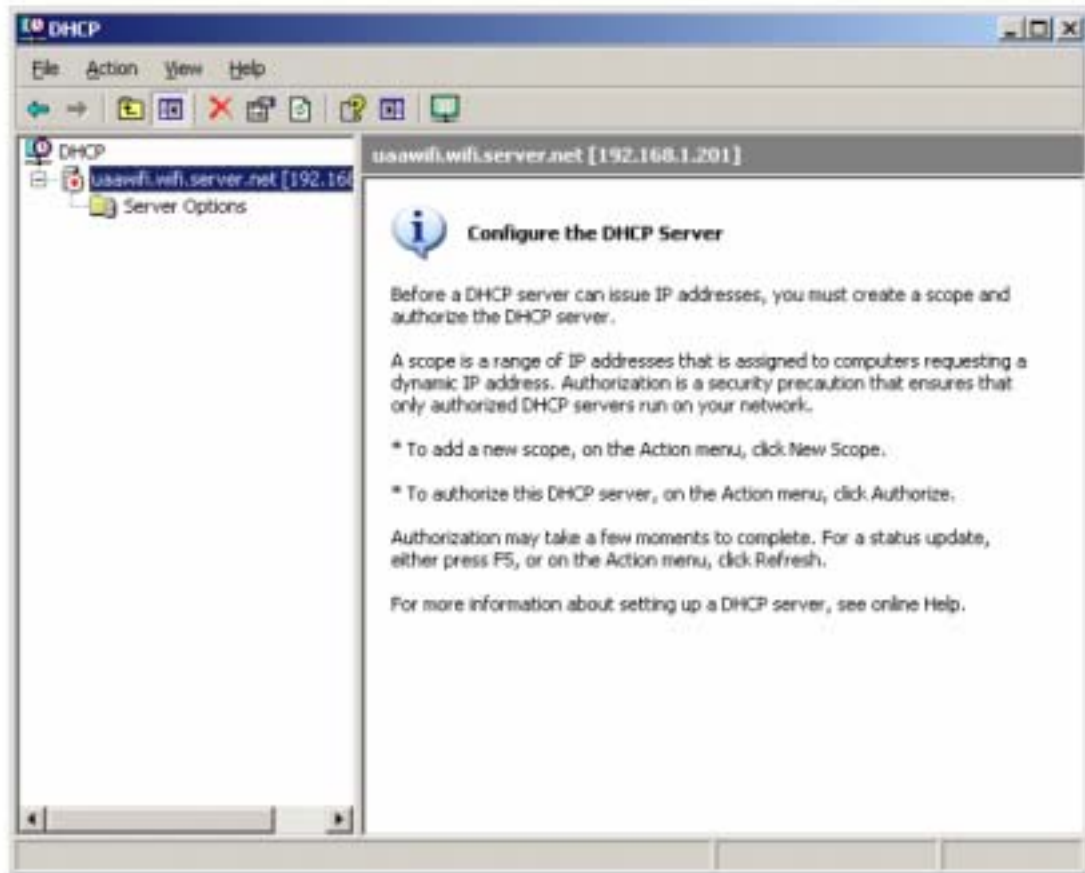


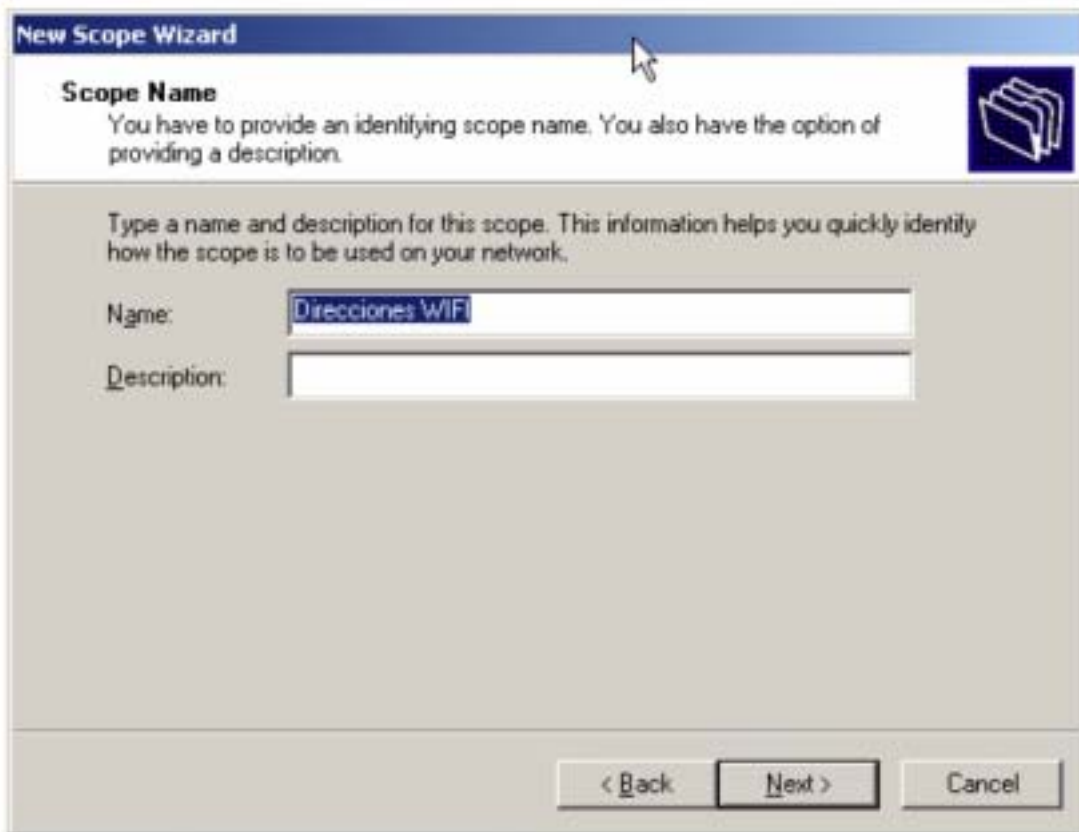






### 3.- Configurar DHCP





**New Scope Wizard**

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length:

Subnet mask:

< Back   Next >   Cancel

En esta imagen se aprecian los rangos de las direcciones IP, de donde deben iniciar hasta donde finalizan. Algunos campos vacíos muestran que están por default.

**New Scope Wizard**

**Add Exclusions**  
Exclusions are addresses or a range of addresses that are not distributed by the server.

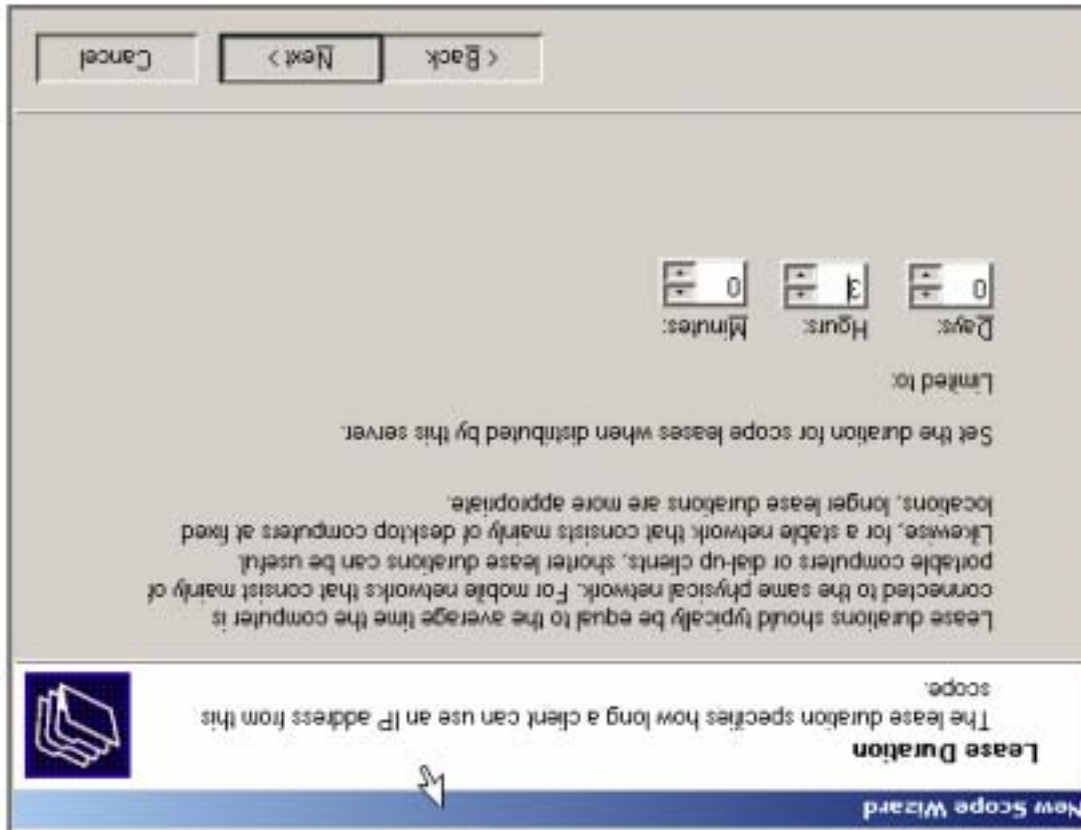
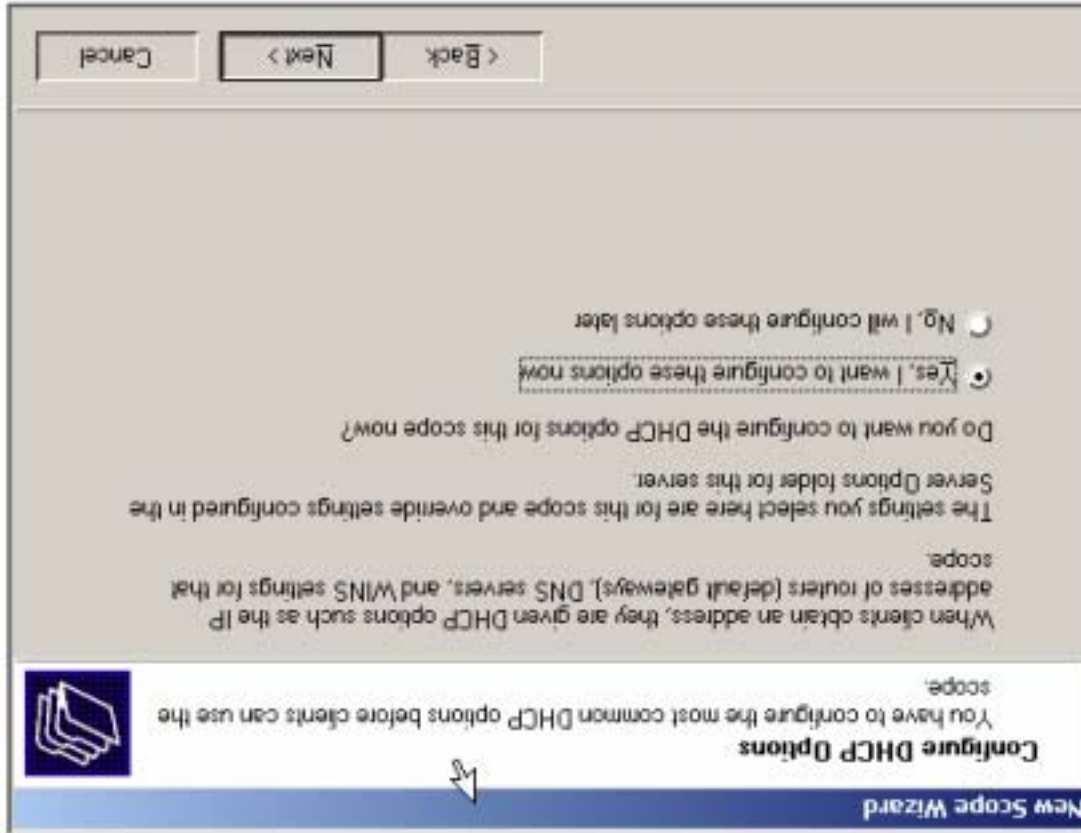
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:    End IP address:    Add

Excluded address range:

Remove

< Back   Next >   Cancel



**New Scope Wizard**

**Router (Default Gateway)**  
 You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

**New Scope Wizard**

**Domain Name and DNS Servers**  
 The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

**New Scope Wizard**

**WINS Servers**  
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:  IP address:

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

**New Scope Wizard**

**Activate Scope**  
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

Yes, I want to activate this scope now

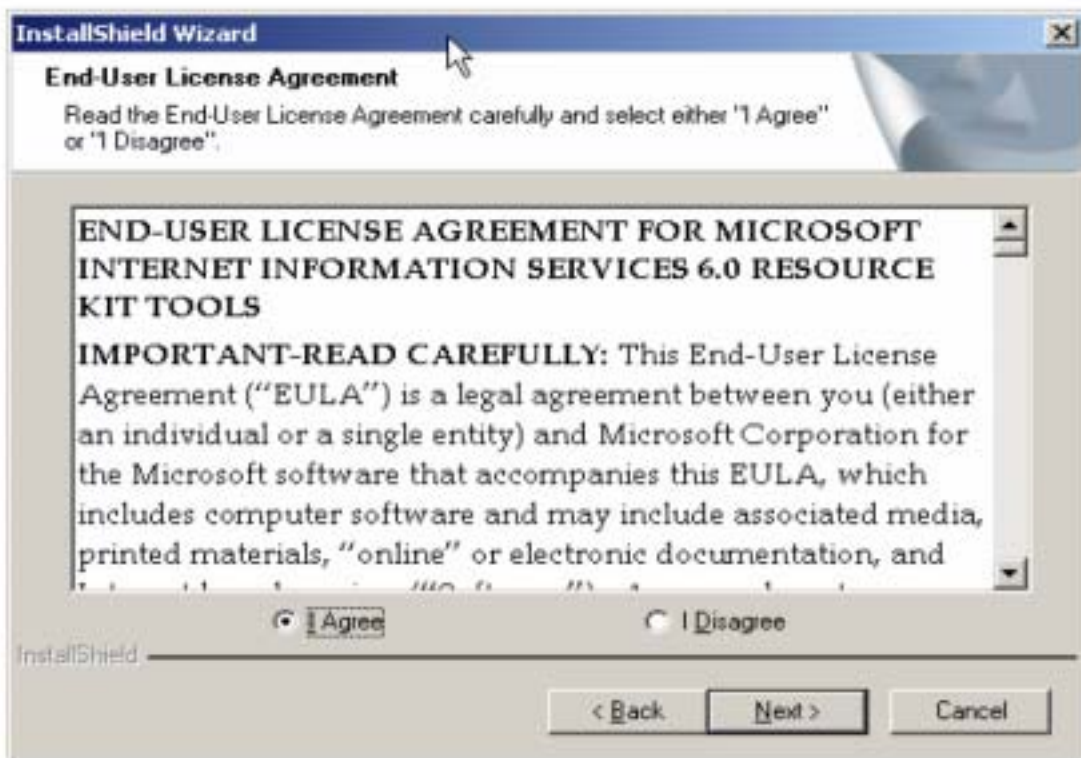
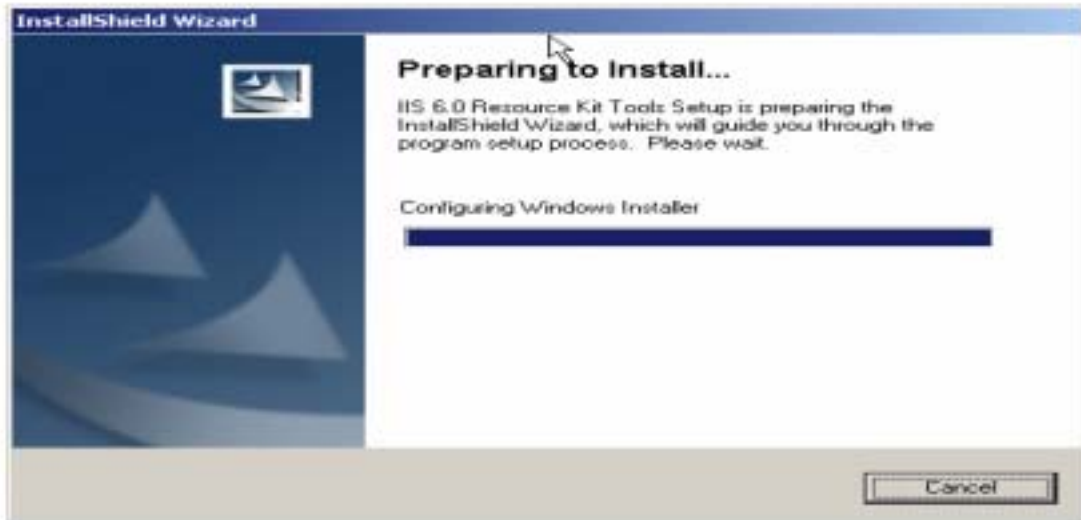
No, I will activate this scope later

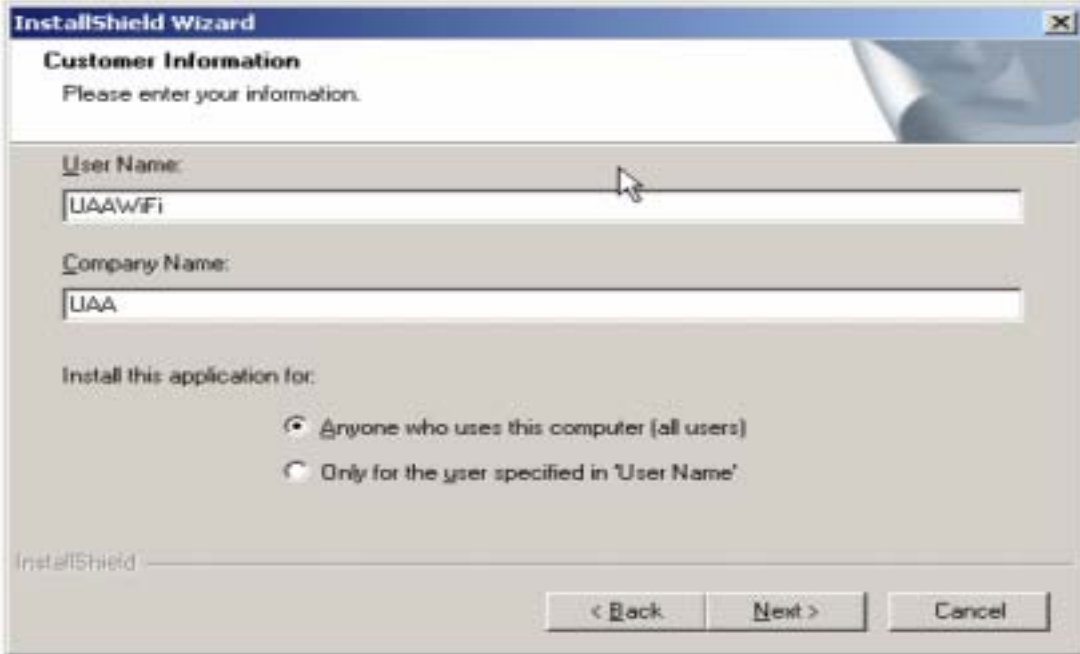




#### 4.- Configurar Certificado Servidor y Cliente Certificado Servidor

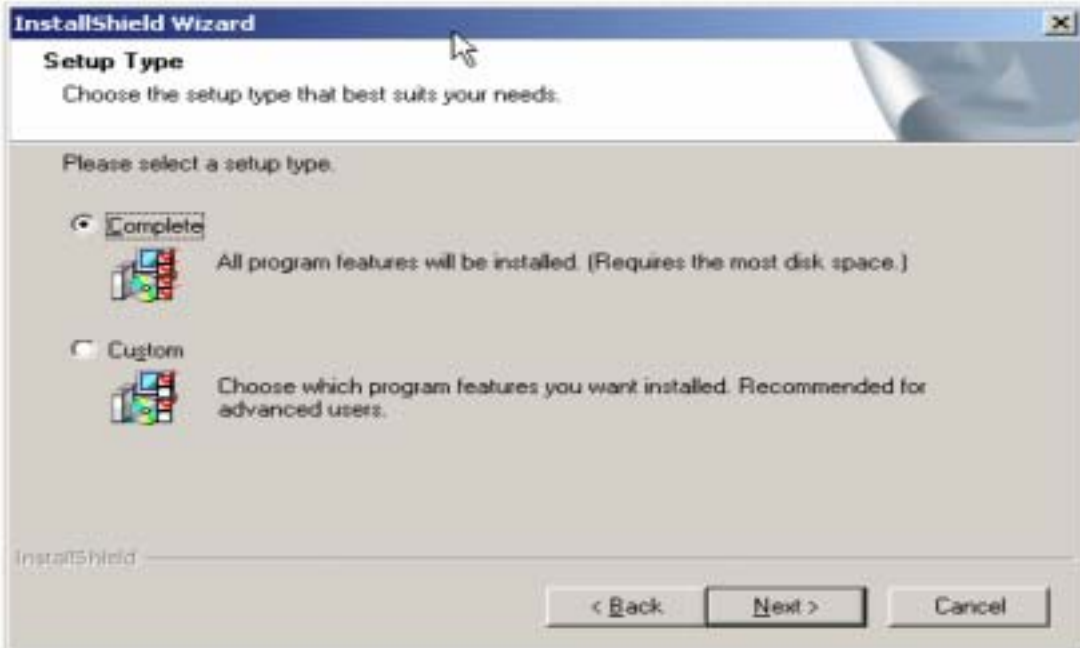
En el proceso de esta instalación, se refiere a la instalación de un programa que se necesita para dicha configuración, es el Microsoft IIS 6.0 Resources Kit.



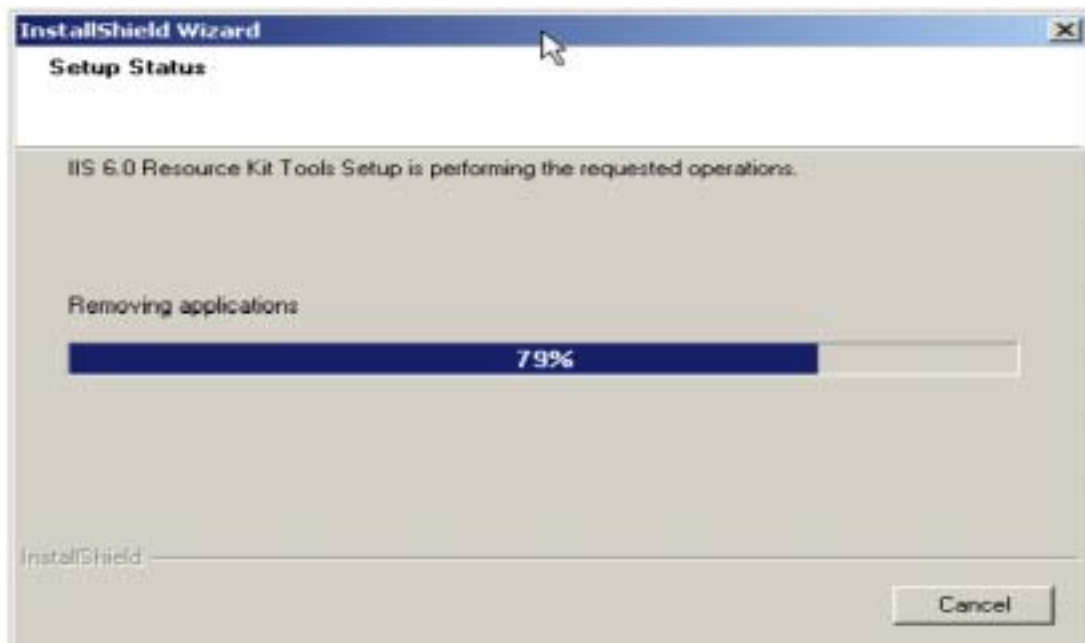
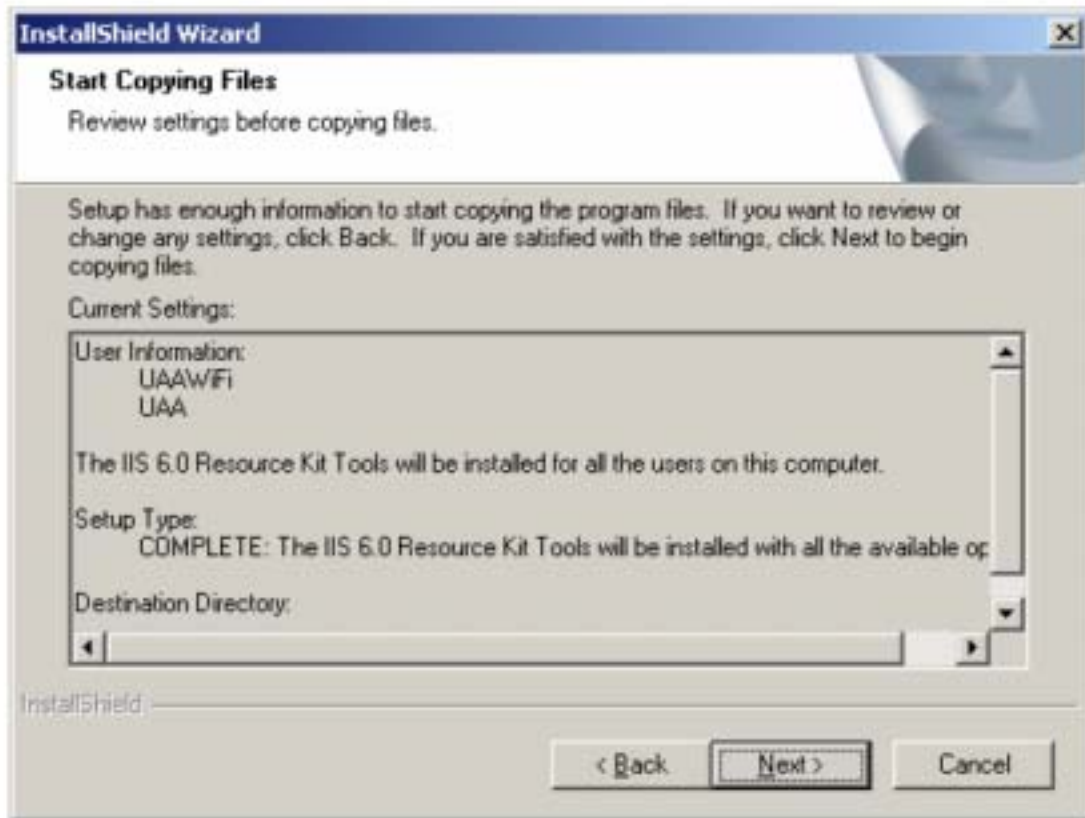


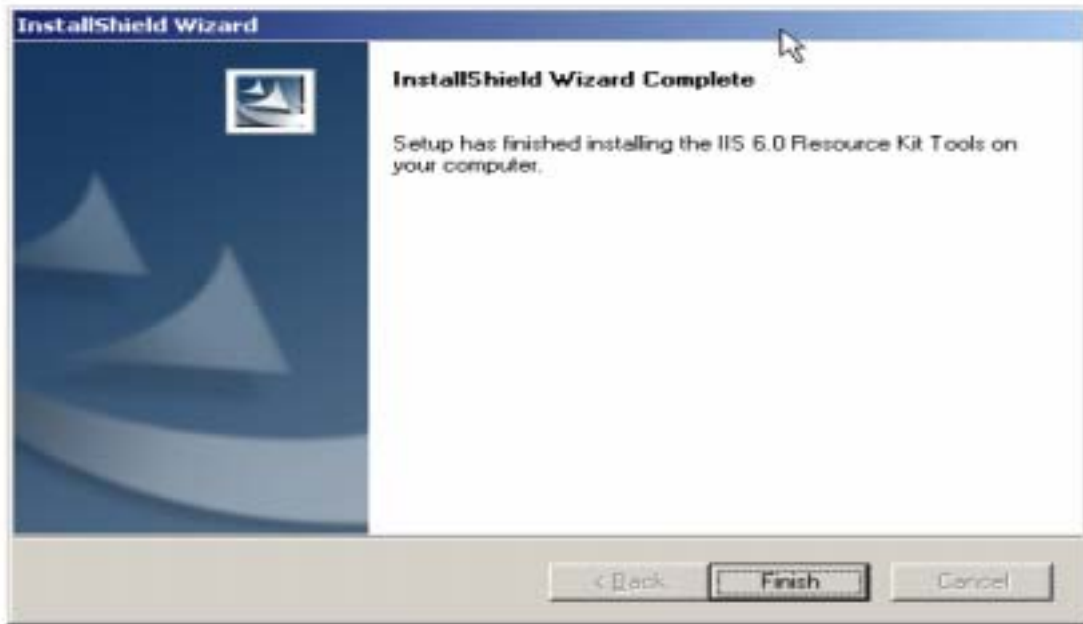
The screenshot shows the 'InstallShield Wizard' window with the 'Customer Information' tab selected. The window title is 'InstallShield Wizard'. Below the title bar, the text reads 'Customer Information' and 'Please enter your information.' There are two text input fields: 'User Name:' containing 'UAAWiFi' and 'Company Name:' containing 'UAA'. Below these fields, the text says 'Install this application for:' followed by two radio button options: 'Anyone who uses this computer (all users)' (which is selected) and 'Only for the user specified in 'User Name''. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

En el campo de esta imagen se le agrega un nombre para agregar información a los campos siguientes. En este caso será UAAWiFi.



The screenshot shows the 'InstallShield Wizard' window with the 'Setup Type' tab selected. The window title is 'InstallShield Wizard'. Below the title bar, the text reads 'Setup Type' and 'Choose the setup type that best suits your needs.' There is a prompt: 'Please select a setup type.' Below this, there are two radio button options: 'Complete' (which is selected) and 'Custom'. The 'Complete' option is accompanied by a small icon of a computer and the text 'All program features will be installed. (Requires the most disk space.)'. The 'Custom' option is also accompanied by a small icon of a computer and the text 'Choose which program features you want installed. Recommended for advanced users.' At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.





Al finalizar el asistente de instalación nos dirigimos a la ventana de comandos para ejecución de comandos para cambiar de directorios para la configuración de este asistente.



```

C:\WINDOWS\system32\CMD.exe - selfssl /N:C=usawifi.wifi.server.net /K:1024 /V:1825 /S:1 /P:443
Microsoft Windows [Version 5.2.3798]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>CD "C:\Program Files\IIS Resources\SelfSSL

C:\Program Files\IIS Resources\SelfSSL>selfssl /N:C=usawifi.wifi.server.net /K:1024 /V:1825 /S:1 /P:443
Microsoft (R) SelfSSL Version 1.0
Copyright (C) 2003 Microsoft Corporation. All rights reserved.

Do you want to replace the SSL settings for site 1 (Y/N)?y

```

En el caso de la imagen se muestra así, pero para otro tipo de configuración profesional se muestra:

La configuración siguiente muestra el cambio de directorio:

```
>CD "C:\Program Files\IIS Resources\SelfSSL
```

```
>selfssl /N:CN=nombreservidor.dominio.com /K:1024 /V:1825 /S:1 /P:443
```

Finaliza con el cambio de configuraciones del asistente, se debe decir que si (y).

**/N:CN** es el nombre del servidor y completamente el nombre del dominio calificado

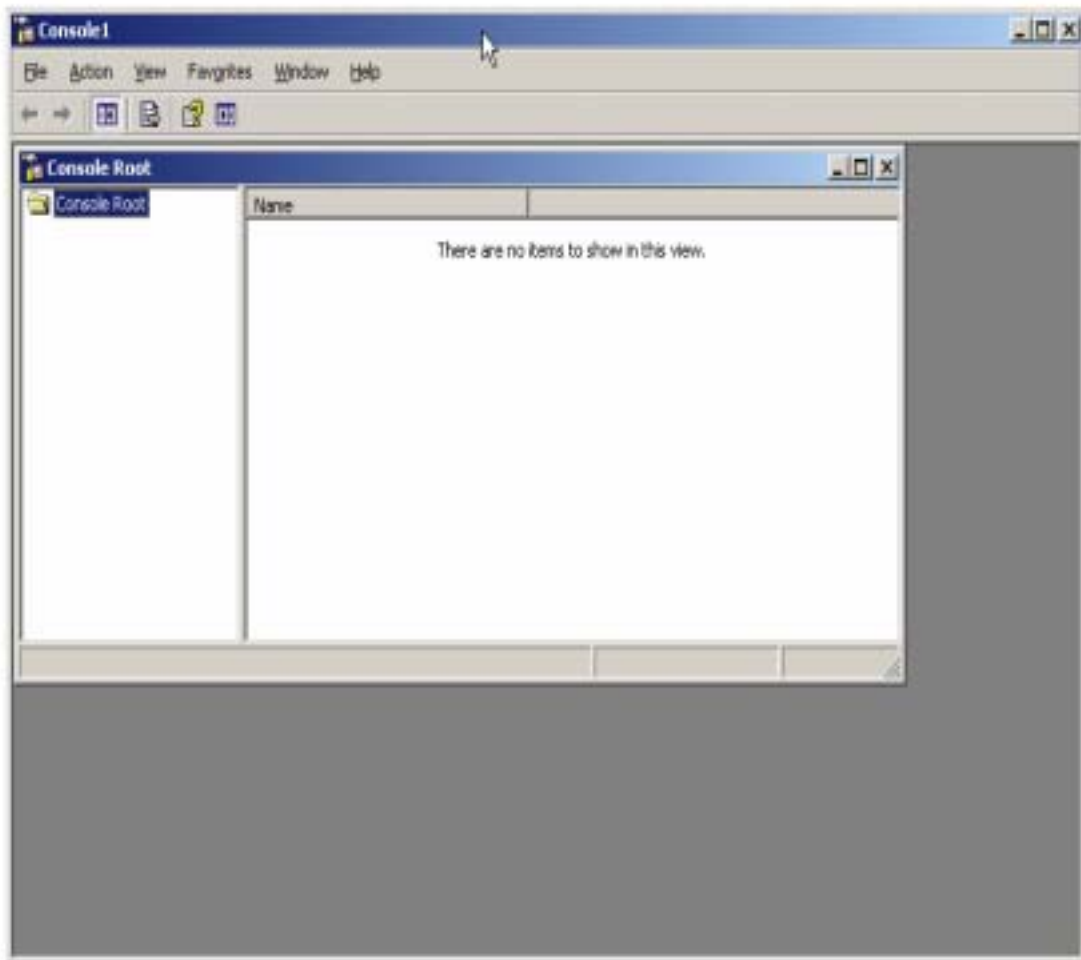
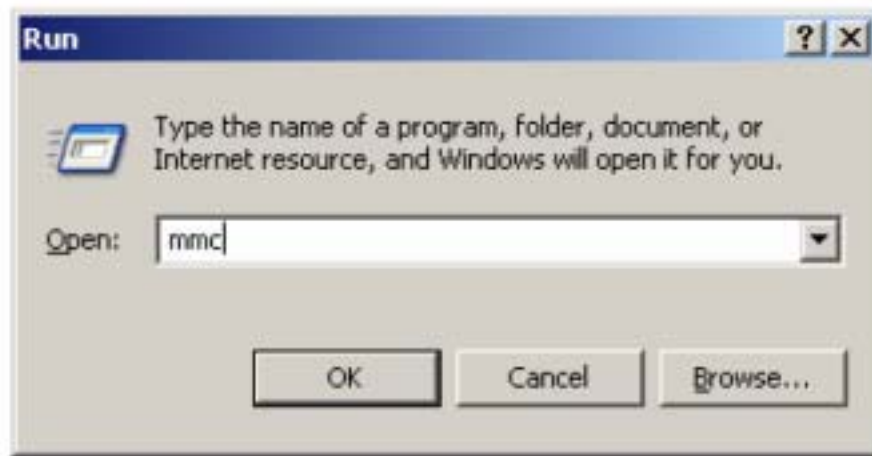
**/K** es el numero bits asignados para la RSA Key

**/V** es el numero de días para que el certificado expire 1825 días es igual a 5 años

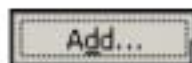
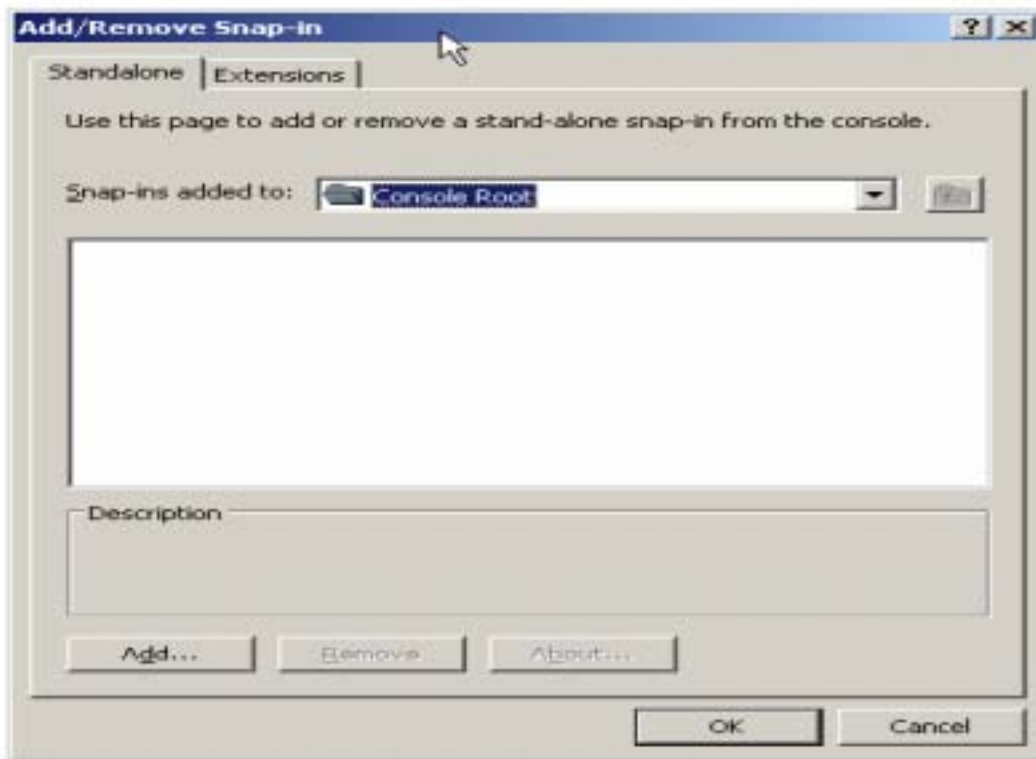
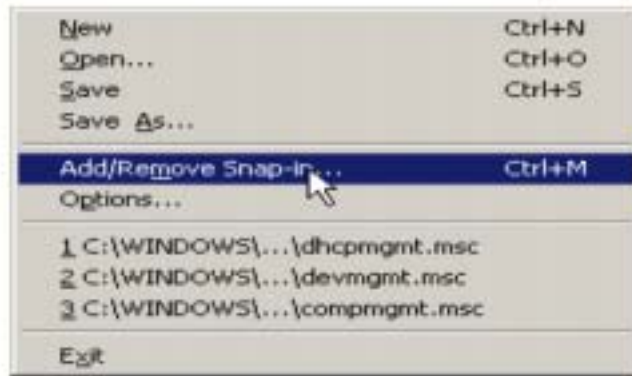
**/S** es el número del sitio del IIS

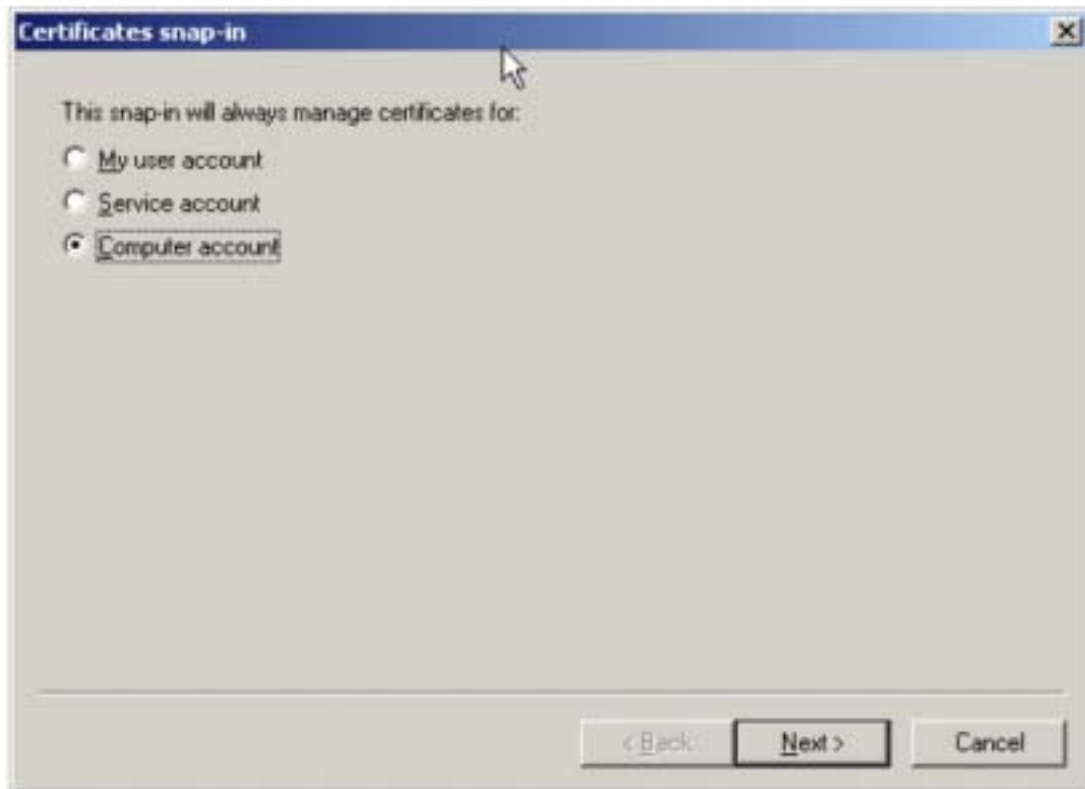
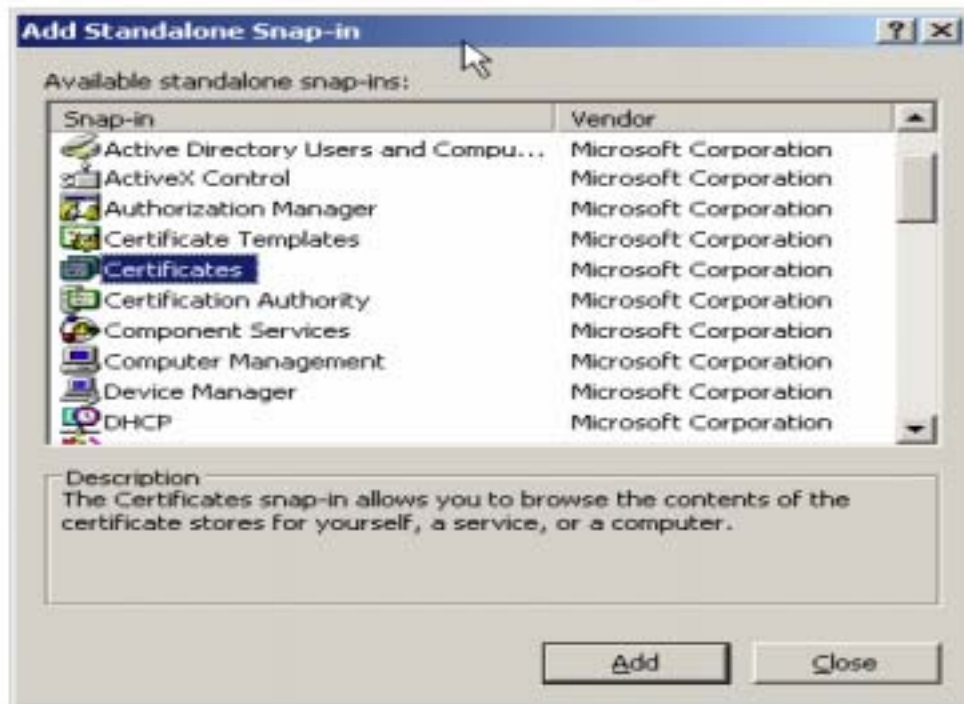
**/P** es el número del puerto TCP. 443 es el puerto estándar.

A continuación se configura la consola de certificados para la creación de un certificado para el usuario.

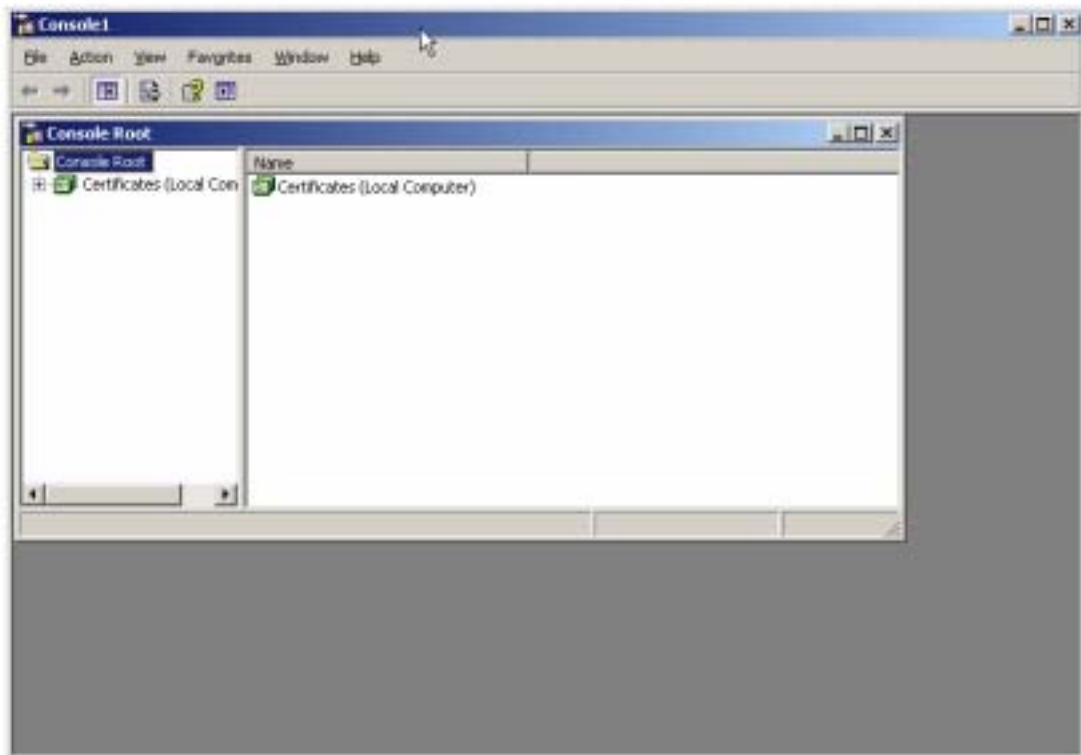
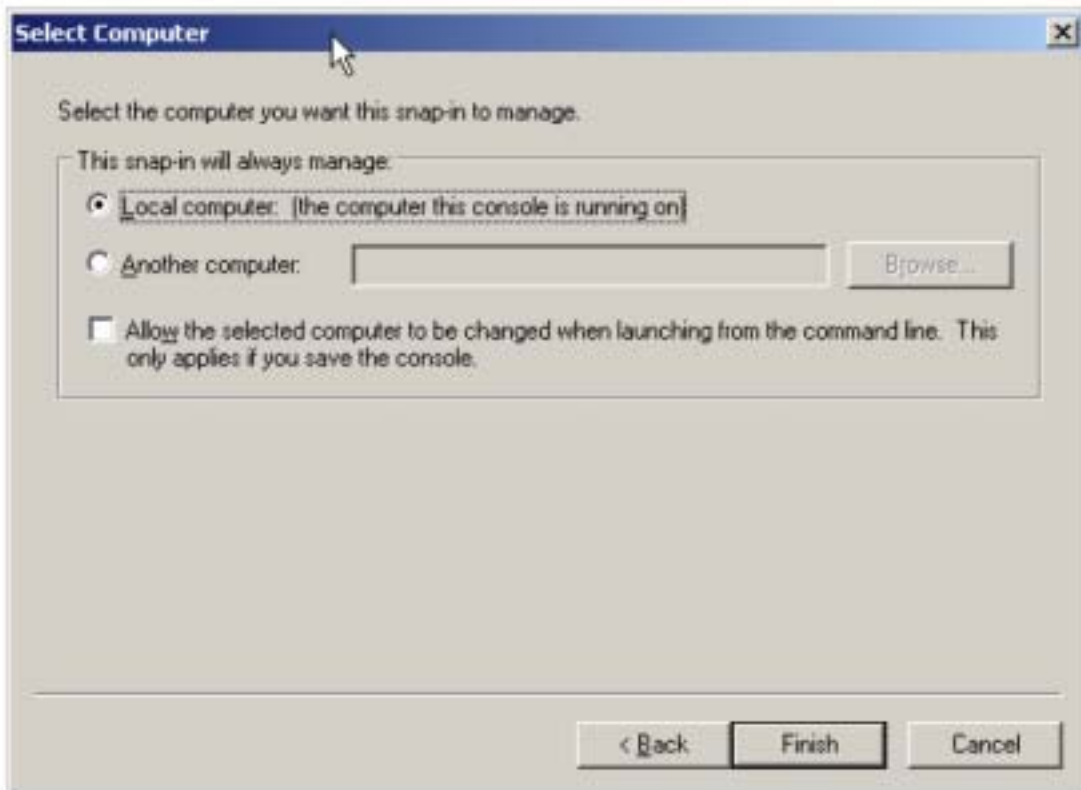


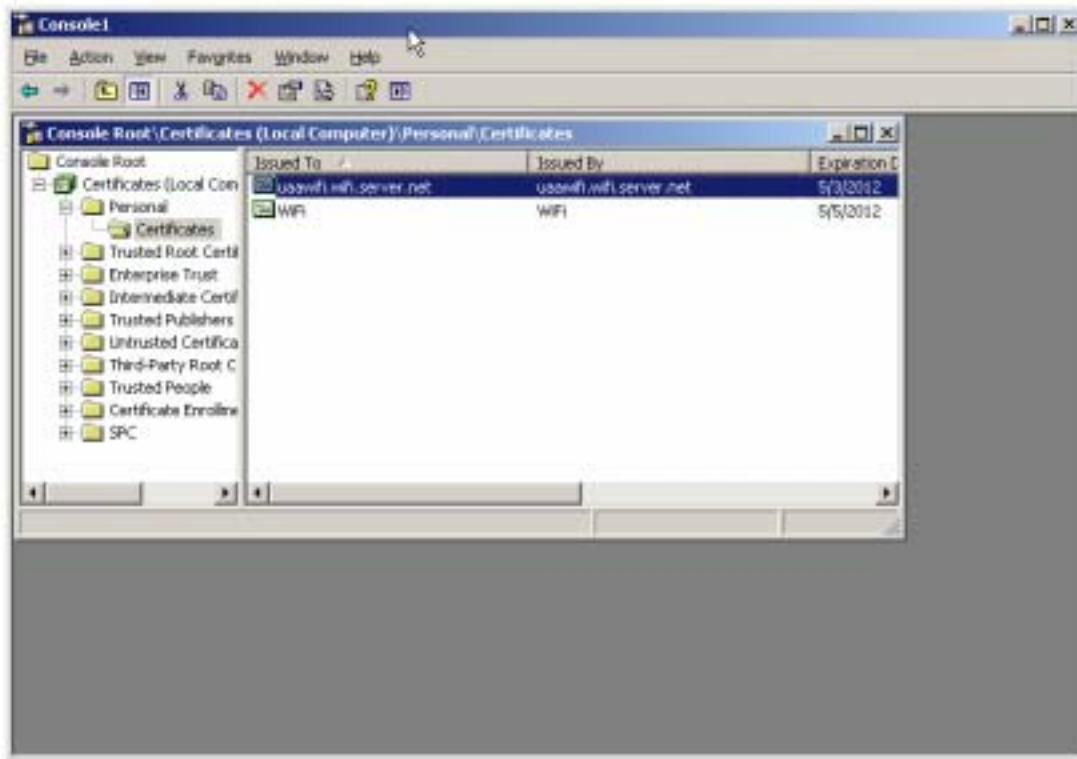
En el menú archivo se agregan los complementos para crear el certificado del cliente.



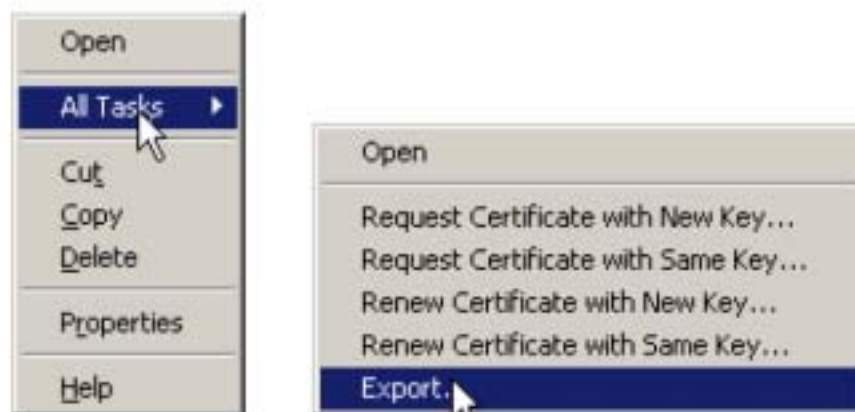




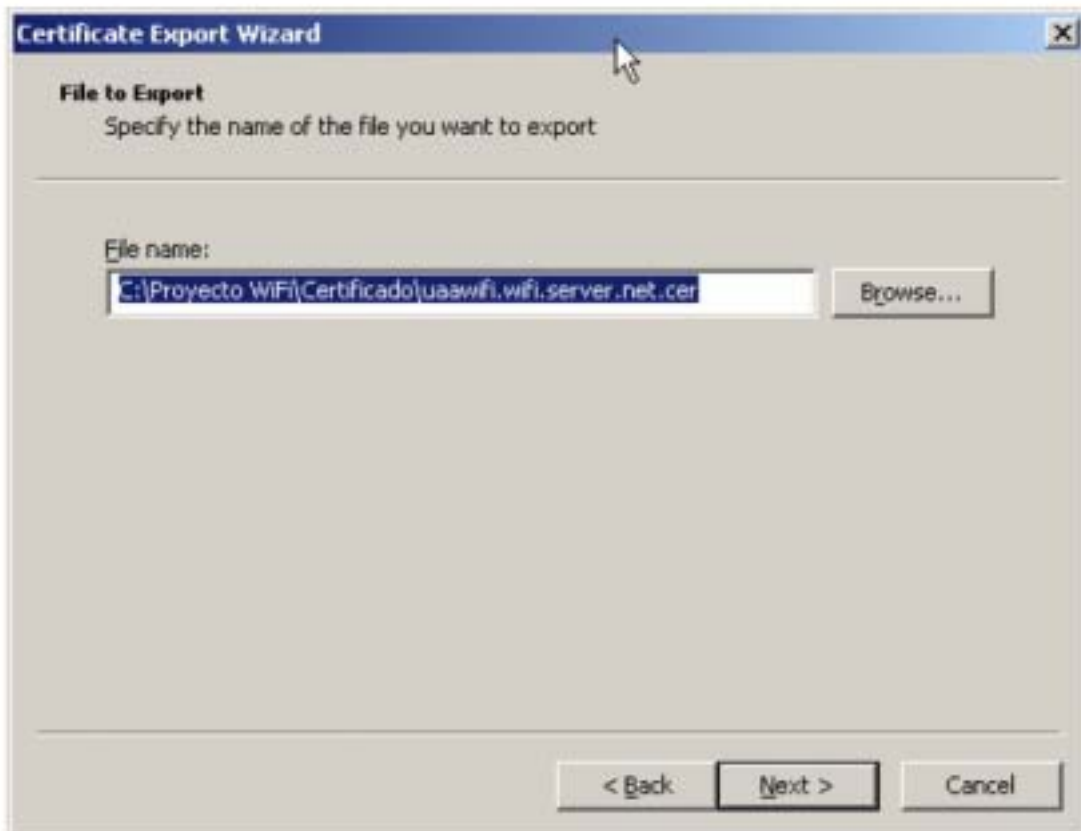
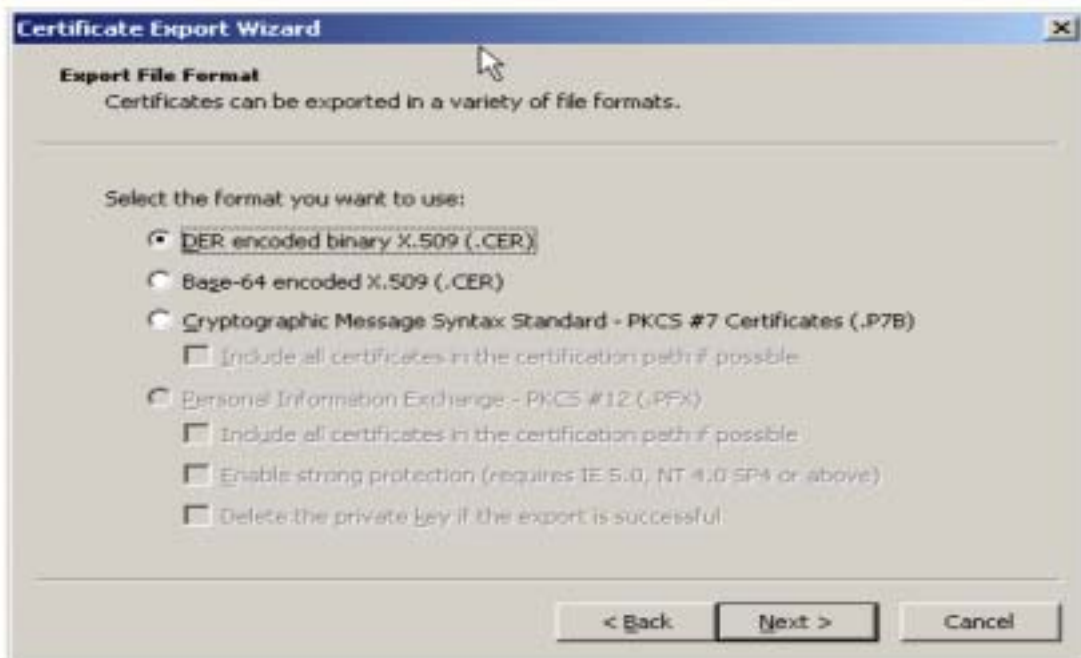




Al final se podrá apreciar el certificado para el cliente y posteriormente exportarlo en el servidor y quede guardado y finalmente importarlo en la computadoras cliente.



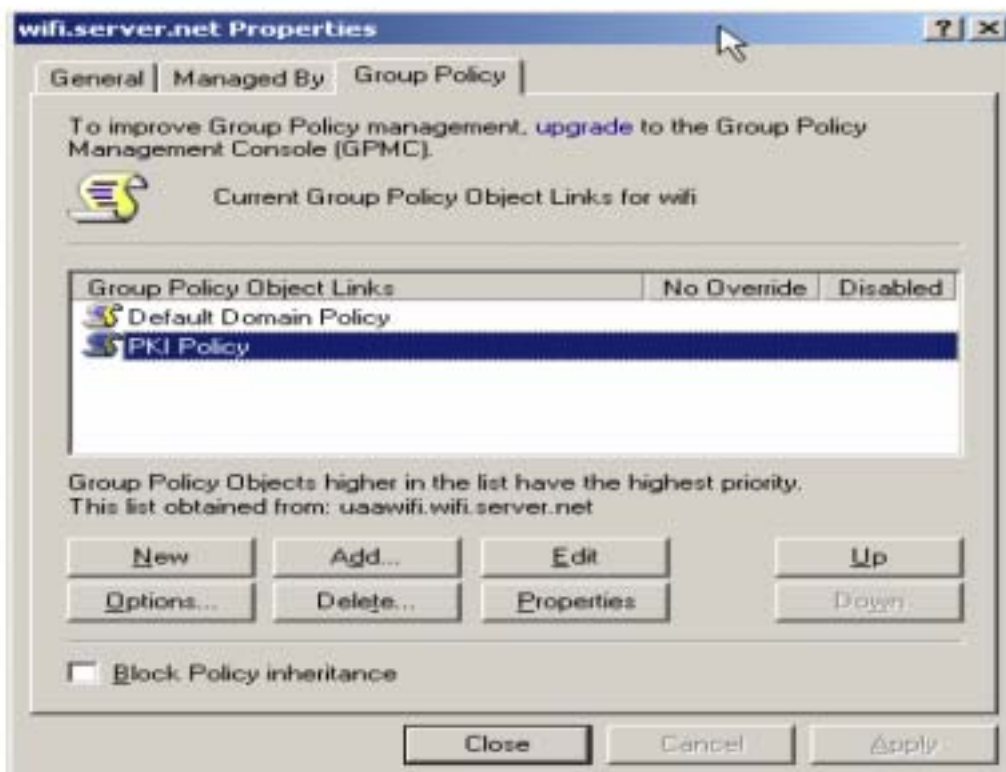
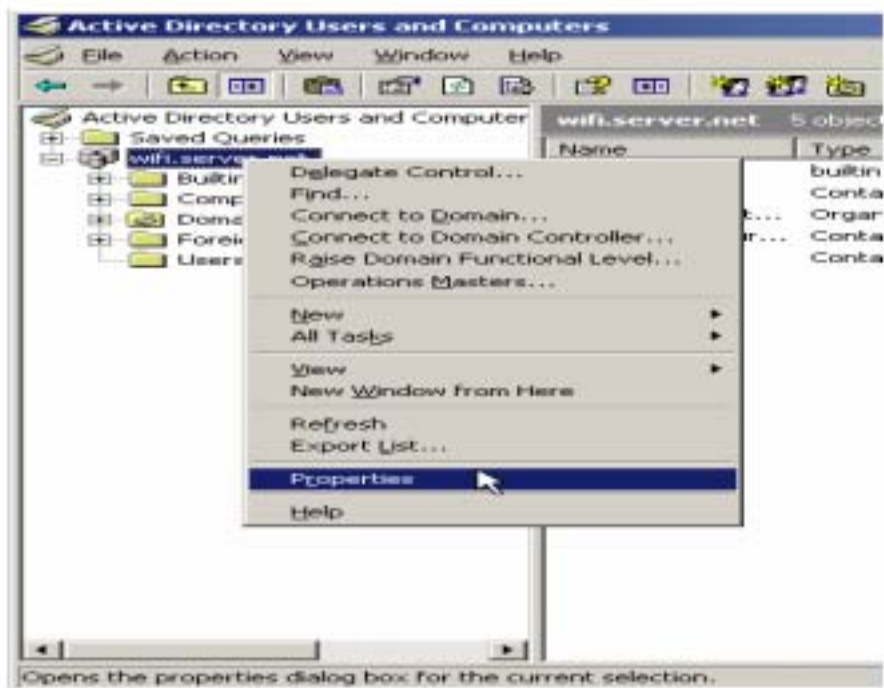




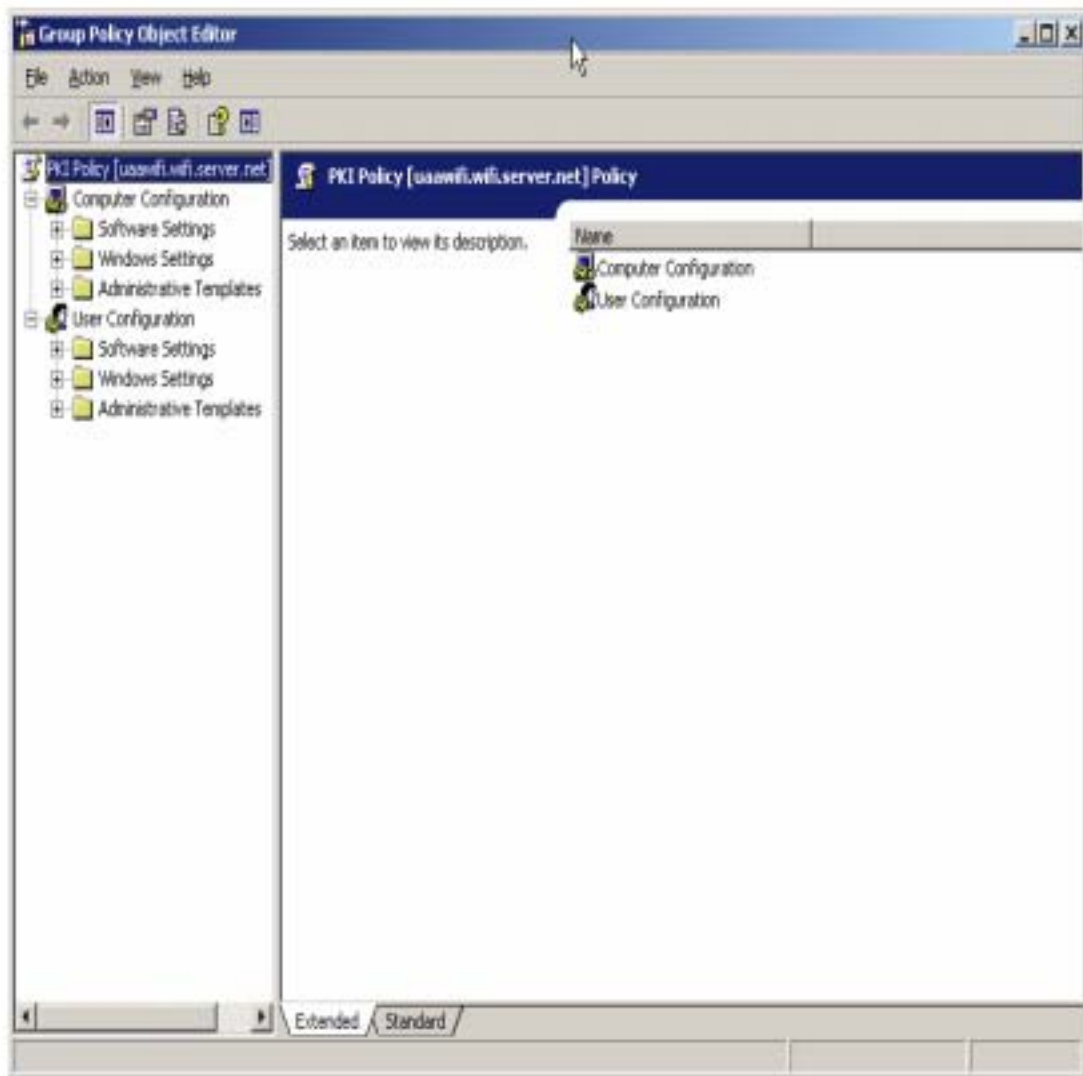
En esta imagen se aprecia el directorio de donde se guardara dicho certificado cliente para después proporcionarlo a las computadoras cliente.

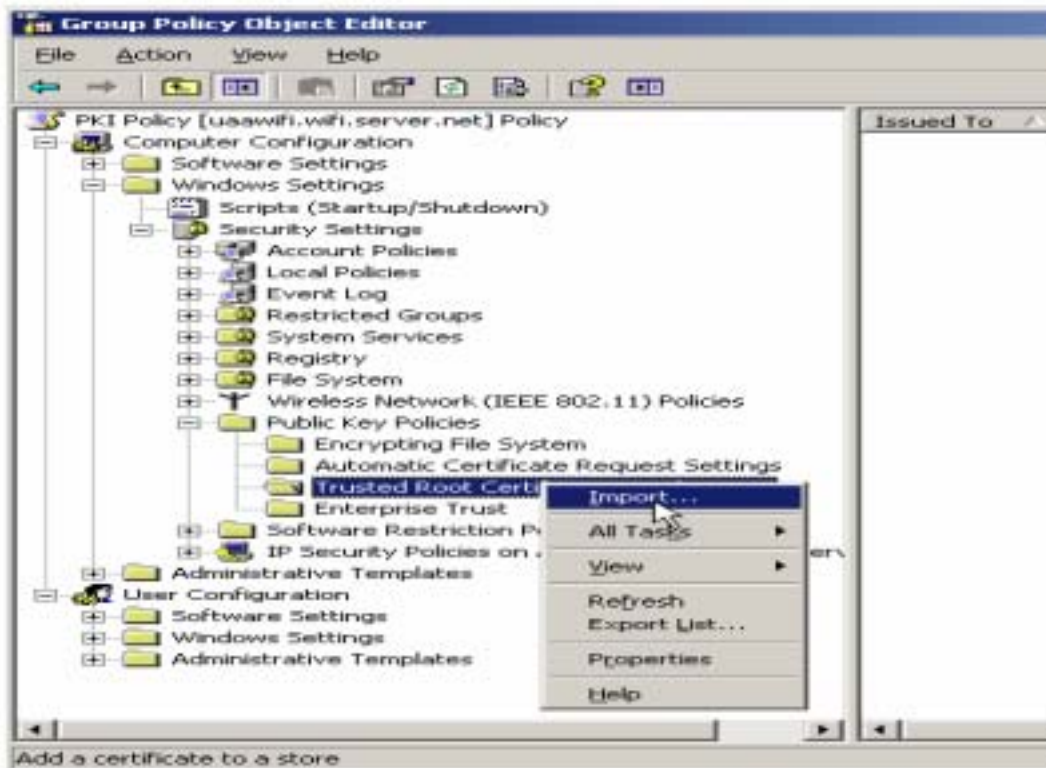


## Configurar el Directorio Activo de Computadoras y Usuarios (Active Directory Users and Computers)



En el botón edit se configuran las siguientes políticas:





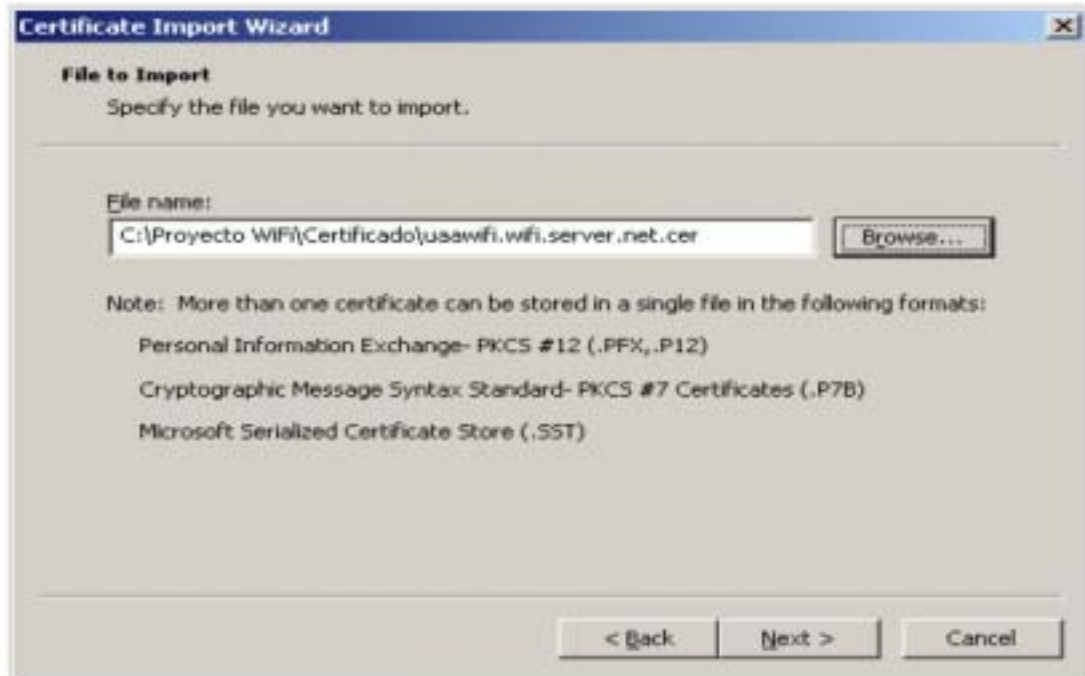
Esta imagen muestra como se importa el certificado para la edición de políticas que la relacionan para el acceso de computadoras clientes con el servidor.

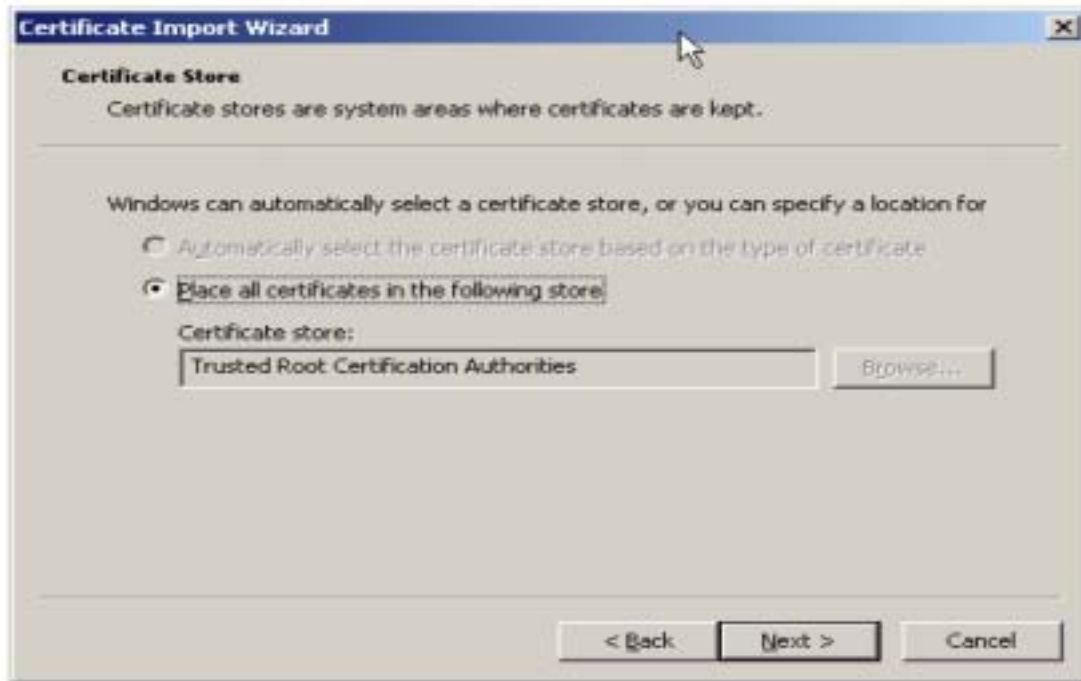






Se busca la ubicación del certificado en el directorio en el cual fue guardado para realizar la importación del mismo.





## Instalación del Certificado Cliente







## 5.- Configurar Access Point

La configuración es muy sencilla, se abre el explorador de Internet y se le da la IP y la clave que viene por default, o si lo prefiere configurarlo con su propio disco de instalación y así asignar las direcciones que sean necesarias para su uso. En este caso veamos las siguientes imágenes:



|                   |     |   |     |   |     |   |     |
|-------------------|-----|---|-----|---|-----|---|-----|
| IP Address :      | 192 | . | 168 | . | 1   | . | 250 |
| Subnet Mask :     | 255 | . | 255 | . | 255 | . | 0   |
| Default Gateway : | 192 | . | 168 | . | 1   | . | 201 |


Mode:

Network Name (SSID):

Channel:

SSID Broadcast:

Current Encryption: WPA-Enterprise



Status: SES Inactive

---

| Setup                   | Wireless          | Administration      | Status |
|-------------------------|-------------------|---------------------|--------|
| Basic Wireless Settings | Wireless Security | Wireless MAC Filter |        |

Security Mode:

---

Encryption:

RADIUS Server:  .  .  .

RADIUS Port:

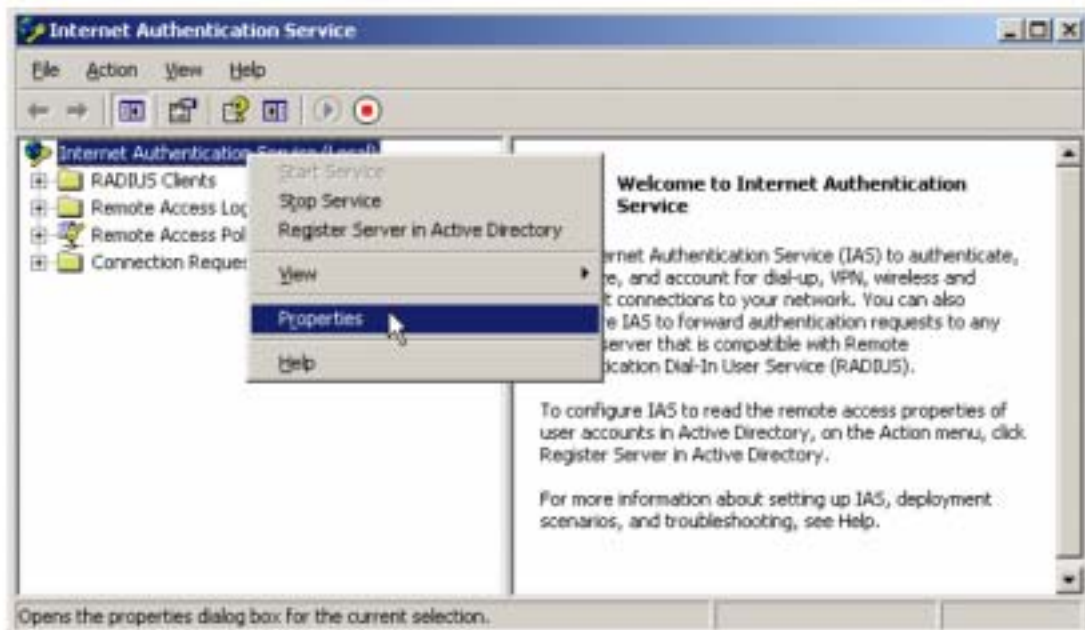
Shared Secret:

Key Renewal:  seconds

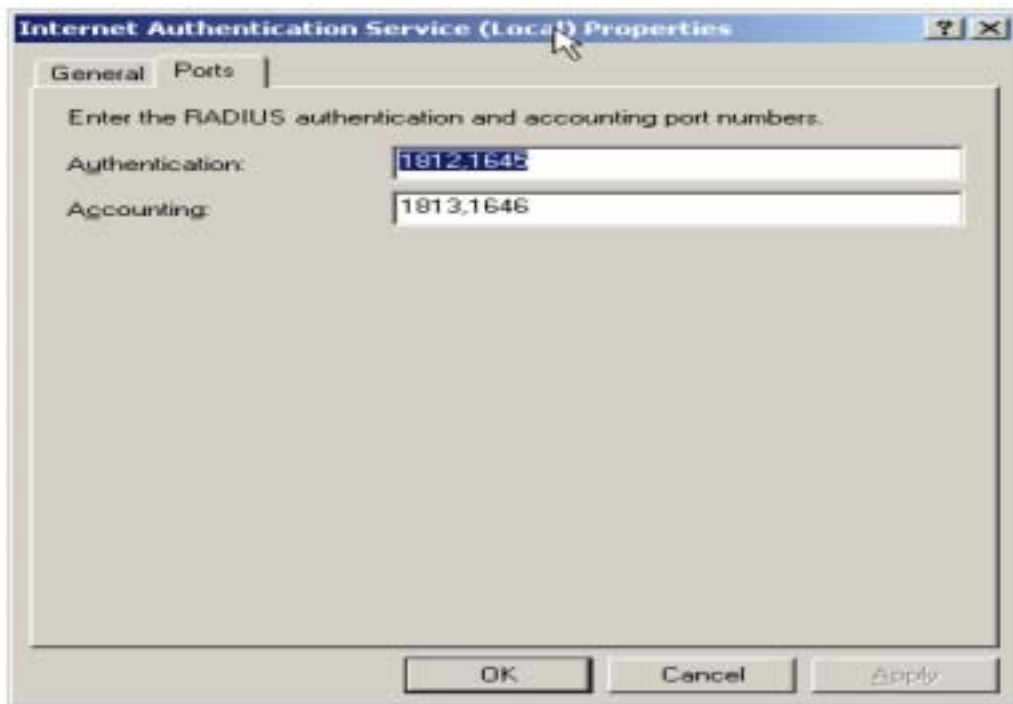
Al final se guardan las configuraciones (save settings).

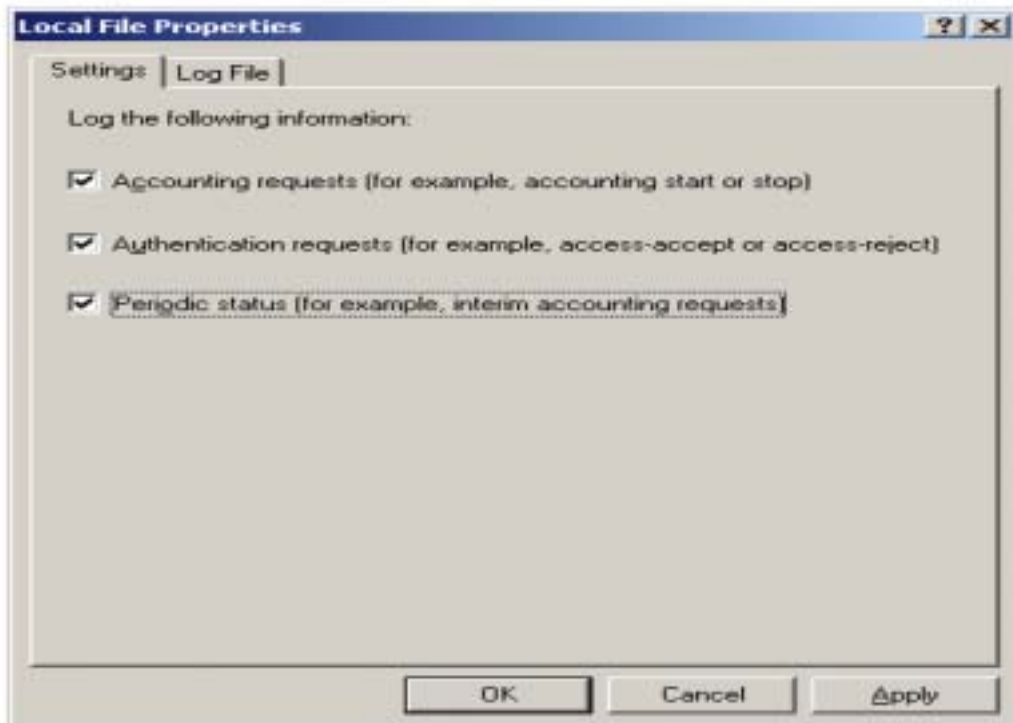
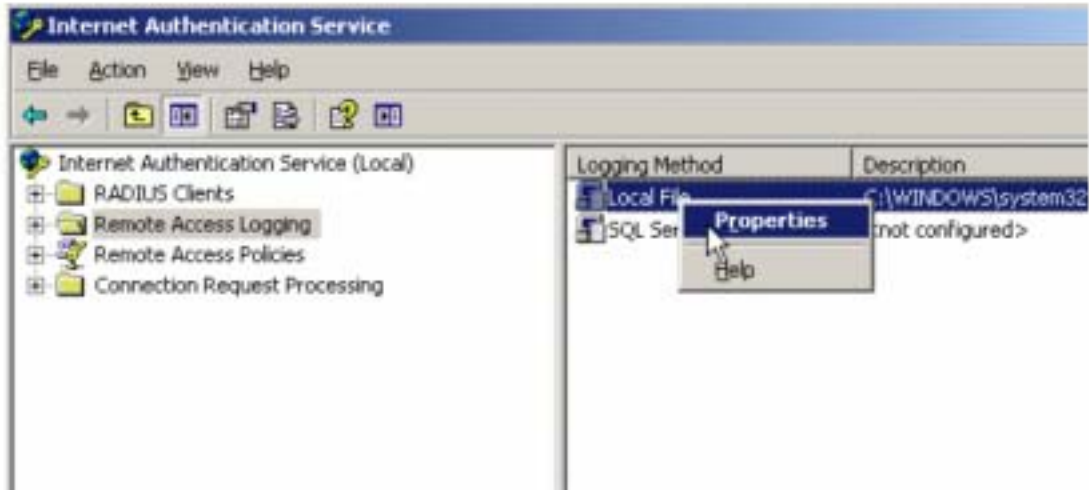
## 6.- Configurando el Radius

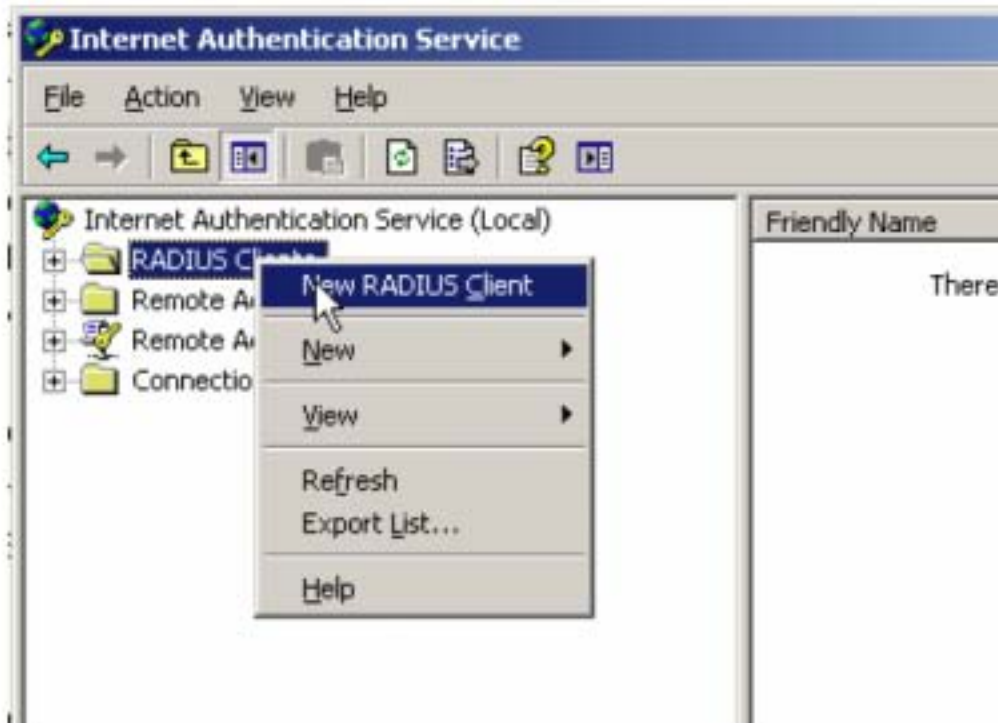
Se ejecuta el IAS (servicio de autenticación de Internet). Algunas configuraciones de dejan por default.



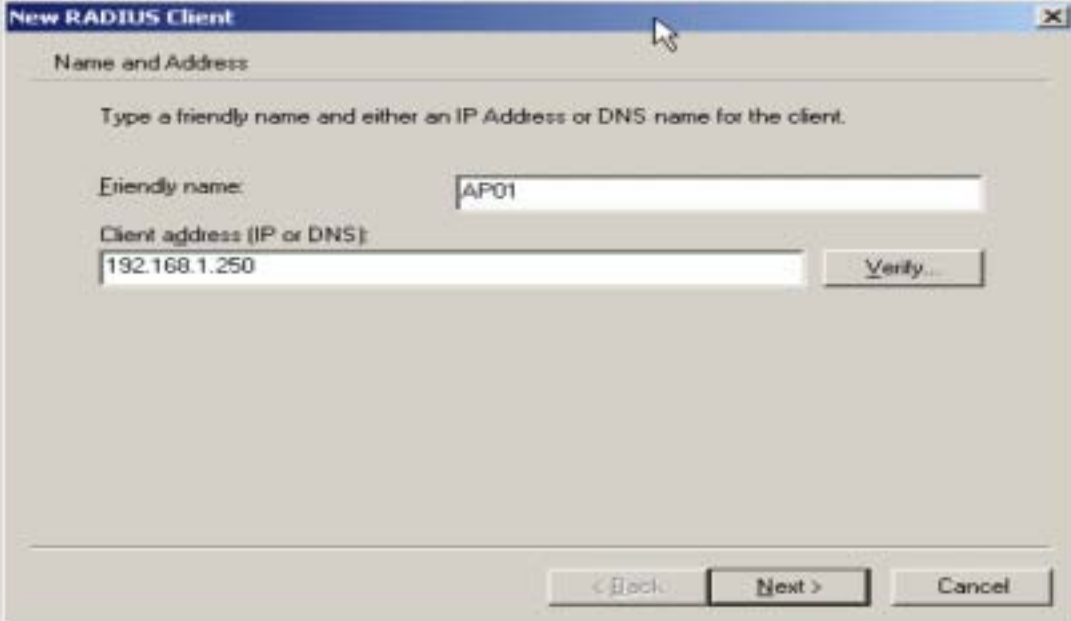








Al asignar los nuevos clientes radius se esta configurando que sean por donde comunicar los Access points



**New RADIUS Client**

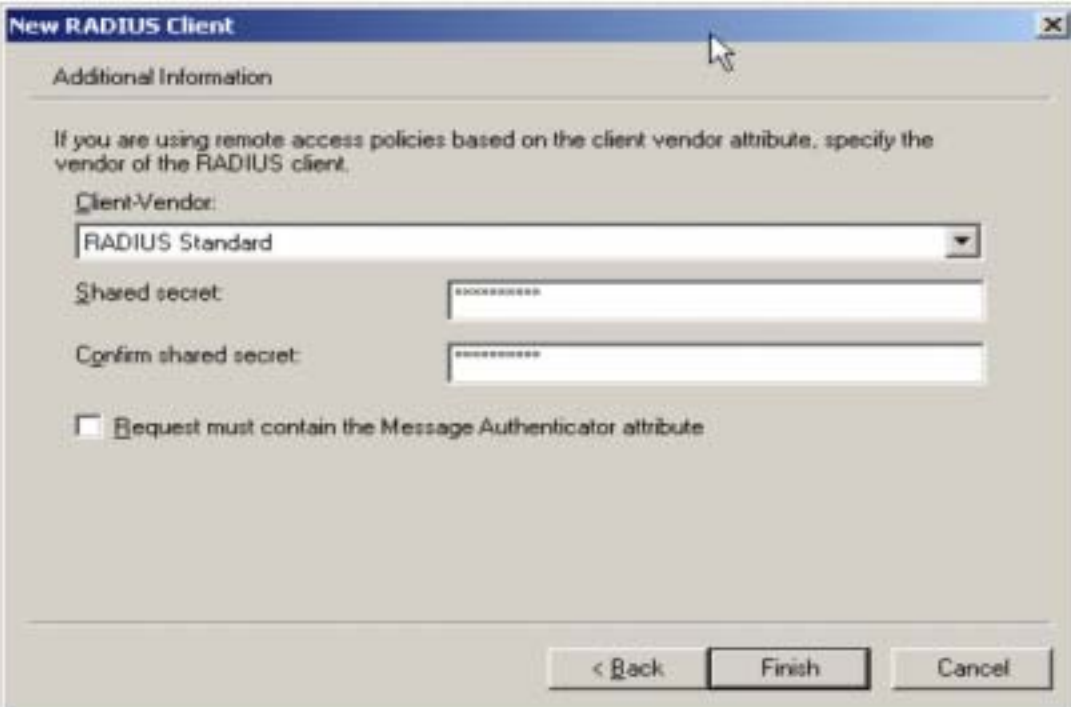
Name and Address

Type a friendly name and either an IP Address or DNS name for the client.

Friendly name:

Client address (IP or DNS):

< Back   Next >   Cancel



**New RADIUS Client**

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

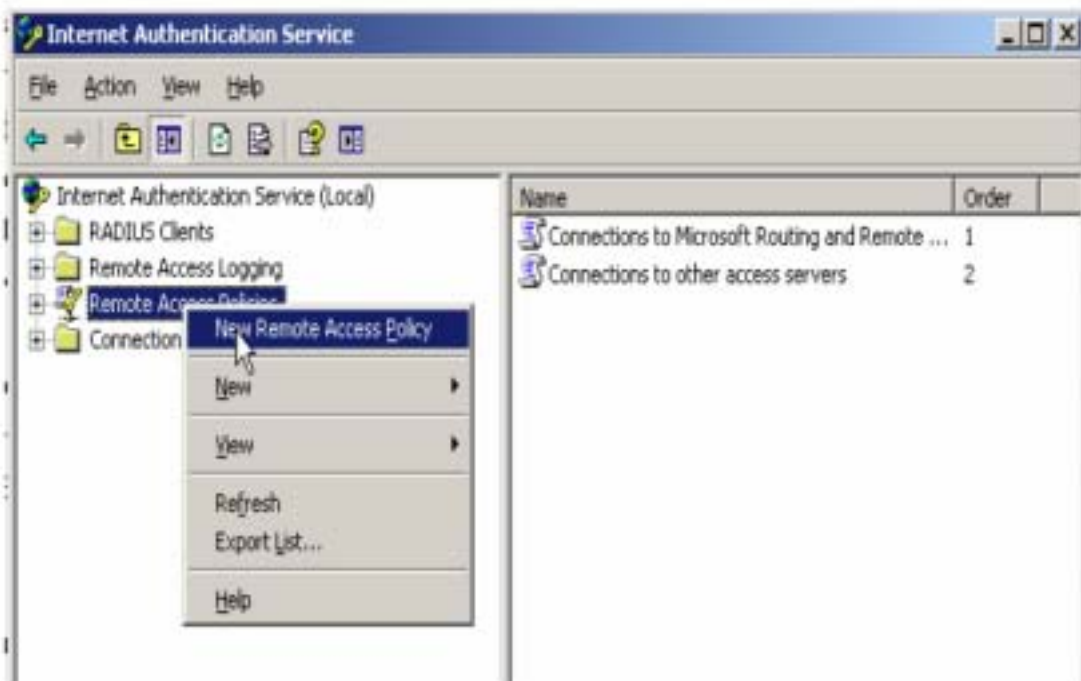
Client-Vendor:

Shared secret:

Confirm shared secret:

Request must contain the Message Authenticator attribute

< Back   Finish   Cancel



**New Remote Access Policy Wizard**

**Policy Configuration Method**  
The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario.

Set up a custom policy.

Type a name that describes this policy.

Policy name:

Example: Authenticate all VPN connections.

< Back   Next >   Cancel

**New Remote Access Policy Wizard**

**Access Method**  
Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

VPN  
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

Dial-up  
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

Wireless  
Use for wireless LAN connections only.

Ethernet  
Use for Ethernet connections, such as connections that use a switch.

< Back   Next >   Cancel

**Select Groups** [?] [X]

Select this object type:

From this location:

Common Queries

Name:

Description:

Disabled accounts  
 Non expiring password

Days since last logon:

Search results:

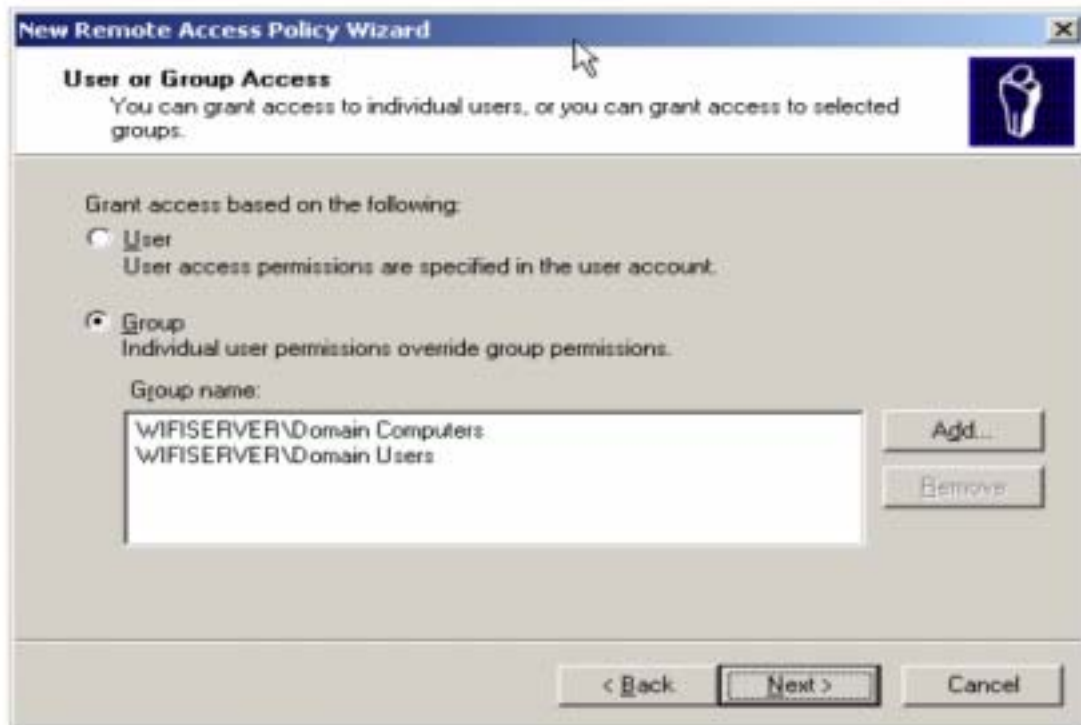
| Name (RDN)                  | Description          | In Folder            |
|-----------------------------|----------------------|----------------------|
| DnsUpdateProxy              | DNS clients who...   | wifi.server.net/U... |
| Domain Admins               | Designated admi...   | wifi.server.net/U... |
| Domain Computers            | All workstations ... | wifi.server.net/U... |
| Domain Controllers          | All domain contr...  | wifi.server.net/U... |
| Domain Guests               | All domain guests    | wifi.server.net/U... |
| Domain Users                | All domain users     | wifi.server.net/U... |
| Enterprise Admins           | Designated admi...   | wifi.server.net/U... |
| Group Policy Creator Owners | Members in this ...  | wifi.server.net/U... |
| Schema Admins               | Designated admi...   | wifi.server.net/U... |

**Select Groups** [?] [X]

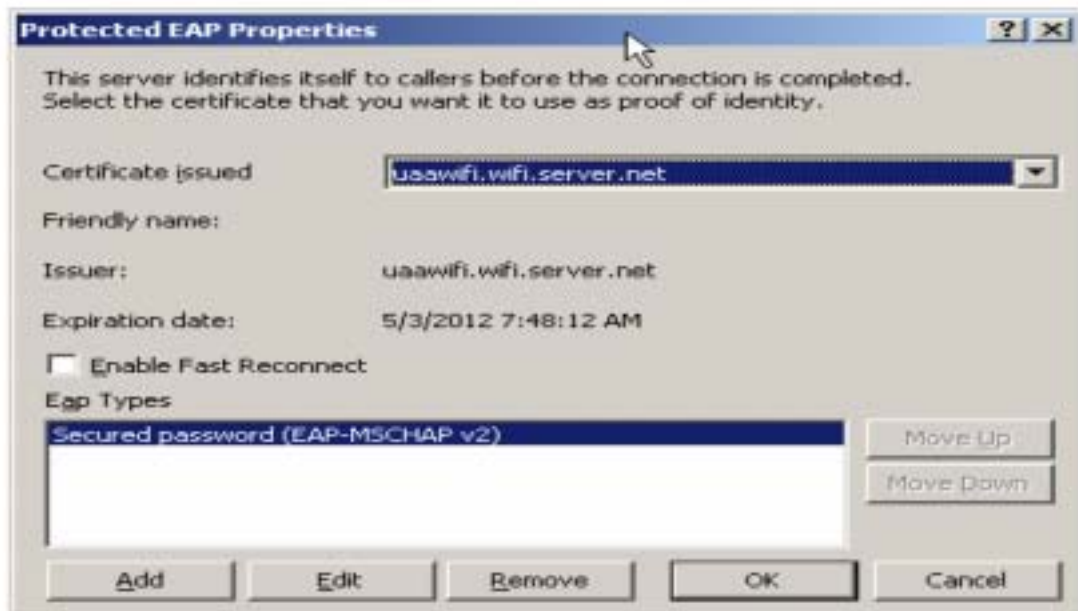
Select this object type:

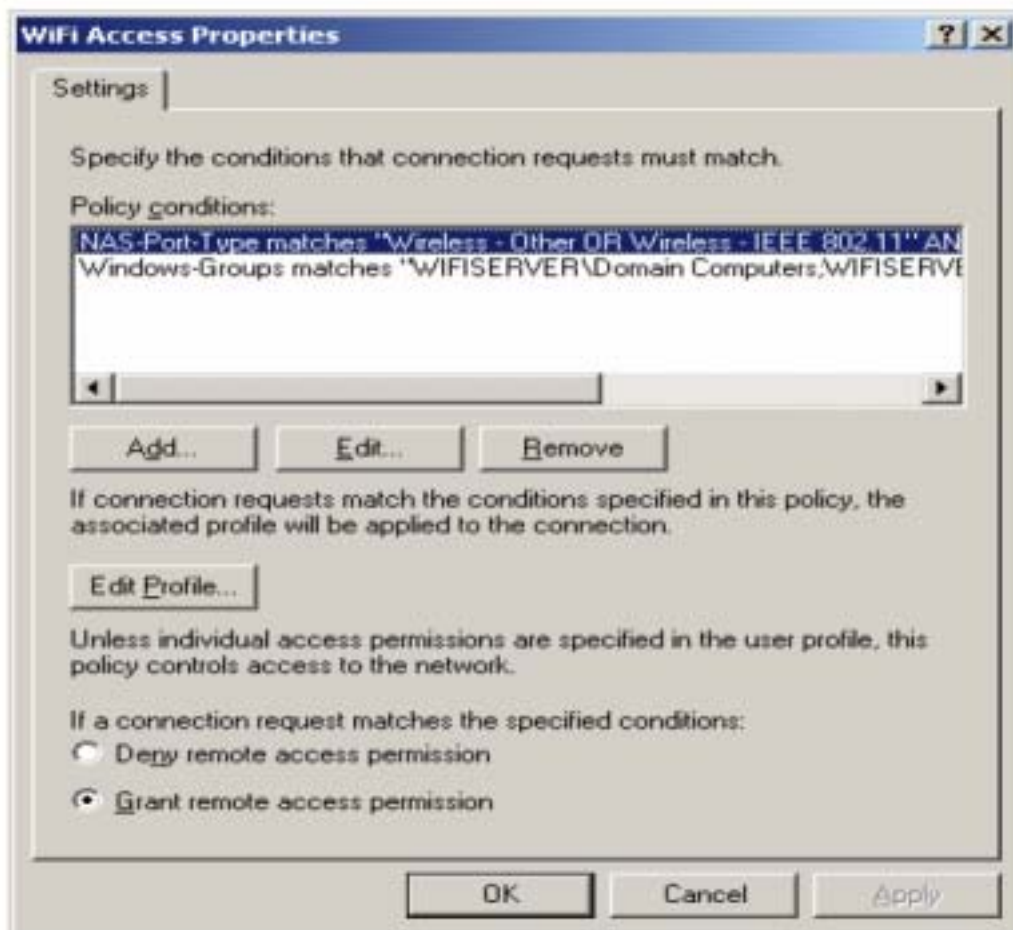
From this location:

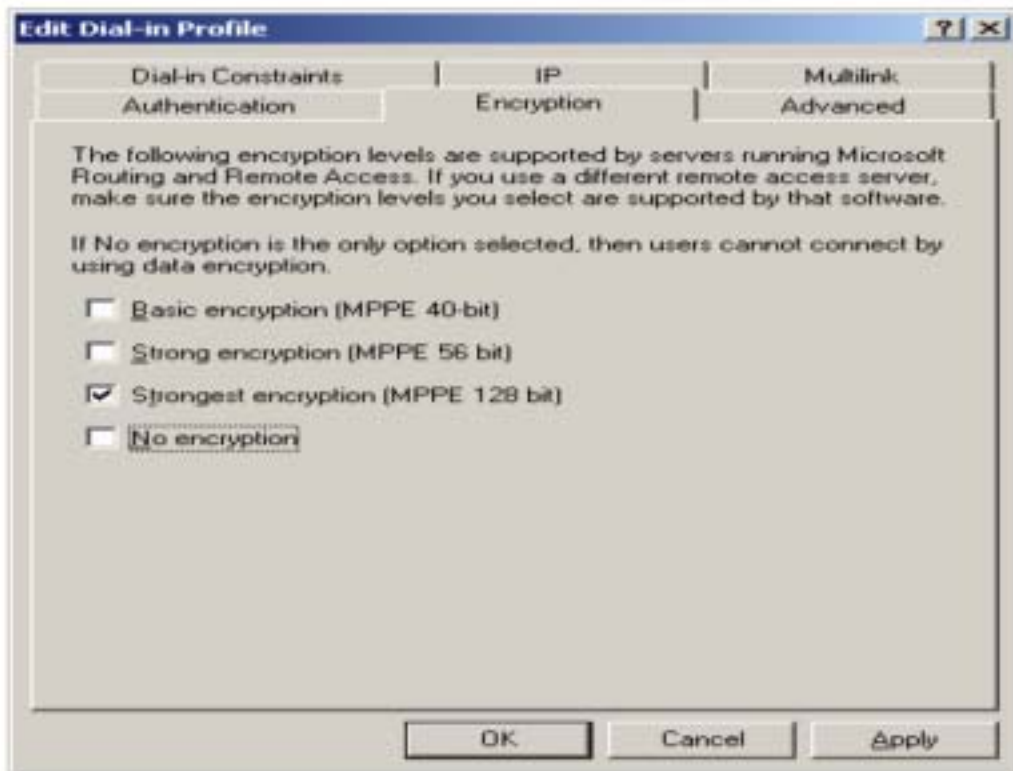
Enter the object names to select (examples):











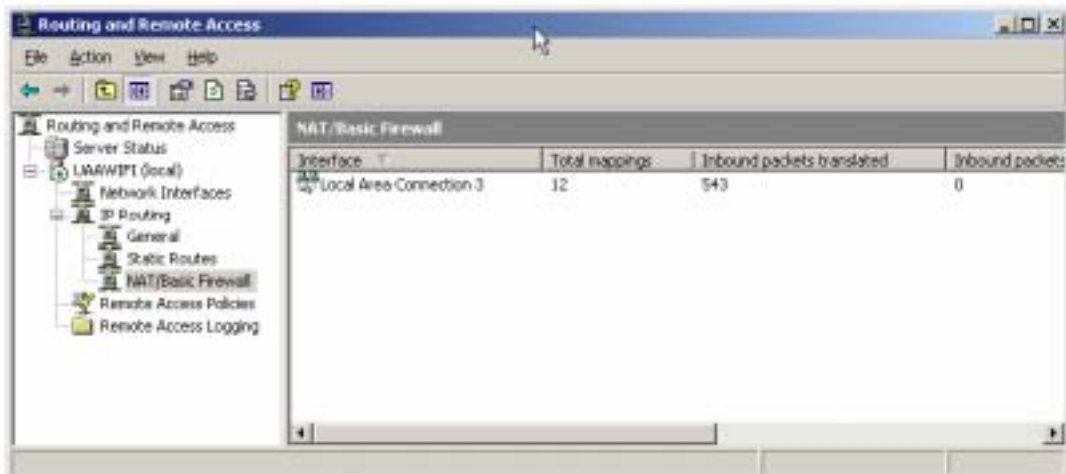
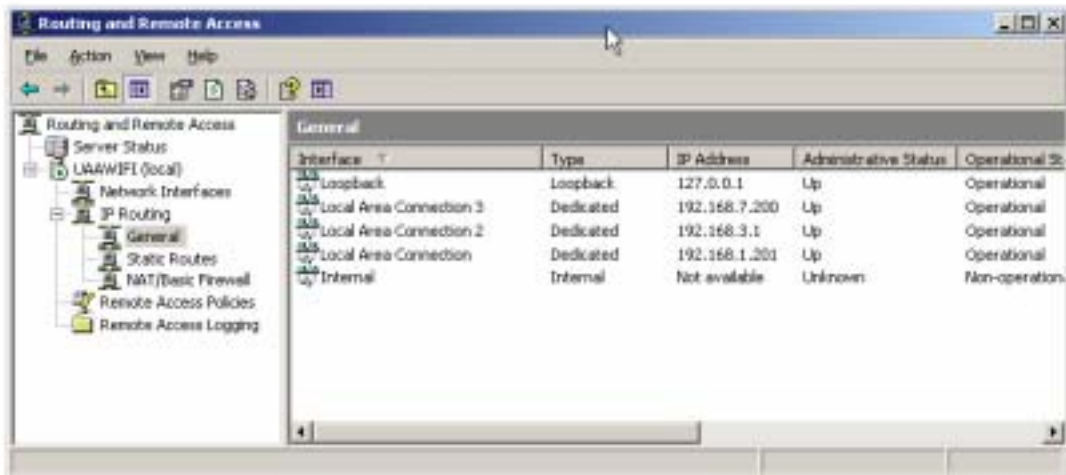
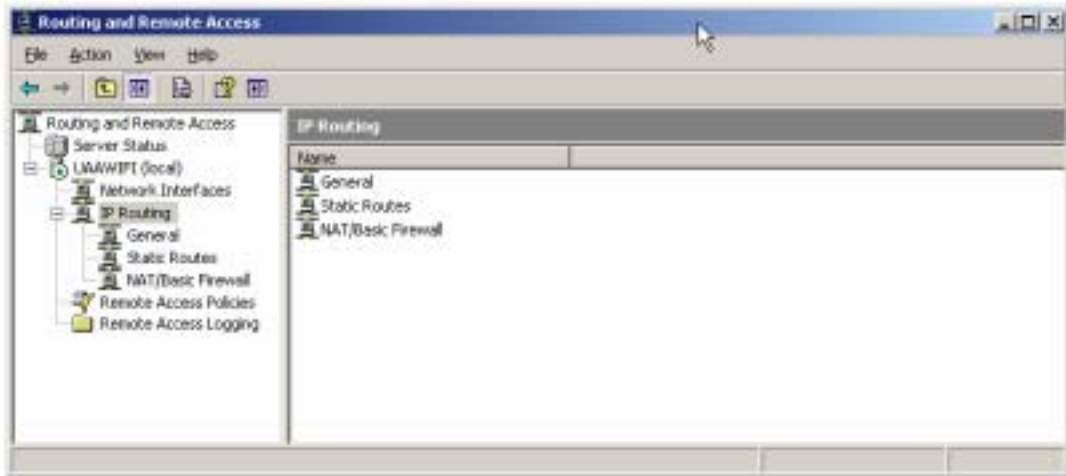
## **7.- Configuración del de Servicio Activo (Active Directory Service) Windows 2003**

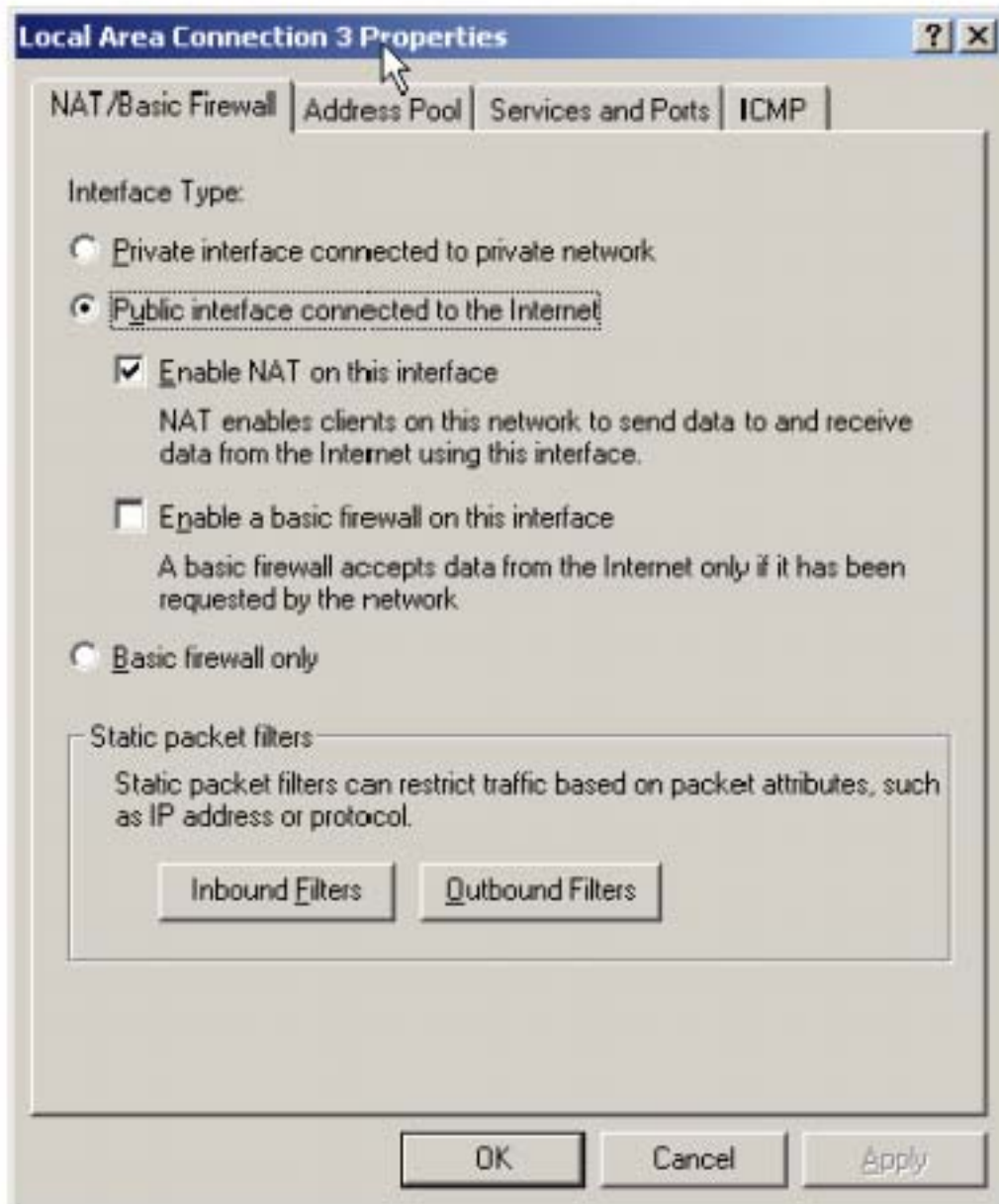
Como ultimo paso en el Directorio de Servicio Activo (Active Directory Service), se debe crear un grupo usuarios inalámbricos y computadoras que ya fue creado. En las propiedades de las cuentas de usuario se dirige a propiedades de Dial – In y seleccionar el control de acceso (Control Access) a través de la política de acceso remoto (Remote Access Policy), opción en la sección de permiso de acceso remoto (Remote Access Permission section).

Nota: Si el control de acceso (Control Access) a través de la política de acceso remoto esta deshabilitado entonces el nivel funcional de corriente del dominio esta probablemente configurado para Windows 2000. Cambia esta configuración, clic derecho en el nombre del dominio del Directorio Activo (Active Directory) y selecciona el nivel funcional del dominio en este caso Windows 2003 de la lista, una vez hecho este procedimiento estará completa, el control de acceso (Control Access) a través de la política de acceso remoto (Remote Access Policy).

## **8 .- Configurando Router y Acceso Remote (Routing and Remote Access)**

Una parte final es configurar el router del servidor, para el envio y recibimiento de paquetes, en este caso el acceder a Internet, mediante las siguientes imágenes se puede apreciar como debe estar configurado.





## CONCLUSIONES

Las redes inalámbricas permiten la independencia de la ubicación y la compatibilidad con la itinerancia para la conectividad de red en el hogar o en la pequeña empresa. Puede configurar una red inalámbrica con un punto de acceso inalámbrico (modo de infraestructura) o sólo con clientes inalámbricos (modo ad hoc). Las redes inalámbricas pueden tener mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en la industria.

El uso de computadoras móviles es interesante, por ejemplo, una de las características y requisitos en Internet es que debe de tener una dirección de red fija y esta es almacenada en las tablas de ruteo, para poder encontrar la dirección de una estación cuando se requiere. La computación móvil rompería con este esquema básico de Internet, por eso el estudio del modelo presentado resulta interesante, pues es una propuesta para solucionar el problema ya descrito.

En este proyecto se utilizó la tecnología necesaria que satisfacía y ayudó a resolver el problema con recursos necesarios. Este estudio es factible, ya que la tecnología, protocolos, estándares, etcétera están al alcance. El proveer un servicio como el descrito en este proyecto será muy útil y conlleva a todo usuario que este dentro del área de cobertura dispondrá de Internet inalámbrico para su equipo ya sea fijo o móvil en cualquier parte de su domicilio.

Los usuarios requieren cada vez de más movilidad y los que cuenten con un equipo de cómputo móvil se vuelven un candidato evidente y factible para una red inalámbrica. Esto permitirá al usuario moverse a distintas ubicaciones como lo es su sala, pasillos, habitaciones, el jardín o área de descanso del hogar siempre y cuando este en el área de cobertura y aún tener acceso a los datos en red. La tecnología inalámbrica permitirá a los usuarios enviar y recibir datos en recintos cerrados y abiertos, es decir, en cualquier punto del alcance de una estación base inalámbrica.

En conclusión, el proyecto realizado para esta propuesta de tesis fue un éxito, hubo muchos contratiempos al seleccionar el software ideal para la realización del proyecto, junto con la configuración, ya que es un amplio sistema con muchos campos a configurar e instalar. Lo que resulta de esto es una experiencia más en el campo de las Telecomunicaciones ya que la tecnología está ahí, solo es darle forma, uso y aplicación de todo para implementar algo y así proveer un servicio que realmente es factible para la comunidad que lo desea.



## BIBLIOGRAFÍA

- DOCUMENTO IEEE "Redes Híbridas" Pág. 21-26  
1992 universidad de Aveiro, Portugal  
Rui T. Valadas, Adriano C. Moreira, A.M. de Oliveira Duarte.
  
- DOCUMENTO IEEE "Ruteando con TCP/IP" pag 7-12  
1992 IBM T.J. Watson Reserach Center  
Charles E. Perkins.
  
- DOCUMENTO IEEE "Características de una Radio LAN" pag 14-19  
1992 LACE Inc.  
Chandos A. Rypinski.
  
- Revista PC/Tips Byte pag 94-98  
artículo: "Redes Inalámbricas"  
Abril 1992 Nicolas Baran.
  
- Revista PC/Magazine pag 86-97  
artículo: "Sin Conexión"  
Marzo 1995 Padriac Boyle.
  
- Guía Completa de Windows 2000 Profesional  
Meter Norton, John Mueller y Richard Mansfield  
Prentice Hall
  
- Wireless Home Networking by Danny Briere, Walter R. Bruce III, and  
Pat Hurley  
Cisco Networking Essentials  
Volume I  
Cisco Networking Essentials  
Volume II
  
- TechRepublic's ultimate guide to enterprise wireless LAN security  
Version 1.0 January 10, 2007  
By George Ou

- Wireless Networking in Windows 2003

[http://www.windowsnetworking.com/articles\\_tutorials/Wireless-NetworkingWindows-2003.html](http://www.windowsnetworking.com/articles_tutorials/Wireless-NetworkingWindows-2003.html)

by Andrew Z. Tabona

- Las notas del producto “Troubleshooting Microsoft Windows XP-based Wireless Networks in the Small Office or Home Office” en <http://www.microsoft.com/downloads/details.aspx?FamilyID=35c7e5ad-59e7-477b-9d27-6a7030e67002&displaylang=en>

- Sitio Web de Wi-Fi en <http://www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx>

- Wi-Fi Protected Access (WPA) Overview en <http://www.microsoft.com/technet/community/columns/cableguy/cg0303.mspx>