

# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE INGENIERÍA

"RED INALÁMBRICA PARA EL LABORATORIO DE REDES"

**TESIS**

PARA OBTENER EL TITULO DE **INGENIERO EN COMPUTACIÓN** PRESENTAN

**HUGO CAMPOS GUTIÉRREZ**
**VICTOR HUGO DOMÍNGUEZ LEÓN**



DIRECTORA DE TESIS: M.C. MARÍA JAQUELINA LÓPEZ BARRIENTOS

MÉXICO D. F. ABRIL 2006

# AGRADECIMIENTOS

*A las siguientes personas e instituciones que me apoyaron durante mi etapa de licenciatura: Gracias!!!!!!!!!*

A mi padre por apoyarme de forma incondicional y en todo lo que fue necesario durante mi carrera profesional, en especial durante mi estancia en la Facultad de Ingeniería. Por darme aliento para seguir en ingeniería y siempre confiar en mí.

A mi hermana por apoyarme de manera constante y creer siempre en mí. Por estar siempre al pendiente de las cosas que me hacían falta.

A mis tíos maternos en especial a mi tía Victoria y a mí tío Alfredo por estar al pendiente de mis estudios.

A la Universidad Nacional Autónoma de México y a la Facultad de Ingeniería por haberme dado la oportunidad de formar parte de esta gran institución. Pero en especial a los profesores que me dieron clases por transmitirme parte de su conocimiento.

A la maestra María Jaquelina López Barrientos por apoyarnos en la realización de nuestra tesis, por su opinión y comentarios para mejorar la tesis.

Al Programa en Tecnología en Computo (PROTECO) por transmitirme parte del conocimiento en computo que ahora tengo y dejarme pertenecer a esta familia tan unida y especial.

A todos mis compañeros de la universidad, que digo compañeros a mis amigos del alma por estar en las buenas y en las malas durante nuestra estancia en Ingeniería, en especial a Piero, Bety, Oscar Jiménez (el rata), Julia, Victor Hugo, Lety, Alejandro González, Israel, Ricardo, Miguel Ángel (oxido), Roberto Juárez, Oscar, Ulises (hombre), Antonio (tigre), Isaías (Shagui), Gaudencio, Josué (toro), Adán, Carlos Omar, Jorge Placencia, Edgar (chano) y demás compañeros que compartieron algún momento conmigo, gracias por su amistad.

A mis compadres que siempre estuvieron a mi lado y nunca me dejaron caer Cesar (mame), Albert (gallo), Adrián (flys), Alain (mamado), Lalo (mac), Marcos, Edgar y Joel.

Pero un agradecimiento muy especial a Dios y mi Madre que siempre fue mi ángel de la guarda, que siempre me dio ánimos para seguir y ser lo que ahora soy, gracias mamá en donde quiera que te encuentres.

Hugo Campos Gutiérrez.

A la mujer que jamás me ha dejado de ayudar en ningún momento de mi vida, por más difícil que este sea. De la que no he recibido más que amor, comprensión y apoyo en todas las decisiones que he tomado, dándome su consejo siempre buscando lo mejor para mí y para quienes me rodean.

Gracias Ma.

A la mujer que ha estado junto a mi a lo largo de varios años, la que aun en finales de Termodinámica estuvo ayudándome, la que se que estará conmigo en las buenas y en las malas.

Gracias Erika.

A mi familia mas cercana, aquellos que no necesitaron decir jamás que me apoyaban porque sus acciones lo demostraban, siempre he tenido su apoyo implícito e incondicional.

Gracias Maria, Juan Manuel y Raúl.

A todos mis amigos, les agradezco el que hayan podido aguantar mi forma de ser a veces tan difícil, se que también cuento con ustedes para lo que sea.

Gracias Alex, Lety, Alejandra, Said, Oscar, Bety, Carelia.

A mi amigo y compañero de tesis, por estar en este proyecto que significa el punto final de una de las etapas más importantes en mi vida que es el término de nuestra carrera.

Gracias Hugo.

Y por supuesto gracias a la UNAM y a la Facultad de Ingeniería.

Victor Hugo Domínguez León

*Introducción* ---- *1*

*Capítulo 1. Panorama general* ---- *5*

**1.1. Historia de las redes inalámbricas** ---- **6**

**1.2. Descripción de una red inalámbrica** ---- **12**

**1.3. Arquitectura de Red** ---- **13**
1.3.1. Modelo TCP/IP ---- 16
1.3.2. Modelo OSI ---- 18
1.3.3. Comparación entre el modelo TCP/IP y el modelo OSI ---- 22

**1.4. Clasificación de las redes por cobertura** ---- **23**
1.4.1. Red de Área Local (LAN - Local Area Network) ---- 23
1.4.2. Red de Área Metropolitana (MAN - Metropolitan Area Network) ---- 23
1.4.3. Red de Área Extensa (WAN- Wide Area Network) ---- 23

**1.5. Ventajas y desventajas de una red wireless vs. una red cableada** ---- **24**
1.5.1. Ventajas ---- 24
1.5.2. Desventajas ---- 25

*Capítulo 2. Redes inalámbricas* ---- *28*

**2.1. Tipos de redes inalámbricas.** ---- **29**
2.1.1. IEEE 802.11 (Wireless LAN, Wi-Fi) ---- 29
2.1.2. IEEE 802.15 (Bluetooth) ---- 30
2.1.3. IEEE 802.16 (Banda Ancha Inalámbrica o WiMAX) ---- 31

**2.2. Topologías** ---- **31**
2.2.1. Topología infraestructura ---- 33
2.2.2. Topología Ad Hoc ---- 35

**2.3. Protocolos** ---- **36**
2.3.1. Mobile IP ---- 36
2.3.2. WAP ---- 37
2.3.3. WEP ---- 39

**2.4. Estándares** ---- **41**
2.4.1. Arquitectura de capas 802.11 ---- 41
2.4.2. IEEE802.11a ---- 43
2.4.3. IEEE802.11b ---- 45
2.4.4. IEEE802.11e ---- 46
2.4.5. IEEE802.11f ---- 46
2.4.6. IEEE 802.11g ---- 47
2.4.7. IEEE802.11h ---- 50
2.4.8. IEEE802.11i ---- 52

**2.5. Elementos** ---- **52**
2.5.1. Access Point ---- 53
2.5.2. Bridges ---- 54
2.5.3. Repeaters ---- 55
2.5.4. Routers y Gateways ---- 56
2.5.5. Antenas ---- 57

*Capítulo 3. Diseño e implementación de la red* ---- *61*

**3.1. Análisis de la red existente en el laboratorio.** ---- **62**

**3.2. Determinación de la mejor opción para la red.** ---- **63**
3.2.1. Sistema operativo ---- 63

3.2.2. Análisis de los prerrequisitos en los equipos ---- 64
3.2.3. Análisis del equipo a utilizar ---- 65

**3.3. Implementación ---- 71**
3.3.1. Configuración de los access point ---- 72
3.3.2. Configuración de las tarjetas de red ---- 75

***Capítulo 4. Pruebas a la red ---- 79***

**4.1. Pruebas de conectividad ---- 80**

**4.2. Pruebas de alcance ---- 81**
4.2.1. Horizontal ---- 82
4.2.2. Vertical ---- 83

**4.3. Pruebas de autenticación WEP ---- 84**

**4.4. Pruebas al filtrado de MAC ---- 86**

**4.5. Análisis de protocolos ---- 88**

**4.6. Análisis de calidad de señal ---- 91**

***Capítulo 5. Prácticas ---- 98***

**5.1. Prácticas. ---- 99**
5.1.1. Práctica 1. Instalación del hardware y red inalámbrica ad-hoc ---- 99
5.1.2. Práctica 2. Configuración avanzada de una red inalámbrica infraestructura. ---- 109
5.1.3. Práctica 3. Filtrado por MAC ---- 116
5.1.4. Práctica 4. Análisis de tráfico ---- 121

**5.2. Aplicación de las prácticas ---- 126**
5.2.1 Práctica 1 ---- 126
5.2.2 Práctica 2 ---- 126
5.2.3 Práctica 3 y 4 ---- 127

***Conclusiones ---- 128***

***Bibliografía y mesografía ---- 133***

**Bibliografía ---- 134**

**Mesografía ---- 136**

# INTRODUCCIÓN

Las redes inalámbricas han evolucionado mucho en los últimos años ya que han demostrado ser una muy buena alternativa en ciertos casos, por mencionar sólo algunos; su bajo costo comparado con una red tradicional, por su versatilidad, ya que pueden montarse prácticamente en cualquier lugar, etc.

Hoy en día dichas redes tienen un auge importante en ambientes académicos y empresariales, aunque desde dos puntos de vista muy diferentes.

En un ambiente académico una red se diseña e implementa no sólo pensando en que nos proporcione el servicio para el que fue pensada, sino que se construye para optimizar, investigar, desarrollar y/o probar nuevas características que sirvan para hacerla más robusta, rápida y/o segura.

En un ambiente empresarial lo que se busca es funcionalidad, es decir, que la red haga lo que tenga que hacer sin saber en realidad cómo lo hace.

Sin embargo, siempre debe haber gente que sepa cómo es que funcionan estas redes y en su caso cómo mejorarlas, éste es uno de los problemas con que se enfrentarán los nuevos ingenieros en su vida profesional.

Siendo la Facultad de Ingeniería de la UNAM una de las instituciones más importantes del país y que se ha distinguido por lo bien equipada en lo que se refiere a laboratorios está, se planteó la implementación de una red inalámbrica (wireless), para que se cuente con lo último en tecnología en el laboratorio de redes y seguridad, así como para que los alumnos que cursen materias relacionadas con el área de redes y seguridad tengan un lugar donde poner en práctica los conocimientos adquiridos en el salón de clase y así adquirir las habilidades prácticas que tanto se requieren para la actividad laboral al egresar de esta facultad.

Los objetivos de este trabajo son:

**General:**

Diseñar e implementar una red inalámbrica, para el laboratorio de redes y seguridad.

**Particulares:**

- Conocer el funcionamiento de una red wireless.
- Entender el funcionamiento de los diferentes dispositivos de una red wireless (Access Point, bridges, routers, etc.)
- Hacer una comparativa entre una red wireless y una cableada, para conocer ventajas y desventajas ya implementadas ambas.
- Que la red sea versátil, esto es, que pueda montarse y desmontarse fácilmente dependiendo las necesidades del laboratorio.
- Estar a la vanguardia en la tecnología respecto a otras universidades y así salir mejor preparados.
- Que la red sea utilizada por los alumnos para hacer pruebas.
- Diseñar prácticas para ser desarrolladas por los alumnos que asistan al laboratorio como parte de su formación académica en las asignaturas de redes y seguridad.

Así, para alcanzar los objetivos mencionados, es que en el capítulo 1, damos un panorama general de las redes inalámbricas, y estudiamos algunos conceptos básicos que se utilizan en capítulos posteriores.

En el capítulo 2, hacemos una revisión de los tipos de redes existen en la actualidad, así como sus características.

En el capítulo 3, analizamos la red que ya existe en el laboratorio y buscamos la mejor opción para la wireless del laboratorio de acuerdo a las necesidades de los profesores y alumnos que harán uso de dicha red, así como el equipo con el que se cuenta, ya teniendo este estudio previo entonces pasamos a implementar la red.

En el capítulo 4 se presentan las pruebas hechas a la red, tanto para revisar la funcionalidad de la red así como para comprobar que será una red funcional para los alumnos y profesores.

Y por último en el capítulo 5, diseñamos y probamos algunas prácticas pensadas en que sean una guía para el alumno que se enfrentará a la administración de las redes inalámbricas, por lo que en este capítulo se presentan dichas prácticas así como los resultados obtenidos al probarlas con alumnos de asignaturas de Redes de Computadoras y de Temas Especiales de Computación: Fundamentos de Seguridad Informática.

# CAPÍTULO 1. PANORAMA GENERAL

En este capítulo se da una panorámica de las redes de datos inalámbricas, conceptos generales, la arquitectura de una red en general, clasificación de las redes según su cobertura y terminamos el capítulo haciendo una comparación entre una red cableada y una inalámbrica.

## 1.1. Historia de las redes inalámbricas

Es apenas discutible que la demanda para la transferencia de datos sin cables fue originada por los dispositivos móviles ya que hasta mediados de los 90, las PC de escritorio y los servidores gobernaban el mercado (hablamos solamente de los cables). El montón de cables se podía remeter cuidadosamente detrás del escritorio. En cuanto a la red local, al cableado telefónico y otros, quedaban satisfechos con cableado estructurado.

Por supuesto, había tareas que no se podrían solucionar con los cables, o se podían solucionar pero el costo era demasiado alto, por ejemplo, el querer instalar una red en un edificio que por sus valiosas características arquitectónicas no permitía perforaciones o remodelaciones y por lo tanto hacer una instalación de cableado estructurado era imposible, aunque el costo del cableado no fuera demasiado alto. Otro ejemplo, en el que el costo de la instalación de la red resultaba muy elevado era cuando se trataba de cubrir áreas muy grandes. En estos casos, las conexiones sin cables tuvieron que ser utilizadas a pesar de su precio alto, además de que dependía de las condiciones de la atmósfera, entre otros factores por lo que se utilizaron transmisores de microonda de 54Mbit/s o sistemas del láser; pero en la oficina simplemente no había alternativa a los cables.

Mientras tanto, las tecnologías sin cables no podían ser utilizadas en cualquier lugar, tuvieron que ser unificadas de alguna manera. Por otra parte, las computadoras portátiles empezaron a bajar de costo, por lo que creció la demanda para una tecnología inalámbrica, barata y de conexión flexible para el uso en la oficina. Consecuentemente, la IEEE en 1991 aprobó oficialmente el proyecto que desarrollaba "una especificación del control de acceso al medio (MAC) y de la capa física (PHY) para la conectividad sin cables para las estaciones fijas, portables y móviles dentro de un área local". Este proyecto tomó seis años y la IEEE ratificó la especificación en el verano de 1997, la IEEE 802.11.

De hecho, esa primera especificación, sin ningún nombre etiquetado todavía, estaba prácticamente igual al que tenemos hoy: dos variantes de la capa física (con una frecuencia oscilante y un espectro difundido), en una gama de 2.4-2.5GHz y pensaron en una tercera capa para la conexión infrarroja de banda ancha, la velocidad era de 1-2Mbit/s, no más.

Pero en la época de 10Mbit/s usando cables esto era realmente bueno. Por lo menos, había sido bueno cuando habían comenzado el trabajo en la especificación.

Para el final del proyecto, la palabra "multimedia" sonaba por todo el mundo, y los desarrolladores tuvieron que hacer algo sobre la velocidad.

La nueva especificación 802.11a, aunque proporcionó rendimiento de procesamiento de datos de 8-54Mbit/s, fue pensado para la frecuencia 5GHz, debido a un número de dificultades técnicas y de organización no era de mucho éxito, semejante a la 802.11b. Este último fue desarrollado junto con la variante de "a", pero con una velocidad de 11Mbit/s, un ancho de banda de 5.5Mbit/s y para una frecuencia de 2.4GHz. Esta versión ratificada a finales de 1999, actualmente está en uso, así como otras versiones que tienen algunas adiciones a la versión principal y se puedan ver como extensiones de la 802.11b.

802.11b probó su viabilidad a finales de la década de los 90’s, pero seguía siendo demasiado costoso hacer la conversión a wireless. Mientras tanto, había ya una necesidad de LANs caseras. Las alternativas como el uso del teléfono existente o del cableado eléctrico no resolvieron siempre todos los requisitos. Así pues, la conexión de radio dio la pauta para ser la solución más evidente.

Algunos valientes intentaron hacer sus propias variantes de menor alcance, pero más baratas. Uno que tenía cierto renombre, era el grupo de trabajo HomeRF que fue apoyado formalmente por muchas compañías respetables entre las cuales se encontraban Compaq, Ericsson Enterprise Networks, Hewlett-Packard, IBM, Intel, Microsoft, Motorola, Philips Consumer Communications, Proxim y Symbionics. Otros miembros con menos presencia fueron Cisco Systems, Harris Semiconductor, Intellon, National Semiconductor, Nortel, Rockwell Semiconductor y Samsung, pero al final sucumbió. La misión de Grupo de Trabajo HomeRF era conseguir la interoperatividad entre el mayor número de dispositivos diferentes que estuviesen ubicados en cualquier punto de la casa. Para ello se estableció un estándar abierto y sin licencia basado en comunicación digital mediante Radio Frecuencia. El resultado fue el desarrollo de SWAP (Shared Wireless Access Protocol).

Actualmente, destaca la implementación de dos soluciones LAN inalámbricas. Se trata de los estándares IEEE 802.11, principalmente 802.11b, y la solución propuesta por el grupo de trabajo HomeRF. Ambas soluciones no son interoperables entre sí ni con otras soluciones de redes LAN inalámbricas.

Mientras que HomeRF está diseñado exclusivamente para el entorno doméstico, 802.11b se está implementando en hogares, en la pequeña y mediana empresa, en grandes organizaciones y en un número cada vez mayor de zonas activas de redes

inalámbricas públicas. Algunos de los principales distribuidores de equipos portátiles los dota o tiene previsto dotarlos con tarjetas NIC 802.11b internas. En la tabla 1.1 se ofrece una comparación de las dos soluciones:

| | **IEEE 802.11B** | **HOMERF** |
|---|---|---|
| Principales fabricantes que lo han admitido | Cisco, Lucent, 3Com WECA | Apple, Compaq, HomeRF Working Group |
| Estado | Se incluye | Se incluye (baja velocidad) |
| Extensión | 50-300 pies (15,24-91,44 cm) | 150 pies (45,72 cm) |
| Velocidad | 11 Mbps | 1, 2, 10 Mbps |
| Aplicación | Hogares, oficinas pequeñas, campus, empresas | Hogar |
| Costo | 75-150 dólares por tarjeta | 85-129 dólares |
| Seguridad | WEP/802.1x | NWID/cifrado |
| Distribuidores | Más de 75 | Menos de 30 |
| Puntos de acceso públicos | Más de 350 | Ninguno |
| Cuota de mercado de las tarjetas NIC inalámbricas | 72% | 21% |

Tabla 1.1. Comparativa entre los protocolos 802.11b y HomeRF

Es bien sabido que los cables alrededor de una PC se utilizan para conectar no sólo con una red, sino también para conectar los periféricos. Un tipo de red inalámbrica que aprovechó esto fue Bluetooth y creó su propia interfaz. Esta interfaz simple y de no gran alcance con una cobertura de hasta 10m y una velocidad de hasta 1Mbit/s, fue probada en la misma frecuencia permitida 2.4GHz. PC-MODEM, teléfono PC-MOVIL, PC-PDA, PC-RATON, resultando exitosa y hoy en día todos estos cables se substituyen con esta tecnología.

Tiempo atrás, el éxito de Bluetooth era tan alto que su precio se elevo mucho. Había también serios problemas con la compatibilidad de los dispositivos que sólo se podían usar con la primera versión de la especificación.

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

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

La tecnología Bluetooth comprende hardware, software y requerimientos de interoperabilidad, por lo que para su desarrollo ha sido necesaria la participación de los principales fabricantes de los sectores de las telecomunicaciones y la informática, tales como: Ericsson, Nokia, Toshiba, IBM, Intel y otros.

Posteriormente se han ido incorporando muchas más compañías, y se prevé que próximamente los hagan también empresas de sectores tan variados como: automatización industrial, maquinaria, ocio y entretenimiento, fabricantes de juguetes, electrodomésticos, etc.

Pero en la actualidad la especificación 802.11 ha probado su efectividad y que es imprescindible. Los fabricantes de las soluciones sin cables de Ethernet cooperaron para solucionar el mismo problema que con Bluetooth, compatibilidad con la norma 802.11 para los productos de diversos fabricantes. La alianza Wi-Fi fue creada y asumió el control de la certificación de la interoperabilidad así como la promoción de la 802.11 en el mercado. La especificación 802.11 ha sido absolutamente un éxito: hay muchos puntos de acceso a la 802.11b alrededor del mundo, incluyendo en lugares públicos (en los aeropuertos, hoteles, conferencias, pasillos, etc.) y actualmente ya es un estándar.

Al trasladarse esta tecnología a la oficina, más compañías prefieren el usar Wi-Fi como conexión de la red corporativa, o tienen por lo menos un punto Wi-Fi integrado en él. En los hogares, donde a menudo cuesta construir una infraestructura regular de cable resulta una importante alternativa.

La única desventaja del Wi-Fi además del precio (éste nunca será demasiado bajo) es su velocidad. Ya que Gigabit Ethernet se está convirtiendo en un estándar de velocidad.

Hay dos soluciones posibles a este problema. Uno es aumentar la velocidad y pulir la frecuencia existente de 2.4GHz; el otro es, ir hasta frecuencias más altas, una clase de salto en la oscuridad. Aunque actualmente la tecnología Wi-Fi se dirige en ambas direcciones.

La primer dirección está representada por el estándar IEEE 802.11g, que es otro desarrollo de 802.11b para alcanzar un ancho de banda más alta. En teoría, debe proporcionar un ancho de banda similar al de 802.11a de 54Mbit/s, pero en un espectro no problemático, generalmente aceptado en el espectro de frecuencias. Por otra parte, este rendimiento más alto viene tomado de la mano con la compatibilidad de los dispositivos de hoy con 802.11b.

La evolución nunca es un proceso fácil y rápido, este caso no es la excepción. Las primeras muestras de los dispositivos de 802.11g, que cumplían con la especificación del bosquejo, no hacían lo que debían hacer, su velocidad verdadera estaba en algunos casos sobre 20Mbit/s y ésa corresponde a la velocidad verdadera de 802.11a; pero tan pronto como se conecte un solo dispositivo de 802.11b a la red, el ancho de banda bajará inmediatamente.

Esto se debe dado que los dispositivos de 802.11g intercambian los paquetes usando métodos absolutamente diversos de trabajo por el rango y el protocolo. Así pues, un cliente de 802.11b será como un hombre oculto entre la gente avistada. Para evitar colisiones y otros problemas técnicos, la estación base realiza una clase de traducción síncrona entre las dos especificaciones 802.11b y 802.11g.

La segunda dirección y que es más radical para pulir los 5GHz de 802.11a a una cosa regular, esta tarea se pone en el último de las especificaciones que mencionamos aquí, la 802.11h. De manera general, 802.11h es lo mismo que 802.11a, pero más tolerante a sus vecinos en frecuencia. Esta calidad es representada por las características tales como la selección de canal (DCS) y transmite el control de energía (TPC). Es decir que cuando hay ruido en la frecuencia, el dispositivo de 802.11h debe cambiar su frecuencia de trabajo o reducir la energía de la señal al mínimo necesario para conectar con un punto alejado de WLAN o ambos.

Esta medida golpea la marca, porque el espectro de 5GHz se reserva en Europa para la comunicación basada en los satélites. Los dispositivos que mantienen esta clase de comunicación tienen prioridad más alta en trabajo sobre esta frecuencia. El estándar de alta velocidad europeo de la comunicación por radio, HiperLAN/2, toma esta cosa en cuenta, mientras que no lo hace la 802.11a. Esto es porqué IEEE está acelerando la ratificación de su versión mejorada, esperando terminar este proceso de la estandardización lo antes posible, 802.11h ofrecerá la compatibilidad hacia con el equipo de 802.11a, con los de 802.11b y con los de 802.11g.

Otro problema, común para ambos pares de estándares, y de requerir la acción inmediata es un nivel más alto de la seguridad. Tales WLANs son a menudo inicialmente susceptibles a las tentativas de “hackeo”, para esto es que surgió 802.11i, una extensión común para ambas capas y que es una extensión al MAC y no nivel de PHY.

Queda por responder una pregunta, la conexión de WLANs con el mundo externo, para ello existe el canal de fibra óptica, una solución ideal para las transferencias de datos de una manera rápida, pero no muy falible para solucionar el problema de la "última milla". Para conectar las redes Wi-Fi con las redes alámbricas de alta velocidad, IEEE tiene un estándar el 802.11a.

La ciudad ideal desde el punto de vista de una red sin cables parece ésa (como lo muestra la figura 1.1) las estaciones base 802.11a que se ponen sobre todo en los rascacielos, postes de  la red celular, tuberías, etc. Su cobertura es hasta los 50km, su frecuencia a partir de 2 a 11GHz, tasa de transferencia de datos de 70Mbit/s por sector (cada estación puede tener hasta seis sectores como éste). En términos de LAN cableadas, estas estaciones desempeñan el papel de interruptores.

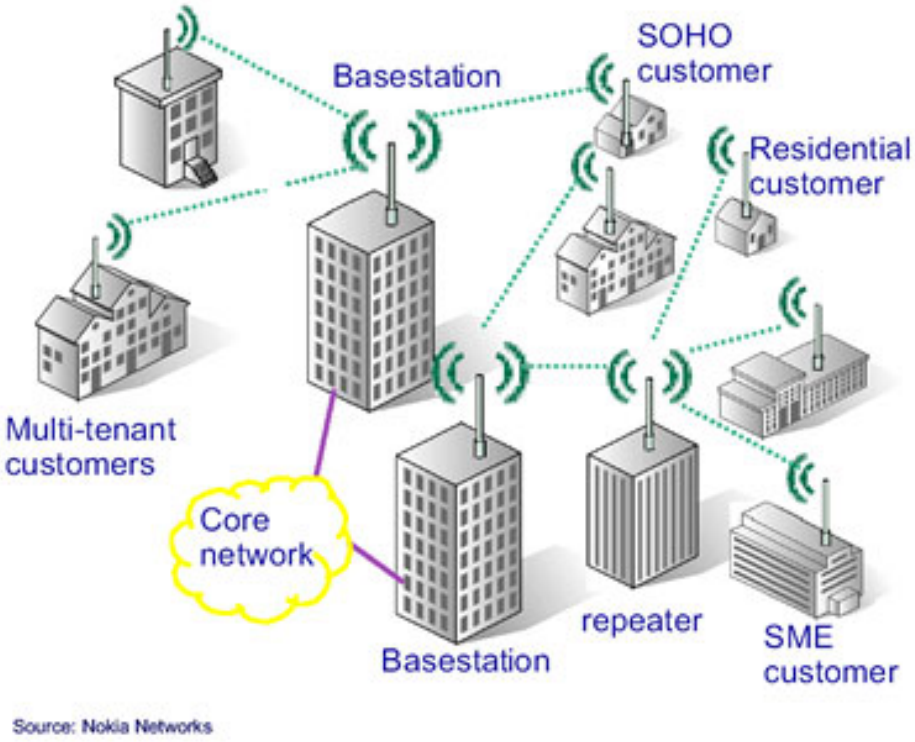



Figura 1.1 Lan Inalámbrica

Sus señales van a los puntos de acceso Wi-Fi instalados en los edificios ordinarios, comerciales o casas. Dividen el tráfico aún más y lo dirigen a las tarjetas Wi-Fi instaladas en las PC y estas PC se comunican con los periféricos Bluetooth.

## 1.2. Descripción de una red inalámbrica

Consideramos una red inalámbrica a aquel sistema que es capaz de conectar equipos terminales a la red de datos sin necesidad de utilizar cables de comunicación para ello.

La definición anterior es muy amplia, y de hecho caben en ella toda una serie de tecnologías; no obstante, dejaremos de lado los extremos, es decir las redes personales y las de área extensa, para centrarnos en lo sucesivo en las redes inalámbricas locales, basadas fundamentalmente en las normas IEEE 802.11, también conocidas con el término Wireless Fidelity (WiFi).

Desde este punto de vista, podemos decir que esta tecnología está suficientemente madura como para ofrecernos prestaciones comparables a las que estamos acostumbrados a utilizar cuando trabajamos con equipos informáticos conectados en red.

Una red inalámbrica utiliza ondas electromagnéticas como medio de transmisión de la información, que viaja a través del canal inalámbrico enlazando los diferentes equipos o terminales móviles asociados a la red. Estos enlaces se implementan básicamente a través de tecnologías de microondas y de infrarrojos.

Este tipo de redes utiliza tecnología de radiofrecuencia minimizando así la necesidad de conexiones cableadas. Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado.

Aún así, debido a que sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 54 Mbps frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general las WLAN se utilizarán como un complemento de las redes fijas.

## 1.3. Arquitectura de Red

Para la realización de una red de computadoras, y para tener una comunicación eficiente entre diferentes nodos que forman a una red a nivel de aplicación, es necesaria la utilización de una arquitectura de Red, la cual, tiene la finalidad de separar el problema de la comunicación en diferentes capas, en donde cada una se encargue de una comunicación a diferentes niveles.

Por ejemplo, en una comunicación telefónica, la comunicación se transmite por medio del cable sin tener conocimiento el usuario de la forma de comunicación (analógica o digital, half o full duplex, etc.), mientras que el usuario se comunica por medio de la voz, lo cual no es importante para el medio (ya que no interesa si se comunica voz, fax, email, etc.).

Una arquitectura básica es representada por la figura 1.2, la cual está formada por cuatro capas.

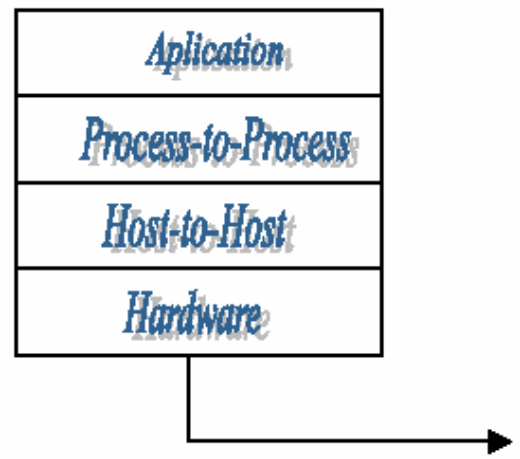



Figura 1.2. Arquitectura básica

Cada capa hace uso de los protocolos correspondientes a las actividades específicas que se realicen en cada nivel, de manera que un protocolo provee un servicio de comunicación entre nodos en los diferentes niveles.

Un protocolo provee dos interfaces:

- Interfaz de Servicio. Define las operaciones que los objetos locales pueden desarrollar en el protocolo (qué funciones/operaciones exporta).
- Interfaz peer-to-peer. Define los mensajes que se pueden intercambiar en puntos remotos. Define la estructura y significado de la comunicación.

Se dice que los protocolos permiten una comunicación punto a punto entre las diferentes capas, es decir, dada la arquitectura mostrada anteriormente, la comunicación punto a punto es representada como lo muestra la figura 1.3.

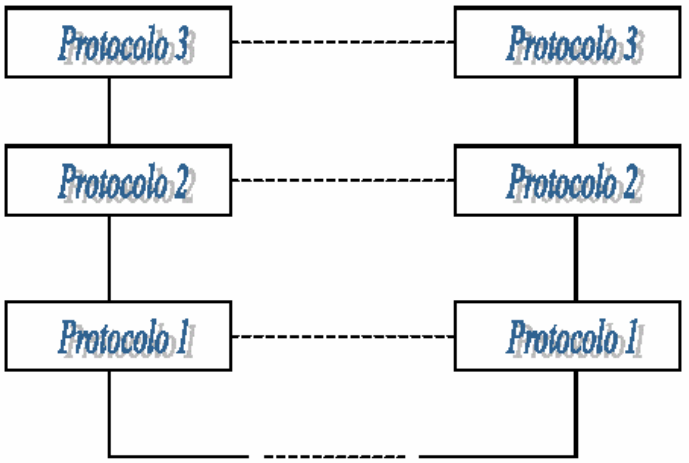



Figura 1.3. Comunicación punto a punto de los protocolos

Con la utilización de arquitecturas de computadoras, tres nuevas definiciones serán dadas:

## *Gráfica (Graph)*

Generalmente el número posible de protocolos que se pueden usar en cada capa es más de uno. De esta forma la gráfica representa todos los protocolos posibles (el diagrama), el cual es llamado Gráfica de protocolos (Protocol Graph).

## *Pila (Stack)*

El conjunto de protocolos utilizados para realizar una conexión específica es llamado pila de protocolos (Protocol Stack).

## *Encapsulamiento (Encapsulation)*

Cada capa recibe datos de las capas superiores y un protocolo no conoce nada acerca del contenido de los datos que recibe (pudiendo ser un e-mail, una transacción bancaria, etc.). El único requerimiento es que los datos lleguen al nodo destino sin alteración.

Para hacer esto, cada capa necesita mandar controles de información para ser reconocida en el otro nodo, esto es la capa 1 del emisor con la capa 1 del receptor, la capa 2 del emisor con la capa 2 del receptor, y así sucesivamente, como se muestra en la figura 1.4. Para hacer posible esta comunicación también llamada punto a punto (peer-to-peer), es necesario colocar un encabezado (header) a cada mensaje, los cuales son alrededor de 10 Bytes. De esta forma se dice que los datos son encapsulados por el protocolo.

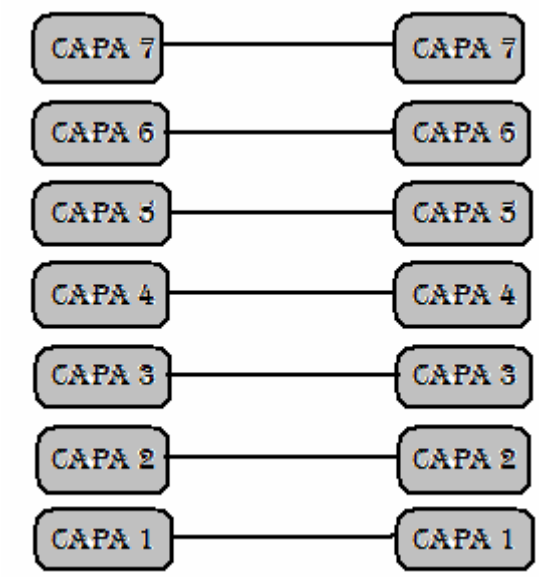



Figura 1.4. Conexión punto a punto entre capas

La ventaja de utilizar una arquitectura de red es la estandarización entre diferentes tipos y marcas de dispositivos como son los servidores, terminales, bridges, routers, switches, etc.

Dos de los estándares más utilizados, y que explicamos a continuación son: el modelo TCP/IP y el modelo OSI.

### *1.3.1. Modelo TCP/IP*

El TCP/IP tiene sus orígenes en un proyecto de investigación llevado a cabo por el DARPA (Defense Advanced Research Projects Agency) en los Estados Unidos en 1969. Este proyecto consistía en una red experimental, la red ARPANET que

comenzó a ser operativa durante 1975 constituyendo un éxito. Durante este periodo se implementaron los protocolos TCP/IP.

Se sugirió en un principio la idea de la implementación de la conmutación de paquetes frente a la conmutación de circuitos, decidiéndose que este modelo debería ser la base para la comunicación de las computadoras militares debido a la seguridad que esto proporcionaba en caso de ataques, la interrupción de un nodo de comunicaciones no implicaría la interrupción automática de las mismas.

En 1983 fue adoptado como estándar el nuevo conjunto de protocolos y todos los nodos de la red ARPANET pasaron a utilizarlo, la utilización de estos protocolos en los sistemas UNIX supuso un último empuje hacia su actual situación de utilización masiva.

A finales de 1983 la red ARPANET se dividió en dos subredes, MILNET y una nueva y más reducida ARPANET. Al conjunto de estas redes se las denominó Internet. En 1990 ARPANET desaparece, pero Internet se convierte en la red de redes.

La suite de protocolos TCP/IP permite a computadoras de todos los tamaños, marcas y sistemas operativos comunicarse entre ellas. Es un modelo en el que todos los protocolos y las aplicaciones están disponibles públicamente sin ningún costo. Éste forma la base de lo que hoy conocemos como Internet, una WAN (Wide Area Network) que conecta a miles de computadoras en el mundo.

Los protocolos normalmente son desarrollados por capas, en el que cada capa corresponde a una parte diferente de la comunicación. TCP/IP consta de cuatro capas que se muestran en la figura 1.5.

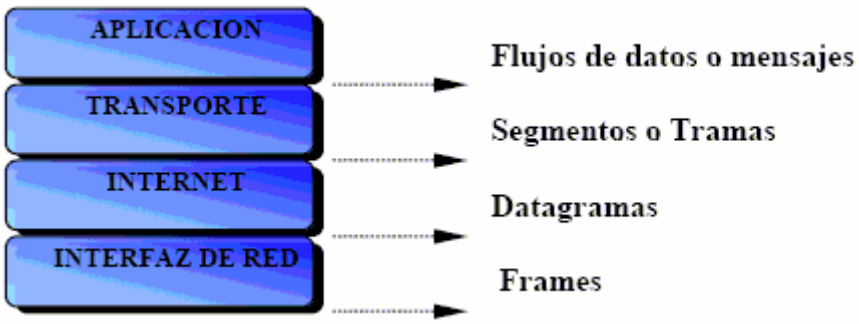



Figura 1.5. Modelo TCP/IP

### *Capa de enlace*

También llamada nivel de enlace de datos, normalmente incluye el driver del dispositivo en el sistema operativo y corresponde a la tarjeta de red en la computadora. Juntos manejan todos los detalles de hardware y la conexión lógica con el cable (o cualquier medio de comunicación que se esté utilizando).

### *Capa de internet*

También llamada capa de red, controla el movimiento de paquetes a través de la red. El ruteo de paquetes, por ejemplo, se encuentra en esta capa: IP (Internet Protocol), ICMP (Internet Control Massage Protocol) e IGMP (Internet Group Management Protocol) también se encuentran aquí.

### *Capa de transporte*

Provee el flujo de datos entre dos computadoras para la capa de aplicación. En el modelo TCP/IP existen dos tipos diferentes de protocolos de transmisión: TCP (Transmission Control Protocol) y UDP (User Datagrams Protocol).

### *Capa de aplicación*

Contiene los detalles de una aplicación en particular. Existen muchas aplicaciones comunes sobre TCP/IP como: FTP (File Transfer Protocol), telnet, SMTP (Simple Mail TransferProtocol).

## *1.3.2. Modelo OSI*

En 1978, la Organización Internacional de Estándares (ISO) creó un estándar universal para intercambio de información entre y dentro de las redes y a través de las fronteras geográficas conocido como Open System Interconection (OSI). Este estándar para la arquitectura de la red tiene siete niveles o capas, como se muestra en la figura 1.6. El Modelo OSI se ha esforzado en conseguir unas normas en

cuanto al diseño de las redes de comunicaciones y en el control de proceso de distribución.

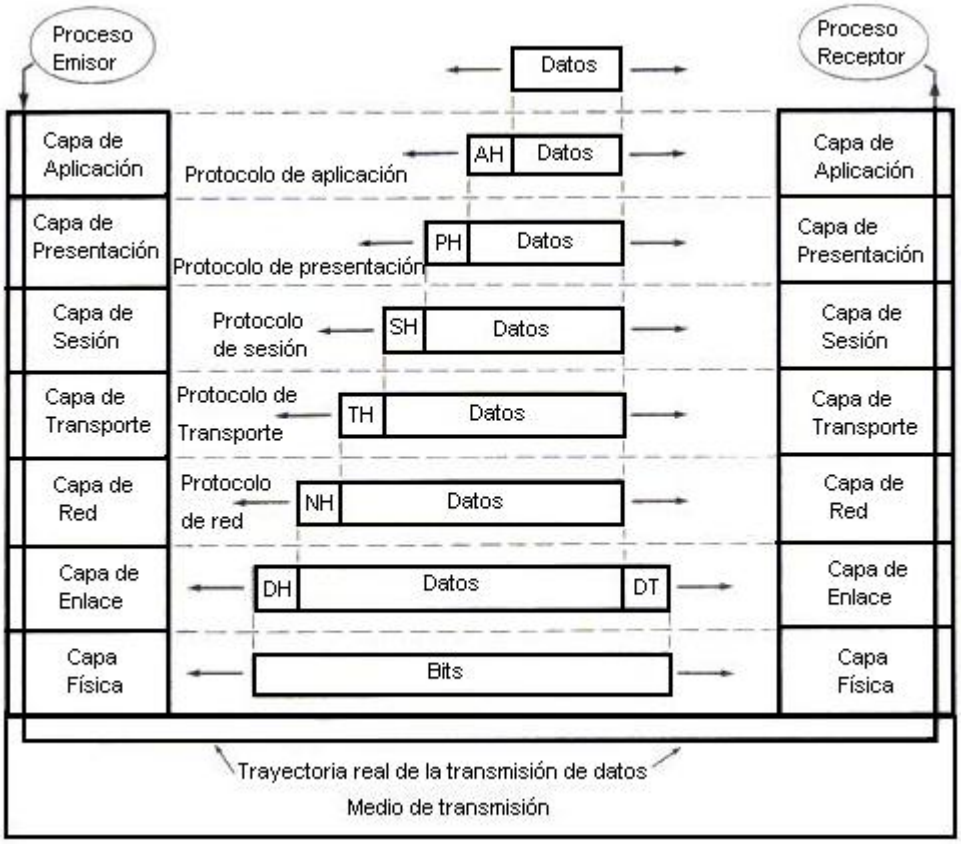



Figura 1.6. Modelo de referencia OSI

## *Capa física*

Este nivel dirige la transmisión de flujo de bits, sin estructura aparente sobre un medio de conexión. Se encuentra relacionado con condiciones electro-ópticas, mecánicas y funcionales de la interfaz al medio de transmisión. A su vez está encargado de aportar la señal empleada para la transmisión de los datos generados por los niveles superiores. En este nivel se define la forma de conectarse el cable a las tarjetas de red, cuántos pines debe tener cada conector y el uso funcional de cada uno de ellos.

Define también la técnica de transmisión a emplear para el envío de los datos sobre el medio empleado. Se encarga de activar, mantener y desactivar un circuito físico. Y es el responsable de hacer llegar los bits desde una computadora a otra.

## *Capa de enlace*

Cuando los paquetes de datos llegan a esta capa, éstos pasan a ubicarse en tramas (unidades de datos), que vienen definidas por la arquitectura de red que se esta utilizando como Ethernet, Token Ring, FDDI, etc. Esta capa se encarga de desplazar los datos por el enlace físico de comunicación hasta el nodo receptor e identifica cada computadora incluida en la red de acuerdo con su dirección de hardware, que viene codificada en la NIC.

La información de encabezamiento se añade a cada trama que contenga las direcciones de envío y recepción. La capa de enlace de datos también se asegura de que las tramas enviadas por el enlace físico se reciben sin error alguno. Por ello, los protocolos que operan en esta capa adjuntarán un Chequeo de Redundancia Cíclica o CRC (Cyclical Redundancy Check) al final de cada trama. El CRC es básicamente un valor que se calcula tanto en la computadora emisora como en la receptora. Si los dos valores CRC coinciden, significa que la trama se recibió correctamente y no sufrió error alguno durante su transmisión.

También controla la forma en que las computadoras acceden a las conexiones físicas de red.

## *Capa de red*

Esta capa es responsable del direccionamiento de mensajes y de la conversión de las direcciones lógicas y nombres, en direcciones físicas. Está encargada también de determinar la ruta adecuada para el trayecto de datos, basándose en condiciones de la red, prioridad del servicio, etc. El nivel de red agrupa pequeños fragmentos de mensajes para ser enviados juntos a través de la red. Es responsable de establecer, mantener y terminar la conexión de red.

## *Capa de transporte*

Se encarga de la recuperación y detección de errores. Garantiza también, la entrega de los mensajes de la computadora originados en el nivel de aplicación. Es el nivel encargado de informar a los niveles superiores del estatus de la red. Provee la corrección de errores y el control del flujo entre los dos puntos finales conectados en la red.

## *Capa de sesión*

Permite que dos aplicaciones residentes en computadoras diferentes establezcan, usen y terminen una conexión llamada sesión. Este nivel realiza reconocimiento de nombres y las funciones necesarias para que dos aplicaciones se comuniquen a través de la red.

## *Capa de presentación*

La capa de presentación puede considerarse como el traductor del modelo OSI. Esta capa toma los paquetes de la capa de aplicación y los convierte a un formato genérico que pueden leer todas las computadoras. Provee servicios como el estudio del formato de los datos, por ejemplo, ASCII o EBCD, etc., y determina el tipo de aplicación requerido.

La capa de presentación también se encarga de cifrar los datos si así lo requiere la aplicación utilizada en la capa superior (de aplicación), así como de comprimirlos para reducir su tamaño. El paquete que crea la capa de presentación contiene los datos prácticamente con el formato con el que viajarán por las restantes capas del modelo OSI, aunque como se ha mencionado las demás capas irán añadiendo elementos al paquete, lo cual puede dividir los datos en paquetes más pequeños.

## *Capa de aplicación*

La capa de aplicación proporciona la interfaz y servicios que soportan las aplicaciones de usuario. También se encarga de ofrecer acceso general a la red.

Esta capa suministra las herramientas que el usuario ve, también ofrece los servicios de red relacionados con estas aplicaciones de usuario, como la gestión de mensajes, la transferencia de archivos y las consultas de bases de datos. Suministra también cada uno de los servicios a los distintos programas de aplicación con los que cuenta el usuario en su computadora. Entre los servicios de intercambio de información que gestiona esta capa se encuentra la WEB, los servicios de correo electrónico conocido como SNMP (Simple Mail Transfer Protocol), entre otras.

### *1.3.3. Comparación entre el modelo TCP/IP y el modelo OSI*

Las similitudes entre ambos modelos son muchas, como podemos ver en la figura 1.7. Ambos se basan en una pila de protocolos independientes con capas bastante similares.

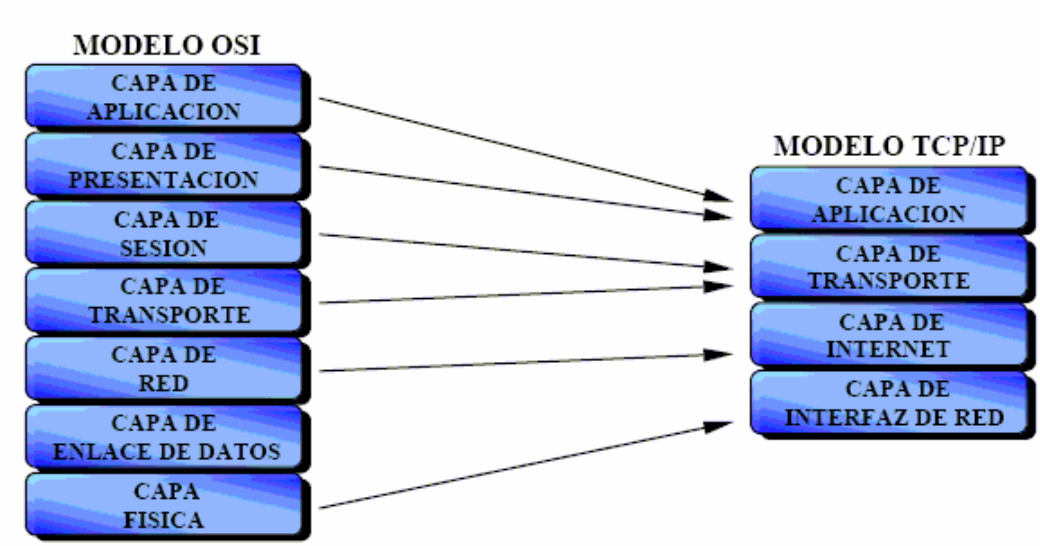



Figura 1.7. Comparación entre el modelo TCP/IP y OSI

El modelo OSI nos introduce tres conceptos básicos: servicios, interfases y protocolos, haciendo explícita la distinción entre estos conceptos. Cada capa ofrece unos servicios determinados a su capa superior, estos nos indican que es lo que hace la capa.

En TCP/IP no se hizo esta distinción, por eso se puede decir que los protocolos del modelo OSI están mejor escondidos que en el modelo TCP/IP.

Podemos también señalar otra diferencia importante en el modelo de capas, el modelo OSI soporta servicios sin conexión y orientados a conexión en el nivel de red pero en el nivel de transporte sólo acepta servicios orientados a conexión, en TCP/IP la capa Internet funciona sin conexión y la capa de transporte nos puede ofrecer servicios sin conexión (UDP) u orientados a conexión (TCP).

El modelo OSI se traduce en una mayor complejidad, un elevado numero de capas en las que a veces se repiten funciones lo que hace que en la mayoría de los sistemas no se lleguen a implementar todas.

# 1.4. Clasificación de las redes por cobertura

De acuerdo a su medida (o cobertura) geográfica, las redes son clasificadas de la siguiente manera:

## *1.4.1. Red de Área Local (LAN - Local Area Network)*

Es una red que cubre una extensión reducida, como una empresa, una universidad, etc. no existen por lo general dos computadoras que disten entre sí más de un kilómetro. Una configuración típica en una red de área local es tener una computadora llamada servidor de archivos en la que se almacena todo el software de control de la red, así como el software que se comparte con las demás computadoras de la red. Las computadoras que no son servidores de archivos, reciben el nombre de estaciones de trabajo. Estos suelen ser menos potentes y tienen software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo.

## *1.4.2. Red de Área Metropolitana (MAN - Metropolitan Area Network)*

Las redes de área metropolitana cubren extensiones mayores como pueden ser una ciudad mediante la interconexión de redes LAN, se distribuye la información a los diferentes puntos de la red, como por ejemplo: bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

## *1.4.3. Red de Área Extensa (WAN- Wide Area Network)*

Las redes de área extensa cubren grandes regiones geográficas como un país, un continente o incluso el mundo. Cables transoceánicos o satélites se utilizan para enlazar puntos que distan grandes distancias entre sí. Con el uso de una WAN se puede conectar de un lado a otro del mundo sin tener que pagar grandes cantidades de dinero. La implementación de una red de este tipo es muy complicada, se utilizan multiplexores para conectar las redes metropolitanas a redes globales utilizando técnicas que permiten que redes de diferentes características puedan comunicarse sin problema. El mejor ejemplo de una red WAN es Internet.

El porqué de la clasificación de acuerdo a su cobertura es basado por el tipo de tecnología utilizada.

Dentro de tecnologías LAN podemos mencionar Ethernet, Fast Ethernet, Switch Ethernet, Giga Ethernet, Token Ring de 4 y 16 Mbps y FDDI.

Dentro de las tecnologías WAN se pueden mencionar X.25, Frame Relay, ISDN, ATM, etc.

## 1.5. Ventajas y desventajas de una red wireless vs. una red cableada

### *1.5.1. Ventajas*

#### *Costo*

El costo de una red inalámbrica se reduce significativamente, ya que en una red cableada se necesitan concentradores o switches, un rack donde estan los dispositivos y a donde llegan todos los cables, un cable que va del dispositivo a cada computadora, rosetas y tarjetas de red, en cambio en una red inalámbrica el punto de acceso permite conexión a varios usuarios, eliminando cables y rosetas.

#### *Movilidad*

La movilidad que ofrece una red inalámbrica es quizá el punto más importante que ofrecen éstas, siendo una muy buena solución en lugares donde se requiere tener acceso a la red desde cualquier punto, tal característica es ideal para personas como los estudiantes que requieren estar conectados en diferentes lugares como puede ser en la biblioteca, laboratorios incluso en sus casas a cualquier hora del día. También es una excelente opción para personas que viajan mucho y requieren estar en contacto con su empresa o proveedores, para la gente que monta exposiciones, es una muy buena alternativa porque pueden poner su red en cualquier lugar y en cualquier momento sin tener que hacer un cableado estructurado que resultaría sumamente costoso.

### *Robustez*

Una red inalámbrica puede ser muy útil en lugares donde las condiciones físicas sean difíciles, esto es, en altas o bajas temperaturas, humedad, agentes químicos, etc., en donde los cables de una red pueden sufrir degradación rápidamente. Esto no quiere decir que los puntos de acceso no sufran degradación en condiciones extremas, pero si pueden estar mucho más alejados de tales condiciones.

### *Provisionalidad*

Las redes inalámbricas, son una buena alternativa para lugares donde se necesita una red por poco tiempo, como pueden ser congresos, expos, ferias, etc.

Dichas redes soportan un número elevado de usuarios transitorios, mientras que las fijas están limitadas a las conexiones ya cableadas exclusivamente.

### *Estética*

Las instalaciones de redes locales se caracterizan por la existencia de infinidad de rosetas (cajas de conexiones) próximas a cada puesto de trabajo, canalizaciones generalmente visibles y cables desde las PC’s hasta el punto de conexión más próximo.

## *1.5.2. Desventajas*

### *Velocidad*

Una red tradicional permite un mayor ancho de banda que una red inalámbrica, una red cableada puede llegar a tener hasta 100 Mbps, mientras que una inalámbrica puede llegar a tener 54 Mbps en el mejor de los casos.

## *Interferencia*

Las redes cableadas prácticamente están exentas de interferencia, las inalámbricas al ser el aire el medio de transmisión están expuestas a mucha mayor interferencia.

## *Calidad de Servicio*

Las redes inalámbricas ofrecen una menor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps, frente a los 100 que puede alcanzar una red cableada. Por otra parte hay que tener en cuenta también la tasa de error debida a las interferencias. Ésta se puede situar alrededor de 10-4 frente a la 10-10 de las redes cableadas. Esto significa que hay 6 órdenes de magnitud de diferencia y eso es mucho. Estamos hablando de 1 bit erróneo cada 10.000 bits o lo que es decir, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo. Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.

## *Soluciones Propietarias*

Como la estandarización está siendo bastante lenta, ciertos fabricantes han sacado al mercado algunas soluciones propietarias que sólo funcionan en un entorno homogéneo y por lo tanto estando atado a ese fabricante. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del sistema como para la recuperación ante posibles fallos. Cualquier empresa o particular que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de acceso, etc.

## *Restricciones*

Estas redes operan en un trozo del espectro radioeléctrico. Éste está muy saturado hoy en día y las redes deben amoldarse a las reglas que existan dentro de cada país. Concretamente en España, así como en Francia y en Japón, existen unas limitaciones en el ancho de banda a utilizar por parte de ciertos estándares.

*Seguridad. En dos vertientes:*

Por una parte seguridad e integridad de la información que se transmite. Este campo está bastante criticado en casi todos los estándares actuales, que, según dicen no se deben utilizar en entornos críticos en los cuales un “robo” de datos pueda ser peligroso.

Por otra parte este tipo de comunicación podría interferir con otras redes de comunicación (policía, bomberos, hospitales, etc.) y esto hay que tenerlo en cuenta en el diseño.

# CAPÍTULO 2. REDES INALÁMBRICAS

En este capítulo se da una breve descripción de los tipos de redes inalámbricas que existen así como las topologías utilizadas por dichas redes, abordamos los protocolos más utilizados, continuamos analizando los estándares de la IEEE y terminamos el capítulo con la explicación de los dispositivos utilizados en una red de este tipo.

# 2.1. Tipos de redes inalámbricas.

Los siguientes son tipos de redes inalámbricas que existen en el mercado y que a continuación explicamos.

Los tipos de redes que existen actualmente son:

- IEEE 802.11x (Wireless LAN, Wi-Fi)
- IEEE 802.15 (Bluetooth)
- IEEE 802.16 (Banda Ancha Inalámbrica)

En este capítulo se trata especialmente el estándar IEEE802.11, porque es el que implantaremos.

## *2.1.1. IEEE 802.11 (Wireless LAN, Wi-Fi)*

La especificación IEEE802.11 define el sistema de distribución como la arquitectura encargada de interconectar diferentes IBSS o redes inalámbricas independientes.

El componente fundamental de este sistema de distribución es el punto de acceso, y además la especificación define lo que llama los servicios de distribución que facilitan y posibilitan el funcionamiento en modo infraestructura. Se definen diferentes servicios para cada componente, según se trate de punto de acceso o estación.

A continuación enumeramos los servicios y exponemos el servicio de asociación, por su carácter básico. Los cinco primeros los implementa el punto de acceso y los dos últimos la estación. La especificación añade en algunos servicios la información necesaria para implementarlo.

- Distribución. Se encarga de llevar un paquete del punto de acceso de origen al de destino.
- Integración. Se encarga de la función de gateway con otros sistemas IEEE802.x. En concreto, define el componente portal que se encargará de aspectos necesarios como redireccionamiento.
- Asociación. Servicio necesario para que una estación pueda adherirse al modo infraestructura y utilizar sus servicios.

- Reasociación. Consiste en el campo de punto de acceso al que se asocia la estación para adherirse al modo infraestructura. También se utiliza para modificar las características de la asociación.
- Autenticación y Deautenticación. Proceso necesario para que la estación se pueda conectar a la wireless LAN y consiste en la identificación de la estación. El proceso pues de conexión, pasa por la autenticación previamente a la asociación.
- Privacidad. Este servicio utilizará WEP para el encriptado de los datos en el medio.
- Reparto de MSDUs entre STAs. Éste es el servicio básico de intercambio.

El comité IEEE encargado de la tecnología de red de área local desarrolló el primer estándar para redes LAN inalámbricas (IEEE 802.11). El IEEE revisó ese estándar en octubre de 1999 para conseguir una comunicación por RF (radio frecuencia) a velocidades de datos más altas. El IEEE 802.11b resultante describe las características de las comunicaciones LAN RF de 11 Mbps.

Especificaciones para 1-2 Mbps en la banda de los 2.4 GHz. usando salto de frecuencias (FHSS) o secuencia directa (DSSS). Se transmite en diferentes bandas de frecuencias, saltando de una a otra en forma aleatoria pero predecible. Emisor y receptor deben compartir generador de números aleatorios y semilla.

### *2.1.2. IEEE 802.15 (Bluetooth)*

Bluetooth es una especificación abierta de una tecnología inalámbrica para redes basadas en radiofrecuencia, de bajo costo y con un único chip.

En 1994 Ericsson comienza unos estudios sobre la posibilidad de implementar pequeñas redes inalámbricas. Ericsson quería convertir Bluetooth en un estándar mundial, para ello inició contactos con diversas empresas.

En la primavera de 1998, cinco compañías (Ericsson, Intel, IBM, Nokia y Toshiba) forman el Bluetooth Consortium. Que tiempo después se convirtió en un estándar aprobado por la IEEE, el IEEE 802.15.

Una de las ventajas de esta tecnología es que el chip Bluetooth cuesta aproximadamente cinco dólares. Aunque suponemos que ese será el costo de fabricación, puesto que los dispositivos Bluetooth son bastante caros.

Hoy en día existe el llamado SIG (Bluetooth Special Interest Group), que conforman más de 1600 compañías. Esto significa que, aunque se pregona como un estándar abierto, es necesario pertenecer a este grupo para poder fabricar dispositivos bluetooth.

### *2.1.3. IEEE 802.16 (Banda Ancha Inalámbrica o WiMAX)*

La especificación 802.16 de la IEEE provee conectividad en áreas metropolitanas y velocidades de hasta 75Mb/sec. Los sistemas que cuentan con WiMAX pueden ser utilizados para transmitir señales en distancias tan lejanas como 30 millas. Sin embargo, en promedio un punto de acceso con esta especificación el cubrirá probablemente entre 3 a 5 millas.

Wi-FI y WiMAX son tecnologías que se complementan, WiMAX es la tecnología de última milla, esto quiere decir que conecta negocios y hogares al Internet de alta velocidad. Mientras que Wi-FI provee la conectividad de red local dentro de un edificio o un hogar. En las computadoras, o computadoras portátiles del futuro, se pudiera tener tanto comunidad de WiMAX como de Wi-FI para conectarse al Internet de alta velocidad.

## 2.2. Topologías

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y ad hoc. En este trabajo se utilizan los términos infraestructura y ad hoc, dado que son las más comunes y engloban a todas las demás topologías. Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

Una topología de infraestructura como la mostrada en la figura 2.1, es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica.

El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

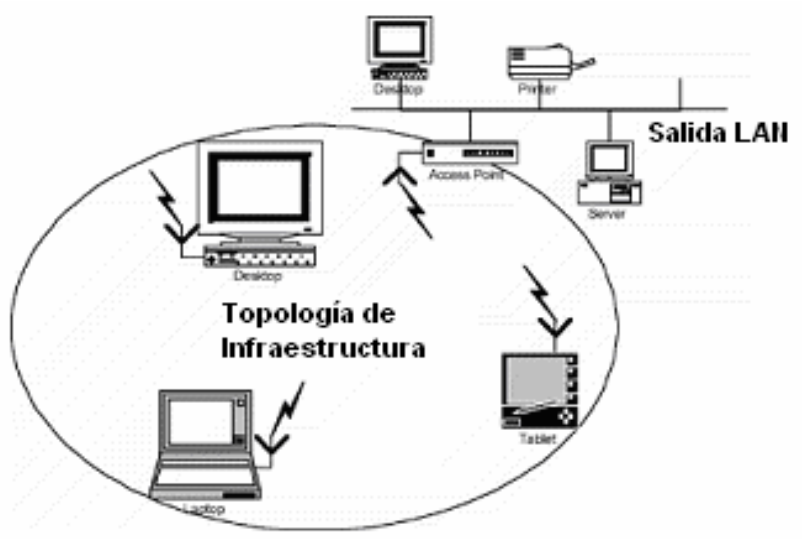



Figura 2.1. Topología infraestructura.

En una topología ad hoc (figura 2.2) los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

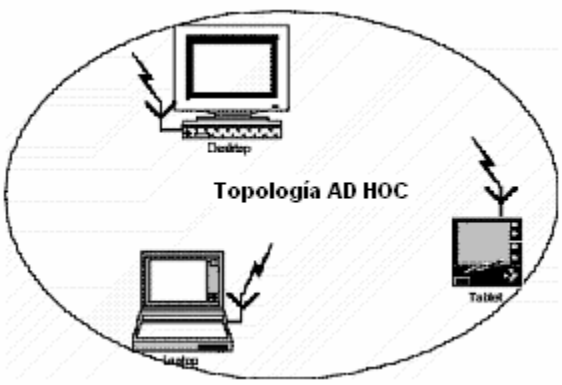



Figura 2.2. Topología ad hoc

Por ejemplo, cuando se combinan con la nueva generación de software y soluciones par a par inteligentes actuales, estas redes inalámbricas ad hoc pueden permitir a los usuarios móviles colaborar, participar en juegos de equipo, transferir archivos o comunicarse de algún otro modo mediante sus PC o dispositivos inteligentes sin cables.

### *2.2.1. Topología infraestructura*

El dispositivo portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian así mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

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

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada.

Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representan la parte del protocolo que evita las colisiones. Se debe notar que en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

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

### *2.2.2. Topología Ad Hoc*

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

Una red móvil ad-hoc es una colección de nodos móviles autónomos que se comunican entre si mediante enlaces wireless, dónde no existe una infraestructura de red fija y la administración se realiza de forma descentralizada. En este nuevo entorno, los nodos participan en la toma de decisiones, realizando las funciones propias del mantenimiento de la red y tomando parte en los algoritmos de encaminamiento.

El termino ad hoc, aunque podría ser interpretado con connotaciones negativas tales como “improvisado” o “desorganizado”, en el contexto de las redes inalámbricas hace referencia a redes flexibles, en las cuales todas las estaciones ofrecen servicios de encaminamiento para permitir la comunicación de estaciones que no tienen conexión inalámbrica directa.

En relación a las redes cableadas, las redes ad hoc presentan cambios de topología frecuentes e impredecibles debido a la movilidad de sus estaciones. Estas características impiden la utilización de protocolos de encaminamiento desarrollados para redes cableadas y crean nuevos retos de investigación que permitan ofrecer soluciones de encaminamiento eficientes que superen problemas tales como topología dinámica, recursos de ancho de banda y batería limitada y seguridad reducida.

Las computadoras de la red inalámbrica que quieren comunicarse entre ellos necesitan configurar el mismo canal y ESSID en modo ad hoc. Cabe mencionar que el ESSID es un identificador de red inalámbrica. Es algo así como el nombre de la red, pero a nivel WIFI.

Cuando un medio de red nuevo se introduce en un nuevo entorno siempre surgen nuevos retos. Esto es cierto también en el caso de las redes LAN inalámbricas. Algunos retos surgen de las diferencias entre las redes LAN con cable y las redes

LAN inalámbricas. Por ejemplo, existe una medida de seguridad inherente en las redes con cable, ya que la red de cables contiene los datos. Las redes inalámbricas presentan nuevos desafíos, debido a que los datos viajan por el aire, por ondas de radio.

Otros retos se deben a las posibilidades únicas de las redes inalámbricas. Con la libertad de movimiento que se obtiene al eliminar las ataduras (cables), los usuarios pueden desplazarse de sala en sala, de edificio en edificio, de ciudad en ciudad, etc., con las expectativas de una conectividad ininterrumpida en todo momento.

Las redes siempre han tenido retos, pero éstos aumentan cuando se agrega complejidad, tal como sucede con las redes inalámbricas. Por ejemplo, a medida que la configuración de red continúa simplificándose, las redes inalámbricas incorporan características (en ocasiones para resolver otros retos) y métrica que se agrega a los parámetros de configuración.

## 2.3. Protocolos

### *2.3.1. Mobile IP*

El protocolo IP móvil permite que computadoras configuradas para funcionar en una subred determinada cambien de subred y sigan funcionando exactamente como lo harían si estuvieran en su subred original, sin tener que cambiar su configuración. Es decir, mantienen las conexiones que hubiesen establecido hasta el momento, siguen recibiendo los paquetes dirigidos a su dirección original, y pueden acceder a los recursos de la subred original como si estuviera dentro de ella.

Para ello, es necesario que en ambas subredes existan agentes (el de la red original es el Home Agent, y el de la subred visitada es el Foreign Agent), que se encargan de facilitar la movilidad. Además, también es necesario que en la computadora que cambia de subred o Nodo Móvil tenga instalado un software que le permita registrarse en cada subred que visita con el Foreign Agent correspondiente solicitando una dirección provisional (que suele ser la del propio agente), y con su Home Agent informándole de su dirección actual a la cual deberá redirigir el tráfico que reciba en su dirección original. La figura 2.3. muestra la movilidad de IPv4.

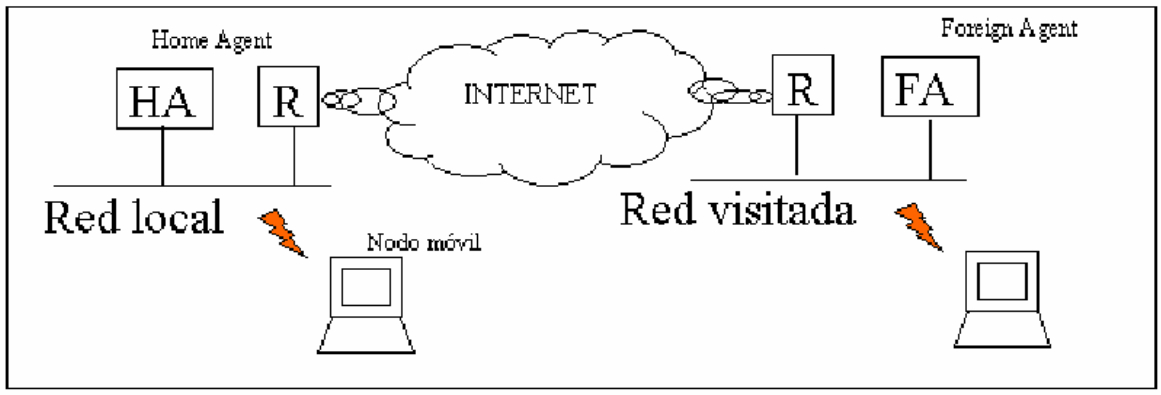



Figura 2.3. Movilidad de IPv4

La terminal móvil tiene dos direcciones IP:

- Dirección Local (Home Address): Se trata de una dirección Fija. Es con la que la terminal mantiene las conexiones y corresponde con su red local.
- Dirección de Auxilio (Care-of Address): Se trata de una dirección dinámica o cambiante. Es la que corresponde a la red en que se encuentre el nodo móvil en un momento dado.

En la red local, un Agente Local (Home Agent) sabe qué Dirección de Auxilio tiene en cada momento el nodo móvil:

Recoge los datagramas destinados a la Dirección Local del nodo móvil los reenvía dentro de un nuevo datagrama dirigido a la Dirección de Auxilio (túnel).

### *2.3.2. WAP*

WAP o Wireless Application Protocol es un estándar global desarrollado para poder ofrecer los servicios de Internet a los usuarios móviles. A pesar de que WAP está basado en la tecnología de Internet, WAP e Internet se encuentran lado a lado. Una persona o una empresa que tiene un sitio de Internet puede hacer disponible la información para un usuario móvil mediante la transformación de páginas de Internet a páginas de WAP.

WAP es el resultado del interés compartido por los líderes de la industria por crear un estándar abierto que permita ofrecer aplicaciones móviles avanzadas y acceso a

los contenidos de Internet a los usuarios de teléfonos móviles. Pero ¿Por qué este nuevo protocolo? El entorno móvil es muy diferente al tradicional de las Tecnologías de la Información (IT). Así, las especificaciones WAP se basan tanto en los estándares de Internet como en los nuevos protocolos basados en Internet, optimizados específicamente para el entorno móvil.

WAP tiene en cuenta también el factor limitativo de la red móvil -necesidad de comprimir los datos, tiempo de espera y limitado ancho de banda - y las limitaciones en los terminales: CPUs menos potentes, menor capacidad de memoria, autonomía limitada, pequeñas pantallas y diferentes dispositivos de entrada. Unas limitaciones que no impedirán que WAP sea el próximo líder en el próximo Boom de Internet desde el World Wide Web.

Con WAP, los usuarios accederán a Internet y otros servicios móviles mientras estén en el área de cobertura, independientemente de los fabricantes y operadores, gracias a la compatibilidad de los productos y soluciones, al tratarse de una plataforma común y abierta. Al disponer de un modelo común de programación y un mismo lenguaje para el desarrollo de aplicaciones, se reduce el riesgo de la fragmentación del mercado, a la vez que se le moviliza para la rápida adopción de un estándar consistente, lo que beneficia a todos: usuarios finales, operadores y la industria de las telecomunicaciones.

Los usuarios de teléfonos móviles se acostumbrarán rápidamente a los servicios WAP, ya que no será necesario aprender una nueva y compleja interfase en los aparatos móviles. Además, con el uso de la tecnología estándar de Internet, será posible optimizar los contenidos a las características de las redes actuales y futuras de telefonía móvil.

Como un estándar abierto que es, WAP proporcionará la misma tecnología a todos los vendedores independientemente de los sistemas de redes. Así, habrá terminales y soluciones compatibles con WAP de múltiples fabricantes. De hecho, ha sido adoptado ya por fabricantes que representan un 75% del mercado mundial y por operadores que actualmente cuenta con más de 100 millones de abonados en todo el mundo.

Al ofrecer una vía tecnológica también abierta, los operadores pueden seleccionar la mejor alternativa entre una amplia gama de productos. Asimismo, WAP ofrece potenciales economías de escala, al animar a los fabricantes de móviles y otros dispositivos a invertir en el desarrollo de nuevos productos compatibles. En cuanto a la Infraestructura de Redes WAP, se puede destacar que soporta Servicios de

Mensajes Cortos (SMS), Circuit Switched Data, Unstructures Supplementary Service Data (USSD) así como el inminente General Packet Radio Service (GPRS).

Por otra parte, la compañía tiene soluciones de red completas para la creación e implementación de GPRS Data Service, que incluye en su núcleo tanto el protocolo de Internet (IP) como infraestructuras de redes de radio en este sistema, que ofrece la mejor conectividad para las aplicaciones WAP.

### *2.3.3. WEP*

Wired Equivalent Privacy, (Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire. En ningún caso es compatible con IPSec.

*Características*

Según el estándar, WEP debe proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar IEEE 802.11 proporciona mecanismos de seguridad mediante procesos de autenticación y cifrado. Una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o sólo a aquellas que estén incluidas en una lista predefinida. En un sistema de clave compartida, sólo aquellas estaciones que posean una llave cifrada serán autenticadas.

Aunque los sistemas WLAN pueden resistir las escuchas ilegales pasivas, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en

el estándar 802.11, pero se considera una importante característica del algoritmo WEP.

*Cifrado*

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un *valor de comprobación de integridad* (ICV). Dicho valor de comprobación de integridad se concatena con el texto en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

*Autenticación:*

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red. De los dos niveles, la autenticación mediante clave compartida es el modo seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el *desafío (challenge)*. La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y

compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP. Si no está habilitado, el sistema revertirá de manera predeterminada al modo de sistema abierto (inseguro), permitiendo en la práctica que cualquier estación que esté situada dentro del rango de cobertura de un punto de acceso pueda conectarse a la red. Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes. Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. En tales redes, no es posible realizar una autenticación individualizada; todos los usuarios, incluyendo los no autorizados, que dispongan de la clave compartida podrán acceder a la red. Esta debilidad puede tener como resultado accesos no autorizados, especialmente si el sistema incluye un gran número de usuarios. Cuantos más usuarios haya, mayor será la probabilidad de que la clave compartida pueda caer en manos inadecuadas.

## 2.4. Estándares

### *2.4.1. Arquitectura de capas 802.11*

Este estándar define dos capas (como lo muestra la figura 2.4): la física y la MAC.

La capa física proporciona una serie de servicios a la capa MAC o capa de acceso al medio. Diferentes tecnologías de capa física se definen para transmitir por el medio inalámbrico.

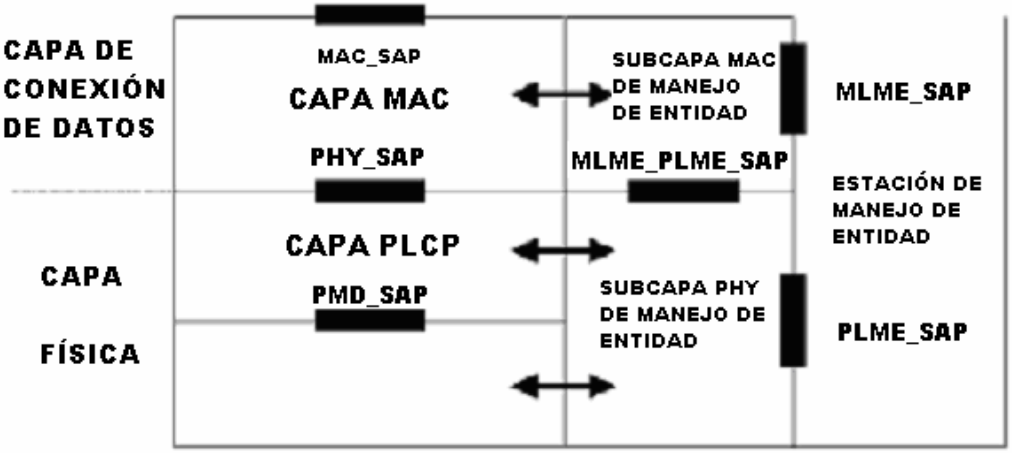



Figura 2.4. Capas definidas por IEEE802.11

La capa física de servicios consiste en dos protocolos: PLCP y el PMD.

La primera capa se refiere a una función de convergencia, esto es de capa física, que adapta las capacidades del sistema físico dependiente del medio (PMD). Esta función es implementada por el protocolo PLCP o procedimiento de convergencia de capa física, que define una forma de mapear MPDUs o unidades de datos MAC en un formato de tramas susceptibles de ser transmitidas o recibidas entre diferentes estaciones o STASs a través de la capa PMD.

Un sistema PMD, cuya función define las características y un medio de transmitir y recibir a través de un medio sin cables entre dos o más STAs.

La comunicación entre MACs de diferentes estaciones se realiza a través de la capa física mediante de una serie de puntos de acceso al servicio, donde la capa MAC invoca las primitivas de servicio.

Además de estas capas, podemos distinguir la capa física de gestión. En esta capa podemos distinguir la estructura MIB (Management Information Base) que contienen por definición las variables de gestión, los atributos, las acciones y las notificaciones requeridas para gestionar una estación. Consiste en un conjunto de variables donde podemos especificar o contener el estado y la configuración de las comunicaciones de una estación.

### *2.4.2. IEEE802.11a*

Banda de 5 GHz, específica la capa física y la capa MAC.

Extensión de 802.11 para proporcionar 54 Mbps usando OFDM.

El estándar IEEE802.11a es una evolución del IEEE802.11, el cual fue desarrollado para proporcionar conectividad multimedia inalámbrica a terminales portátiles, en ambientes de área local, llamados WLAN.

En contraste, la banda de los 5 GHz utilizada por el estándar IEEE802.11a está a salvo de interferencias por otras tecnologías y tiene más ancho de banda disponible, lo que permite trabajar hasta una tasa de 54 Mbps, en incrementos de canales de 20 MHz de ancho de banda. El método de modulación utilizado por este estándar está basado en Multicanalización por División de Frecuencias Ortogonales (OFDM), también conocido como Modulación Multiportadora; este método consiste en dividir una señal de información de alta velocidad en múltiples sub-señales de información y transmitirlas en paralelo utilizando frecuencias portadoras ortogonales.

Las ventajas de OFDM son:

- Alta eficiencia espectral (la ortogonalidad de las portadoras permite el traslape del espectro).
- Rechazo a interferencia de RF (no todas las portadoras son afectadas por la interferencia de RF).
- Menor distorsión por propagación multitrayectoria (puesto que las sub-señales se transmiten a menor velocidad, la duración del símbolo es mayor y no le afecta al receptor el esparcimiento de retardo tanto como a los sistemas de portadora única).

La ortogonalidad en OFDM se debe a la relación precisa que existe entre las sub-portadoras que forman un símbolo OFDM. Cada sub-portadora contiene exactamente un número entero de ciclos en un intervalo de tiempo dado T.

El estándar IEEE802.11a define 8 canales en la banda de 5.15 a 5.35 GHz, y 4 en la banda de 5.725 a 5.825 GHz. La tasa de 54 Mbps es suficiente para soportar las necesidades presentes y futuras de tráfico a nivel de WLAN, tal como transmisión

de audio digital, telefonía con voz sobre IP (VoIP), acceso a Internet, televisión digital, transmisión de ráfagas de DVD y servicios de video por demanda (VoD).

Los parámetros de modulación de IEEE802.11a dependen de la tasa de bit deseada, y se asignan de acuerdo a la tabla 2.1.

| Tasa Mbps | Modulación | Tasa de codificación (R) | Bits/ portadora | Bits/ símbolo OFDM | Datos/ símbolo OFDM |
|---|---|---|---|---|---|
| 6 | BPSK | ½ | 1 | 48 | 24 |
| 9 | BPSK | ¾ | 1 | 48 | 36 |
| 12 | QPSK | ½ | 2 | 96 | 48 |
| 18 | QPSK | ¾ | 2 | 96 | 72 |
| 24 | 16-QAM | ½ | 4 | 192 | 96 |
| 36 | 16-QAM | ¾ | 4 | 192 | 144 |
| 48 | 64-QAM | 2/3 | 6 | 288 | 192 |
| 54 | 64-QAM | ¾ | 6 | 288 | 216 |

Tabla 2.1. Tasas de bit para IEEE802.11a

La figura 2.5 muestra la arquitectura de una red local inalámbrica de acuerdo al estándar IEEE802.11, donde sus principales componentes son:

- AP: Punto de acceso, tiene funcionalidad de estación y proporciona acceso a los servicios de distribución a través del medio inalámbrico.
- BSS: Conjunto de servicio básico, contiene estaciones controladas por una función de coordinación sencilla.
- ESS: Conjunto de servicio extendido, agrupa LAN's y BSS's y aparece como un BSS sencillo ante la capa de control de enlace lógico.
- DS: Sistema de distribución, usado para interconectar un conjunto de BSS's y LAN's para crear un ESS.

- STA: Estación, cualquier dispositivo que contenga las capas física y MAC de acuerdo al estándar IEEE802.11.
- SS: Servicio de estación, conjunto de servicios que soportan el transporte de unidades de datos de servicio MAC (MSDU's) entre estaciones dentro de un BSS.

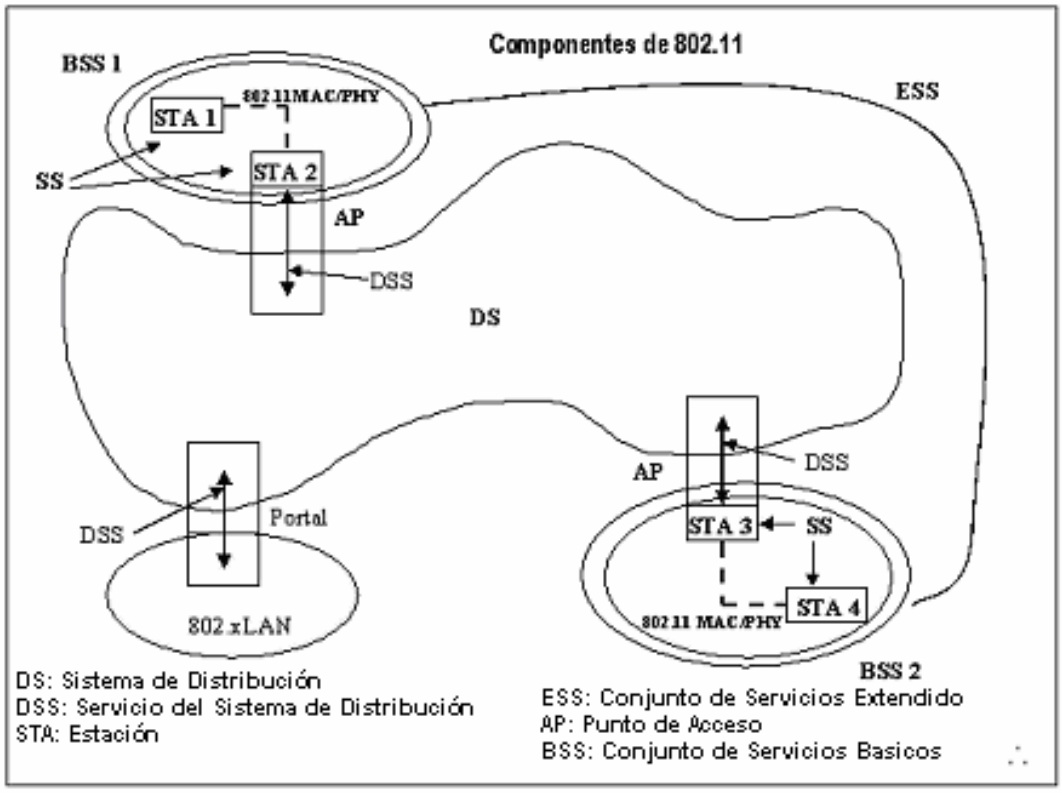



Figura 2.5. Arquitectura de red IEEE802.11

## *2.4.3. IEEE802.11b*

La denominación Wi-Fi (Wireless-Fidelity) aplicada al protocolo inalámbrico IEEE802.11b significa que vía radio, mantiene con fidelidad las características de un enlace Ethernet cableado, capaces de interoperar con productos de otros fabricantes.

Por extensión se conoce como WiFi 5 al protocolo IEEE 802.11a que es el nuevo estándar de la misma familia para la banda de 5 GHz. Dado que estos protocolos Wi-Fi ya están implementados en múltiples productos comerciales, podemos considerar que se han convertido en el estándar inmediato para las aplicaciones WLAN en detrimento del estándar Hiperlan2 del ETSI.

Banda de 2.4 Ghz, específica la capa física y la capa MAC hasta 11 Mbps. Extensión de 802.11 para proporcionar 11 Mbps usando DSSS. Utiliza una nueva forma de modulación, CCK (complementary coding keying), para proporcionar 11 Mbps (con caídas a 5.5 Mbps, 2 Mbps y 1 Mbps).

En 802.11b existe un protocolo de encriptación llamado WEP (Wireless Encryption Protocol), a continuación enumeramos algunas de sus características:

- Razonablemente fuerte.
- Computacionalemente eficiente.
- Exportable internacionalmente.
- Opcional.
- Recientemente roto (U. Berkeley).

### *2.4.4. IEEE802.11e*

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.

Se aplicará a los estándares físicos a, b y g de 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.

### *2.4.5. IEEE802.11f*

Interoperatividad de puntos de acceso de distintos fabricantes (por ejemplo, itinerancia).

Los estándares mencionados hasta ahora permiten la conexión de las terminales dentro de una misma subred IP. Hasta ahora si queremos movernos sobre diferentes sub-redes IP debemos utilizar soluciones de un mismo fabricante. Actualmente el IEEE está desarrollando un nuevo estándar que define la intercomunicación entre Puntos de Acceso de distintos fabricantes (facilitando el roaming). Entre otros temas la norma define el registro de un punto de acceso dentro de una red y el intercambio de información cuando un usuario se mueve por una zona cubierta por AP (Access Point) de diferentes fabricantes. Esta norma es conocida como IEEE 802.11f.

## *2.4.6. IEEE 802.11g*

En Junio de 2003, el Instituto de Ingeniería Eléctrica y Electrónica ratificó el nuevo estándar 802.11g que viene a mejorar el 802.11b tan utilizado en las redes inalámbricas, en la figura 2.6 se muestran estas mejoras. Según los expertos, este nuevo estándar ofrecerá a usuarios y proveedores WLAN una mayor flexibilidad a la hora de seleccionar el sistema que mejor se adapte a sus necesidades y favorecerá el crecimiento industrial de los distintos productos wireless.

Sin duda el rápido desarrollo e implantación obliga a los profesionales de esta área a formarse y mantenerse actualizados de todas las novedades y así evitar decisiones incorrectas que podrían evitarse con un mayor conocimiento de la tecnología.

El estándar 802.11g es una extensión de 802.11 para proporcionar de 20 a 54 Mbps usando DSSS y OFDM. Es compatible con 802.11b además que tiene mayor alcance y menor consumo de potencia que 802.11a.

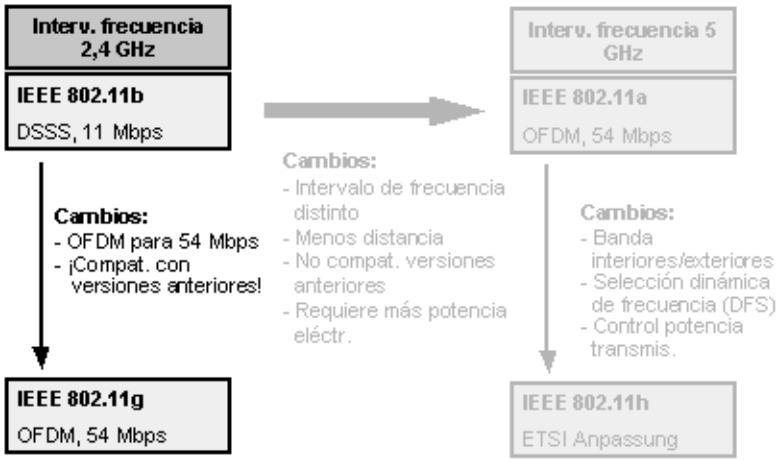


Figura 2.6. Mejoras del estándar 802.11b.

El estándar IEEE 802.11g alcanza velocidades más altas y es compatible con los equipos 802.11b ya existentes. El 802.11g opera en la misma banda de frecuencia de 2,4 GHz y con los mismos tipos de modulación DSSS que el 802.11b a velocidades de hasta 11 Mbps, mientras que a velocidades superiores utiliza tipos de modulación OFDM más eficientes.

Esta compatibilidad con versiones anteriores protege la inversión de los clientes en varios aspectos. Una tarjeta de interfaz de red IEEE 802.11g, por ejemplo, puede funcionar con un punto de acceso 802.11b y viceversa, a velocidades de hasta 11 Mbps. Para lograr velocidades más altas, de hasta 54 Mbps, tanto el punto de acceso como la tarjeta de red deben ser compatibles con el estándar 802.11g. El borrador del estándar también especifica tipos de modulación opcionales (como OFDM/CCK) diseñados para mejorar la eficiencia en una instalación íntegramente 802.11g. En instalaciones grandes, la ventaja de tener aproximadamente los mismos alcances de transmisión efectivos es que la estructura WLAN 802.11b ya existente se puede mejorar fácilmente para lograr velocidades más altas sin necesidad de instalar puntos de acceso adicionales en muchos lugares nuevos a la hora de cubrir una zona determinada.

En comparación con el estándar IEEE 802.11a, el 802.11g tiene un ancho de banda utilizable más bajo, lo que redunda en un menor número de usuarios WLAN de alta velocidad. Aunque las modulaciones OFDM permiten una velocidad más alta, el ancho de banda disponible total en la banda de frecuencia de 2,4 GHz no varía. El motivo es que el IEEE 802.11g todavía está restringido a tres canales en la banda de 2,4 GHz.

- Ofrece las mismas distancias de funcionamiento que el IEEE802.11b.
- Previsión sobre la disponibilidad de los productos: Primer trimestre 2003.

La modulación OFDM se ha desarrollado para ser utilizada en sistemas 802.11a que ya operen en las bandas de 5 GHz. El mayor problema a la hora de introducir la modulación OFDM en la banda de 2,4 GHz fue hacerla compatible con los productos 802.11b heredados.

El principal mecanismo para compartir canales en el sistema 802.11 es CSMA/CA. Para que este método funcione, cada radio debe ser capaz de detectar a todas las demás radios asociadas al mismo punto de acceso (incluido, obviamente, el propio AP). Pero con sistemas 802.11g que utilizaran OFDM, las radios 802.11b heredadas serían incapaces de detectar a los nuevos dispositivos.

El grupo de trabajo IEEE 802.11g solucionó este problema utilizando una función de solicitud de envío/preparado para enviar (RTS-CTS) que ya incorporan todos los dispositivos 802.11.

Para que una red IEEE 802.11 funcione correctamente, todos los nodos deben encontrarse dentro del radio de alcance del punto de acceso (el radio de alcance es de unos 100 metros, aunque en muchos casos depende de la potencia del Access Point), aunque no suceda lo mismo entre ellos. Es lo que se conoce como problema del "nodo oculto". En situaciones como ésta, se puede invocar el mecanismo de RTS-CTS para reducir la posibilidad de colisión. En IEEE 802.11g, la función RTS-CTS se puede utilizar para facilitar el funcionamiento de la red cuando hay una mezcla de clientes 802.11g y clientes 802.11b heredados operando en el mismo BSS (Basic Service Set).

Todos los clientes y puntos de acceso 802.11g deben ser capaces de retroceder y operar exactamente como un dispositivo 802.11b heredado. De esta forma, la migración a la tecnología 802.11g es fácil y dinámica. Mientras se van adquiriendo e instalando nuevos puntos de acceso 802.11g, los puntos de acceso 802.11b heredados pueden permanecer en servicio y ser totalmente compatibles con los clientes 802.11g más nuevos.

IEEE 802.11g (versión "draft" o provisional desde Octubre 2002). Con multiplexación OFDM permite hasta 54 Mbps de capacidad máxima en la banda de 2.4 Ghz. Permite interoperabilidad con IEEE 802.11b utilizando un interfaz aire SS-DS y ofreciendo hasta 11 Mbps de capacidad.
Aunque OFDM sea una tecnología excelente para las aplicaciones WLAN de interior, las leyes de la física indican que el alcance de la comunicación es proporcional a la longitud de onda. En otras palabras, los objetos dispersan y atenúan la energía de radiofrecuencia de un modo más eficaz cuanto más alta sea la frecuencia utilizada.

En un espacio abierto, las diferencias de propagación no deberían suponer ningún problema. Sin embargo, la mayoría de sistemas WLAN funcionan en interiores, donde los espacios abiertos son limitados y casi todas las señales de radio tienen que atravesar paredes, mobiliario y otros obstáculos.

Los equipos IEEE 802.11a alcanzan velocidades de datos más altas en enlaces cortos o en un vestíbulo donde es posible la propagación por un espacio abierto. No

obstante, la velocidad de los datos disminuye rápidamente cuando la señal debe atravesar paredes y otros obstáculos.
Los productos IEEE 802.11g son capaces de conseguir velocidades de datos más elevadas y con mayor alcance que los productos con tecnología 802.11a. La combinación de OFDM y la mejor capacidad para atravesar paredes de sus 2,4 GHz confieren a los productos 802.11g una ventaja clara sobre otras tecnologías WLAN de alta velocidad. La capacidad para proporcionar una cobertura de gran rendimiento en un área comparativamente grande desde un único punto de acceso supone un factor importante de costo.

Un punto de acceso 802.11b de 2,4 GHz, por ejemplo, no podrá trabajar con una tarjeta de interfaz de red 802.11a de 5 GHz. No obstante, estos estándares pueden coexistir perfectamente, como lo ilustra la figura 2.7.

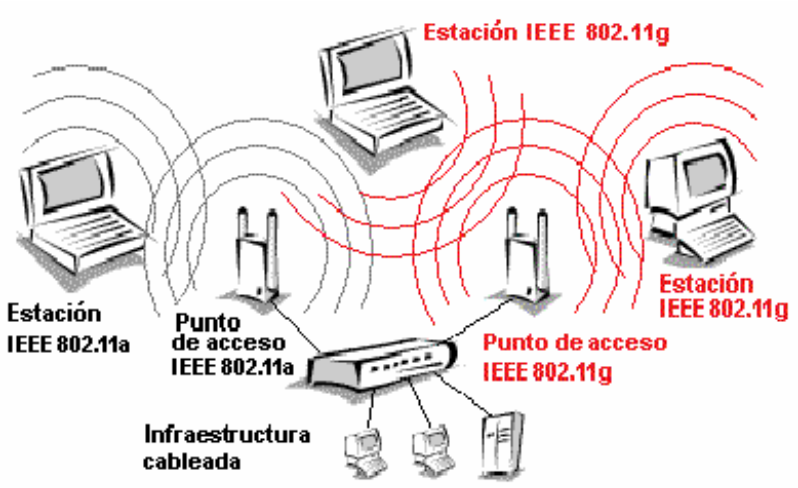



Figura 2.7. Coexistencia de diferentes estándares.

Por ejemplo: un usuario 802.11a y un usuario 802.11b que utilicen puntos de acceso y cliente separados, conectados a la misma red LAN, pueden operar en el mismo espacio físico y compartir recursos de la red, como la banda ancha o el acceso a Internet.

## *2.4.7. IEEE802.11h*

Cambios de especificaciones IEEE802.11 a especificaciones ETSI, los cuales se muestran en la figura 2.8.

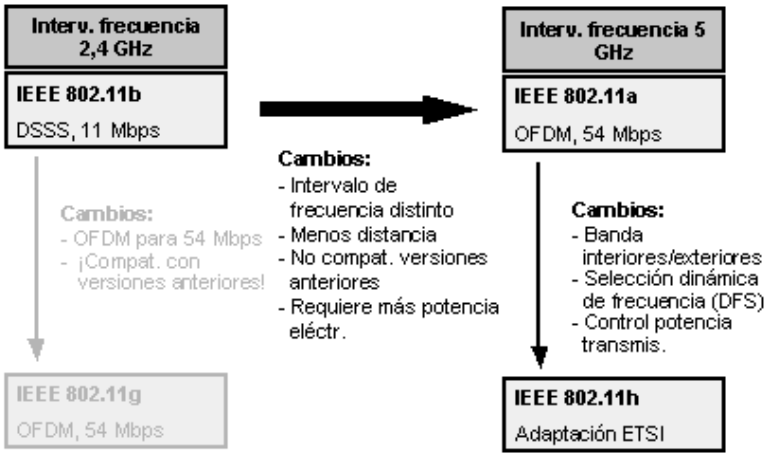



Figura 2.8. Cambios a las especificaciones IEEE802.11

Al adoptar la banda de frecuencia de 5 GHz y utilizar la modulación OFDM, el estándar IEEE 802.11a goza de dos notables ventajas respecto al 802.11b. Incrementa la velocidad máxima de transferencia de datos por canal (de 11 Mbps a 54 Mbps) y aumenta el número de canales sin solapamiento.

La banda de 5 GHz (banda UNII) está formada por tres sub-bandas, UNII1 (5,15 - 5,25 GHz), UNII2 (5,25 - 5,35 GHz) y UNII3 (5,725 - 5,825 GHz). Cuando se utilizan tanto UNII1 como UNII2, hay 8 canales sin solapamiento disponibles; mientras que con la banda de 2,4 GHz sólo hay 3. El ancho de banda total disponible en la banda de 5 GHz también es mayor que en la banda de 2,4 GHz (300 MHz por 83,5 MHz). Así pues, una WLAN basada en el 802.11a puede admitir un mayor número de usuarios de alta velocidad simultáneos sin peligro de que surjan conflictos. Un inconveniente de utilizar la banda de 5 GHz es que las frecuencias utilizadas no están estandarizadas internacionalmente.

Asimismo, deben hacerse algunas transacciones en cuanto a compatibilidad y alcance. Como los estándares 802.11a y 802.11b operan en bandas de frecuencia distintas, los productos no son compatibles. El asunto de la compatibilidad se complica un poco más al no estar reflejados los requisitos europeos ETSI en el estándar IEEE 802.11a. Así pues, tecnologías como Dynamic-Frequency-Selection (DFS) y Transmit-Power-Protocol (TPC) están englobadas en el estándar IEEE 802.11h.

La frecuencia de funcionamiento más alta del estándar 802.11a tiene como consecuencia un alcance relativamente más corto. Se necesitarán más puntos de

acceso 802.11a para cubrir la misma zona. Pero incluso con estos inconvenientes, las pruebas iniciales demuestran que los productos 802.11a ofrecen un rendimiento casi tres veces superior al de los 802.11b en cuanto a alcances en interiores.

### *2.4.8. IEEE802.11i*

Pretende rediseñar la seguridad WiFi, incorporando nuevas funcionalidades. Estuvo disponible hasta finales de 2003 y se aplicará a los estándares físicos a, b y g de 802.11.

Estándar que define la encriptación y la autentificación para complementar completar y mejorar el WEP, mejoras de la seguridad WEP (WEP2). Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP).

El estándar 802.11i también ofrece caché esencial para permitir la reconexión rápida con servidores cuando una persona vuelva. Proporciona autenticación previa para una itinerancia rápida entre los puntos de acceso de la red.

El resultado final práctico de la ratificación de 802.11i es que el mercado de la tecnología inalámbrica debe mejorar de nuevo ya que el firmware se actualiza y hay nuevos productos que entran en el mercado. Con 802.11i, toda la cadena de seguridad para la conexión, intercambio de credenciales, autenticación y codificación se vuelve mucho más sólida y eficaz en la protección frente a ataques dirigidos y no dirigidos. Ahora la red y la integridad de sesión sólo tienen que gestionarse y no protegerse.

## 2.5. Elementos

Se enumeran a continuación los principales tipos de equipos empleados para la construcción de infraestructuras de redes inalámbricas y que serán empleados por los equipos terminales de cliente para una apropiada interconexión.

Aunque se clasifican de una manera formal, en la realidad los equipos de los fabricantes suelen integrar modos híbridos de funcionamiento que diluyen dicha

estructuración. Por ejemplo es ya normal encontrar gateways que operan además como puntos de acceso y bridges, o bridges como APs y repeaters.

Además de esta clasificación, en casi todos los casos existen modelos de interior, pensados para operar en lugares cerrados y protegidos, y de exteriores, más robustos y con mayor margen de temperaturas de funcionamiento.

### *2.5.1. Access Point*

Es un nodo especial en una red inalámbrica que actúa como punto centralizador y gestor del tráfico del resto de equipos (terminales de cliente) subscritos a él y dentro de la celda de cobertura.

Dispone comúnmente de una interfaz ethernet que le permite estar interconectado a una red cableada (LAN), además de la interfaz inalámbrica por la cual se conectan los equipos de dicha naturaleza. Permite la comunicación entre ambas interfaces y entre los propios equipos inalámbricos a nivel 2 (modelo OSI). En general en una misma localización puede coexistir más de un punto de acceso siempre que no interfieran fuertemente sus frecuencias de funcionamiento. Los equipos presentes estarán subscritos sólo a uno. Este dispositivo se muestra en la figura 2.9.




Figura 2.9. Access Point

Esta definición de punto de acceso es muy genérica de tal forma que otros equipos inalámbricos como routers y bridges realmente se pueden considerar como APs. Sin embargo los fabricantes mantienen esta definición para catalogar los equipos más genéricos y elementales, aunque funcionalmente en realidad se pueden equiparar a bridges que unen un segmento de red cableada y otro (de alguna forma virtual o no cableado) inalámbrico.

La configuración de estos equipos es muy sencilla, apenas necesitando la introducción de su dirección IP (en la mayoría de ellos se puede activar el cliente DHCP que poseen y de esta forma la capturan automáticamente), la del gateway por defecto, los parámetros de la parte inalámbrica y su securización.

### *2.5.2. Bridges*

Son elementos que interconectan dos o más redes locales (a nivel 2 OSI). En el mundo wireless el concepto se matiza: deben interconectar redes locales fijas. Esta definición expone su principal uso, la interconexión de redes fijas separadas por una distancia física la cual se ha cubierto mediante un segmento inalámbrico.

Poseen dos interfaces, uno ethernet y otro inalámbrico. En cada red fija se ubica un bridge inalámbrico, orientando las antenas de ambos equipos para la mejor recepción. En redes con edificios distantes, se suelen instalar antenas directivas de alta ganancia en los techos, lo que permite cubrir distancias en visión directa de hasta unos pocos kilómetros. Este dispositivo se muestra en la figura 2.10.



Figura 2.10. Bridge

Los parámetros inalámbricos (canal de frecuencia, bitrate, identificador de servicio-SSID, etc.) de ambos extremos deben ser idénticos para posibilitar la comunicación. Virtualmente se pueden encadenar un número ilimitado de parejas de bridges para enlazar infraestructuras muy distantes o con obstáculos entre si.

La configuración de estos dispositivos suele ser también bastante simple, requiriendo adicionalmente a los parámetros indicados para un AP poco más que la introducción de la dirección IP del bridge del otro extremo.

Los bridges que se encuentran comercialmente disponibles suelen agregar otras funcionalidades como son el disponer de otros modos de operación: como AP, repeater e incluso como adaptador de red para equipos de cliente.

### *2.5.3. Repeaters*

Permiten extender la cobertura de APs mediante la regeneración y reenvío de información a zonas anteriormente sin suficiente señal. Teóricamente poseen una única interfaz inalámbrica, que les permite conectarse por un lado al punto de acceso para el cual operan, y por otro lado a los equipos inalámbricos que se le subscriben. A continuación en la figura 2.11. se muestra este dispositivo.



Figura 2.11. Repeater

Operan con los mismos parámetros que el AP para el cual trabajan (frecuencia, bitrate, etc.). La ventaja de extender de esta forma la cobertura de las redes tiene su precio: dado que toda la información que un equipo le transmite la tiene que remitir al AP, la eficiencia de la solución es inferior al 50%. También es factible encadenar numerosos repeaters para ampliar todavía más el alcance, pero numerosos problemas que aparecen por colisiones, retardos de señal y penalización en el uso del espectro, no aconsejan emplear más de uno.

En el mercado apenas existen como tal estos equipos. Dependiendo del fabricante, muchos gateways como APs y bridges pueden configurarse en modo de funcionamiento repeater, siendo la solución empleada.

### *2.5.4. Routers y Gateways*

Poseen capacidad de enrutamiento (niveles 3 y 4 OSI) de los paquetes de información que los atraviesan. Una de sus interfaces es inalámbrica, existiendo al menos otra fija ethernet a la cual se suele denominar puerto WAN. La mayoría de modelos existentes en el mercado no posee funcionalidades puras de router, sino que están especialmente diseñados para actuar como gateway entre la red inalámbrica directamente gestionada por el equipo (genéricamente llamada LAN) y las redes externas (red local de empresa, red de acceso a Internet u otras). Por ello con frecuencia se les denomina gateway. El dispositivo se puede observar en la figura 2.12.



Figura 2.12. Router

Su complejidad interna es superior al resto de los otros equipos. No sólo realizan labores de mayor procesamiento de la información como el enrutamiento, sino que además han sido enriquecidos con funcionalidades avanzadas en networking (traducción de direcciones por NAT y PAT o servidor DHCP de direccionamiento propio) y seguridad (firewall interno avanzado, listas de acceso por dirección MAC ethernet, bloqueo de acceso a urls para control paterno, restricción de uso por franja horaria, etc.).

Además de lo anterior, suelen proporcionar en la parte LAN, además del interfaz wireless, un conmutador ethernet integrado de varios puertos. Ya menos frecuente, también algunos modelos poseen un servidor interno de impresión junto a un puerto serie, paralelo o USB para conectar una impresora. Igualmente existen modelos que poseen un interfaz para interconectarse directamente con redes ADSL.

Aunque por el momento raramente presente, pronto se extenderá la gestión de redes privadas virtuales (VPNs) e incluso proporcionar voz sobre IP (VoIP).

De forma análoga al resto de los equipos, los gateways pueden proporcionar modos de configuración que les permiten operar como puntos de acceso, repeaters e incluso bridges.

Con toda esta riqueza de funciones, los gateways reúnen en un único equipo las prestaciones que hasta el momento necesitaban varios (un router, un AP wireless, un módem ADSL, un firewall, etc.) y a un precio muy competitivo.

### *2.5.5. Antenas*

Actualmente ya hay fabricantes que ofrecen antenas que aumentan la capacidad de TX/RX (transmisión y recepción) de los dispositivos wireless, en especial de los Access Point (aunque actualmente ya se puede comenzar a aplicar también a las Tarjetas de Red) se puede modificar enormemente la capacidad de **TX/RX** gracias al uso de antenas especiales. Estas antenas se pueden dividir en tres tipos:

## *1) Antenas direccionales (o directivas)*

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz de luz concreto y estrecho pero de forma intensa (más alcance).

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. En la figura 2.13 se muestra una antena de este tipo.



Figura 2.13. Antena Direccional

## *2) Antenas omnidireccionales*

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance.

Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional. En la figura 2.14 se muestra una antena omnidireccional.



Figura 2.14. Antena Omnidireccional

## *3) Antenas sectoriales*

Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con un haz de luz más ancho de lo normal. En la figura 2.15 se muestra una antena del tipo sectorial.



Figura 2.15. Antena Sectorial

Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar tres antenas sectoriales de 120º ó 4 antenas sectoriales de 90º. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

# CAPÍTULO 3. DISEÑO E IMPLEMENTACIÓN DE LA RED

En este capítulo se hará el análisis de la red existente en el laboratorio de Redes y Seguridad, el sistema operativo, el equipo de cómputo y el equipo de red a utilizar, también se mostrará brevemente la forma de configurar dicho equipo en dos diferentes sistemas operativos, así como la implementación de la red y algunas consideraciones y detalles que hay que tomar en cuenta al instalar dichos equipos.

# 3.1. Análisis de la red existente en el laboratorio.

De acuerdo al análisis de la red existente en el laboratorio se determinó que la topología empleada es una estrella física y bus lógico, la cual está compuesta por un Switch 3Com de 24 puertos de 10/100, así mismo se cuenta con un servidor con sistema operativo Linux Red Hat 9 el cual presta el servicio de DHCP y cuenta con dos tarjetas de red para poder brindar el servicio de Internet empleando NAT (Network Address Translation).

Dicha red está compuesta por nueve computadoras de las cuales cinco tienen sistema operativo Windows XP y Linux, una tiene Windows XP y las tres restantes tienen Linux únicamente como se muestra en la figura 3.1.

La tecnología utilizada en esta red es Ethernet la cual tiene una velocidad de 10 Mbps.

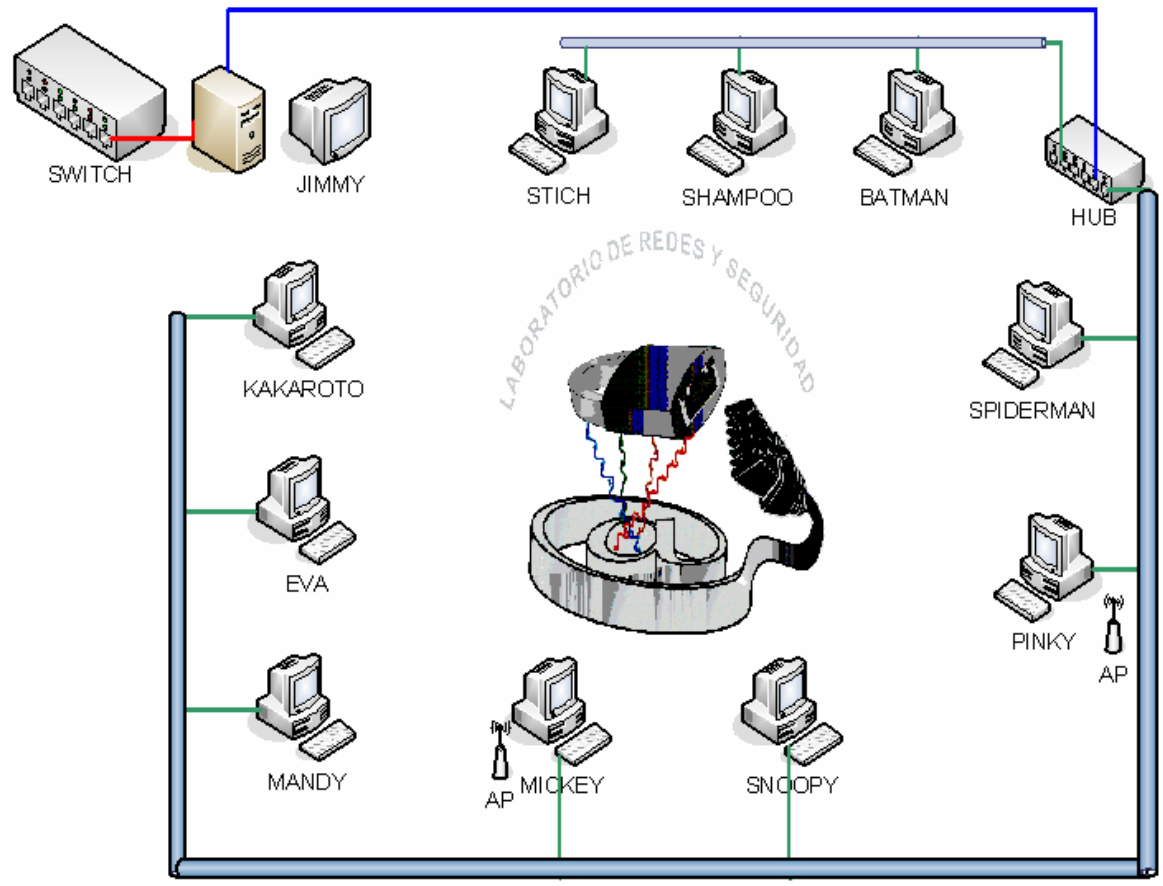



Figura 3.1. Red Actual del laboratorio

# 3.2. Determinación de la mejor opción para la red.

## *3.2.1. Sistema operativo*

*Características del sistema operativo Linux*

Este sistema operativo tiene como una de sus características principales el ser muy estable, sin embargo suele ser difícil su utilización, por eso es recomendable tener experiencia utilizando dicho sistema operativo a nivel de administración, ya que puede resultar difícil la instalación y/o configuración del hardware y software, esto es porque el usuario debe tener conocimiento del sistema operativo, pero una vez instalado y configurado es muy estable lo cual se traduce en menos molestias para el usuario, es decir, no pierde tiempo haciendo correcciones y ajustes a su sistema.

*Características del sistema operativo Windows*

El sistema operativo Windows es mucho más amigable en el sentido de la instalación y/o configuración, ya que el usuario no requiere tener conocimientos avanzados del sistema operativo para la instalación y/o configuración, sin embargo al ser un sistema operativo sumamente gráfico muy comúnmente tiene problemas de memoria, lo cual vuelve al sistema inestable lo que con frecuencia se traduce en tiempos muertos para el usuario.

Se hicieron pruebas muy básicas a nivel de usuario, como analizar que tarjeta es más facil de instalar y configurar, que interfaz gráfica es más amigable para el usuario, para determinar cual es el mejor sistema operativo para la red del laboratorio, sin embargo debemos destacar que se probaron ambos sistemas operativos porque este proyecto es primeramente académico, y los estudiantes deben tener una visión integral de este tipo de redes tanto teórica como práctica.

De acuerdo a nuestra experiencia y a las pruebas realizadas especialmente llevadas a cabo para este proyecto con los sistemas operativos Windows en sus diferentes versiones (XP, 9x, etc.) y Linux en sus diferentes distribuciones (Debian, RH, Fedora, Mandrake, etc.), llegamos a la conclusión de que ambos sistemas operativos son una buena opción para usarse como clientes en una red inalámbrica.

## *3.2.2. Análisis de los prerrequisitos en los equipos*

En este apartado se presenta el análisis de las características y prerrequisitos de una serie de equipos para que funcionen correctamente en una red inalámbrica.

### *A) Computadoras Personales (PC´s)*

Las computadoras tecnológicamente más recientes tienen suficiente memoria en RAM y capacidad en disco duro, para que casi cualquier dispositivo funcione sin ningún problema y las tarjetas de red inalámbrica no son la excepción.

En el sistema operativo Windows XP es recomendable tener al menos 128 MB en RAM, ya que este sistema requiere de mucha memoria, en las versiones anteriores de Windows como son 2000, ME y 98SE, se puede tener menos capacidad en RAM, pero no es recomendable tener menos de 128 MB, ya que este sistema operativo es muy gráfico y requiere de más memoria.

En Linux, se puede tener una PC con menos cantidad de memoria de la que se considera para operar con ambientes Windows, aunque siempre es recomendable tener al menos 128 MB, esto es porque al ser un sistema operativo en el que la instalación puede ser personalizada no se suele instalar muchas aplicaciones que usarían memoria, lo cual permite un mejor uso de nuestros recursos.

Para ambos sistemas operativos, la capacidad del disco duro hoy en día no es ninguna limitante, para tener una tarjeta de red inalámbrica y muchos más dispositivos instalados y funcionando en la computadora, ya que dichos discos duros ahora son de capacidades suficientes. Pero se debe tener al menos 5MB de espacio libre en disco duro para instalar el driver de la tarjeta de red inalámbrica y las utilerías de la misma.

Así mismo se be contar con una ranura PCI libre en la tarjeta madre para poder instalar la tarjeta de re red inalámbrica y un lector de CD’s para instalar el driver y utilerías de la misma.

### *B) Computadoras Portátiles - Laptops*

Las laptops más recientes ya traen la tarjeta de red inalámbrica internamente, lo cual hace que desaparezcan los problemas de compatibilidad entre tarjeta y laptop,

sin embargo en laptops que no tienen la tarjeta integrada se requiere una tarjeta externa, para lo cual es necesario considerar el sistema operativo del equipo así como la versión con la que esté trabajando.

Generalmente en Windows no hay problema para que sea reconocida la tarjeta de red externa, más sin embargo en Linux hay que estar seguro que existen los drivers correspondientes para su funcionamiento antes de adquirir la tarjeta.

En estos equipos también es recomendable tener más memoria en RAM si se tiene exclusivamente Windows, en el caso de Linux, como se mencionó antes se puede tener menos memoria RAM sin que el sistema tenga problemas.

Al igual que en una PC se debe tener al menos 5MB de espacio libre en disco duro para instalar el driver de la tarjeta de red inalámbrica y las utilerías de la misma. Unidad lectora de CD's y contar con una ranura CardBus libre para instalar la tarjeta de red inalámbrica.

### *3.2.3. Análisis del equipo a utilizar*

Los criterios bajo los cuales se decidió qué equipo utilizar fueron básicamente que cumpliera con:

- El estándar IEEE 802.11B.
- Las expectativas de uso a corto y mediano plazo.

Teniendo en cuenta eso, se decidió por los siguientes equipos:

#### *Access Point (AP11B Punto de Acceso IEEE802.11b)*

*Descripción*

El punto de acceso AP11B de MSI (figura 3.2) es compatible con IEEE802.11b, y conecta una o más computadoras habilitadas para sistema inalámbrico con una red Ethernet o módem para Cable/DSL para una conexión de alta velocidad.

Las antenas de alta ganancia del AP11B ofrecen un rango de operación de hasta 150 metros en el interior, suministrando un roaming continuo a través de su infraestructura LAN.




Figura 3.2. Access Point AP11B

*Características*

*Transmisión de datos en 11 Mbps / Alcance interior de 45-150m.*

El AP11B funciona con aplicaciones de datos intensivas como multimedia y video/audio incluso a través de paredes, pisos y techos.

Interoperable con cualquier dispositivo en conformidad con 802.11b.

El AP11B cumple con las normas IEEE 802.11b y Wi-Fi, permitiendo una completa interoperabilidad con cualquier producto inalámbrico con certificación Wi-Fi.

Seguridad WEP para asegurar la privacidad.

Soporta encriptamiento WEP de 64/128 bits, lo que asegura que la señal de red sea segura y privada eliminando así problemas con usuarios que no pertenezcan a la red.

*Diseño de Antena superior*

La antena bipolar provee una recepción y transmisión polarizada superior para la mejor calidad de señal.

*Especificaciones*

En la tabla 3.1, se muestran las especificaciones técnicas del access point utilizado en la red.

| | |
|---|---|
| **Transmisión de datos** | 11, 5.5, 2, 1 Mbps y auto-fallback. |
| **Normas** | IEEE 802.11b<br>IEEE 802.3u 10/100BaseTX |
| **Alcance** | 45-150 metros (interior), 300-480 metros (exterior). |
| **Frecuencia** | 2.4 GHz |
| **Tipo de Radio Inalámbrico** | DSSS (Direct Sequence Spread Spectrum). |
| **Tipo de Modulación** | CCK, BPSK, y QPSK. |
| **Opciones de Encriptamiento de Datos WEP** | 64/128 bits |
| **Antena** | Un patch interno de alta ganancia, una bipolar externa. |
| **Soporte de Protocolos** | TCP/IP, DHCP Client, HTTP. |
| **Interfase con cable** | Un Ethernet IEEE 802.3u 10/100BaseTX, RJ-45 con Auto MDI/MDI-X. |
| **Configuraciones Personalizadas** | Modo Red, ESSID, Canales, Tasa Tx, Umbral RTS/CTS, Umbral de Fragmentación, WEP, Filtro Mac, Firmware actualizable. |

| | |
|---|---|
| **Indicadores LED** | Energía, Estado de Tráfico inalámbrico, WEP, Ethernet |
| **Potencia de Salida** | Hasta +18dBm |
| **Sensibilidad** | • -82dBm@11Mbps.<br>• -85dBm@5.5Mbps.<br>• -87dBm@2Mbps.<br>• -88dBm@1Mbps. |
| **Consumo de Energía** | Modo de Transmisión ≤ 310mA |
| **Adaptador de Energía** | • 110~120AC<br>• 220~240AC<br>• DC output: 12V DC<br>• Output current: 500mA |
| **Voltaje de Entrada** | 5VDC |
| **Dimensiones (WxDxH)** | 124.5 x 88.5 x 24.5mm (sin stand) |
| **Peso** | • Con stand: 233g<br>• Sin stand: 133g |
| **Ambiente de Operación** | • Temperatura de Operación: 0~50˚C (32~122˚F)<br>• Temperatura de Guardado: -30~70˚C (-22~158˚F)<br>• Humedad: hasta 40˚C (104˚F) con 85% sin condensación |

Tabla 3.1. Especificaciones del Access Point.

### *Tarjeta de red (PC11B2 Tarjeta PCI IEEE802.11b Inalámbrica)*

*Descripción*

La tarjeta PC11B2 de MSI (figura 3.3) entrega hasta 11Mbps en tasa de transmisión de datos en la frecuencia de 2.4GHz. Trabaja con dispositivos bajo normas IEEE 802.11b y es apta para operar con aplicaciones de datos intensivas incluyendo video streaming MPEG en tiempo real. Además, la tarjeta PC11B2 ayuda a prevenir el acceso a información vital de la red a fin de asegurar las transmisiones mediante encriptamiento WEP y 802.11i TKIP en 64/128 bits.



Figura 3.3. Tarjeta de Red Inalámbrica

*Características*

- Transferencia de datos de 11Mbps

  La PC11B2 entrega una tasa de transferencia de datos de hasta 11Mbps.

- Interoperable con dispositivos compatibles con 802.11b

  La PC11B2 es compatible con normas IEEE 802.11b, permitiendo una completa interoperabilidad con cualquier producto inalámbrico con certificación IEEE 802.11b.

*Transmisiones Seguras*

- WEP: Encriptamiento seguro WEP (Wired Equivalent Privacy) de 64/128 bits para asegurar las transmisiones inalámbricas de datos por LAN.
- SSID: Sólo estaciones que utilizan el mismo SSID (Service Set ID) tienen permiso para comunicarse entre sí.

*Especificaciones*

En la tabla 3.2, se mencionan las especificaciones técnicas de la tarjeta instalada para esta red.

| | |
|---|---|
| **Formato** | 32-bit PCI v2.2 |
| **Normas** | IEEE 802. 11b |
| **Alcance de Frecuencia** | 2.4GHz a 2.4835GHz<br>Direct Sequence Spread Spectrum (DSSS) |
| **Rango de Datos** | 11, 5.5, 2, 1 Mbps, Auto Fall-Back |
| **Canales de Operación** | • US & Canada: 11 canales<br>• Europa: 1 a 13 canales<br>• Francia: 4 canales<br>• España: 2 canales<br>• Japón: 13 canales |
| **Modulación** | • DBPSK @ 1Mbps<br>• DQPSK @ 2Mbps<br>• CCK @ 5.5 y 11Mbps |
| **Protocolo de Acceso** | CSMA/CA con ACK (Medio-Duplex) |
| **Antena** | Bipolar |
| **Seguridad/Encriptamiento** | 64-/128-bit WEP |
| **Alcance/Cobertura (Espacio abierto)** | 350m @ 11Mbps |
| **Voltaje de Operación** | 3.3V |
| **Consumo de Energía** | • Modo Sleep: <50mA<br>• Modo Escucha: <120mA<br>• Modo Recepción: <180 mA<br>• Modo Transmisión: < 372mA |
| **Potencia de Salida** | 17 ± 1dBm |
| **Temperatura de Operación** | 0 a 60˚C |
| **Humedad de Operación** | 0 a 90% (sin condensación) |
| **Sistemas Operativos** | Windows® 98SE/ME/2000/XP, Linux |
| **Certificaciones** | FCC Part 15, CE, Wi-Fi |

| | |
|---|---|
| **Dimensiones (WxDxH)** | 122 x 64 x 19mm |
| **Peso** | 55g |

Tabla 3.2. Especificaciones de la Tarjeta de Red

## 3.3. Implementación

De acuerdo al diseño de la red existente y a las características estudiadas en el capítulo anterior de una red inalámbrica, se optó por implementar este tipo de red en el laboratorio.

La red inalámbrica consta de dos access point y dos tarjetas de red inalámbricas, uno de los access point (unamfi) tiene como medida de seguridad el uso de una clave WEP para una conexión segura (el protocolo es explicado en el capítulo 2).

El otro access point (labredes) no cuenta con clave de acceso para la realización de ciertas prácticas de laboratorio, por lo cual está abierto a todos los usuarios que cuenten con una tarjeta de red inalámbrica.

La diferencia entre conectarse a uno o a otro, es que en "unamfi" al necesitarse una clave WEP implica que son usuarios conocidos, es decir, son usuarios que el administrador sabe que tienen una cuenta para conectarse al AP y la ventaja es que la conexión se hace a una velocidad máxima de 11 Mbps, mientras que en "labredes" al ser abierto a todos los usuarios, es decir, cualquiera que tenga un equipo con una tarjeta inalámbrica que cumpla el estándar IEEE802.11b la conexión se hace a una velocidad máxima de 2 Mbps.

La idea de tener estos dos tipos de conexión es para que al conectarse al access point cerrado como un usuario conocido tenga un servicio más robusto, como un ancho de banda mayor, una dirección IP permanente, además de contar con una conexión segura.

Mientras que al conectarse al access point abierto, es para uso un poco más ligero, como revisar correo, bajar algún documento urgente, así como para proyectos de investigación en redes inalámbricas en el área de seguridad.

Las tarjetas de red fueron instaladas en dos PC's con sistema operativo Windows XP, ya que no existen drivers para el sistema operativo Linux.

A pesar de que el sistema operativo Linux ha crecido en usuarios, las grandes compañías aún no se preocupan lo suficiente en tener soporte para plataformas diferentes a la que se usa comúnmente, así que los desarrollos para esas plataformas son hechas por personas que han trabajado mucho con esos sistemas operativos y se dan cuenta de las necesidades que existen.

### *3.3.1. Configuración de los access point*

La configuración de los access point "unamfi" y "labredes" se muestra y explica a continuación en la tabla 3.3 y tabla 3.4 respectivamente.

Para "unamfi" se tiene la siguiente configuración básica.

| | |
|---|---|
| **LAN Settings** | |
| **LAN IP Address** | 192.168.2.253 |
| **Subnet Mask** | 255.255.255.0 |
| **DHCP Client** | Off |
| **LAN MAC Address** | 00:0C:76:C9:D5:03 |
| | |
| **Wireless Settings** | |
| **SSID** | unamfi |
| **Channel** | 7 |
| **Accept Authentication Type** | Shared Key |
| **Encryption** | 40 bits |
| **Number of Associated Clients** | 0 |
| **Maximum Link Speed** | 11 Mbps |

Tabla 3.3. Configuración del Access Point unamfi.

**LAN IP Address**, indica la dirección IP asignada al Access Point.

**Subnet Mask**, indica la mascara de red de la red a la que pertenece el Access Point.

**DHCP Client**, indica si se quiere asignar de forma automática la dirección IP al Access Point, para ello se debe tener instalado un servidor DHCP.

**LAN IP Address**, indica la dirección física o dirección MAC del access point.

**SSID**, indica el nombre que se le asigno a la red, y sólo tarjetas de red inalámbricas que utilizan el mismo SSID tienen permiso para comunicarse entre sí.

**Channel**, indica el canal de operación.

**Accept Authentication Type**, indica el tipo de autentificación que utilizará el Access Point, al ser esta una red segura, se usa una llave compartida.

**Encryption**, indica el número de bits a utilizar en la encriptación de datos.

**Number of Associated Clients**, indica el número de tarjetas inalámbricas conectadas al Access Point.

**Maximum Link Speed**, indica la velocidad máxima a la que se podrán conectar los equipos al Access Point.

Para "labredes" se tiene la siguiente configuración básica.

| **LAN Settings** | |
|---|---|
| **LAN IP Address** | 192.168.2.254 |
| **Subnet Mask** | 255.255.255.0 |
| **DHCP Client** | Off |
| **LAN MAC Address** | 00:0C:76:C9:DB:24 |

| **Wireless Settings** | |
|---|---|
| **SSID** | labredes |
| **Channel** | 7 |
| **Accept Authentication Type** | Open System |
| **Encryption** | None |
| **Number of Associated Clients** | 1 |
| **Maximum Link Speed** | 2 Mbps |

Tabla 3.4. Configuración Access Point labredes.

**LAN IP Address**, indica la dirección IP que tiene asignada el Access Point.

**Subnet Mask**, indica la mascara de red de la red a la que pertenece el Access Point.

**DHCP Client**, indica si se quiere asignar de forma automática la dirección IP al Access Point, para ello se debe tener instalado un servidor DHCP.

**LAN IP Address**, indica la dirección física o dirección MAC de la tarjeta de red inalámbrica.

**SSID**, indica el nombre que se le asignó al Access Point, y sólo tarjetas de red inalámbricas que utilizan el mismo SSID tienen permiso para comunicarse entre sí.

**Channel**, indica el canal de operación.

**Accept Authentication Type**, indica el tipo de autentificación que utilizara el Access Point, en este caso no emplea ningún tipo por lo que marcar que esta abierto.

**Encryption**, indica el número de bits a utilizar en la encriptación de datos.

**Number of Associated Clients**, indica el número de tarjetas inalámbricas conectadas al Access Point.

**Maximum Link Speed**, indica la velocidad máxima a la que se podrán conectar los equipos al Access Point.

Como se puede apreciar la configuración de estos access points es similar, sin embargo varia la configuración de uno a otro, ya que en ***unamfi*** se activa la clave WEP y por lo tanto hay que introducir una clave que puede ser de 40 bits o de 128 bits, para tener como mencionamos anteriormente dos diferentes tipos de conexiones (Abierto y con clave WEP o cerrado). Y en el access point ***labredes*** se disminuye el ancho de banda a 2Mb.

## *3.3.2. Configuración de las tarjetas de red*

## *En el sistema operativo Windows*

Para configurar la tarjeta de red inalámbrica bajo el sistema operativo Windows, en particular en *Windows XP Profesional* resulta muy sencillo ya que todo se hace de forma gráfica y se hace de la siguiente manera.

El primer paso es ir a la sección de Conexiones de Red y la forma es dar un clic con el Mouse en ***Inicio → Conexiones de Red → Mostrar Todas las Conexiones*** una vez allí aparecerá un icono con el nombre ***Conexión de Área Local*** al cual hay que dar un clic derecho con el Mouse y seleccionar ***Propiedades*** con lo cual nos aparecerá una ventana en donde se muestra lo que actualmente utiliza la conexión de red.

Una vez identificado esto seleccionar la opción que dice ***Protocolo de Internet (TCP/IP)*** y dar un clic en ***Propiedades*** al hacer esto aparecerá otra ventana en donde se muestran las propiedades del protocolo de Internet (TCP/IP), al llegar a este punto hay dos posibles opciones de configuración la primera es si se quiere que el servidor DHCP proporcione automáticamente las direcciones IP a la tarjeta de red inalámbrica para ello se tiene que elegir las siguientes opciones:

***a) Obtener una Dirección IP Automáticamente*** y
b***) Obtener una Dirección de Servidor DNS Automáticamente***.

La otra opción es si queremos proporcionarle de forma manual la dirección IP a la tarjeta de red inalámbrica para ello se debe seleccionar una de las siguientes opciones:

a***) Usar la Siguiente Dirección IP*** y proporcionar lo siguiente:

Dirección IP: **192.168.2.60** (Por ejemplo, el ultimo número esta en el rango de 1 a 254)
Mascara de Red: **255.255.255.0**
Puerta de Enlace: **192.168.2.1**

***b) Usar la Siguiente Dirección de Servidor DNS*** y teclear lo siguiente (para el caso de la UNAM):

Servidor DNS Primario: **132.248.10.2**
Servidor DNS Secundario: **132.248.204.1**

Una vez elegida cualquiera de las dos opciones, ya sea de asignar la IP de forma automática o hacerlo manualmente y haber tecleado lo necesario, dar ***Aceptar*** a todas las ventanas.

La opción que se elija depende si se cuenta con una dirección IP, con las direcciones del servidor de nombres, la dirección de la puerta de enlace y la mascara de red. Si no se cuenta con estos datos mencionado se debe de elegir la opción de obtener una dirección IP automáticamente. Ahora, tiene ventajas el contar con una dirección IP ya que el ancho de banda de la conexión será de 11 Mbps y si no se cuenta con dicha dirección IP, es decir, se elige de forma automática, se tendrá un ancho de banda de 2 Mbps, es decir, se tendrá una conexión mas lenta que en la otra opción.

## *En el sistema operativo Linux*

La configuración de la tarjeta de red inalámbrica en el sistema operativo Linux, se puede hacer básicamente de dos formas, la primera de ellas es de forma temporal, es decir, la configuración de la tarjeta permanecerá mientras la computadora esté encendida y esto se hace con el siguiente comando:

*Ifconfig eth0 192.168.2.60 netmask 255.255.255.0*

La segunda forma, es configurar la tarjeta de forma permanente, esto puede hacerse de dos formas, en distribuciones más amigables como Fedora, ya existe la posibilidad de hacerlo en forma gráfica, sin embargo aquí mencionaremos la forma de hacerlo editando archivos.

### *En Fedora.*

En este sistema el archivo que debe editarse para la configuración de la tarjeta es el siguiente.

En el subdirectorio /*etc/sysconfig/network-scripts* existe el archivo llamado *ifcfg-ethx* la *x* indica el número de tarjeta, esto es, si sólo se tiene una tarjeta el archivo tendrá el nombre *ifcfg-eth0* y así sucesivamente.

El archivo tiene las siguientes líneas, se numeraran para explicar las más importantes.

```
1.  DEVICE=eth0
2.  BOOTPROTO=none
3.  HWADDR=00:0D:56:59:E1:18
4.  ONBOOT=yes
5.  TYPE=Ethernet
6.  DHCP_HOSTNAME=
7.  IPADDR=192.168.2.100
8.  NETMASK=255.255.255.o
9.  USERCTL=no
10. PEERDNS=no
11. GATEWAY=192.168.2.1
12. IPV6INIT=no
```

En la línea número 1, es donde se define el nombre del dispositivo, en este caso por ser la única tarjeta es el *eth0*.

En la línea 4, el parámetro "ONBOOT" es para decirle al sistema que levante la tarjeta al iniciar si se pone un "yes".

En la línea 7, se configura la dirección IP que tendrá la tarjeta.

La línea 8, tiene la mascara de red

Y por último la línea 11, tendrá la dirección del equipo de salida.

## *En Debian*

En la distribución Debian, la configuración es similar que en Fedora, la diferencia es que se edita el archivo *interfaces* que está en el subdirectorio */etc/network*, dicho archivo tiene las siguientes líneas que se enumeran a continuación para explicarlas.

```
iface eth0 inet static
  1.address 192.168.2.100
```

```
2.netmask 255.255.255.0
3.network 192.168.2.0
4.broadcast 192.168.2.255
5.gateway 192.168.2.1
```

En la línea 1, se configura la dirección IP de la tarjeta.
En la línea 2, se tendrá la mascara de red.
En la línea 3, se pondrá la red.
En la línea 5, se configura el equipo de salida.

Las direcciones IP que se usan en esta red son no homologadas, el segmento utilizado es el 192.168.2.0/254, dichas IP pueden ser asignadas a cada dispositivo de manera manual o en caso de tener un cliente de DHCP instalado el servidor del laboratorio le asignará automáticamente una IP.

Como se puede apreciar, la configuración en el sistema operativo Windows es mucho más sencilla, ya que no tenemos que buscar el archivo que debemos modificar para cambiar los parámetros como en Linux, sin embargo en ninguno de los dos casos se requiere mucha experiencia para configurar una tarjeta de red.

# CAPÍTULO 4. PRUEBAS A LA RED

En este capítulo presentamos las pruebas realizadas a la red, las cuales nos permitirán evaluar su estado, asimismo, con estas pruebas podremos determinar si es funcional, y si podemos hacer mejoras, para garantizar que todos los usuarios que hagan uso de ella tengan un servicio de calidad.

# 4.1. Pruebas de conectividad

A continuación se da una descripción de las pruebas de conectividad hechas a los access ponits ***labredes*** y ***unamfi***, se comienza con *labredes*.

## *A) Conexión a labredes*

Para hacer este tipo de prueba lo que se realizó fue generar tráfico desde la terminal con la tarjeta inalámbrica, esto se logró descargando un archivo grande que fue una imagen ISO, y generando tráfico ICMP por medio del comando PING hacia la dirección www.google.com como lo muestra la figura 4.1 y así verificar que la conexión entre la tarjeta de red y el access point de nombre ***labredes*** no se perdía, esto nos permitió comprobar que se tiene una buena conexión entre los dispositivos antes mencionados, sin que se pierda conectividad.

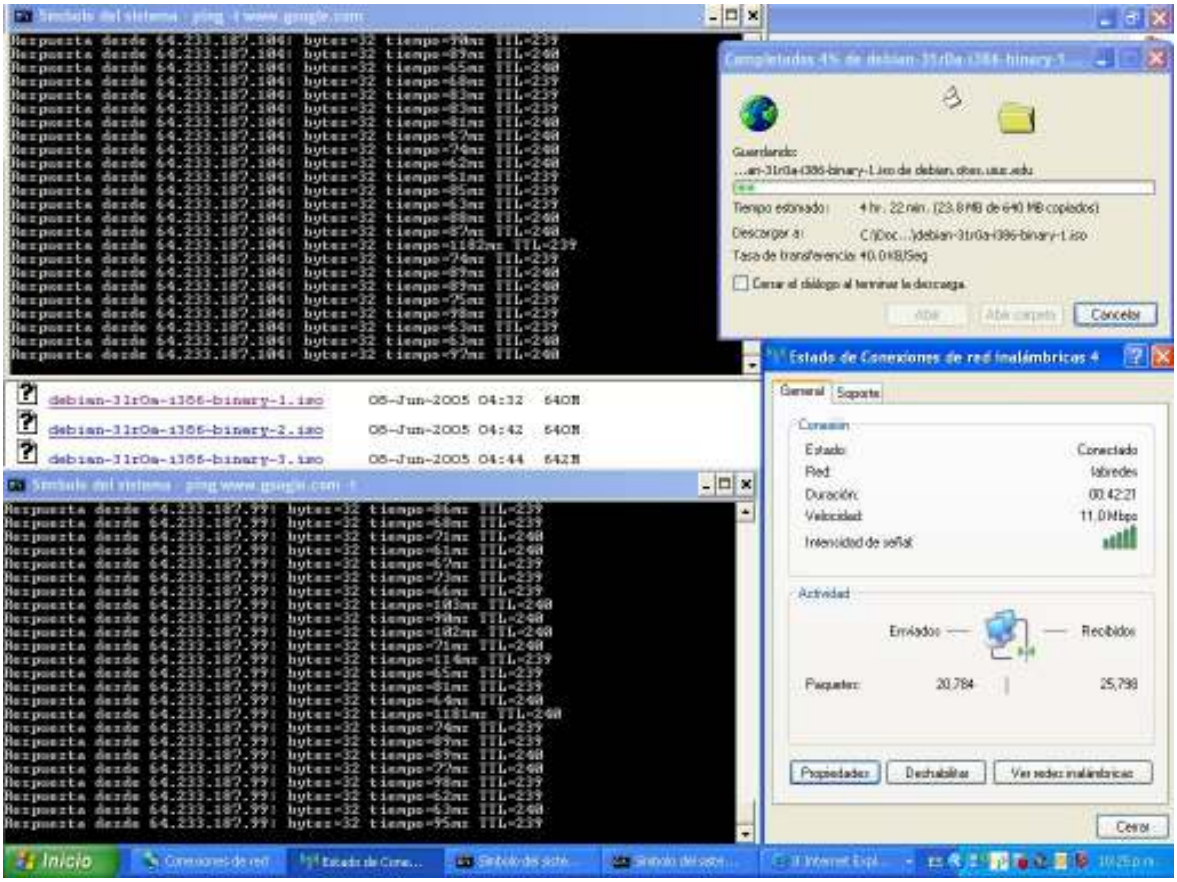



Figura 4.1. Pruebas de conexión al Access Point ***labredes***

### *B) Conexión unamfi*

La prueba que se le hizo al segundo access point fue la misma que al ***labredes***, como lo muestra la figura 4.2. Comprobando al igual que en el anterior access point no se pierde la conexión entre la tarjeta de red y el access point de nombre ***unamfi*** y que dicha conexión tiene una recepción muy buena.

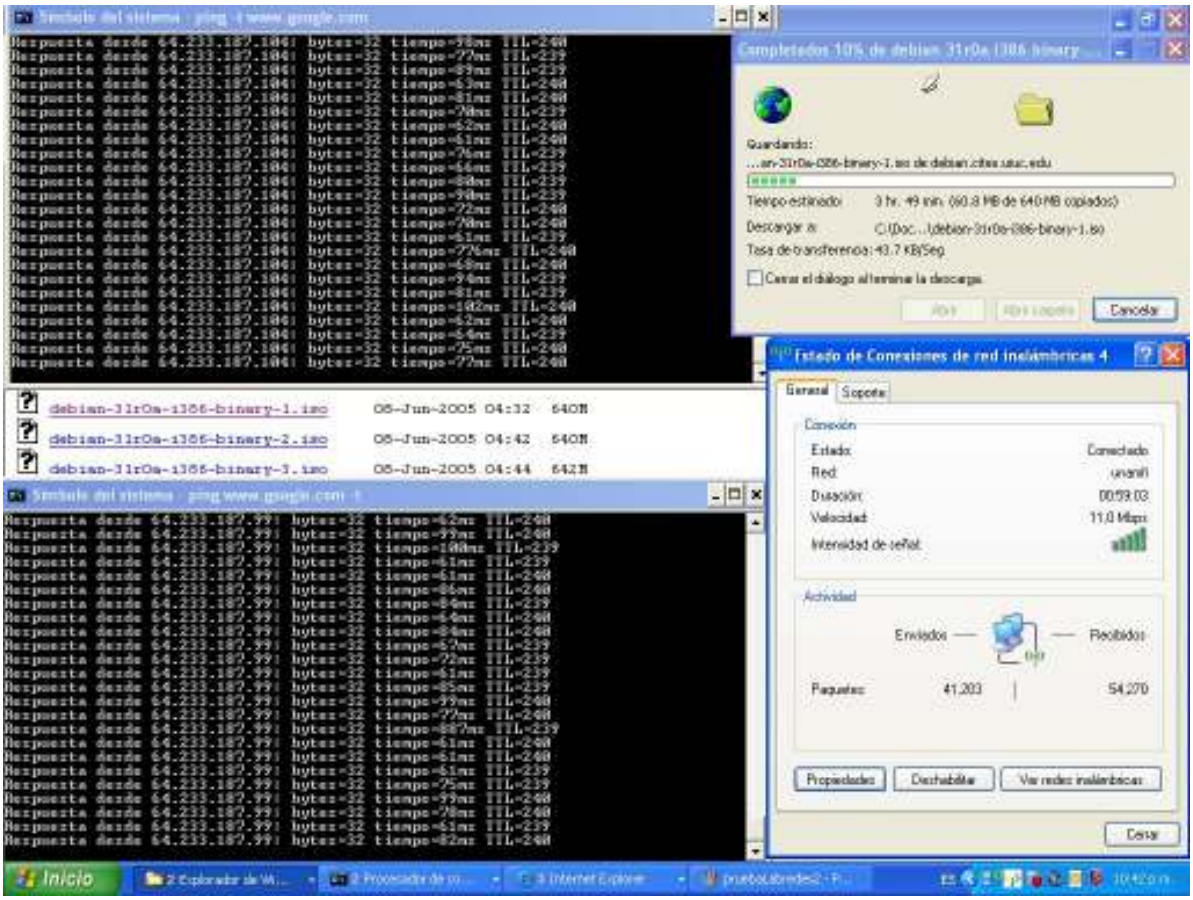


Figura 4.2. Pruebas de conexión al Access Point ***unamfi***

## 4.2. Pruebas de alcance

En estas pruebas de alcance lo que se pretendió fue tener un aproximado de la longitud que puede alcanzar la señal del access point, para esto se realizaron pruebas horizontales y verticales.

### *4.2.1. Horizontal*

Esta prueba se realizó con una laptop, salimos del laboratorio e hicimos una aproximación de la distancia que puede alcanzar la señal, aproximadamente a los 12 metros la señal se vuelve inestable como se muestra en la figura 4.3, estas pruebas fueron realizadas con un comando PING y descargando una imagen ISO.

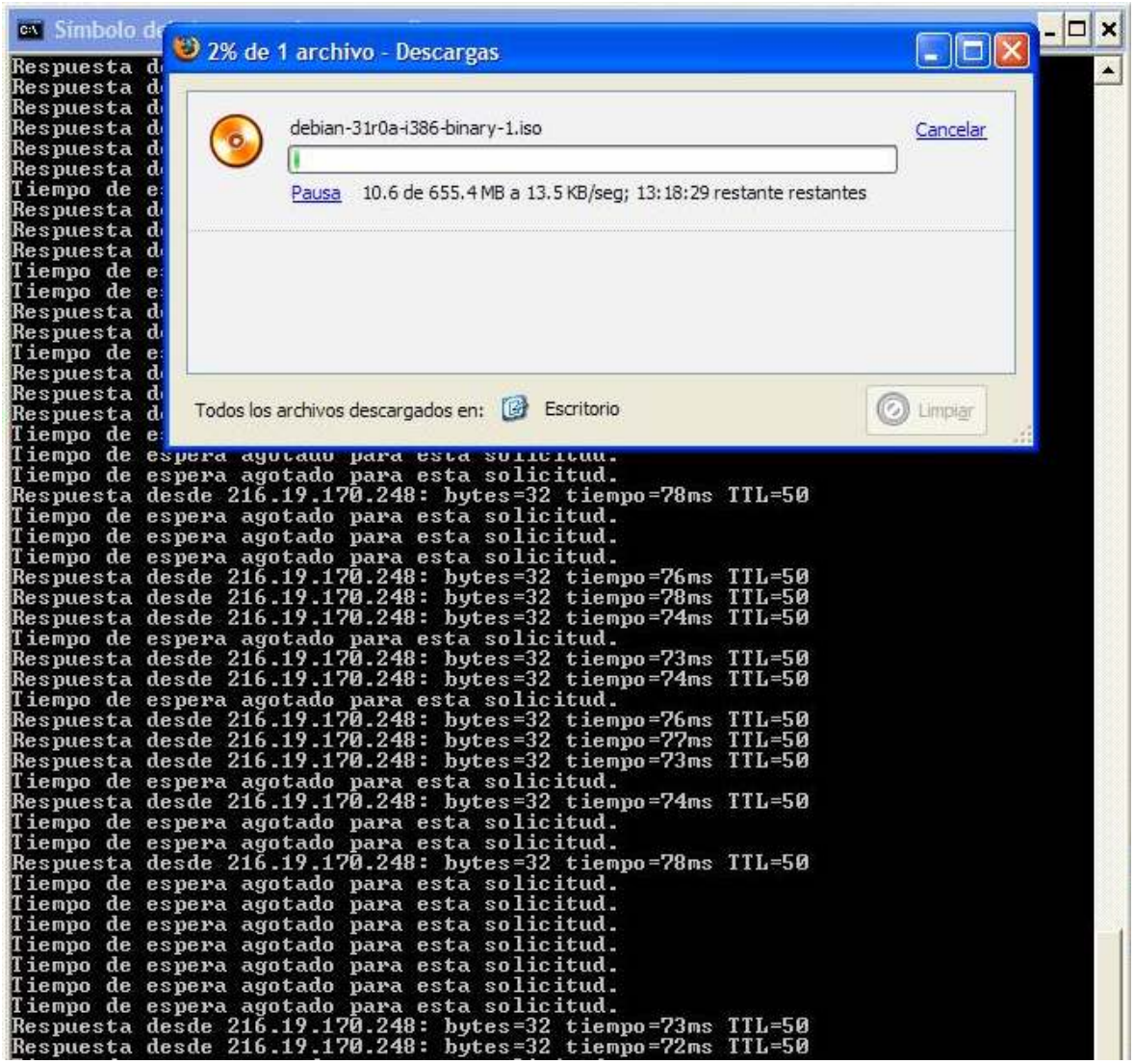


Figura 4.3. Pruebas de alcance horizontal.

Es una distancia considerable, hay que tomar en cuenta que la señal no atraviesa muchas bardas, sólo cruza un cubículo, lo que quiere decir que sólo se interponen dos cristales.

### *4.2.2. Vertical*

Para la realización de esta prueba al igual que la de distancia horizontal, salimos con una laptop a verificar la distancia de la señal, en este caso la señal sólo logró llegar hasta el primer piso del edificio Valdez Vallejo, después de ahí la señal se vuelve inestable como lo muestra la figura 4.4.

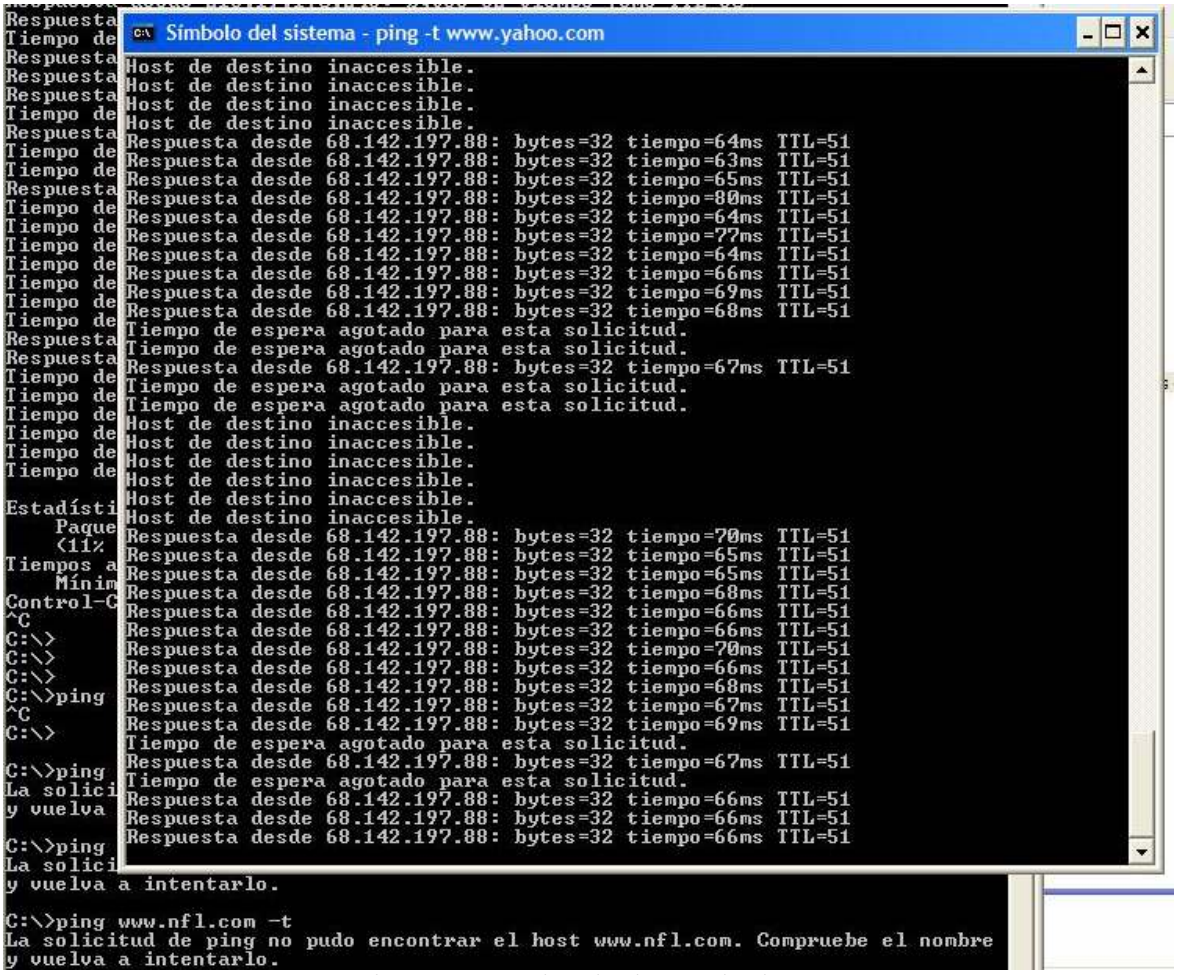


Figura 4.4. Pruebas de alcance de altura.

Debemos tomar en cuenta que en este caso la señal debe atravesar muchos más obstaculos que en la prueba de longitud horizontal, es a esta causa que atribuimos la poca distancia alcanzada.

## 4.3. Pruebas de autenticación WEP

Estas pruebas se refieren a que en los access point se configurará la opción de autenticación mediante clave WEP, cabe mencionar que existen dos opciones para esta configuración que tienen que ver con el tamaño de la clave, se tiene la opción de 40 y 128 bits, lo que se traduce en una clave de 10 ó 26 dígitos hexadecimales respectivamente, en estas pruebas por facilidad configuramos una clave de 40 bits (10 dígitos), sin embargo en la práctica es mejor utilizar una clave robusta que contenga números y letras, dicha configuración también es sensible a mayúsculas y minúsculas.

Como se mencionó, el primer paso fue asignar una clave WEP de 40 bits al access point, una vez configurada el segundo paso fue tratar de conectarse a dicho access point y al teclear una contraseña incorrecta el resultado fue un error que dice conectividad limitada o nula así como también muestra el icono de conexión a red con un signo de admiración indicándonos que hay un error con la conexión a la red inalámbrica como lo muestra la figura 4.5.

Así mismo al teclear en la línea de comandos las siguientes sentencias ipconfig /all y ping –t www.google.com nos mandan dichos comandos errores, comprobando de forma mas rotunda que no se tiene conexión de red inalámbrica.

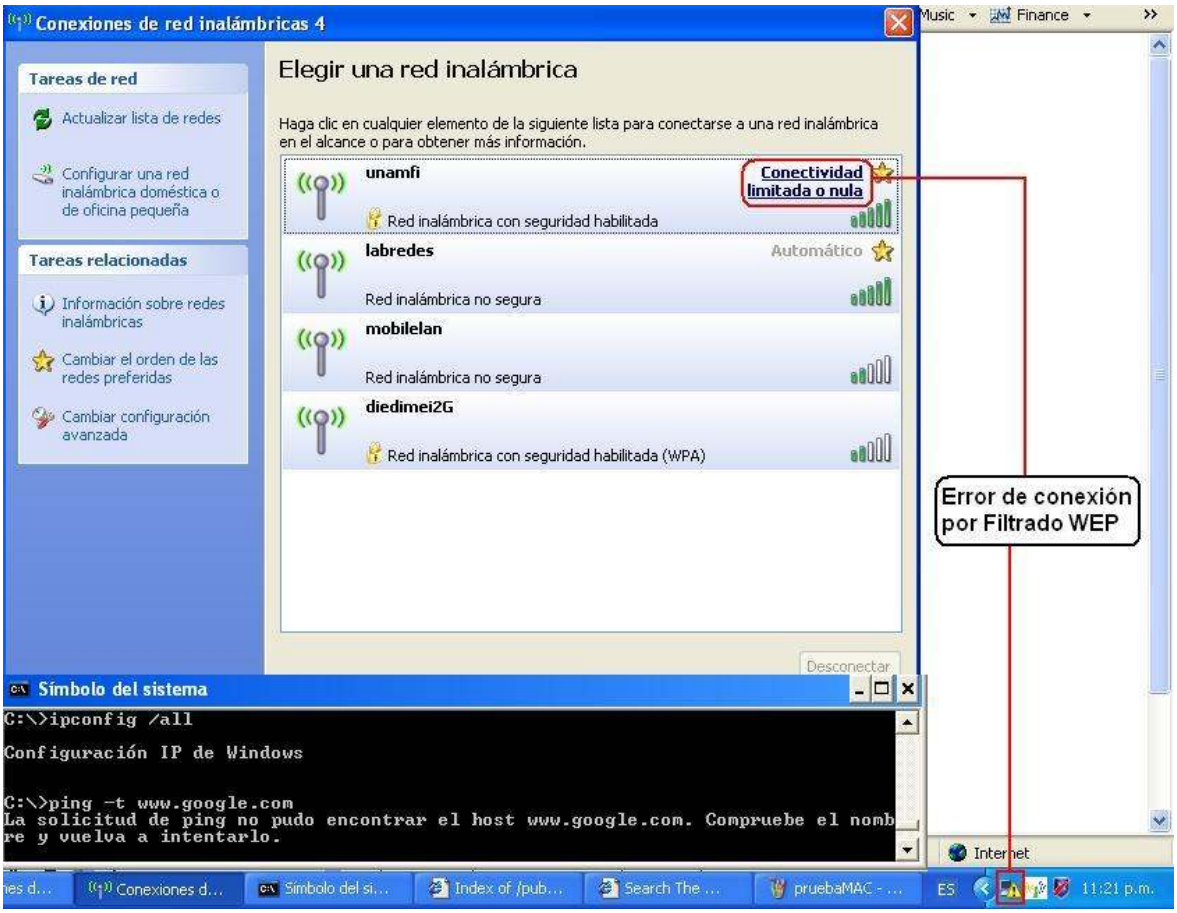



Figura 4.5. Pruebas de autenticación mediante WEP

Otra prueba de verificación que se realizó respecto a la clave WEP fue el introducir una clave WEP de longitud más pequeña y otra de longitud más grande obteniendo un error como el que se muestra en la figura 4.6.

Con lo cual tampoco nos deja establecer una conexión de red de forma satisfactoria. Teniendo así seguridad que sólo podrán establecer una conexión los usuarios válidos con los access point que se encuentran en el laboratorio de redes y seguridad, se debe considerar que la elección de la clave deberá ser robusta y bien resguarda por el usuario.

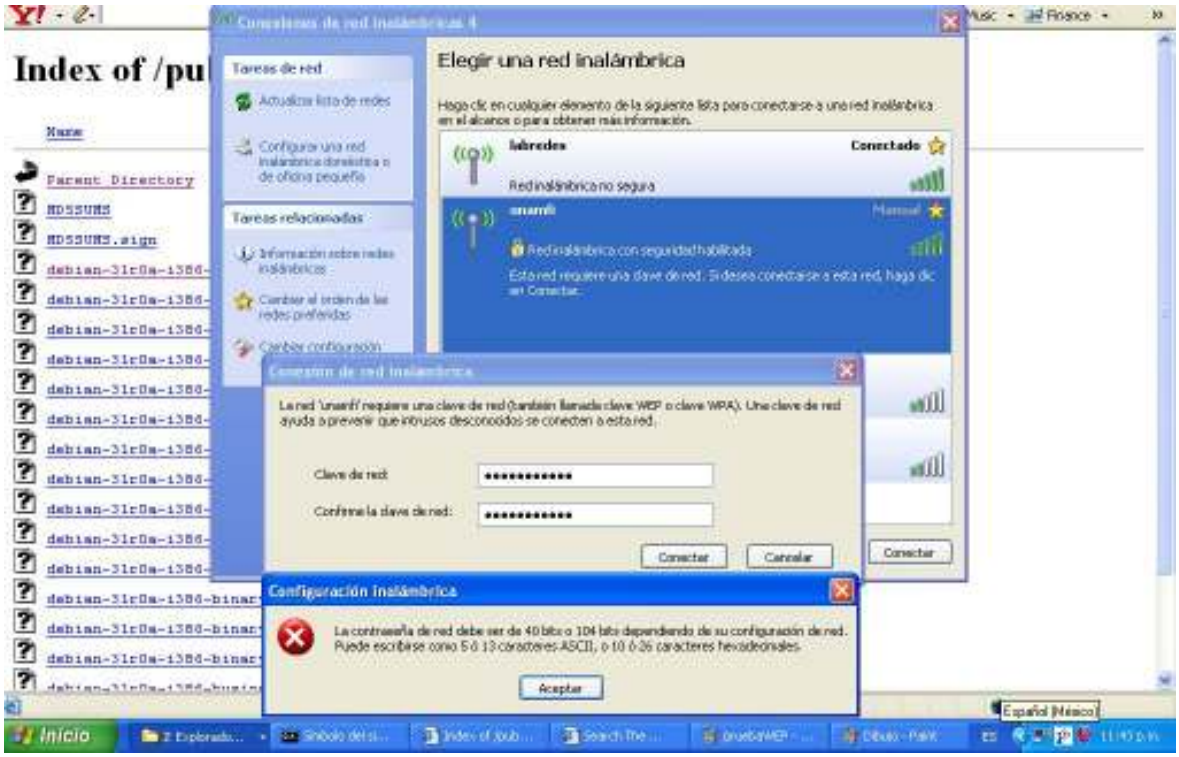



Figura 4.6. Prueba 2 de autenticación mediante WEP

Estas pruebas se hicieron tanto en el access point de nombre ***unamfi*** como en ***labredes.***

## 4.4. Pruebas al filtrado de MAC

Esta prueba consistió en hacer un filtrado por dirección MAC, esto es, el access point se configura para que sólo se puedan conectar a él clientes conocidos, esto quiere decir que tiene que conocer la dirección MAC del cliente para dejarlos conectarse, en las figuras 4.7 y 4.8 se muestra como al aplicar la configuración se pierde la conexión de los access point ***unamfi*** y ***labredes*** respectivamente.

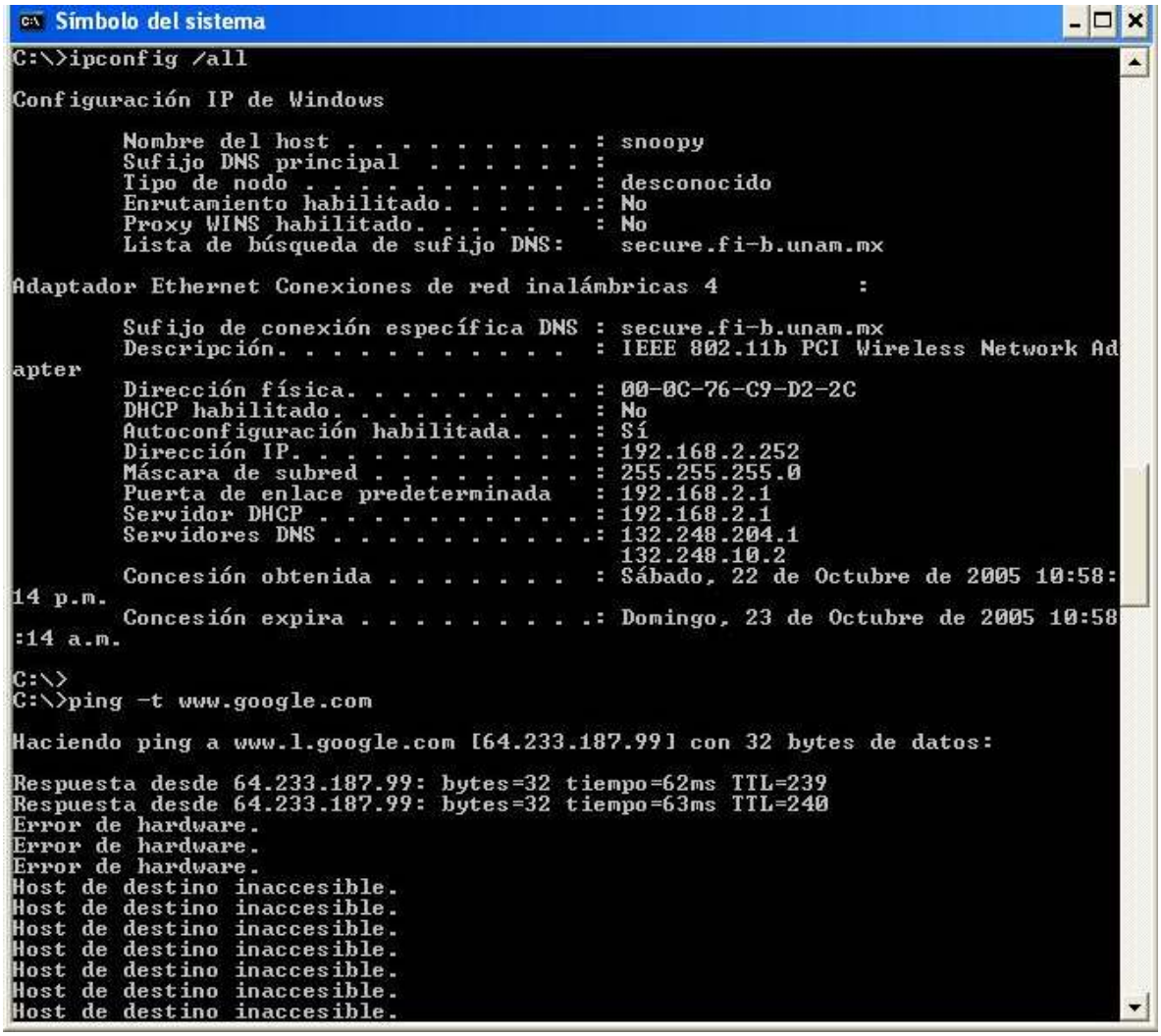



Figura 4.7. Prueba de filtrado MAC en el access point ***unamfi***

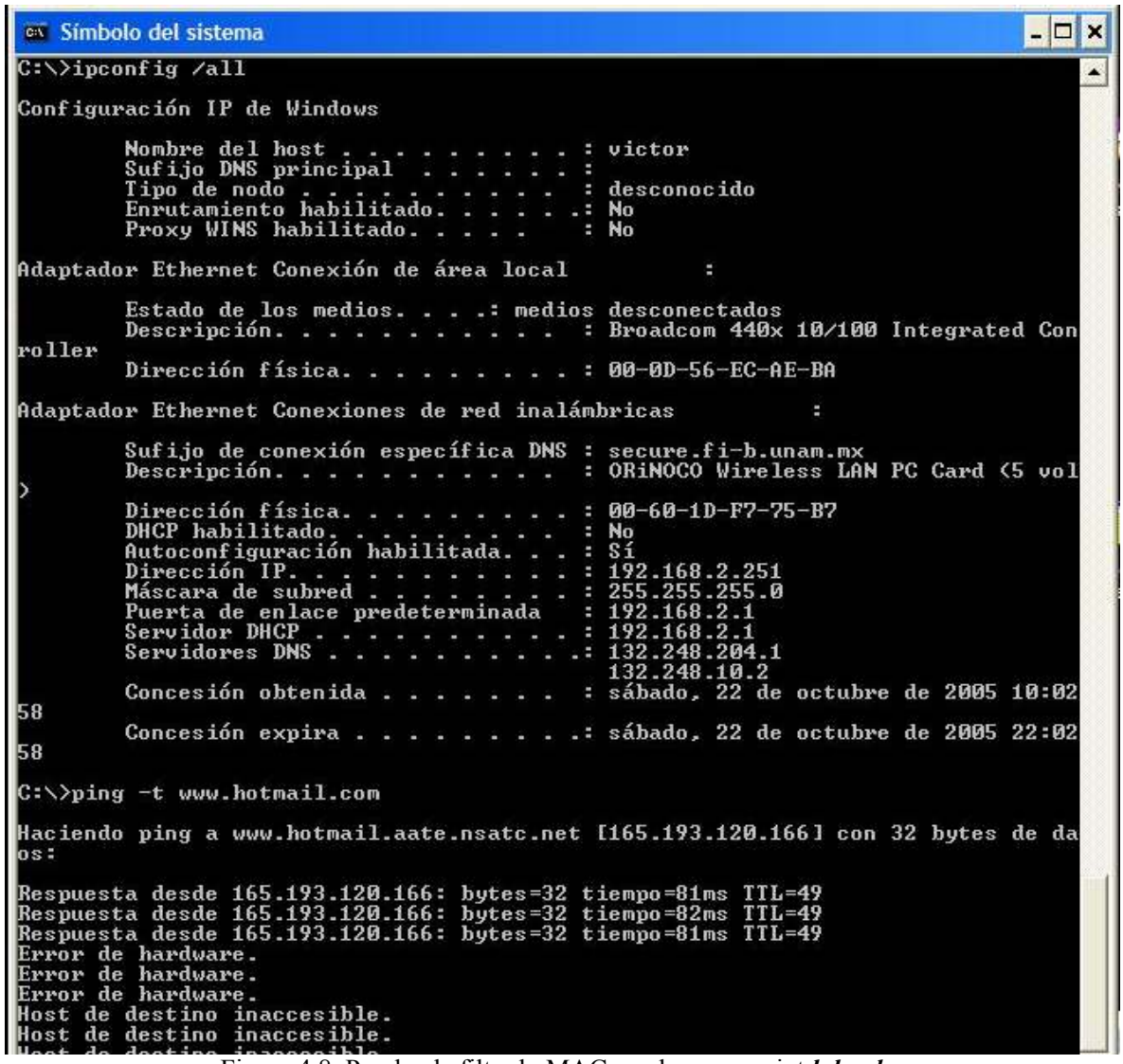



Figura 4.8. Prueba de filtrado MAC en el access point ***labredes***

## 4.5. Análisis de protocolos

Esta prueba en realidad no es específica de una red inalámbrica, sin embargo la quisimos incluir ya que es una muy buena herramienta para la administración de una red.

El analizador de protocolos que utilizamos fue ***Ethereal***, en la figura 4.9, se muestra parte del reporte que se obtiene después de capturar el tráfico de la red por unos minutos.

Dicha prueba consiste en la ejecución del software para capturar la información de paquetes y protocolos que están siendo utilizados en la red, para después analizarla, y así tener bajo control la administración de la red.

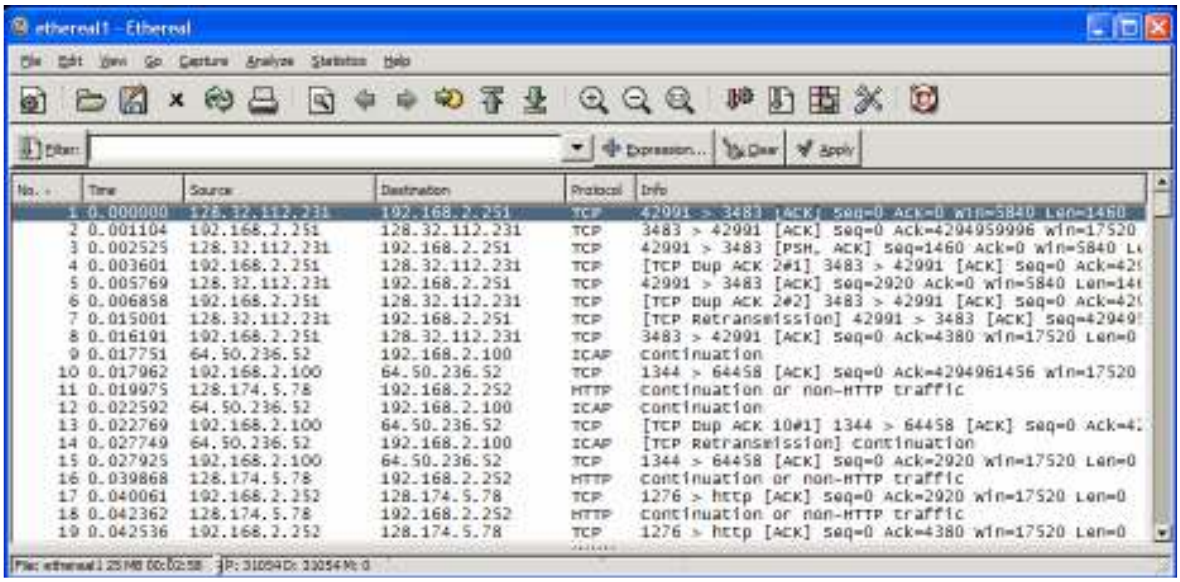


Figura 4.9. Reporte del analizador de protocolos.

A continuación se muestran algunas estadísticas interesantes que se pueden obtener con esta herramienta.

En la figura 4.10, se muestra un resumen de la captura, como es el tiempo que duró dicha captura, cantidad de paquetes, promedios de bits y bytes por segundo, etc.

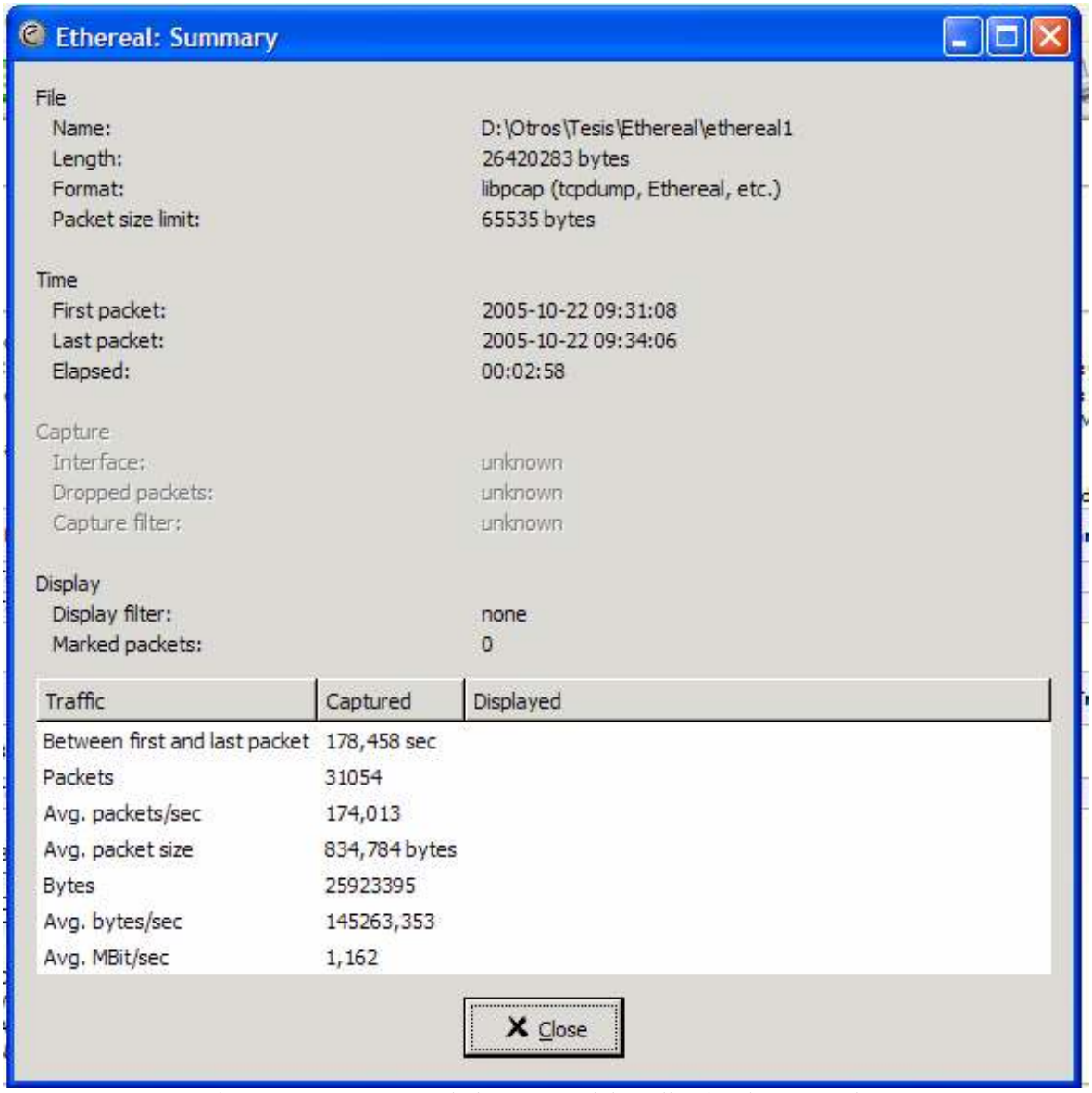
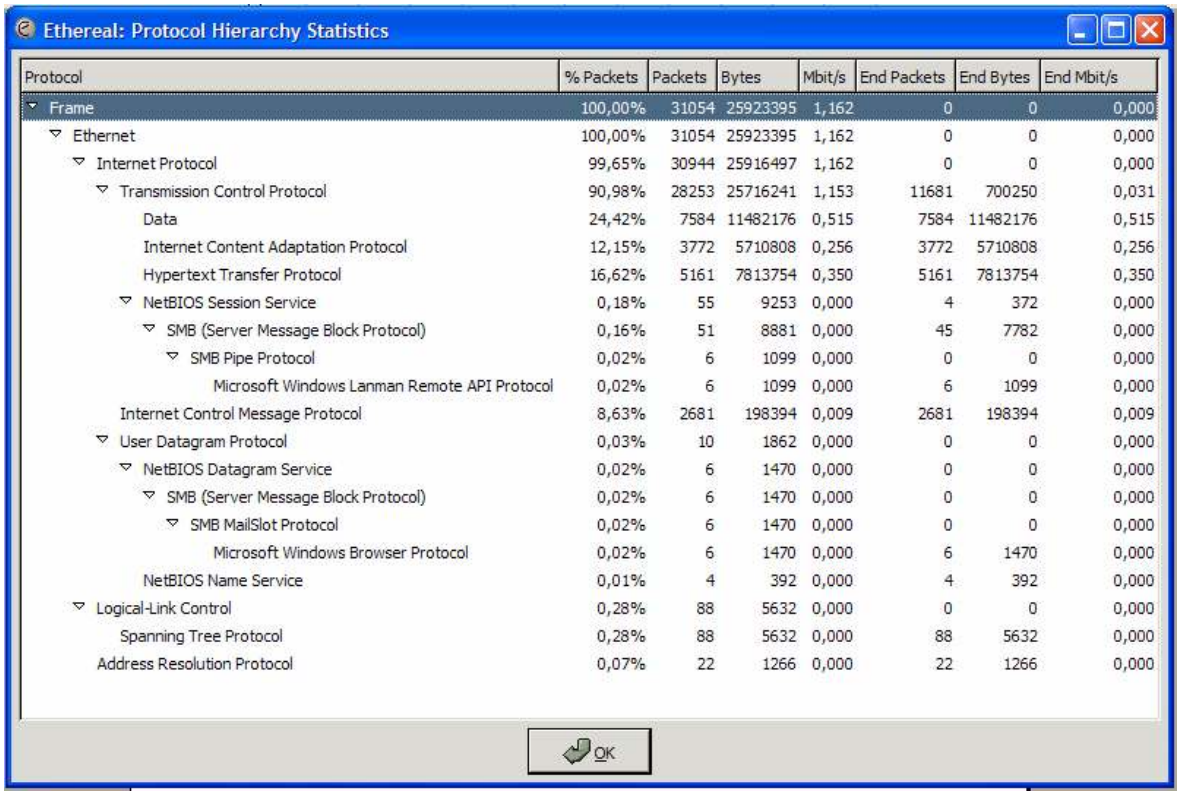



Figura 4.10. Resumen de la captura del analizador de protocolos.

La figura 4.11. nos muestra a detalle la información del tráfico que fue capturado de la red, así como el número de paquetes de cada protocolo, bytes, etc.




| Protocol | % Packets | Packets | Bytes | Mbit/s | End Packets | End Bytes | End Mbit/s |
|---|---|---|---|---|---|---|---|
| Frame | 100,00% | 31054 | 25923395 | 1,162 | 0 | 0 | 0,000 |
| Ethernet | 100,00% | 31054 | 25923395 | 1,162 | 0 | 0 | 0,000 |
| Internet Protocol | 99,65% | 30944 | 25916497 | 1,162 | 0 | 0 | 0,000 |
| Transmission Control Protocol | 90,98% | 28253 | 25716241 | 1,153 | 11681 | 700250 | 0,031 |
| Data | 24,42% | 7584 | 11482176 | 0,515 | 7584 | 11482176 | 0,515 |
| Internet Content Adaptation Protocol | 12,15% | 3772 | 5710808 | 0,256 | 3772 | 5710808 | 0,256 |
| Hypertext Transfer Protocol | 16,62% | 5161 | 7813754 | 0,350 | 5161 | 7813754 | 0,350 |
| NetBIOS Session Service | 0,18% | 55 | 9253 | 0,000 | 4 | 372 | 0,000 |
| SMB (Server Message Block Protocol) | 0,16% | 51 | 8881 | 0,000 | 45 | 7782 | 0,000 |
| SMB Pipe Protocol | 0,02% | 6 | 1099 | 0,000 | 0 | 0 | 0,000 |
| Microsoft Windows Lanman Remote API Protocol | 0,02% | 6 | 1099 | 0,000 | 6 | 1099 | 0,000 |
| Internet Control Message Protocol | 8,63% | 2681 | 198394 | 0,009 | 2681 | 198394 | 0,009 |
| User Datagram Protocol | 0,03% | 10 | 1862 | 0,000 | 0 | 0 | 0,000 |
| NetBIOS Datagram Service | 0,02% | 6 | 1470 | 0,000 | 0 | 0 | 0,000 |
| SMB (Server Message Block Protocol) | 0,02% | 6 | 1470 | 0,000 | 0 | 0 | 0,000 |
| SMB MailSlot Protocol | 0,02% | 6 | 1470 | 0,000 | 0 | 0 | 0,000 |
| Microsoft Windows Browser Protocol | 0,02% | 6 | 1470 | 0,000 | 6 | 1470 | 0,000 |
| NetBIOS Name Service | 0,01% | 4 | 392 | 0,000 | 4 | 392 | 0,000 |
| Logical-Link Control | 0,28% | 88 | 5632 | 0,000 | 0 | 0 | 0,000 |
| Spanning Tree Protocol | 0,28% | 88 | 5632 | 0,000 | 88 | 5632 | 0,000 |
| Address Resolution Protocol | 0,07% | 22 | 1266 | 0,000 | 22 | 1266 | 0,000 |

Figura 4.11. Detalle del tráfico de la red.

Este tipo de herramientas son muy útiles para la administración de una red, ya que nos permite conocer lo que está pasando por nuestra red, y con ello tener mayor control sobre ella y saber qué medidas tomar en caso de ser necesario, como por ejemplo, si la red está muy congestionada saber porqué y que usuario o usuarios son los causantes.

## 4.6. Análisis de calidad de señal

Para lograr saber cual es la calidad de señal utilizamos un software llamado wavemon, dicho programa fue diseñado para monitorear dispositivos inalámbricos, despliega continuamente información actualizada de los niveles de señal, así como información general y particular de la red inalámbrica.
En la figura 4.12 podemos ver la primera pantalla tomada en el laboratorio estando conectados al access point *labredes*.

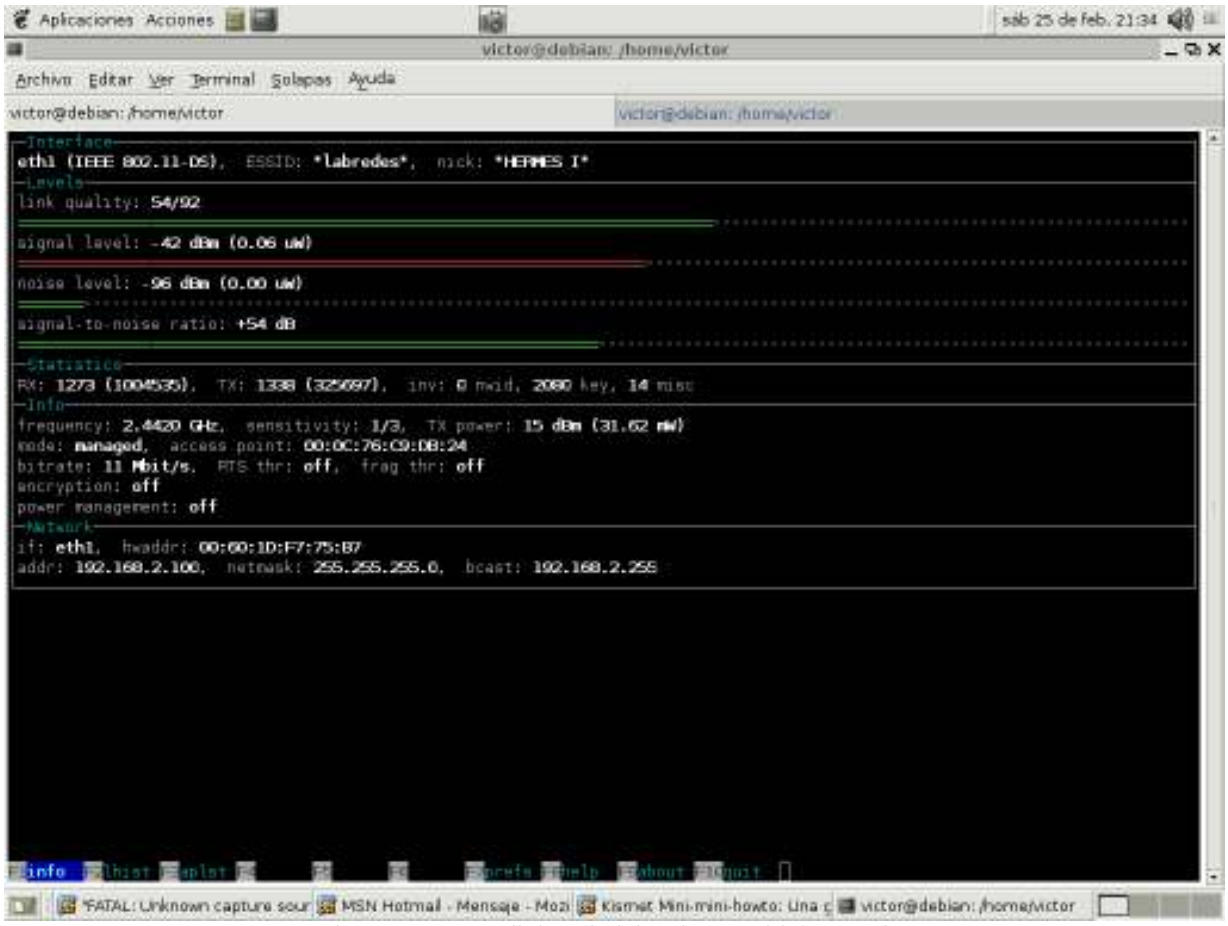


Figura 4.12. Medición de labredes en el laboratorio.

Como mencionamos, este software nos muestra el nivel de la señal, nivel de ruido, así como datos de la red, como son: tipo de red, frecuencia, bitrate, entre otros datos. Al estar cerca del access point nuestra señal es muy buena.

En la figura 4.13, se muestra una imagen del mismo access point, pero ya no en el laboratorio sino afuera del edificio aproximadamente a unos 7 metros, vemos como la señal ha disminuido un poco, sin embargo sigue siendo aceptable.



Figura 4.13. Medición de labredes a 7 metros aproximadamente.

Por último, para el mismo access point se tomo una figura mas (figura 4.14), esta vez alejados aproximadamente 20 metros, la señal a esta distancia ya es mala sin embargo aun podemos detectar la señal y conectarnos al access point.

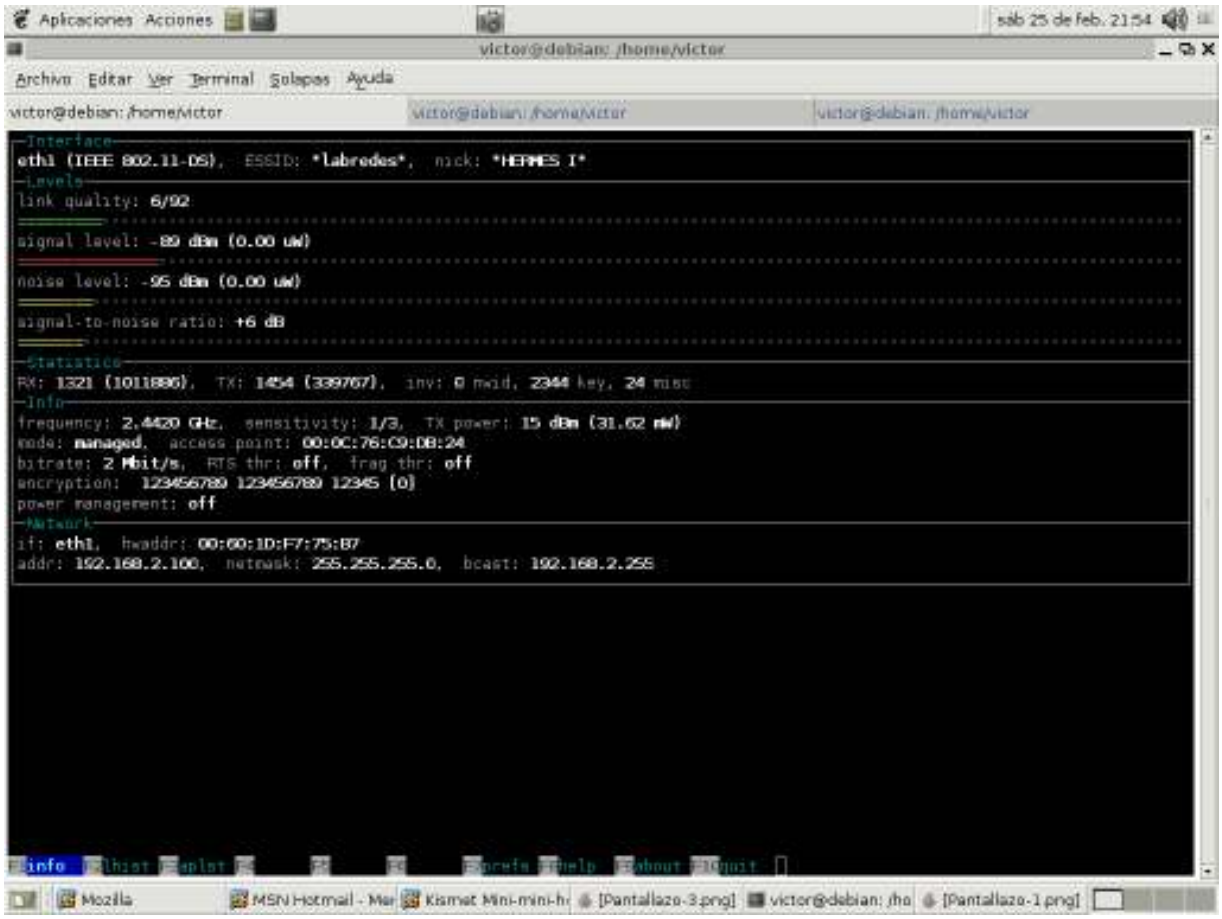


Figura 4.14. Medición de labredes en a 20 metros aproximadamente.

Para el otro access point *unamfi* se tomaron las mismas mediciones, obteniendo resultados semejantes a los del primero, en la figura 4.15 estando dentro del laboratorio vemos una muy buena señal.

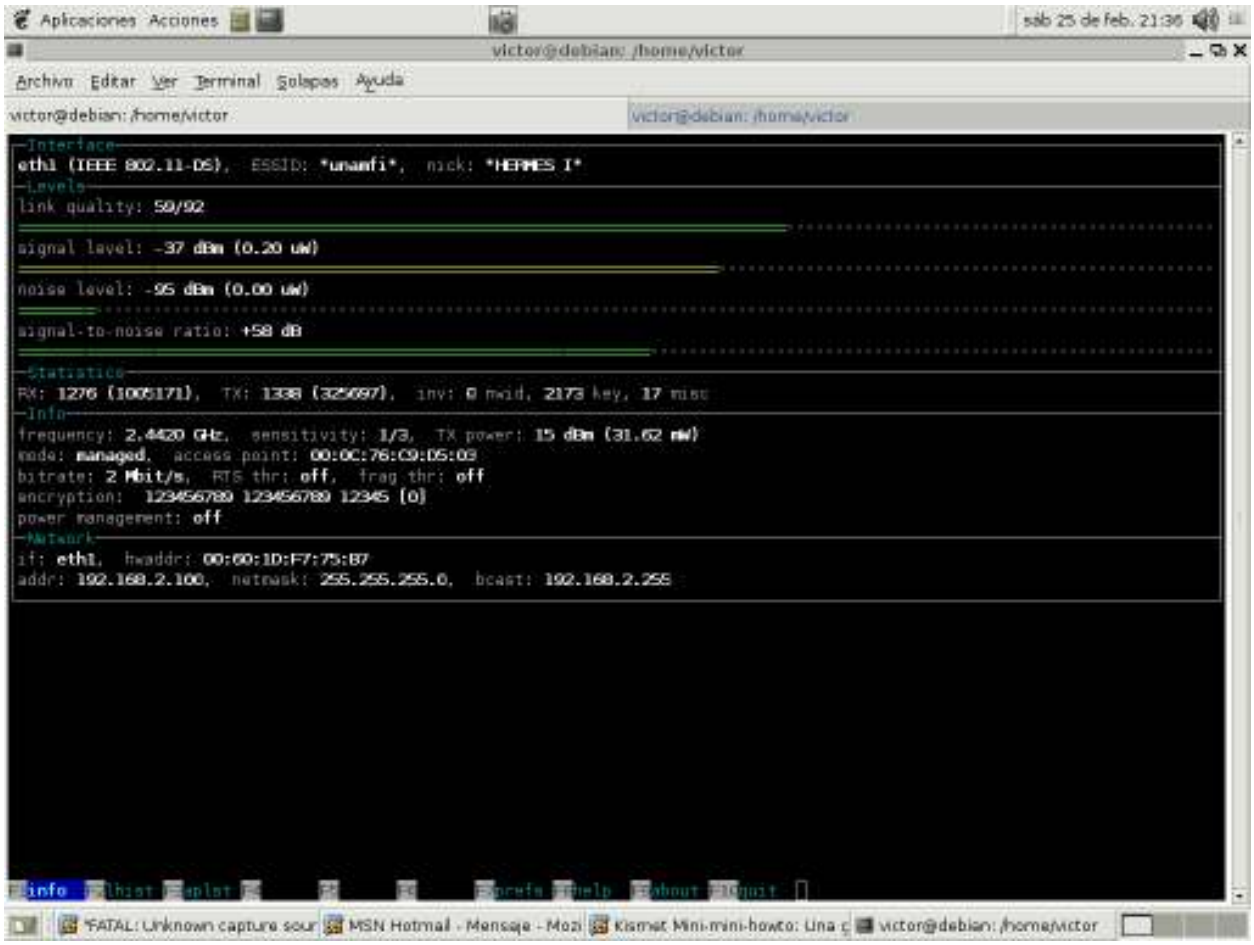



Figura 4.15. Medición de unamfi en el laboratorio.

En la figura 4.16 la señal disminuye, dado que estamos aproximadamente a 7 metros, la señal es aceptable.

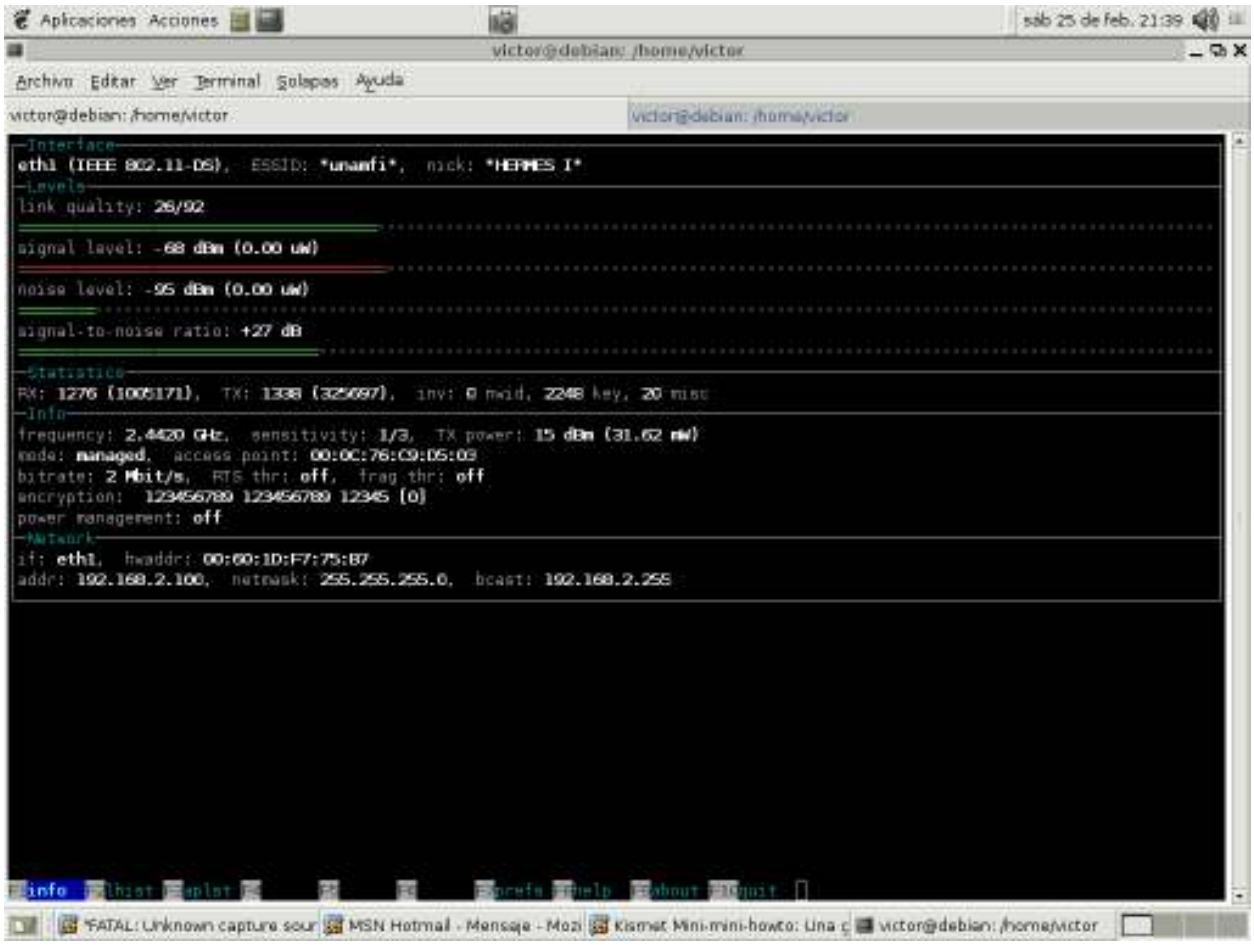


Figura 4.16. Medición de unamfi a 7 metros aproximadamente.

Y por último en la figura 4.17, se muestra una señal muy débil a unos 20 metros de distancia.

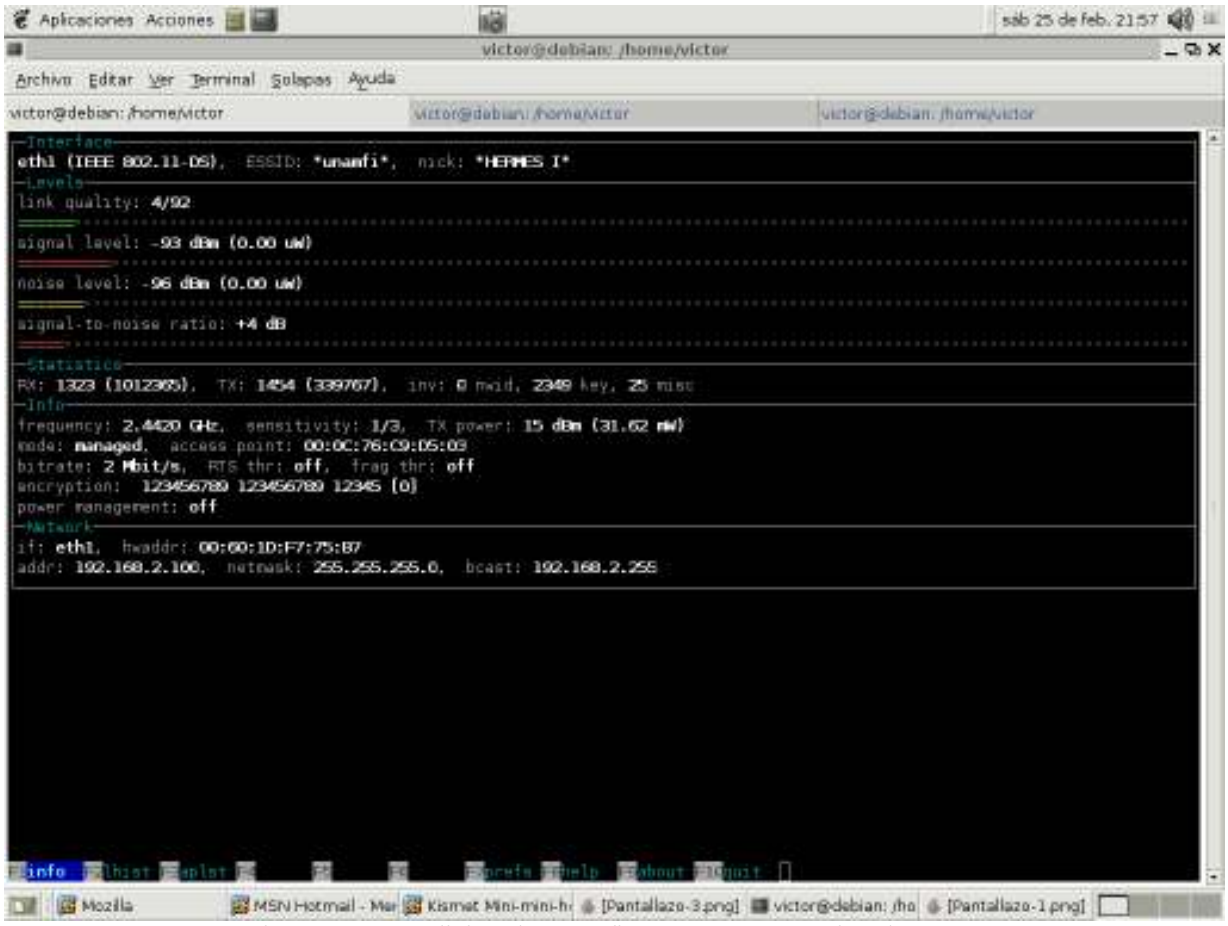



Figura 4.16. Medición de unamfi a 20 metros aproximadamente.

# CAPÍTULO 5. PRÁCTICAS

El objetivo de este capítulo es crear una serie de prácticas que ayuden al alumno en el área de Redes y Seguridad a visualizar de forma práctica lo visto en clase para reafirmar sus conocimientos teóricos y así pueda salir mejor preparado para el campo laboral. Así mismo son una guía para los usuarios del laboratorio de redes y seguridad para saber cómo configurar la red, el access point y las tarjetas inalámbricas en diferentes configuraciones.

# 5.1. Prácticas.

## *5.1.1. Práctica 1. Instalación del hardware y red inalámbrica ad-hoc*

### *5.1.1.1. Cuestionario previo*

1. ¿Qué es una de red de computadoras?
2. ¿Cuál es la definición de una tarjeta de red inalámbrica?
3. ¿Qué es una dirección IP?
4. ¿Qué es TCP/IP?
5. ¿Qué es una red inalámbrica ad-hoc?

### *5.1.1.2. Objetivo*

El alumno aprenderá a instalar una tarjeta de red inalámbrica, configurará una red inalámbrica ad-hoc y entenderá su uso, limitantes, alcances.

### *5.1.1.3. Material*

2 Computadoras
2 Tarjeta de Red Inalámbrica

### *5.1.1.4. Descripción*

### *Paso 1.*

Se debe de colocar la tarjeta de red inalámbrica en la ranura PCI de la tarjeta madre de la computadora que se quiera tener con tarjeta de red inalámbrica, para ello primero, apague el sistema y quite la caja del equipo para ubicar la ranura PCI disponible sobre la tarjeta madre. Inserte la tarjeta PCI en la ranura firmemente, después, sujételo con un tornillo. Colocar la tapa de nuevo y conectar la antena externa, como se muestra en la figura 5.1.

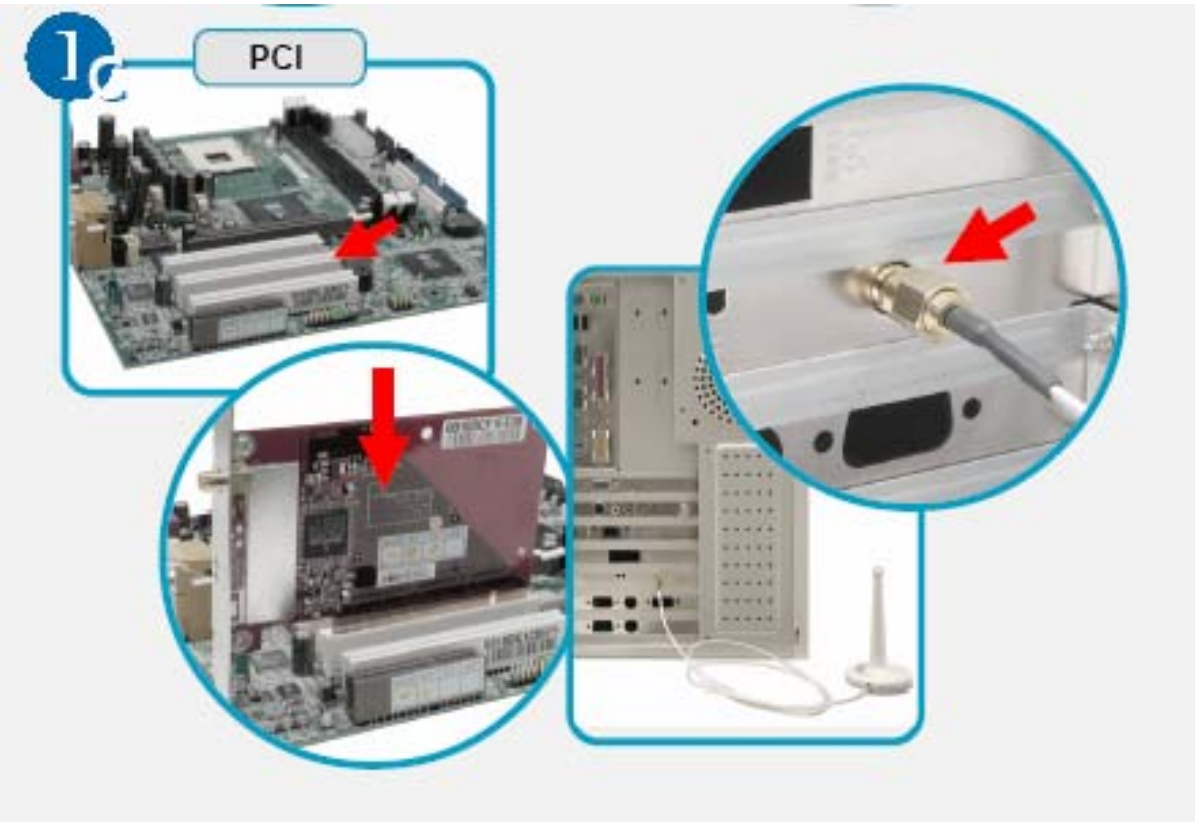



Figura 5.1. Instalación tarjeta PCI

Si no sabe cómo instalar la tarjeta PCI, pida ayuda al encargado del laboratorio o a su profesor.

## *Paso 2.*

Una vez hecho el paso 1 se debe de instalar el software de la tarjeta de red que viene en el CD de instalación de la misma, para ello haga lo siguiente:

El sistema detectará un dispositivo nuevo e instalará su controlador. Inserte el CD de software en la unidad de CD-ROM, y el programa de instalación iniciará automáticamente. Haga clic sobre la opción de controlador correspondiente al de su tarjeta de red inalámbrica para continuar, como se muestra en la figura 5.2.

*Consejo: Si no inicializa, haga clic* 

*sobre la barra de tareas; después seleccione Ejecutar y escribir* ***E:\setup.exe****, donde* ***E*** *es su unidad CD-ROM.*




Figura 5.2. Instalación del software de la Tarjeta PCI.

*Windows XP/ 2000*

1. Elegir opción "Instalar el software automáticamente" y hacer clic en Next >
2. La ventana Asistente InstallShield aparece, haga clic en Next >
3. Lee y acepta el Contracto de Licencia, y haga clic en Next >
4. Escriba la información del usuario y haga clic en Next >
5. Haga clic en Install, después haga clic en Next > para completar la instalación.
6. El icono MSI Inalámbrico LAN aparece en el área de estado.

*Windows ME/98SE*

1. El sistema reiniciará después de configurar el dispositivo nuevo; haga clic en Restart
2. Después de reiniciar, el sistema buscará nuevamente por el hardware nuevo; elegir Cancel para continuar instalación con Asistente InstallShield.
3. Hacer clic en Next > en la ventana del Asistente InstallShield.
4. Lee y acepta el Contracto de Licencia; después haga clic en Next >
5. Escriba la información del usuario y haga clic en Next >

6. Haga clic en Install, después, haga clic en Finish cuando se complete la instalación.

*Consejo: La pantalla podrá pedirle para insertar el CD de Recurso Windows 98SE durante la instalación; prepare el CD necesario para continuar el procedimiento cuando se le pregunte.*

7. Haga clic en Yes para reiniciar el equipo cuando se le pregunte.

8. Después de reiniciar, el icono MSI Inalámbrico LAN aparece en área de estado.

Anote las descripciones de iconos MSI Inalámbrico Lan:

 - _____.

 - _____.

 - _____.

## *Paso 3.*

Para continuar con la configuración de la tarjeta de red, hay que ir a ***Inicio*** → ***Conexiones de Red*** → ***Mostrar Todas las Conexiones*** una vez allí aparecerá un icono con el nombre de ***Conexión Inalámbrica de Red*** al cual hay que dar un clic derecho con el Mouse y seleccionar ***Propiedades*** con lo cual nos aparecerá una ventana en donde se muestra lo que actualmente utiliza la conexión de red, como se muestra en la figura 5.3.

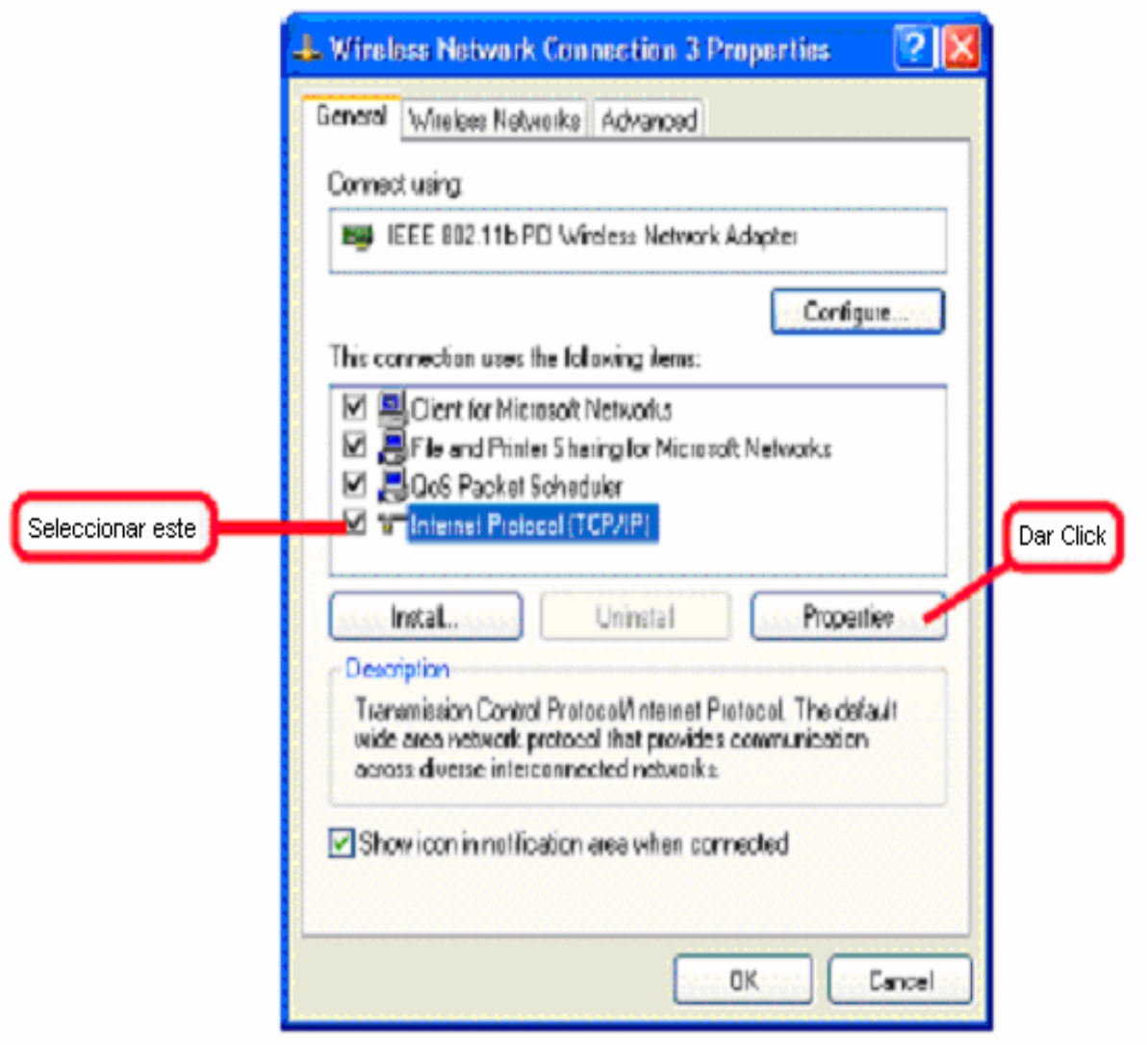



Figura 5.3. Propiedades de la Conexión de Red Inalámbrica

Una vez identificado esto seleccionar la opción que dice ***Protocolo de Internet (TCP/IP)*** y dar un clic en ***Propiedades***.

¿Por qué se elige la opción TCP/IP?

Al hacer esto aparecerá otra ventana en donde se muestran las propiedades del protocolo de Internet (TCP/IP) en la pestaña de ***General***, al llegar a este punto hay dos posibles opciones de configuración:

Aquí se dividirá al grupo en dos, para que cada uno de ellos haga una configuración diferente y al final de la práctica intercambien puntos de vista.

La primera opción es si se quiere que el servidor DHCP proporcione automáticamente la dirección IP a la tarjeta de red inalámbrica para ello se tiene que elegir las siguientes opciones:

*a) Obtener una Dirección IP Automáticamente* y
b*) Obtener una Dirección de Servidor DNS Automáticamente*.

La segunda opción es si queremos proporcionarle de forma manual la dirección IP a la tarjeta de red inalámbrica, para ello se debe seleccionar una de las siguientes opciones:

a***)*** *Usar la Siguiente Dirección IP* y proporcionar lo siguiente:

Dirección IP: **x.x.x.x**, dicha dirección IP debe estar dentro del segmento del laboratorio.

¿Por qué?
_____
_____
_____

Máscara de Red: **255.255.255.0**
Puerta de Enlace: **192.168.2.1**

***b) Usar la Siguiente Dirección de Servidor DNS*** y teclear lo siguiente (para el caso de la UNAM):

Servidor DNS Primario: **132.248.10.2**
Servidor DNS Secundario: **132.248.204.1**

Una vez elegida cualquiera de las dos opciones, como lo muestra la figura 5.4, ya sea de asignar la IP de forma automática o hacerlo manualmente y haber tecleado lo necesario, dar ***Aceptar*** a todas las ventanas.

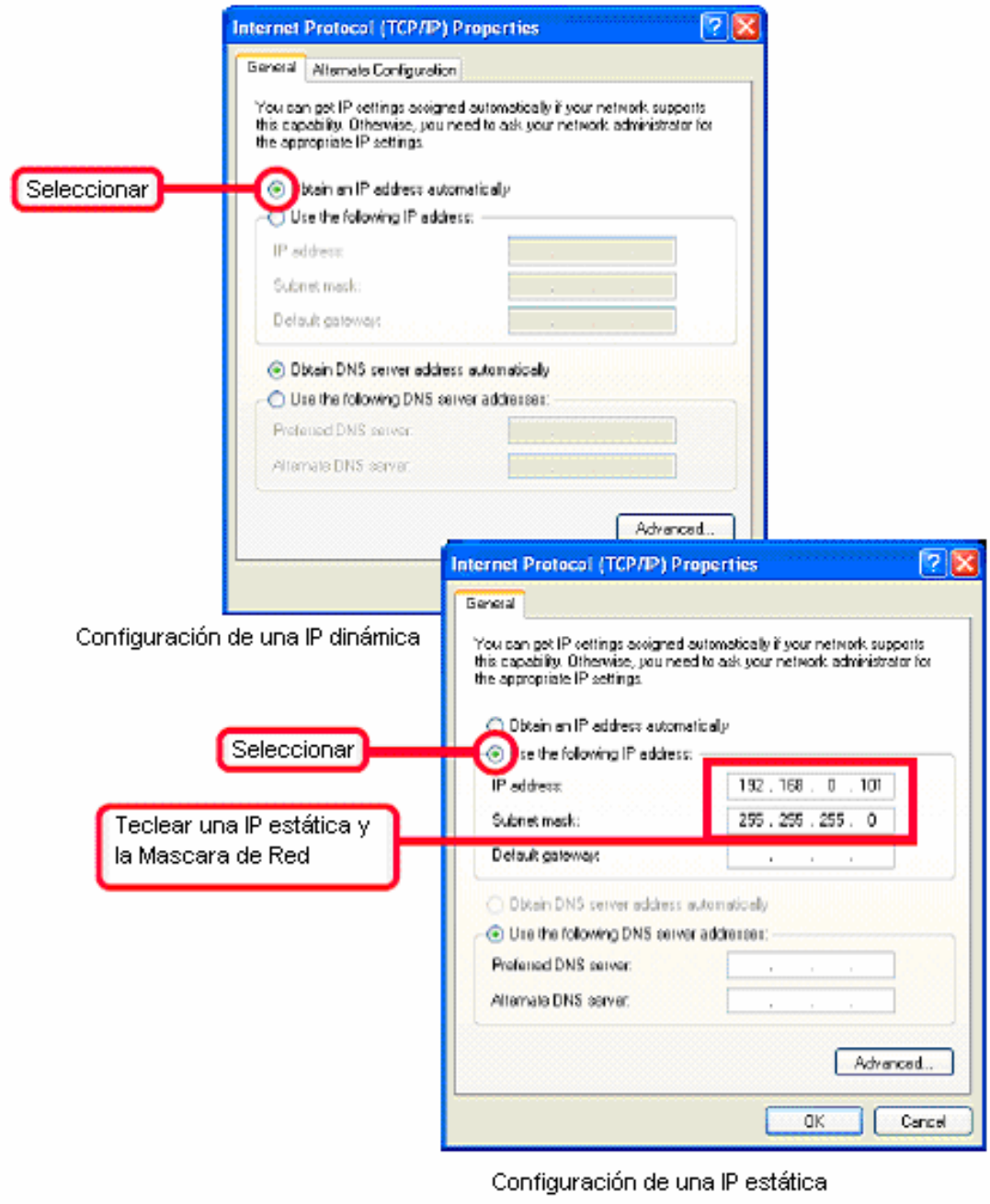



Figura 5.4. Configuración de la IP.

¿Qué diferencias existen entre una y otra configuración?

¿Es mejor alguna de las dos? Justifique su respuesta

¿Cuándo se puede usar una y otra?

## *Paso 4.*

En este paso se configurará una red inalámbrica ad-hoc. Para poder realizar este punto se necesita tener instaladas dos tarjetas inalámbricas.

Ya que está instalada la tarjeta inalámbrica ir a conexiones de red, con el botón derecho del Mouse seleccionar *propiedades* y seleccionar la pestaña *Redes inalámbricas*, en el cuadro de diálogo de propiedades del adaptador de red inalámbrico, seleccionar *Agregar* en *Redes preferidas*. En la pestaña *asociación* escribir el nombre de nuestra red inalámbrica.

Active la casilla de verificación Ésta es una red de equipo a equipo (ad hoc) y desactive la casilla de verificación La clave la proporciono yo automáticamente.

En Autenticación de red, haga clic en Abierta. En Cifrado de datos, haga clic

En *Clave de red*, escriba la clave WEP. Vuelva a escribir la clave WEP en *Confirme la clave de red*.

En *Índice de la clave*, seleccione 1.

Configurar una dirección IP en Protocolo Internet (TCP/IP), repetir los pasos para la segunda tarjeta y hacer pruebas con pings.

Con esto tendremos una red Ad-hoc funcionando. En la figura 5.5 se muestra un ejemplo del cuadro de diálogo **Propiedades de red inalámbrica** para una red inalámbrica ad hoc con la siguiente configuración:

- SSID: labfi
- Está habilitada la autenticación de sistema
- Está habilitado WEP
- Está habilitado el modo ad hoc

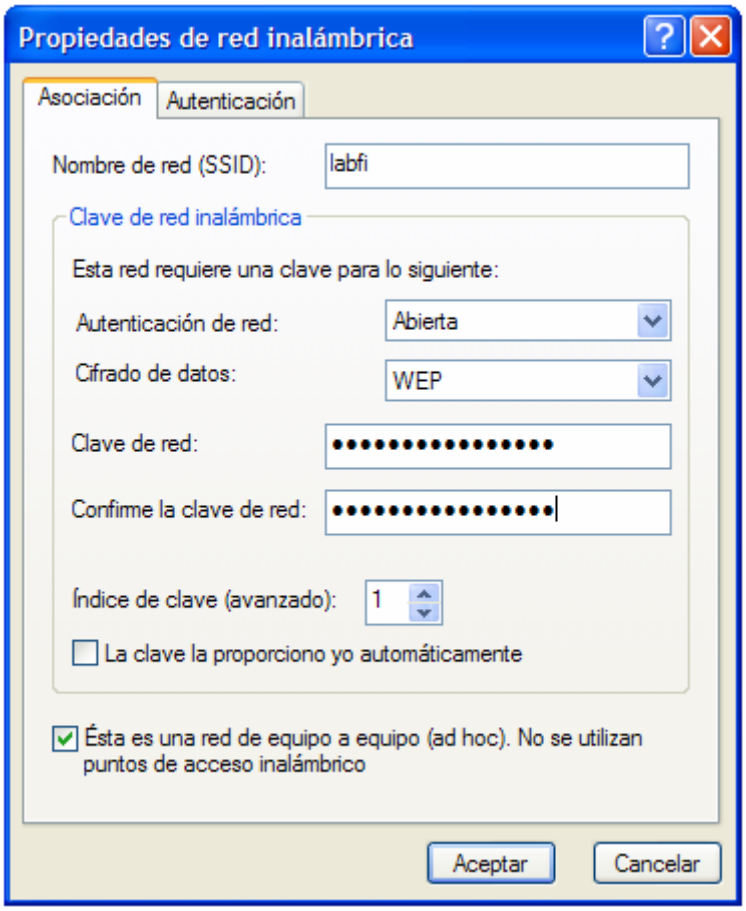



Figura 5.5. Cuadro de configuración de una red ad-hoc

### *5.1.1.5. Conclusioness.*

¿Es útil una red ad-hoc?
¿En que casos es preferible montar una red ad-hoc?
¿Cuál es el alcance de este tipo de redes?

## *5.1.2. Práctica 2. Configuración avanzada de una red inalámbrica infraestructura.*

### *5.1.2.1. Cuestionario previo*

1. ¿Qué es una red inalámbrica infraestructura?
2. ¿Qué es un access point?
3. ¿Para que sirve un servidor DHCP?

### *5.1.2.2. Objetivo*

El alumno configurará de forma avanzada la red de tipo infraestructura, así mismo instalará y configurará un servidor DHCP en una computadora con sistema operativo Linux.

### *5.1.2.3. Material*

1 Servidor con sistema operativo Linux
2 Tarjetas inalámbricas
2 Access point

### *5.1.2.4. Descripción*

### *Paso 1.*

Para realizar esta práctica se deben tener instaladas y configuradas al menos dos tarjetas de red inalámbricas (Práctica 1). El segmento de red ha utilizar es el que ya esta configurado en el laboratorio (192.168.2.0 con mascara 255.255.255.0).

Vamos a configurar uno de los access point, este tiene por default una IP para acceder a su configuración, así que se debe de entrar a esta dirección IP (esta IP puede ser la que se muestra en la figura 5.6) y cambiarla por una del segmento de red correspondiente.

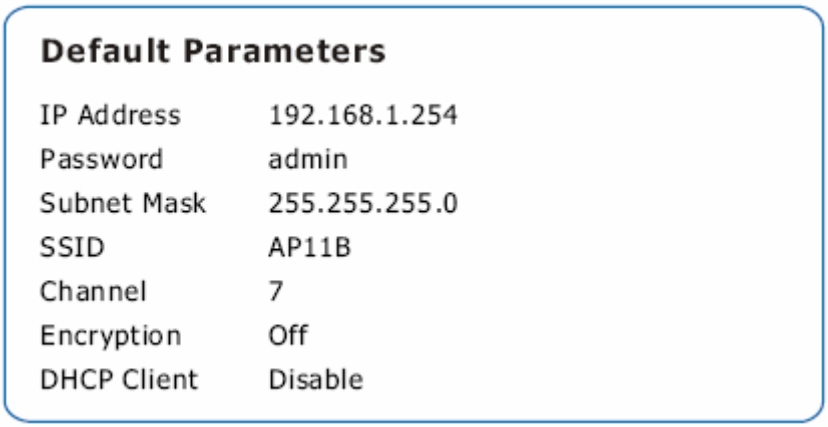



Figura 5.6. Configuración por default del Access Point.

Para cambiar esta configuración se debe acceder a la IP por default desde un navegador para poder cambiar esta configuración, esta IP se debe de teclear en la parte de dirección, como lo muestra la figura 5.7.

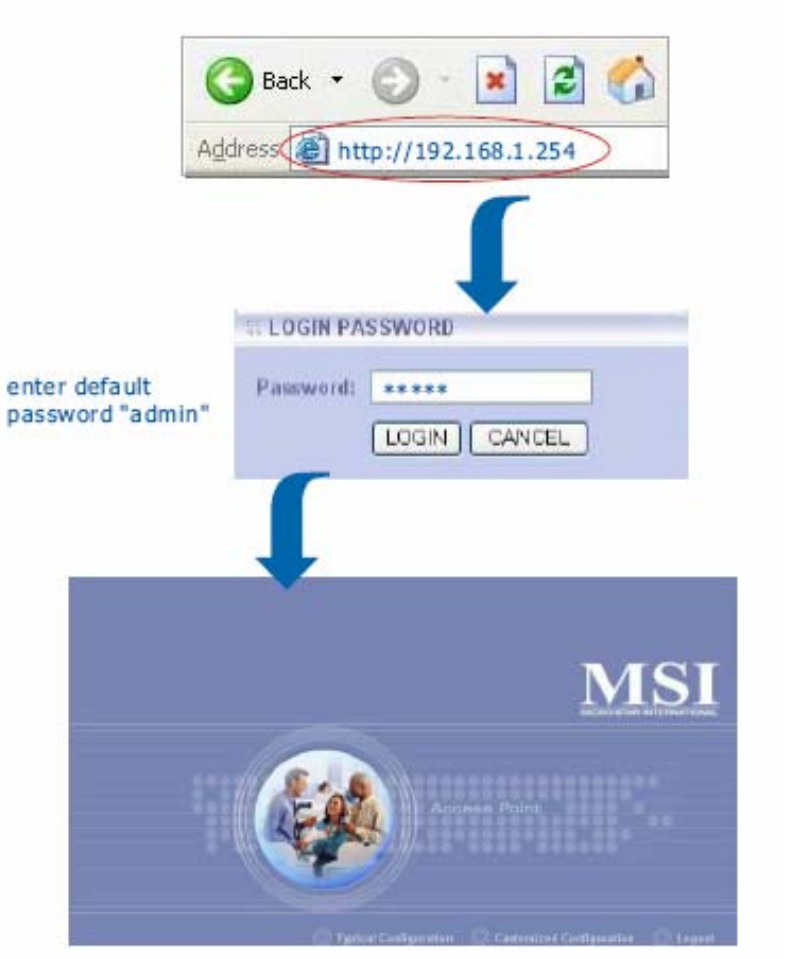



Figura 5.7. Configuración del Access Point.

A continuación se debe de configurar la IP, la mascara de red y la puerta de enlace, como se muestra en la figura 5.8. Que para nuestro segmento de red pueden ser los valores siguientes:

Dirección de Red: 192.168.2.254
Mascara de Red: 255.255.255.0
Puerta de Enlace (Geteway): 192.168.2.1

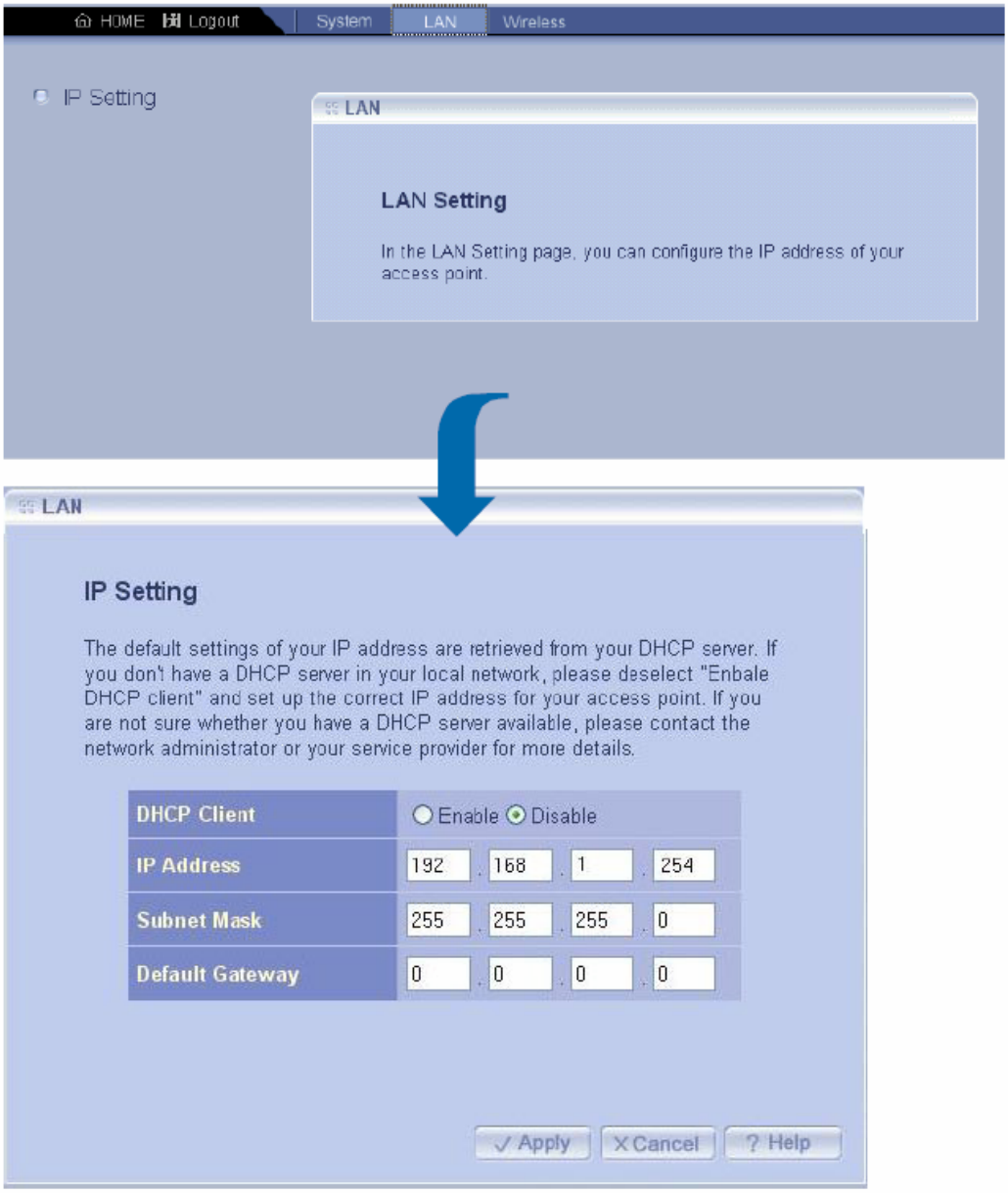



Figura 5.8. Configuración de IP del Access Point.

¿Qué pasa si el access point tiene una dirección IP fuera del segmento de red del laboratorio?

Después de teclear estos valores dar ***Apply*** en la ventana actual y probar la conexión a red. Como lo muestra la figura 5.9.

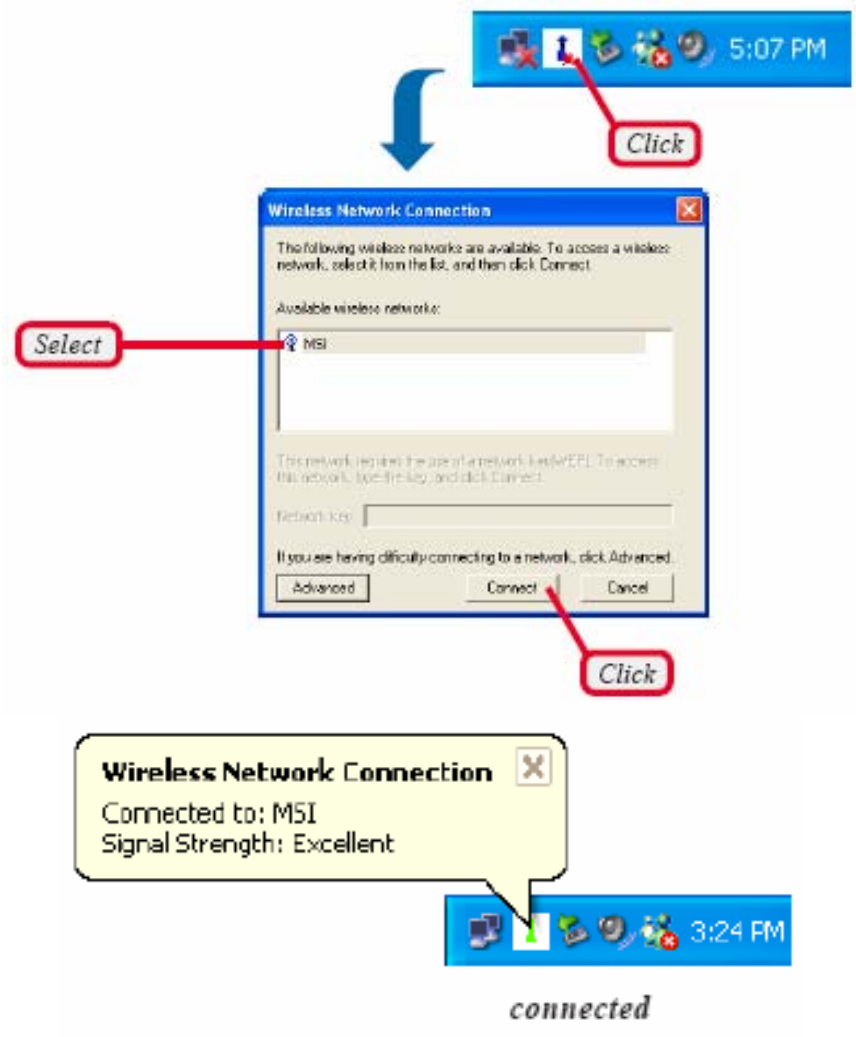



Figura 5.9. Conexión Red Inalámbrica.

*Paso 2.*

En este paso llevaremos a cabo la instalación y configuración del servidor DHCP. Para ello debemos descargar el paquete DHCP rpm, (usamos rpms porque nuestro servidor tiene Red Hat y éste usa paquetes rpm) esto se podrá hacer del servidor del laboratorio.
Para instalarlo teclear lo siguiente:

*rpm –ivh "nombre del paquete"*

¿Para que nos sirven las opciones ivh en el comando rpm?

_____
_____
_____

Ya que tenemos instalado el paquete, el siguiente paso es la configuración, el archivo de configuración es el que se llama dhcpd.conf, que se encuentra en el directorio /etc.

A continuación se listaran y explicaran algunos de los parámetros que se pueden configurar en este archivo.

- authoritative;
- one-lease-per-client on;
- server-identifier ppfm.atenea.dom;
- default-lease-time 604800;
- max-lease-time 604800;
- option subnet-mask 255.255.255.0;
- option broadcast-address 192.168.2.255;
- option routers 192.168.2.254;
- option domain-name-servers 192.168.1.10;
- option domain-name "seguridad.unam.mx";
- ddns-domainname " seguridad.unam.mx ";
- ddns-update-style ad-hoc;
- ddns-updates on;
- option netbios-name-servers 192.168.2.10;
- subnet x.x.x.x netmask y.y.y.y {
  range a.a.a.a b.b.b.b;
  }

*authoritative*; Supone que la configuración correcta para la red es la definida en el servidor DHCP y tratará de reasignar datos a los clientes mal configurados. Este parámetro puede ser global o asignado a una declaración de subred. Los cambios realizados en el servidor marcado como authoritative tienen una rápida propagación en la subred ya que se reconfigura cualquier cliente con la antigua configuración.

*authoritative*; tiene el significado opuesto al anterior parámetro.

*one-lease-per-client on*; cuando esta opción está en "on" y un cliente solicita una asignación, el servidor libera automáticamente cualquier otra asignación que tenga ese cliente. Se supone que si el cliente hace una solicitud es porque ha olvidado que tuviera alguna, es decir, tiene una sola interfaz de red. Si no se da esta situación en los clientes hay que usar este parámetro con precaución.

*server-identifier 192.168.2.1*; este parámetro identifica el nodo que alberga el servicio DHCP. Sólo se deber usar cuando el nodo tenga más de una dirección IP asignada al interfaz.

*default-lease-time 604800;* indica el tiempo de asignación en segundos.

*max-lease-time 604800*; indica el tiempo máximo de asignación en segundos.

*ddns-updates on;* activa la actualización DNS con los valores asignados mediante DHCP.

*ddns-domainname "seguridad.unam.mx";* indica el dominio en el que se actualizan los DNS

*ddns-update-style interim;* esta línea indica el método de actualización DNS automática con los valores de la IP asignados por DHCP. Más adelante veremos como hay que modificar las zonas en el archivo /etc/named.conf para permitir la actualización.

*option subnet-mask 255.255.255.0;* definimos la máscara general de red que vamos a utilizar.

*option broadcast-address 192.168.1.255*; definimos la dirección de difusión de la red.

*option routers 192.168.2.1;* definimos el gateway de la red.

*option domain-name-servers 192.168.2.10*; definimos la dirección del servidor DNS de la red.

*option domain-name "atenea.dom";* definimos el nombre del dominio DNS que se añade a los nombres de host.

*option netbios-name-servers 192.168.2.10*; definimos la dirección del servidor WINS para NetBios.

Y por último definimos la red en la que queremos hacer asignaciones y los rangos de direcciones que puede asignar el servidor DHCP.

subnet _____
range _____

Iniciar el demonio de DHCP y hacer pruebas de que en realidad esta asignando IPs dentro del segmento especificado.

¿Cómo se pueden realizar estas pruebas?
_____
_____
_____

### *5.1.2.5. Conclusiones.*

¿En qué casos nos es preferible tener una red inalámbrica infraestructura?
¿Por qué es útil un servidor DHCP?
¿Cuándo debemos utilizar un servidor DHCP?

## *5.1.3. Práctica 3. Filtrado por MAC*

### *5.1.3.1. Cuestionario previo*

1. Escriba una pequeña descripción de cada una de las capas del modelo OSI.
2. ¿Cuál es la definición de la dirección MAC (***Me****dia* ***A****ccess* ***C****ontrol address*)?
3. ¿Qué es ARP (Address Resolution Protocol)?

### *5.1.3.2. Objetivo*

El alumno aprenderá a habilitar en el access point un sistema de filtrado basado en MAC (a veces llamado también filtrado por hardware), que sólo permitirá el acceso a la red a tarjetas de red concretos, identificados con su MAC.

### *5.1.3.3. Material*

1 Access Point
2 Tarjetas de Red Inalámbrica

### *5.1.3.4. Descripción*

### *Paso 1.*

Para poder realizar esta práctica hay que tener instaladas al menos dos tarjetas de red inalámbrica en computadoras diferentes para que a una de ellas no se le permita el acceso al access point.

¿Qué comando se puede utilizar para determinar la dirección MAC de la tarjeta en Windows y en Linux?

Windows _____
Linux _____

*Paso 2.*

Una vez hecho el paso 1 se tiene que acceder al access point desde un navegador empleando su dirección IP asignada (por ejemplo: 192.168.2.254), como se ve en la figura 5.10. Una vez que se accedió al access point ir a la parte de Wireless, como lo muestra la figura 5.11.

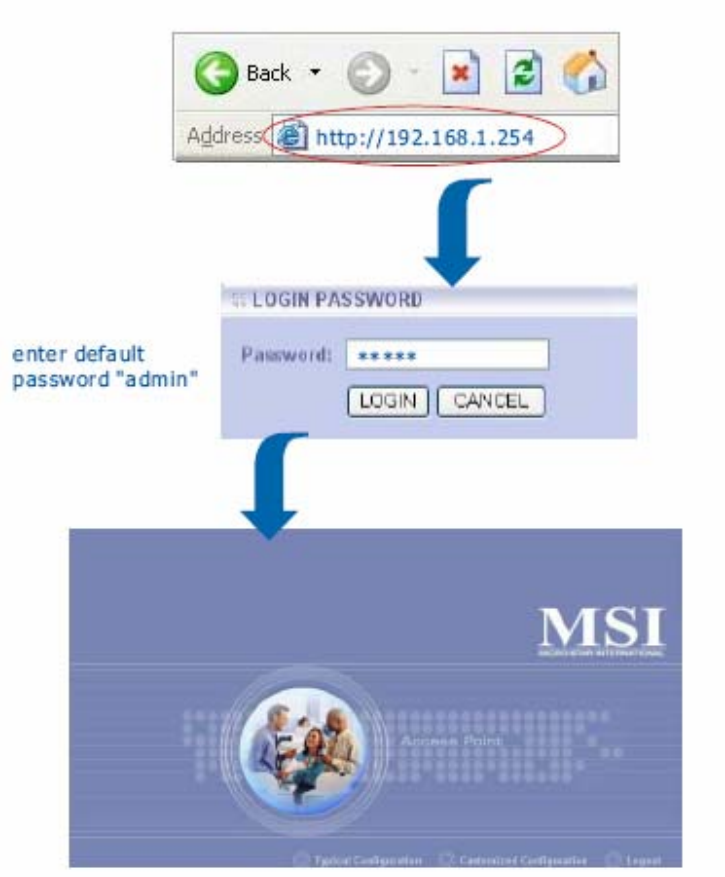



Figura 5.10. Acceso al Access Point.




Figura 5.11. Sección Wireless del Access Point.

## *Paso 3.*

Ir a la subsección de Association Control, como lo muestra la figura 5.12. Y en esta parte teclear la dirección MAC identificada en el paso 1 de la tarjeta de red que se quiere negar el acceso al access point.

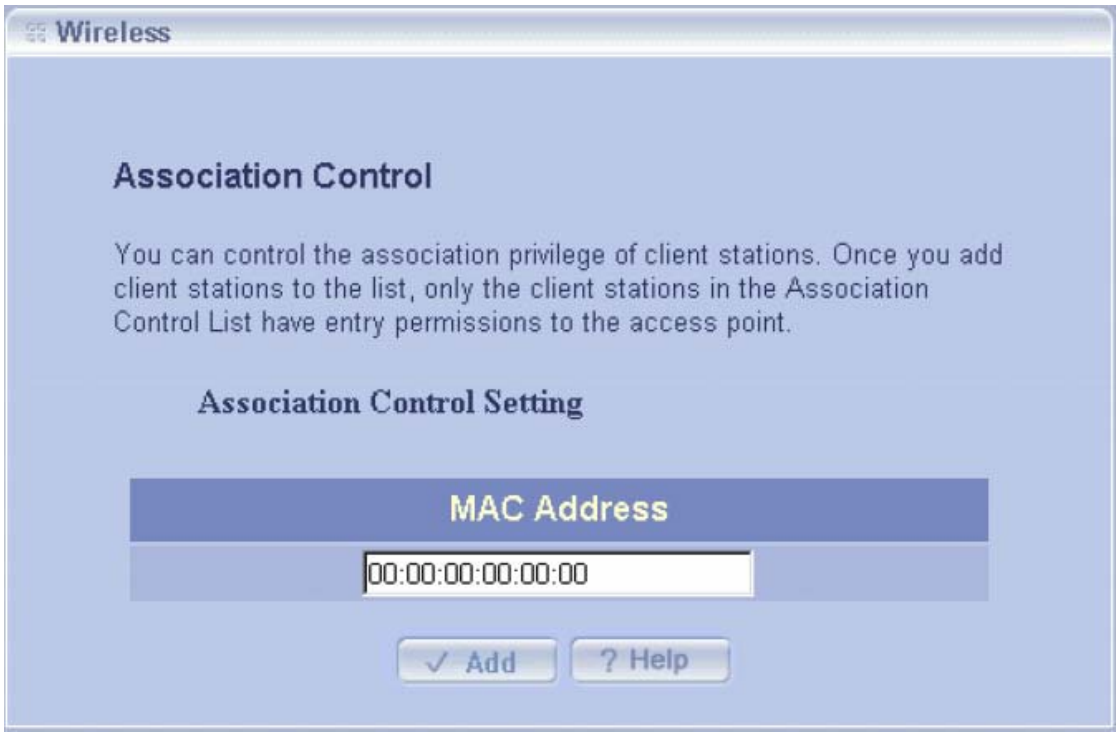



Figura 5.12. Sección Association Control.

*Paso 4.*

Probar que en realidad la tarjeta de red seleccionada ya no tiene acceso al access point, haciendo un *ping* a la dirección IP de la puerta de enlace (por ejemplo: 192.168.2.1, como se muestra en la figura 5.13. Además al intentar conectarse al access point marcara un error como el de la figura 5.14.

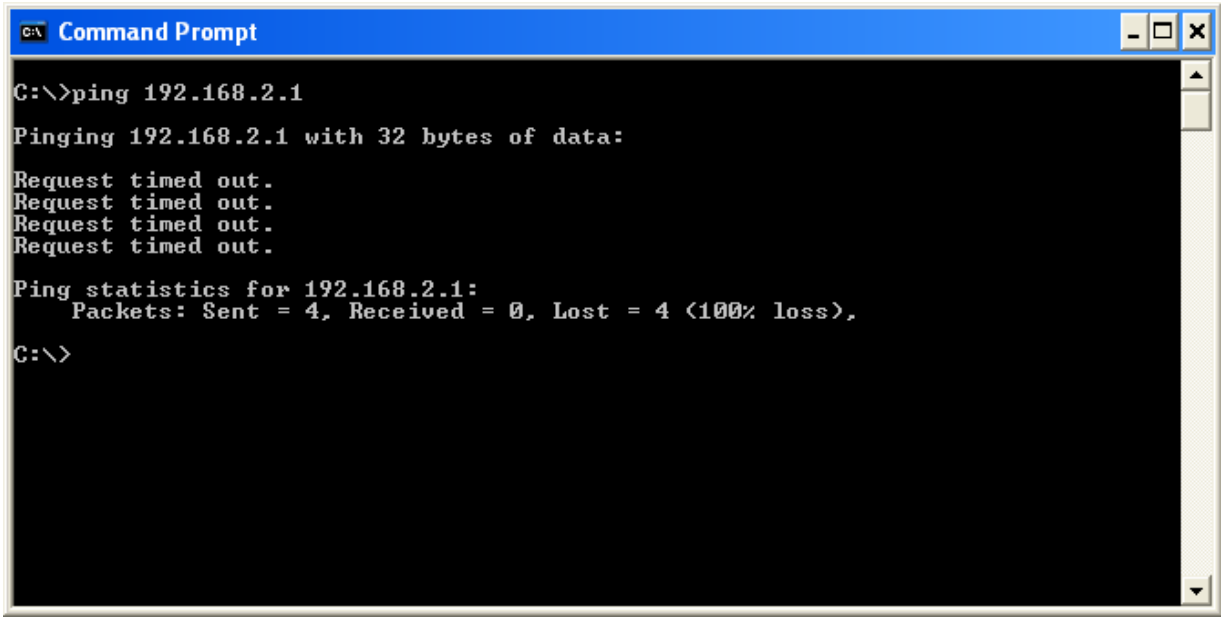



Figura 5.13. Comprobación de la Tarjeta de Red.

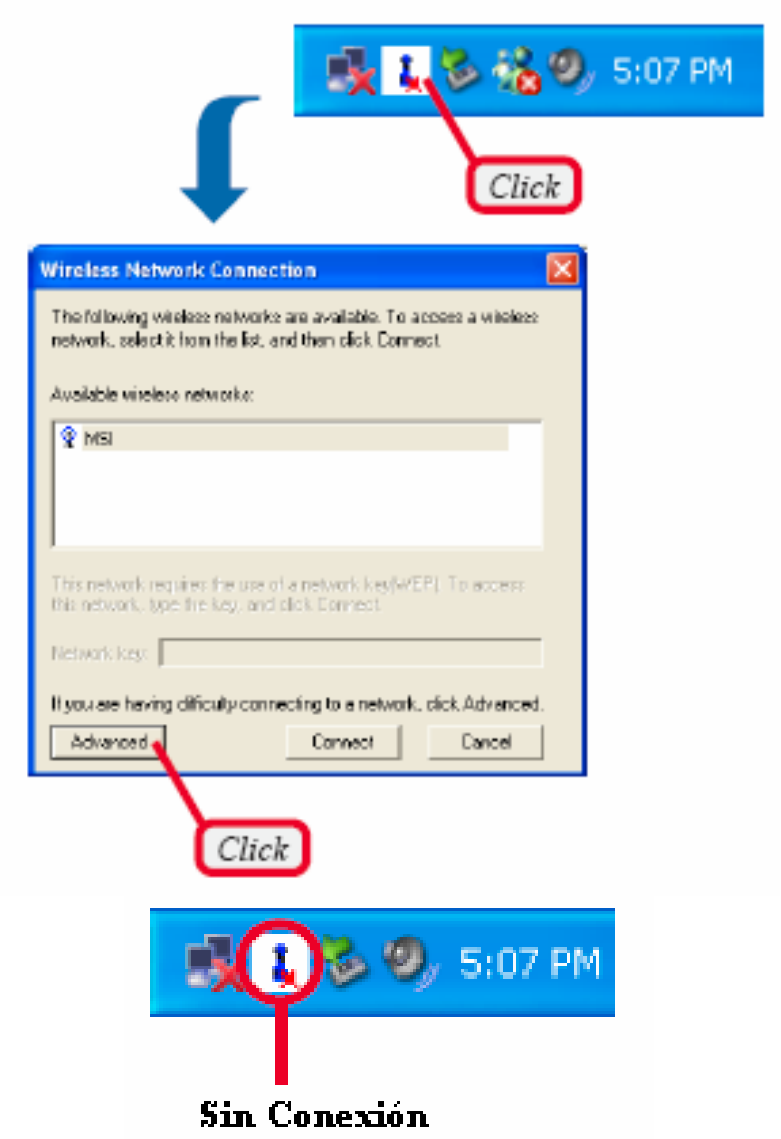



Figura 5.14. Error  cuando no esta conectada a la red

## *5.1.3.5. Conclusiones.*

¿En qué  casos es útil filtrar por MAC?
Si filtramos por MAC, ¿esta nuestra red completamente segura? Explique su respuesta.

## *5.1.4. Práctica 4. Análisis de tráfico*

### *5.1.4.1. Cuestionario previo*

1. ¿Qué es un analizador de tráfico?
2. ¿Para que nos sirve analizar el tráfico de una red?
3. ¿Qué tipos de analizadores de tráfico existen?

### *5.1.4.2. Objetivo*

El alumno instalará dos diferentes analizadores de tráfico en diferentes sistemas operativos y analizará e interpretará los resultados que éstos arrojen acerca de que tipo de tráfico esta pasando por la red del laboratorio.

### *5.1.4.3. Material*

Red del laboratorio
1 Computadora con sistema operativo Windows, con Ethereal instalado
1 Computadora con sistema operativo Linux, con Ntop instalado

### *5.1.4.4. Descripción*

### *Paso 1.*

Aquí se instalarán los dos analizadores de tráfico.

Empezaremos con Ethereal en Windows. Se deberá descargar el ejecutable, esto lo podrá hacer del servidor del laboratorio. Para instalarlo sólo se debe ejecutar.

Para Ntop en Linux se instalará por medio del sistema de paquetes particular de cada distribución. Por ejemplo, para Debian con el comando apt-get, para Fedora/RH se podrá utilizar YUM o bajar el paquete rpm e instalarlo.

## *Paso 2.*

En este paso se analizará el tráfico del laboratorio con las dos aplicaciones propuestas.

### ***Ntop***

Inicie el Ntop

#/etc/init.d/ntop start

Inicie un navegador

# mozilla &

En la barra de direcciones del navegar escriba http://localhost:3000

Seleccione el menú Stats

En la sección “Summary” verifique la carga de la Red “Network Load” y la distribución según el protocolo “Traffic”

En la sección “Hosts” determine las estaciones que están generando más tráfico en la red y note el tipo de tráfico como se muestra en la figura 5.15.

¿Es suficiente la información que se obtiene con esta herramienta o quisiera más información? Justifique su respuesta.

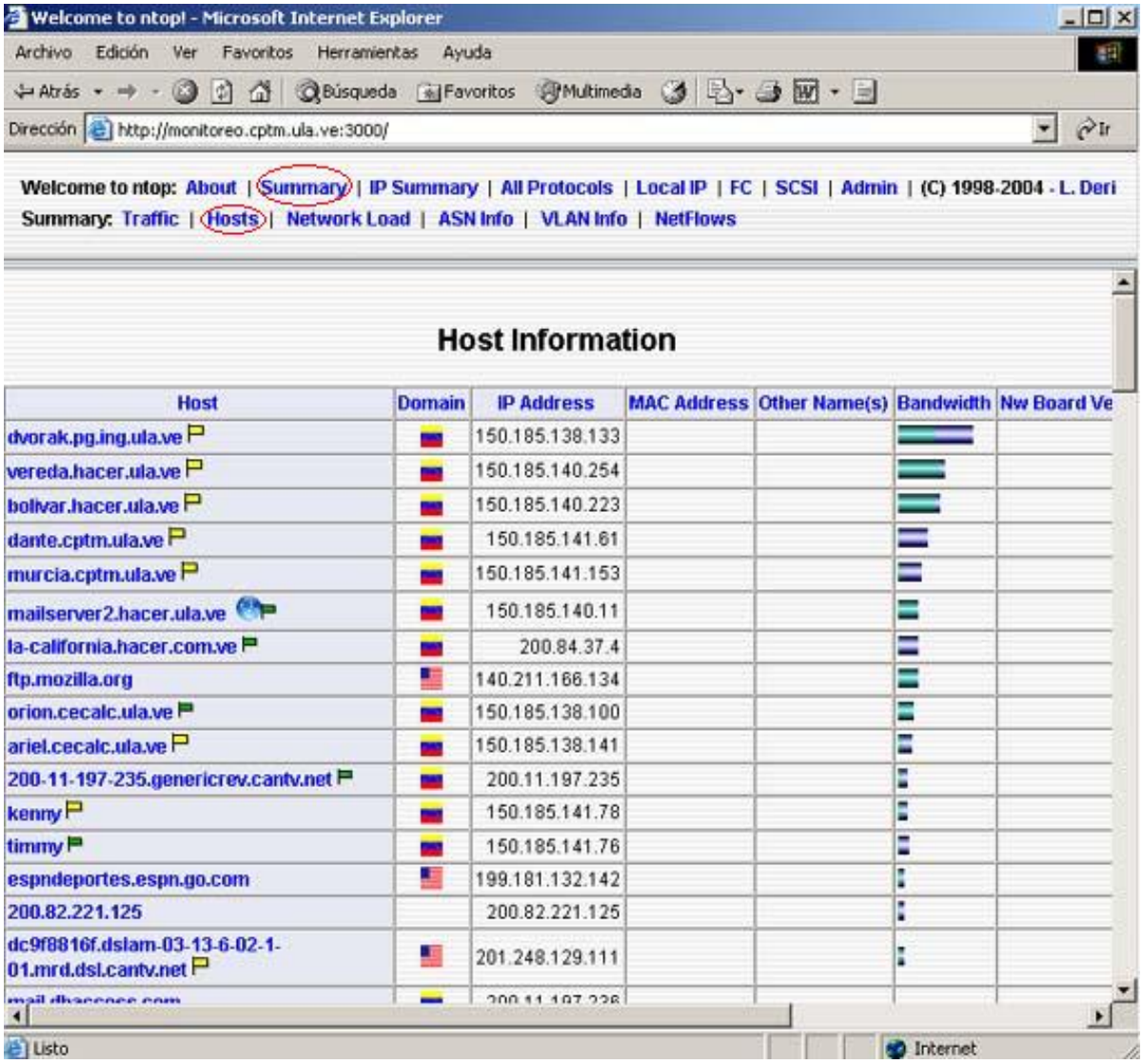



Figura 5.15. Host que generan más tráfico

## *Ethereal.*

Iniciar Ethereal, deberá aparecer una pantalla como la que se muestra en la figura 5.16.

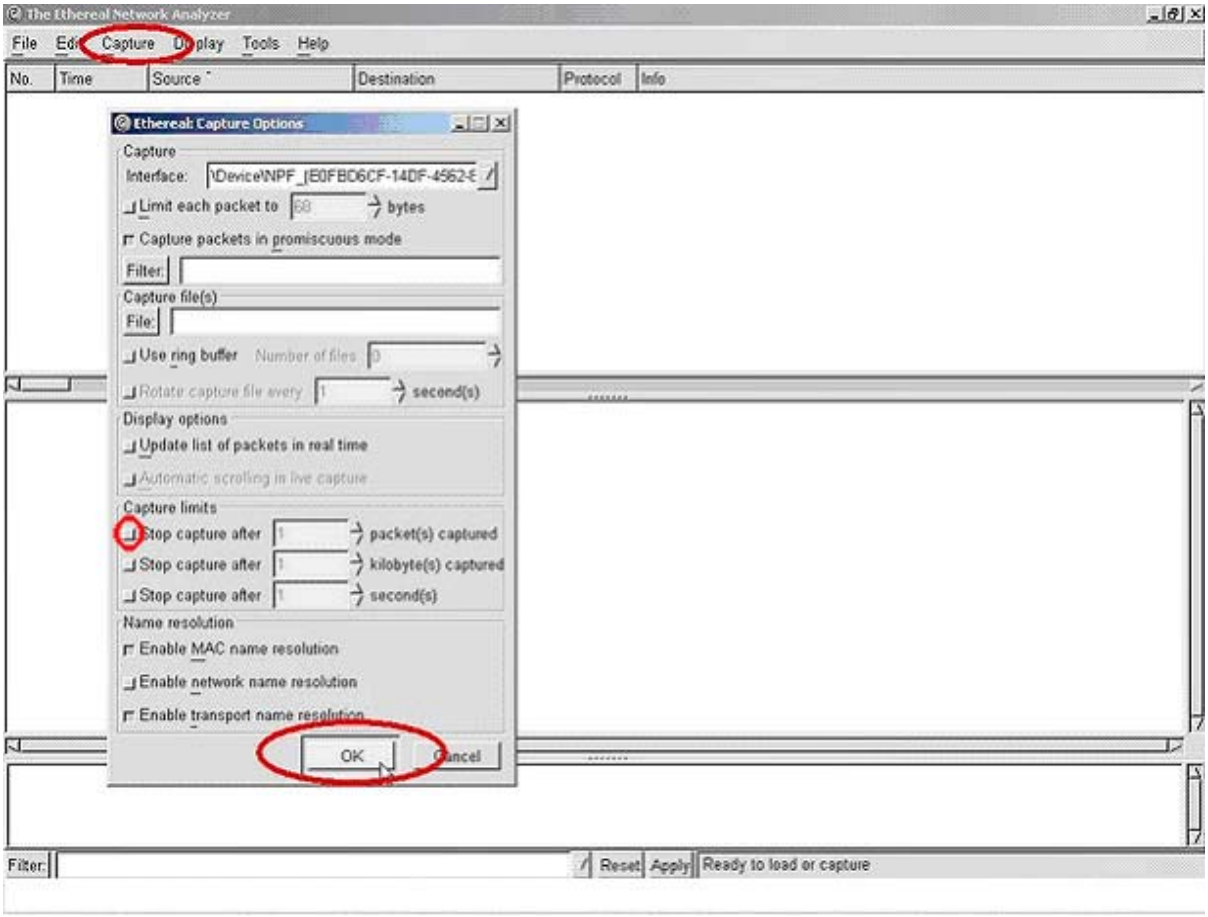



Figura 5.16. Pantalla inicial de Ethereal

Realizar un clic en captura, en el campo “Stop capture after” escriba 100 y luego presione el botón OK.

Analice los resultados de la captura y determine el tipo de tráfico existente en la red.

Compare los resultados con los obtenidos con el Ntop.

Discuta los Resultados

_____
_____
_____

### *5.1.4.5. Conclusiones.*

¿Qué medidas de seguridad podemos tomar al conocer el tráfico que esta pasando por nuestra red?

¿Se puede optimizar la red conociendo el tráfico que circula por ella? Explique se respuesta.

## 5.2. Aplicación de las prácticas

Para llevar a cabo esta parte se organizaron grupos de 10 alumnos a fin de probar las prácticas propuestas. Esta actividad se llevó a cabo en el laboratorio de Redes y Seguridad con alumnos de las asignaturas de: Redes de Computadoras y Temas Especiales de Computación: Fundamentos de Seguridad Informática.

En todos los casos se les entregó a los alumnos el material con una semana de anticipación a fin de que pudieran desarrollar el trabajo previo indicado y leer anticipadamente la práctica.

### *5.2.1 Práctica 1*

Esta práctica se desarrolló los días 18 y 19 de octubre del 2005 con alumnos de la clase de Redes de Computadoras, los alumnos comentaron a su llegada que el trabajo que realizamos sobre la Red Inalámbrica para el Laboratorio de Redes y Seguridad es muy interesante ya que a ellos les sirve mucho dado que aun no llevan en la clase de Redes de Computadoras teoría sobre redes inalámbricas y comentaron que mejor que ver la teoría y la práctica al mismo tiempo.

Al finalizar esta práctica los alumnos asistentes a la práctica nos dijeron que la práctica fue bastante ilustrativa dado nunca habían tenido contacto con equipo inalámbrico y aunque la práctica fue muy básica les ayudo a comprender más sobre las redes de computadoras, así como el funcionamiento básico de las redes inalámbricas.

### *5.2.2 Práctica 2*

La práctica 2 se realizó los días 3, 4 y 17 de noviembre, esta práctica se realizó en tres ocasiones dado que asistieron alumnos de la clase de Redes de Computadoras y de la clase de Temas Especiales de Computación: Fundamentos de Seguridad Informática. En esta sesión de práctica los alumnos nos comentaron al final de la práctica que les resultó algo cortas en tiempo, que les hubiera gustado que durara más y que también les gustaría que existieran mas equipos dado que al contar unicamente con dos equipos con tarjeta de red inalámbrica sólo dos alumnos pueden llevar a cabo lo que dice la práctica y que los demás permanecen como espectadores. Pero a pesar de esto y de que la práctica es muy sencilla les gustó

dado que nunca habían trabajado con access point, con tarjetas de red inalámbrica, ni nunca habían configurado un servidor DHCP en Linux, además nos dijeron que esta práctica les ayudará para salir mejor preparados para el campo laboral dado que en muchas instituciones están migrando o ampliando sus redes de forma inalámbrica.

Por último comentaron que sería interesante adquirir mas equipo y de prestaciones superiores para que se puedan hacer unas prácticas más completas, así como poder hacer la instalación de una tarjeta de red inalámbrica en el sistema operativo Linux.

### *5.2.3 Práctica 3 y 4*

Esta práctica se realizó los días 10 y 11 de noviembre, en la cual un día asistieron los alumnos de la clase de Redes de Computadoras y el otro día los alumnos de la clase de de Temas Especiales de Computación: Fundamentos de Seguridad Informática. En esta sesión se realizaron las prácticas 3 y 4 dado que las dos tienen que ver con seguridad informática.

Para esta práctica los alumnos nos comentaron que les gustó mucho debido a que fue muy ilustrativa dado que nunca habían manejado el filtrado por MAC ni habían visto ningún analizador de tráfico para redes y que rara vez se puede ver esto en una sesión de laboratorio, aunque como en la práctica anterior dijeron que se debería de equipar el laboratorio con más equipos inalámbricos para que todos los asistentes puedan poner en práctica lo solicitado. Por último nos dijeron que la explicación que dimos sobre la práctica fue bastante clara y concisa, y eso les ayudó a comprender más lo ya visto en la clase de teoría.

# CONCLUSIONES

Como parte final de este trabajo se hace un análisis con base en la información de los capítulos anteriores sobre la situación de las redes inalámbricas.

Dado que la intención principal de esta tesis era diseñar e implementar una red que sirviera a los alumnos de los últimos semestres a tener contacto directo con este tipo de tecnologías es que se decidió utilizar una red de tipo infraestructura, ya que es el tipo de red que no está aislada, es decir, sirve para tener salida a Internet; esta característica lleva implícitos muchos detalles que hay que tomar en cuenta, uno de los más importantes es la seguridad.

El grado de dificultad de la implementación de una red inalámbrica depende principalmente del tamaño de la misma, ya que hay que tener en consideración muchas cosas, por ejemplo, el número de usuarios que se van a conectar a la red, equipos suficientes para que se tenga el alcance necesario en el lugar donde será implementada, cuantos perfiles existirán, entre otros, sin embargo, el primer problema al que nos enfrentamos fue de tipo económico, ya que el laboratorio no contaba con el equipo necesario para la instalación de una red de este tipo.

Afortunadamente pudimos librar este problema y llevar a cabo nuestro proyecto, aunque con muchas limitantes técnicas porque al ser tan sencillos nuestros equipos no pudimos implementar muchas características que hoy en día se están utilizando.

A lo largo de este trabajo nos encontramos con otro tipo de cosas que en un principio no estaban contempladas porque estrictamente no pertenecen a la implementación de redes; por ejemplo, tuvimos que administrar algunas aplicaciones en un servidor Linux para tener un mejor control de la red y ofrecer ciertas comodidades a los usuarios, algunos ejemplos de esto son: la instalación y configuración de un servidor DHCP que es el que permite al usuario conectarse a la red sin tener que configurar nada en su dispositivo inalámbrico; NAT es la aplicación que nos permite tener una red no homologada, y Ethereal nos permite analizar y así controlar el tipo de tráfico que está pasando por la red.

Este trabajo nos permitió también no sólo profundizar en el estudio de las redes inalámbricas, sino que nos dio una visión integral de lo que un administrador de red debe enfrentar día a día.

Este sólo fue el primer paso para que nuestra facultad cuente con una red inalámbrica robusta de carácter didáctico, ya que si bien, la facultad cuenta con redes inalámbricas, éstas son de servicio y se requiere un espacio en el cual los estudiantes de ingeniería en el ramo de la computación tengamos la oportunidad de

adquirir conocimientos prácticos en el quehacer de las redes, ya que como se ha comentado, hay mucho que hacer al respecto en este proyecto.

Dejamos a las siguientes generaciones, la implementación de muchas características de seguridad que no pudieron ser probadas en este momento, como el uso de WPA, autenticación cliente-servidor mediante un servidor Radius, creación de perfiles más robustos y creación de políticas de seguridad, entre otras muchas otras características que una red importante debe tener.

A continuación se hace un breve resumen de los resultados obtenidos en cada uno de los capítulos que conforman nuestro trabajo de tesis:

Capítulo 1

Este capítulo contiene una panorámica general de lo que es una red inalámbrica, se presentan conceptos y definiciones, algunos de ellos son ampliamente analizados en los capítulos siguientes, se dio fin al capítulo 1 haciendo una valoración de las características buenas y malas que conlleva la implantación de una red inalámbrica.

Como hemos visto, las redes inalámbricas han venido a cubrir algunos aspectos que anteriormente era imposible satisfacer con las redes hasta entonces conocidas o que resultaba altamente costoso satisfacerlos, estas características han hecho que su evolución y presencia en el mercado haya crecido rápidamente.

Este crecimiento hace que los nuevos ingenieros relacionados con el diseño, análisis, implantación y monitoreo de redes deban estar capacitados para entender, utilizar y mejorar las tecnologías que están cambiando al mundo, por lo que contar con una red inalámbrica en la cual se puedan hacer prácticas relacionadas con su instalación, administración y uso es fundamental para dichos ingenieros.

Capítulo 2

Este capítulo nos permitió decidir que tipo de topología implementar para nuestro proyecto; se decidió instalar una topología de infraestructura dado que se puede implementar si ya se cuenta con una red alambrada, no se eligió la Ad Hoc porque se planea que la red conviva con una red alambrada, cosa que no nos permite hacer esta última topología. Así mismo nos apegamos al estándar IEEE 802.11 en su especificación b, lo cual nos parece lo más adecuado y eficiente para nuestras necesidades, ya que al ser la red inalámbrica para un propósito estudiantil no

necesitamos de grandes velocidades. Pero no por ello vamos a descuidar la calidad de la señal de la red inalámbrica. Por ultimo se empleo un Access Point dado que sólo requerimos que concentre los equipos inalámbricos e irradie la señal a las computadoras que se encuentran en el laboratorio, además que si se tiene una red alambrada se puede conectar a dicha red.

Capítulo 3

En este capítulo comprobamos las diferencias de usar diferentes sistemas operativos, ya que intentamos instalar una de las tarjetas de red en una computadora con sistema operativo Linux Debian, sin embargo después de tratar con diferentes paquetes de drivers para tarjetas de red inalámbrica, no pudimos hacer que ésta funcionara y en Windows XP funcionó sin problemas.

En el servidor instalamos el servicio de DHCP, lo que nos ayudó a entender mejor cómo es que funciona este servicio y a realizar diferentes pruebas entre las tarjetas inalámbricas y las tarjetas convencionales existentes en el laboratorio.

Respecto a la clave WEP, comprobamos que sí es necesaria una forma de autenticar así a nuestros usuarios ya que en el servidor DHCP descubrimos que máquinas desconocidas estuvieron conectadas a nuestra red. Lo cual repercute en el ancho de banda de la red.

Capítulo 4

En este capítulo se hicieron diferentes pruebas a la red como fueron pruebas a la conexión de los Access Point, los alcances de la señal de dichos aparatos, autenticación por WEP, filtrado por MAC y el análisis de protocolos.

Estas pruebas nos sirvieron para determinar qué tan buena es la conexión que se realiza entre una tarjeta de red inalámbrica y un Access Point y si se pierde muy fácil o se mantiene la señal de forma constante; cuáles son los alcances de la señal de los Access Point tanto de forma horizontal y vertical.

Así mismo nos sirvieron para saber que tan seguros son los Access Point con los que se cuenta en el Laboratorio de Redes y Seguridad, al configurar los Access Point para que cuenten con clave WEP y se comprobó que si un usuario intenta

establecer una conexión, si no cuenta con la clave WEP le resultará imposible establecer una conexión.

Por otra parte con respecto al filtrado por MAC se comprobó que al restringir la conexión a todas las computadoras que intenten establecer una conexión, exceptuando a las computadoras que cuentan con tarjeta de red inalámbrica y su MAC está dada de alta en la lista de acceso al Access Point.

También el análisis de protocolos que hicimos a la red nos sirvió para darnos una idea de la cantidad de tráfico que circula por la red y los protocolos más empleados en nuestra red inalámbrica; y así poder tenerla en un estado óptimo.

Desafortunadamente estas pruebas fueron muy básicas, ya que los equipos con los que contamos no tienen soporte para características que se utilizan hoy en día, como son WPA, autenticación cliente-servidor, entre otras.

## Capítulo 5

En este capítulo se presentaron algunas prácticas básicas del uso y configuración de dispositivos de red inalámbricos y aplicaciones que nos permitirán hacer un uso óptimo del equipo con el que se cuenta en el laboratorio.

Si bien, en estas prácticas se intentó cubrir lo más posible en lo referente a configuración, administración y seguridad en dispositivos de redes inalámbricas, lo cierto es que con el equipo que se cuenta en el laboratorio no es posible profundizar en algunos aspectos, en particular la seguridad.

Dejamos sin embargo, una implementación básica de la red inalámbrica del laboratorio de redes, pensando que en el corto plazo se puedan adquirir equipos que permitan al alumno conocer las características reales de los equipos a las que se enfrentarán en el campo laboral.

Éstos nuevos equipos deberán tener soporte de más características de seguridad, como son: autenticación de usuarios usando WPA que mejora al protocolo WEP, el protocolo 802.1x que está basado en una arquitectura cliente-servidor, VPN’s de IPSec, solo por nombrar las más conocidas hoy en día.

# BIBLIOGRAFÍA Y MESOGRAFÍA

# Bibliografía

Wisniewski, Steve
*Wireless and cellular networks*
Upper Saddle River, New Jersey: Pearson/Prentice Hall, 2005

Holtzman, Jack M. y Goodman, David J.
*Wireless and mobile communications*
Boston: Kluwer Academic, 1994.

Mann, Steve
*The wireless application protocol (WAP)*
New York: J. Wiley, 2000.

Toh, Chai-Keong
*Wireless ATM and AD-HOC networks: protocols and architectures*
Boston: Kluwer Academic, c1997

Muller, Nathan J.
*Wireless data networking*
Boston: Artech House, 1995

Briere Danny, Bruce III Walter R. y Hurley Pat
*Wireless home networking for dummies*
New York, New York: Wiley, c2003

Beaulieu, Mark
*Wireless Internet applications and architecture: building professional wireless applications worldwide*
Boston: Addison-Wesley, 2002

Kikta Roman, Fisher Al y Courtney Michael P.
*Wireless Internet crash course*
New York; Mexico City: McGraw-Hill, c2002

Rhoton, John
*The wireless Internet explained*
Boston: Digital, c2002

Flickenger, Rob
*Wireless: los mejores trucos*
Madrid: Anaya Multimedia, 2004

Wesel, Ellen Kayata
*Wireless multimedia communications: networking video, voice, and data*
Massachusetts: Addison-Wesley, 1998

Morrow, Robert K.
*Wireless network coexistence*
New York: McGraw-Hill, 2004

Smith, Clint
*Wireless network performance handbook*
New York: McGraw-Hill, 2003

Geier, James T
*Wireless networks first-step*
Indianapolis, Indiana: Cisco, 2005

Nichols Randall K. y Lekkas Panos C.
*Wireless security: models, threats, and solutions*
New York: McGraw-Hill, 2002

Yacoub, Michel Daoud
*Wireless technology: protocols, standards, and techniques*
Boca Raton: CRC, 2002

Rischpater, Ray
*Wireless web development*
Berkeley, California: Apress, 2000

# Mesografía

http://agalisa.es/article213.html

http://www.xbitlabs.com/articles/mobile/display/wi-fi.html

http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf

http://www.it.uc3m.es/pervasive/documentos/Bluetooth.pdf

http://www.intel.com/netcomms/technologies/wimax/index.htm

http://www.conocimientosweb.net/dt/article1544.html

http://www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/intro.asp

http://www.it.uc3m.es/ividal/articulos/telecom03_adhoc.pdf

http://oasis.dit.upm.es/~cdc/HOWTO-MIP/index.html

http://www.fm.uach.mx/alex/trabajos/escolar/redes/tarea%206.htm

http://www.ericsson.com.mx/soluciones/mobil/wap/

http://www.microsoft.com/latam/technet/articulos/200408/cg0604.mspx

http://biblioteca.dgsca.unam.mx/cu/productos/boletines/msg00051.html

http://www.anixter.es/webaxeuk/ES.nsf/a204a7a2c15550e8c1256b2000369d71/455012b2724355bac1256c1a003da895/$FILE/Spanish%20Wireless.pdf

http://www.sistelec.es/pdf/pdf_airmagnet/WIRELESS.pdf

http://usuario.cicese.mx/~jasan/art_ci4g/ar_ci4gc.html

http://www.redes.upv.es/irc/trabajos/PabloI.pdf

http://www2.alcatel.es/tecnotribuna/docs/art_pdf/b_wifi.pdf

http://217.116.8.23/publicac/publbit/bit138/wifi.pdf

http://www.msicomputer.com/product/p_list.asp?class=com

http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=13&selcat=Wireless

http://www.ceditec.etsit.upm.es/Informes_globales/ceditec_wifi.pdf

http://www.fundacionauna.com/areas/26_estudios/pdf/3.pdf

http://www.wifispain.org/content/view/30/2/1/0/

http://www.34t.com/unique/WiFiAntenas.asp

http://www.e-advento.com/tecnologia/wlan_intro.php

http://www.wi-fi.org/OpenSection/index.asp

http://www.ieee.org/portal/site/iportals/

http://www.intel.com/cd/personal/computing/emea/spa/wireless/245838.htm