

# **CAPITULO I**

## **TECNOLOGÍAS DE REDES INFORMÁTICAS.**

### **1.1. REDES INALÁMBRICAS DE DATOS**

#### **1.1.1. Introducción a la Tecnología Inalámbrica Wireless**

Actualmente las redes de computadoras están presentes en todas las empresas. Las limitaciones aparecen cuando se trabaja con redes externas, especialmente si se trata de comunicar dos puntos distantes entre edificios con problemas de instalación de cableado que no soporte la distancia establecida si los edificios están ubicados un par de kilómetros.

La tecnología Wireless nos permite montar una red con todas sus ventajas en un corto tiempo, sin tener ni un solo cable, basta instalar un punto de red en donde se instala un dispositivo que contendrá los puertos inalámbricos. Además se instala una tarjeta de red inalámbrica a cada equipo.

Montar una red sin hilar cables puede ser muy útil por ejemplo cuando queremos montar un stand en una feria, o cuando vamos a estar de manera provisional en una oficina o cuando trabajamos en una de esas inmensas oficinas diáfanas donde no es fácil hacer una instalación.

La red inalámbrica permite movilidad total, sin necesidad de mayores ajustes técnicos o físicos, como en las ya anticuadas redes fijas, en donde el cableado

estructurado siempre estuvo ligado a costosas mantenciones y costosos cambios al momento de mover o agregar un equipo.

## **1.1.2. Clasificación de redes inalámbricas**

### **1.1.2.1. Wireless PAN (Personal Area Network)**

Se trata de una conexión inalámbrica de corto alcance entre dispositivos personales como PC, teléfonos móviles y PDA. Un estándar común de PAN es Bluetooth, que es una tecnología inalámbrica con un radio de corto alcance para redes de voz y datos a una velocidad de transferencia de 1 Mbsp como máximo.

Permite interconectar dispositivos electrónicos dentro de un rango de pocos metros, para comunicar y sincronizar información. La tecnología líder en esta área es Bluetooth.<sup>1</sup>

Dentro de estas redes se encuentran las siguientes:

#### **a) Bluetooth.**

Es una tecnología que utiliza un rango de frecuencias de los 2,4 GHz a los 2,4835 GHz, aunque esta cambia de país en país. El ancho de banda disponible para los usuarios consigue hasta los 10 Mbps. Es el nombre común de la especificación industrial IEEE 802.15.1, que define un estándar global de comunicación inalámbrica que posibilita la transmisión de voz y datos entre diferentes

---

<sup>1</sup> <http://www.conocimientosweb.net/portal/article246.html>, Anónimo, 1999

dispositivos mediante un enlace por radio frecuencia segura, globalmente y sin licencia de corto rango. Los principales objetivos que se pretende conseguir con esta norma son:

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

Los dispositivos que con mayor intensidad utilizan esta tecnología son los sectores de las telecomunicaciones y la informática personal, como PDAs, teléfonos celulares, ordenadores portátiles, PCs, impresoras y cámaras digitales. Sin embargo, la cobertura que ofrece este tipo de dispositivos es bastante limitada, ya que se reduce a 10 metros.

#### **b) Telecomunicaciones Inalámbrica Digital Mejorada.**

DECT, Digital Enhanced Cordless Telecommunication (Telecomunicaciones Inalámbrica Digital Mejorada). Es un estándar común para la telefonía, mensajería y transmisión de datos sin cables. Consiste en una tecnología de radio aceptada a aplicaciones de voz datos y redes en ambientes residenciales, comerciales y públicos, con requisitos de rango de hasta algunos cientos de metros. DECT opera utilizando señales de radio en el rango de frecuencia de 1880 a 1930 MHz. La potencia de salida de los DECT es muy baja de 0 a 0.01 watt para los teléfonos normales y 0.01 a 12 watt para las estaciones base fijas.

### **c) Infrarrojo.**

Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las computadoras se encuentran en una sola oficina. Un ejemplo de esta tecnología son algunos dispositivos *Bluetooth* que usan infrarrojo para comunicarse.

### **1.1.3. Redes inalámbricas de área local.**

#### **1.1.3.1. Wireless LAN (Local Area Network).**

Las cuales permiten conectar una red de computadores en una localidad geográfica, de manera inalámbrica para compartir archivos, servicios, impresoras, y otros recursos.

#### **1.1.3.2. Wi-Fi.**

Forma inalámbrica de implementar redes locales (“LANs”), sin requerir infraestructura física (cableado) para dar conectividad al usuario, lo que representa una alternativa caracterizada por su rapidez de construcción, puesta en marcha y uso.<sup>2</sup>

### **Ventajas.**

Han logrado la implementación rápida de LANs en edificios corporativos, logran la creación de “puntos calientes”, o “hot spots”, en lugares públicos como hoteles, aeropuertos, y sitios municipales, donde los dueños de computadoras portátiles

---

<sup>2</sup> José A. Carballar Falcón, WI-FI. CÓMO CONSTRUIR UNA RED INALÁMBRICA, 2ª EDICIÓN

(con tarjetas de red Wi-Fi) pueden llegar para conectarse al punto central del hot spot, que a su vez está conectado al Internet.

#### **1.1.3.3. Home RF.**

Tecnología similar a la de Bluetooth, su nombre completo es Home Radio Frequency, proporciona interconexión entre productos electrónicos de consumo dentro del hogar. Utiliza también la misma banda de 2,4 GHz, pero no interfiere con ella gracias al método de salto de frecuencia (protocolo de acceso inalámbrico compartido), que en este caso es de 50 saltos por segundo, en vez del Direct Sequence empleado en otras tecnologías. La distancia que alcanza es 50 metros. Al igual que Bluetooth, Home RF utiliza el salto de frecuencia para evitar interferencias, admite la comunicación de datos hasta 2 Mbits/s y permite conectar hasta un total de 127 dispositivos. Soporta comunicación de voz y datos.

#### **1.1.3.4. Hiper LAN (High Performance Radio LAN).**

Es un conjunto de la red local radiofónica de área (WLAN). Hay dos especificaciones: HiperLAN/1 y HiperLAN/2. Ambos han sido adoptados por los Estándares europeos de Telecomunicaciones. Los estándares de HiperLAN les proporcionan las características y las capacidades semejantes a los estándares del IEEE 802,11 utilizado en los EE.UU.

HiperLAN/1 proporciona comunicaciones a 20 Mbps en la gama de 5 GHz de la frecuencia de radio (RF) el espectro. HiperLAN/2 opera a 54 Mbps en la misma banda de RF. HiperLAN/2 es compatible con 3G (la tercer-generación) sistemas de WLAN para mandar y recibir datos, para las imágenes, y para comunicaciones

de voz. HiperLAN/2 tienen el potencial, y se piensa, para la implementación por todo el mundo en conjunción con sistemas semejantes en la banda de 5 GHz del RF.

#### **1.1.4. Redes Inalámbricas de Área Metropolitana**

##### **1.1.4.1. Local Multipoint Distribution System**

La tecnología de acceso en banda ancha vía radio LMDS (Local Multipoint Distribution System). Esta tecnología convierte las señales que viajan por cable en ondas de radio, que se transmiten por el aire en banda ancha mediante una red de estaciones base colocadas en las azoteas de los edificios.

La estación base se comunica con los terminales de los clientes, paneles de pequeñas dimensiones (26 cm x 26 cm) también situados en las azoteas de los edificios. La comunicación de datos se realiza con una velocidad de hasta 4 Mbps, de forma simétrica (misma velocidad para el envío y recepción de los datos), dedicada.

Al permitir la bidireccionalidad, se pueden ofrecer servicios como la telefonía o el acceso a Internet mediante una plataforma única.

##### **1.1.4.2. WiMAX o IEEE 802.16**

WiMax (Worldwide Interoperability for Microwave Access) Es el estándar 802.16<sup>a</sup> utilizado para transmisión inalámbrica de datos diseñado para áreas

metropolitanas o MAN lo que hace distinto a WiMax es su alcance y su ancho de banda. WiMax ofrece tasas de transferencia de 124Mbit/s a distancias de hasta unos 70 kilómetros de una estación base, utilizando tecnología portátil LMSD.

Utiliza una banda del espectro de 2-11 GHz, facilitando su regulación. Además, como ventaja añadida está en el uso de estaciones base (BS) formadas por antenas emisoras/receptoras con capacidad de dar servicio a unas 200 estaciones suscriptoras (SS) que pueden dar cobertura y servicio a edificios completos.<sup>3</sup>

Esta tecnología de acceso transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias. Está basada en OFDM, y con 256 subportadoras puede cubrir un área de 70 kilómetros permitiendo la conexión sin línea vista, es decir, con obstáculos interpuestos, con capacidad para transmitir datos a una tasa de hasta 75 Mbps con un índice de modulación de 5.0 bps/Hz y dará soporte para miles de usuarios con una escalabilidad de canales de 1,5 MHz a 20 MHz. Este estándar soporta niveles de servicio (SLAs) y calidad de servicio (QoS).

#### **1.1.4.3 Hiper MAN.**

(High Performance Radio Metropolitan Area Networks) Hiper MAN significa Radio de Alto Desempeño de la Red Metropolitana de Area y es un estándar creado por la ETSI, las redes de banda ancha del acceso de la Radio proporciona una comunicación radiofónica de la red en el 2 - 11 bandas de GHz a través de

---

<sup>3</sup> Rob Flickenger, WIRELESS. LOS MEJORES TRUCOS, (Ed. Anaya Multimedia)

Europa y otros países que siguen el estándar de ETSI. HIPERMAN es una alternativa europea a WiMAX o el IEEE 802,16 uniforme.

### **1.1.5. Redes Inalámbricas Globales.**

#### **1.1.5.1. Wireless WAN (Wide Area Network).**

Es una red de computadores que abarca un área geográfica relativamente extensa, típicamente permiten a múltiples organismos como oficinas de gobierno, universidades y otras instituciones conectarse en una misma red. Las WWAN tradicionales hacen estas conexiones generalmente por medio de líneas telefónicas, o líneas estáticas.

A este tipo de redes inalámbricas pertenecen las siguientes tecnologías:

##### **a) CDMA**

Es una tecnología inalámbrica digital que utiliza técnicas de expansión de espectro para distribuir una señal a lo largo de una banda de frecuencias amplia.

Las frecuencias de operación de CMDA en PCs oscila entre los 1850 a 1990 MHz.

##### **b) GSM**

Permite la transmisión digital basada en TDMA, utiliza la idea de compartición de tiempo que permite simultáneamente el acceso de varios usuarios. Introduce comunicaciones de radio de banda ancha, con velocidades de acceso hasta de 2 Mbits/s.

Las frecuencias de operación de GSM entre PCs va desde los 1990 MHz en adelante.

La tecnología GSM tiene entre sus características servicios y soporte que abarca las siguientes áreas:

- Multimedia Mejorados como voz, datos, video y controles remotos.
- Compatibilidad con los dispositivos y medios comunes como el teléfono celular, el correo electrónico, mensajes de localizador, fax, videoconferencia y navegación en Internet.
- Mejor utilización de ancho de banda y alta velocidad (2 Mbits/s).
- Flexibilidad de ruteo ya sea por repetidores, satélite, LAN, etc.
- Operación en frecuencias aproximadas a los 2 GHz para transmisión y recepción.
- Capacidad de Roaming en Europa, América, y algunas partes de Asia.

#### **1.1.6. Otros Tipos de Redes Inalámbricas.**

**1.1.6.1. Red Inalámbrica Punto a Punto.-** Si se dispone de un bajo número de equipos distribuidos en un espacio reducido, hay dispositivos idóneos para poner en marcha una red inalámbrica independiente. En esta red se puede conectar un pequeño número de ordenadores de sobremesa, portátiles, PDAs, impresoras.

**1.1.6.2. Red Inalámbrica con Punto de Acceso.-** El diseño e instalación de la red inalámbrica es adecuada en caso de que disponga de un alto número de equipos, o bien éstos se encuentren distribuidos en un edificio o en un espacio amplio. La red inalámbrica dispondrá de un Punto de Acceso que controlará el tráfico entre los dispositivos inalámbricos.

**1.1.6.3. Redes Inalámbricas Interconectadas.-** Dado que el alcance de una única red inalámbrica es limitado, el utilizar varias redes inalámbricas conectadas entre sí permite ampliar la distancia a la que funcionarán los equipos inalámbricos.

Se utilizan los Puntos de Acceso, que actúan como puentes entre las diferentes redes inalámbricas. De esta forma, los equipos inalámbricos pueden moverse libremente por toda la institución, al tiempo que se mantiene acceso interrumpido a todos los recursos de la red.

**1.1.6.4. Red Inalámbrica Integrada con Red Cableada.-** A la hora de crear una red inalámbrica, o modificar la ya existente, para permitir la conexión de sus usuarios con la red cableada del edificio. Para ello utilizamos un Punto de Acceso, que actuaría como puente entre ambas redes, siendo la conexión entre ellas transparente para los usuarios.

El funcionamiento de la interacción entre las redes cableadas e inalámbricas se explica de forma muy fácil. Ambas redes se basan en el mismo estándar, IEEE

802. La red cableada se conoce como la tecnología Ethernet IEEE 802.3 CSMA/CD y la tecnología Ethernet inalámbrica se conocen como IEEE 802.11 CSMA/CA. Las técnicas para la transmisión de datos también son las mismas, lo que hace muy directa y económica la integración de una red inalámbrica en una red Ethernet cableada.<sup>4</sup>

**1.1.6.5. Enlace entre Dos Edificios.-** Una de las aplicaciones de las redes inalámbricas es la conexión de dos edificios entre sí. Es integrar las redes, tanto cableadas como inalámbricas, de ambos edificios, mediante la utilización de dos Puntos de Acceso de larga distancia, situados en general en la azotea o tejado de los edificios. Dependiendo de la distancia a recorrer, podrá ser aconsejable incluir en la conexión dos antenas direccionales de larga distancia, que permiten recorrer coberturas mayores que con las antenas de los Puntos de Acceso. La única limitación de esta estructura es la necesidad de ofrecer visión directa entre las antenas de ambos edificios.

**1.1.6.6. Redes Públicas de Radio.-** Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia. Estas redes se encuentran de acuerdo al modelo de referencia OSI.

---

<sup>4</sup> <http://www.intel.com/es/home/trends/wireless/nw/transition.htm> , Anónimo, 2000

**1.1.6.7. Redes Infrarrojas.-** La transmisión Infrarroja actualmente es una alternativa para las Redes Inalámbricas. El principio de la comunicación de datos es una tecnología que se ha estudiado desde los 70's, Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar.

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

## **1.2. TOPOLOGÍAS DE LAS REDES INALÁMBRICAS**

Al mencionar el término topología nos referimos a la disposición física de los dispositivos inalámbricos (aunque la disposición lógica también se pueda ver influida).

En el mundo Wireless existen dos topologías básicas:

---

<sup>5</sup> <http://www.e-advento.com/soluciones/wlan.htm> , Anónimo, 2003

### 1.2.1 Topología Ad-Hoc (Par a Par)

Cada dispositivo se puede comunicar con todos los demás en forma directa. Cada nodo forma parte de una red **Peer to Peer** o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre sí.

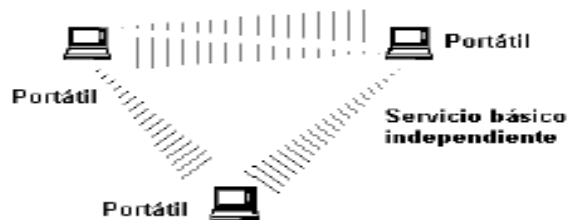


Gráfico 1.- Topología Ad-Hoc

### 1.2.2 Topología Infraestructura.

En el cual existe un nodo central (Punto de Acceso WiFi) que sirve de enlace para todas las demás (Tarjetas de Red Wifi). “Los nodos móviles se comunican con un punto de acceso (Access Point)”. Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP.

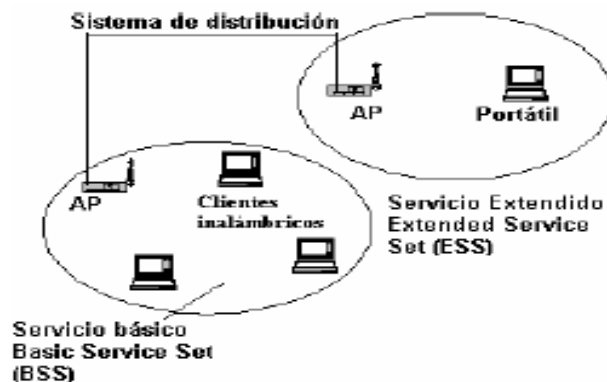


Gráfico 2.- Topología Infraestructura.

### 1.2.3. Modos de Funcionamiento de Dispositivos Inalámbricos.

El modo de funcionamiento es el modo de actuación de cada dispositivo dentro de la topología escogida.<sup>6</sup> Los modos de funcionamiento de los dispositivos inalámbricos son los siguientes:

#### 1.2.3.1 Modos de Radiación Infrarrojos.

Las estaciones con tecnología infrarroja pueden usar tres modos diferentes de radiación para intercambiar la energía óptica entre transmisores-receptores estos son: punto-a-punto, cuasi-difuso y difuso.

##### a) Modo Punto-A-Punto.

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

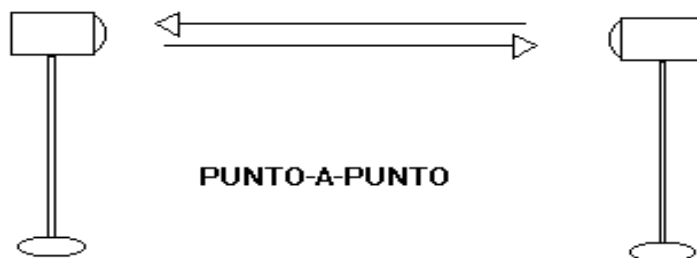


Gráfico 3.- Transmisores-Receptores Punto-a-Punto

<sup>6</sup> Reid Neil & Seide Ron, MANUAL DE REDES INALÁMBRICAS, Editorial McGraw-Hill

### b) Modo Cuasi-Difuso.

A diferencia del modo anterior, el modo cuasi-difuso y difuso son de emisión radial, o sea que cuando una estación emite una señal óptica, ésta puede ser recibida por todas las estaciones al mismo tiempo en la célula. En el modo cuasi-difuso las estaciones se comunican entre si, por medio de superficies reflejantes. No es necesaria la línea de vista entre dos estaciones, pero si deben de estarlo con la superficie de reflexión. Además es recomendable que las estaciones estén cerca de la superficie de reflexión, esta puede ser pasiva ó activa.

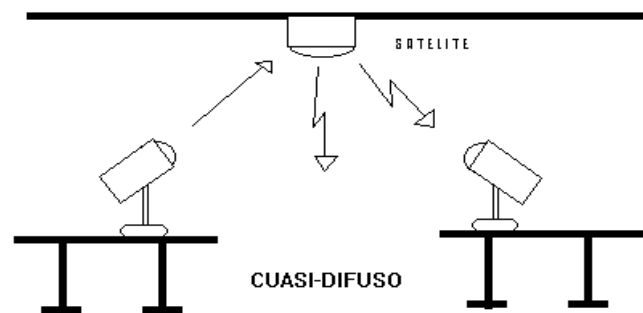
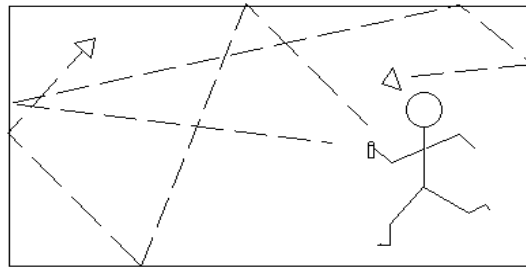


Gráfico.4.- Transmisores-Receptores Cuasi-difuso

### c) Modo difuso.

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



DIFUSO

Gráfico .5.- Transmisores-Receptores Difuso

### 1.3. TECNOLOGÍAS INALÁMBRICAS.

Las tecnologías inalámbricas se clasifican en radiofrecuencia e infrarrojo:



Gráfico .6.- Tecnologías de redes locales inalámbricas.

**1.3.1 Tecnología de Radiofrecuencia.** La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original.

Las tecnologías de radiofrecuencia se dividen a su vez en:

a) **Tecnología de Espectro Disperso.** Consiste en una transmisión de radiofrecuencia confiable y segura, utiliza la banda ISM (902 a 928 MHz, 2400 a

2483.5 MHz y 5,725 a 5,850 MHz), la potencia de radiación es menor a 1 watt, además dispersa la señal en un espectro más amplio.

**b) Tecnología de Banda Angosta.** Transmite y recibe la información del usuario en una frecuencia específica. Mantiene la frecuencia de la señal de radio lo más angosto como es posible, mientras se transmite la información.

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

**d) Salto de frecuencia:** Es una técnica en la que los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Los datos deben ser reconstruidos en base al patrón de salto de frecuencia.<sup>7</sup>

**1.3.2. Tecnología infrarroja.** Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las computadoras se

---

<sup>7</sup><http://www.wl0.org/~sjmudd/wireless/network-structure/english/article.html>, Anónimo, 2002

encuentran en una sola oficina. Un ejemplo de esta tecnología son algunos dispositivos *Bluetooth* que usan infrarrojo para comunicarse.

#### 1.4. DISPOSITIVOS

Hay dos componentes básicos para una red local inalámbrica. Un punto de acceso y un cliente con adaptador de LAN inalámbrica. Los componentes básicos para una red local inalámbrica son:

**1.4.1. Tarjeta de red inalámbrica (*Wireless Adapter Cards*).** Es un dispositivo que sirve para realizar la comunicación inalámbrica con el punto de acceso o con otra tarjeta de red inalámbrica, intercambiando datos y compartir recursos.



Gráfico 7.- Tarjetas de redes inalámbricas PCMCIA y PCI

El WEP (*Wired Equivalent Privacy*), que permite encriptar el tráfico por las redes inalámbricas. WEP se basa en una contraseña que encripta los paquetes que se envían de una estación móvil (cualquier dispositivo con tarjeta inalámbrica) hacia un **Access Point**.

Un mecanismo revisa que el tráfico no sea modificado en tránsito. Por tal se utiliza una misma contraseña que tiene que ser compartida en todas las estaciones móviles y en todos los access point.

### **1.4.2. Punto de Acceso (“Access Point”, AP)**

Un dispositivo que funciona como base para conectar múltiples dispositivos móviles, incluso también entre ellos.

Es un nodo especial en una red inalámbrica que actúa como punto centralizador y gestor del tráfico del resto de equipos (terminales de cliente) suscritos a él y dentro de la celda de cobertura. En general en una misma localización puede coexistir más de un punto de acceso siempre que no interfieran fuertemente sus frecuencias de funcionamiento. La configuración de estos equipos es muy sencilla, apenas ingresando la dirección IP.

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. En resumen es el que crea la red de radio y la comunica con la red local alámbrica. El AP contiene en la primera figura, un puerto 10Base-T.



Gráfico 8.- Punto de acceso (AP)

### **1.4.3. Bridges**

Son elementos que interconectan dos o más redes locales. Si es una 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 unos bridges inalámbricos, orientando las antenas de ambos equipos para la mejor recepción. Los parámetros inalámbricos (canal de frecuencia, 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 bridges del otro extremo.



Gráfico 9.- Bridges.

#### **1.4.4.- Repetidores (Repeaters)**

Permiten extender la cobertura de APs mediante la regeneración y reenvío de información poseen un único interfaz inalámbrico, 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. Operan con los mismos parámetros que el AP para el cual trabajan (frecuencia). 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.

Muchos gateways como APs y bridges pueden configurarse en modo de funcionamiento repeater.



Gráfico 10.- Extensión de cobertura mediante un Repeater.

### 1.4.5. Routers

Poseen capacidad de enrutamiento 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. Actúan como pasarela entre la red inalámbrica directamente gestionada por el equipo (genéricamente llamada LAN) y las redes externas (red local, red de acceso a Internet u otras). Por ello con frecuencia se les denomina gateway (pasarela).

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 y seguridad.



Gráfico 11.- Router

### 1.4.6. Gateways

Los gateways al igual que los demás dispositivos (un router, un AP wireless, un módem ADSL, un firewall), son partes complementarias y necesarias para una red inalámbrica.



Gráfico 12.- Gateway inalámbrico

### 1.4.7. Antenas

Las antenas son dispositivos pasivos que radian energía de radio frecuencia (FR). No crean energía FR, pero enfocan la energía en un área o en una dirección específica, por lo que la fuerza de la señal en esa área o dirección aumenta. El incremento en una dirección viene especificado como Ganancia en unidades dBi. Los dBis están basados en la energía de salida de la antena y en el punto de acceso (AP), aunque no todos los AP soportan conexiones con antenas externas.<sup>8</sup>

Características de las antenas:

Polarización: Indica la orientación de los elementos conductores dentro de la antena. Hay tres tipos:

---

<sup>8</sup> [www.ProyectoExtremaduraWireless.htm](http://www.ProyectoExtremaduraWireless.htm) 2005

- Vertical: Tienen el perfil más alto. Es el tipo de antena más comúnmente usado debido a que no son afectadas por la reflexión horizontal (como agua, tierra,...).
  - Horizontal: Tienen el perfil más bajo. No son afectadas por la reflexión vertical (como por ejemplo edificios).
  - Circular: Tienen un perfil intermedio.
- ❖ Directividad horizontal y vertical.
  - ❖ Ancho de banda de la frecuencia.
  - ❖ Ganancia de energía efectiva (dBi).
  - ❖ Ancho del haz definido en grados a partir del punto 3dB

Uno de los problemas que tienen las antenas es la distorsión multicamino. Esta distorsión ocurre cuando hay más de un camino entre el emisor y el receptor.

Estas múltiples señales se combinan en el RX de la antena y del receptor y causa distorsión en la señal. Para solucionar este problema puede optarse por cambiar la antena o bien la localización de la misma.

#### **1.4.7. 1. Tipos de Antenas**

##### **a) Antenas Omnidireccionales.**

Este es el tipo de antena más común y que viene por defecto en muchos puntos de acceso. Generalmente están formadas por un elemento radiador (dipolo) de una pulgada. Estas antenas irradian la señal en forma de toroide con el fin de dar mayor longitud en horizontal aunque pierden potencia en vertical.

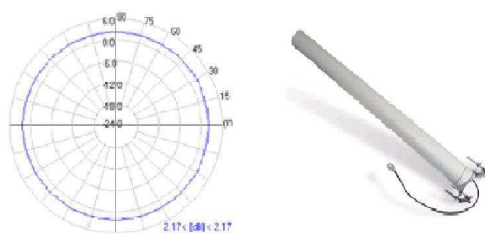


Gráfico 13.-Antenas Omnidireccionales

### b) Antenas Direccionales

Este tipo de antenas concentran su energía en un cono denominado haz, como puede verse en la ilustración que aparece a continuación. El patrón de radiación depende del dominio de la antena direccional en el se encuentre el cliente. Diseñadas para funcionar tanto en interiores como en exteriores.

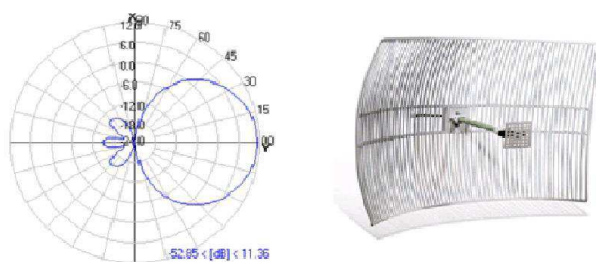


Gráfico 14.-Antenas direccionales

## 1.5. FRECUENCIAS

Según los estándares 802.11 las frecuencias que podemos utilizar para comunicaciones Wireless son aquellas destinadas a libre uso a 2.4 GHz y 5 GHz.

La ley del Ecuador nos restringe todavía más el uso de estas frecuencias ya que la banda de 5GHz está destinada a usos militares. Estamos a la espera de que se destine a uso civil esta frecuencia. La segunda restricción importante que tenemos es la potencia con la que podemos transmitir. Por ahora el límite está en 100mW sin amplificación, a la espera también de que se amplíe a 1W.

### **1.5.1. Frecuencia 2.4 GHz.**

La primera frecuencia que se homologó para poder ser utilizada para comunicaciones digitales inalámbricas es la de 2.4 GHz. Se escogió esta frecuencia porque es una banda destinada a uso libre de radioaficionados, con las limitaciones que hemos comentado anteriormente, y que dependiendo de los países dispone de más o menos canales.

La banda de 2.4 GHz está dentro de la zona de lo que se llaman microondas. Esta banda tiene la peculiaridad que en estas frecuencias existe muy poco ruido. Además al tratarse de frecuencias “próximas” a las de la luz visible tienen un comportamiento bastante similar a ésta, con la pequeña ventaja de que al ser longitudes de onda más largas objetos pequeños como vegetación o tabiques son bastante transparentes a la señal, esto nos permite que no siempre tengamos que tener visión directa entre emisor y receptor. Con otros elementos también existen reflexiones especulares, esto hace que queden “iluminadas” zonas que a simple vista no tendrían porque tener señal.

Los principales enemigos de las ondas electromagnéticas en las que viajan nuestras señales son los metales. Los metales son totalmente opacos, esto hace que un edificio de hormigón armado nos pueda bloquear la señal si se encuentra entre nuestro emisor y nuestro receptor. Algo parecido pasa con los coches (por esto llevan la antena de la radio y del móvil fuera), aunque si los cristales no llevan plomo nos permitan tener algo de cobertura en el habitáculo. Otra pared importante para nuestra señal es la torre del ordenador, ya que es una gran pantalla electromagnética para evitar que señales externas afecten al funcionamiento del ordenador, de este modo siempre será mucho más efectiva una antena que podamos colocar encima de la torre que no una que esté justo detrás (como la mayoría de tarjetas PCI Wireless).

### **1.5.2. Nueva banda 5 GHz**

A medida que las tecnologías Wireless fueron avanzando se vio la necesidad de tener más ancho de banda. Así fue como se homologó la banda de 5 GHz. La elección de esta frecuencia no es gratuita, ya que es aproximadamente el doble de la de 2.4 GHz.

Por su forma una antena está destinada a una frecuencia en concreto: su longitud es proporcional a la longitud de onda de la frecuencia que deseamos transmitir o recibir. De este modo la antena ya será el primer filtro que nos facilitará la entrada de señales de las frecuencias que queremos y atenuará otras frecuencias no deseadas. Los mínimos de atenuación se encuentran en múltiplos de la frecuencia

principal. Así la antena de 2.4 GHz será muy buena a esta frecuencia y bastante buena a 5 GHz que es el doble de la frecuencia principal.

### **1.5.3. Frecuencias en el Ecuador**

El organismo encargado de la regulación en las telecomunicaciones en nuestro país es el CONATEL y el SENATEL entes gubernamentales, cuyos principales objetivos son la prestación de servicios de buena calidad para el usuario en lo que respecta a voz datos y video para lo cual desarrolló un marco jurídico de las telecomunicaciones independiente con funciones de regulación y control del sector.

Dentro de este marco jurídico existe aspectos importantes como:

- Ser el organismo de regulación y administración de las telecomunicaciones que integre a todos los ciudadanos que habitan en el país a través de una política que promueva el acceso de por lo menos un servicio de telecomunicación.
- Administrar de manera técnica el espectro radioeléctrico que es un recurso natural, para que todos los operadores del sector de las telecomunicaciones operen en condiciones de máxima eficiencia.
- Dictar las normas que corresponden para impedir las prácticas que impidan la leal competencia, y determinar las obligaciones que los operadores deban cumplir en el marco que determinan la Ley y reglamentos respectivos.

- Defender los derechos de los ciudadanos en todo momento para que satisfagan su necesidad de comunicarse.
- Estimular a que todos los actores del sector de las telecomunicaciones desarrollen sus actividades en un escenario de leal competencia y que entreguen sus servicios en condiciones de óptima calidad.
- En todo lo posible, adaptar el mercado de las telecomunicaciones a las nuevas tendencias de la tecnología, que asegure que el ciudadano ecuatoriano sea beneficiario de estos adelantos.

#### 1.5.3.1. Frecuencias de Empresas más utilizadas en el Ecuador.

Las frecuencias que más utilizan las empresas en nuestro país oscilan entre los 500Khz a 1800Mhz los mismos que son utilizados en la emisión de señales de radio AM, FM, Canales de Televisión, Radio Localización, Telefonía Móvil.

Red Transporte Inalambrico Empresas					
Banda	Andinatel	Pacifictel	Conecel	Otecel	Telecsa
1 - 2Ghz					x
3 - 4Ghz			x	x	x
5 - 6Ghz					x
7 - 8Ghz					
14 - 15Ghz					
17 - 18Ghz	X	X	x		x

Tabla 1. Proveedoras de frecuencias del Ecuador.

**a) Frecuencias más utilizadas en el Ecuador en la Red de Transporte Inalámbrico.**

Las frecuencias que más se utilizan para la comunicación inalámbrica en nuestro país oscilan entre los 1Ghz a 18Ghz los mismos que son utilizados para el enlace entre el cliente y el proveedor de servicios de Internet.

<b>Rango</b>	<b>Utilización</b>
500 - 1800 kHz	Móvil, Móvil Marítimo, Radionavegación Aeronáutica, Radiodifusión fija, Radiolocalización
1800 - 2200 kHz	Aficionados Fijo y Móvil, Radiolocalización, Radionavegación
100 - 200 Mhz	Operaciones Espaciales, Mete reología por Satélite, Móvil por Satélite, Investigación Espacial, Radiolocalización, Aficionados por Satélite
200 - 300 Mhz	Aficionados Fijo y Móvil, Operaciones Espaciales, Radio Astronomía, Radionavegación Aeronáutica
300 - 400 Mhz	Fijo y Móvil, Móvil por Satélite, Radio Navegación por Satélite
400 - 500 Mhz	Frecuencias Patrón y Señales Horarias por Satélite, Mete reología por Satélite
900 - 1200 Mhz	Fijo Móvil, Radiolocalización S5.XXX, Radionavegación Aeronáutica, Investigación Espacial
1300 - 1500 Mhz	Radio Localización, Exploración de la Tierra por Satélite (pasivo), Radio Astronomía, Operaciones Espaciales, Móvil S5.343
1600 - 1800 Mhz	Móvil por Satélite S5.SSS, Radionavegación Aeronáutica, Radio determinación por Satélite, Móvil S5.380, Mete reología por Satélite

Tabla 2. Rango de frecuencias.

## **1.6. INTRODUCCIÓN A LOS ESTÁNDARES DE LA IEEE.**

### **1.6.1. Estándares para el entorno de la gestión de redes inalámbricas**

El Institute of Electrical and Electronics Engineers (IEEE) fomenta el desarrollo de estándares que suelen convertirse en normas nacionales e internacionales.

Lo mismo que el estándar 802.3 define Ethernet en el entorno cableado, el IEEE ha definido un conjunto de estándares para el entorno de la gestión de las redes inalámbricas, bajo la denominación 802.11<sup>9</sup>.

## **1.6.2. Estándares de la IEEE**

### **1.6.2.1. 802.11**

- Ancho de banda máximo de hasta 2 Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Posible interferencia con hornos microondas, dispositivos bluetooth, y teléfonos DECT, puesto que operan en el mismo espectro de frecuencias.
- Sistemas de modulación FHSS (Espectro Distribuido con Saltos de Frecuencias) y DSSS (Espectro Ensanchado de Secuencia Directa).

### **1.6.2.2. 802.11a**

- Ancho de banda máximo de hasta 54 Mbps.
- Opera en el espectro de 5 Ghz sin necesidad de licencia. Menos saturado.
- No es compatible con 802.11b y 802.11g
- Modulación de OFDM (Multiplexación por División de Frecuencias Ortogonales).

---

<sup>9</sup> [www.ieee.com](http://www.ieee.com) 2005

### **1.6.2.3. 802.11b**

- Ancho de banda máximo de hasta 11Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Las mismas interferencias que para 802.11
- Conocido como WIFI.
- Modulación DSSS.
- Compatible con los equipos DSSS del estándar 802.11.

### **1.6.2.4. 802.11g**

- Ancho de banda máximo de hasta 54 Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Compatible con 802.11b.
- Modulación DSSS y OFDM.

## **1.6.3. Extensiones de Estándares Inalámbricos.**

### **1.6.3.1. 802.11d**

Constituye un complemento al nivel de Control de Acceso al Medio (MAC) en 802.11 para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11. Permitirá a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

#### **1.6.3.2. 802.11e**

Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN. 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.

#### **1.6.3.3. 802.11f**

Su objetivo es lograr la interoperabilidad de Puntos de Acceso (AP) dentro de una red WLAN mutiproveedor. El estándar define el registro a Puntos de Acceso (AP) dentro de una red y el intercambio de información entre dichos Puntos de Acceso cuando un usuario se traslada desde un punto de acceso a otro.

#### **1.6.3.4. 802.11h**

El objetivo es cumplir los reglamentos para redes WLAN a 5 GHz. Los reglamentos para la banda de 5 GHz requieren que los productos tengan control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

#### **1.6.3.5. 802.11i**

Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP). Se aplicará a los estándares físicos a, b y g de 802.11. Estándar que define la encriptación y la autenticación para

complementar completar y mejorar la Privacidad Equivalente Cableada (WEP).  
IEEE 802.1x constituye una parte clave de 802.11i.

#### **1.6.3.6. 802.11j**

Estándar que permitirá la armonización entre el IEEE, el ETSI Hyperlan2, ARIB e HISWANa.

#### **1.6.3.7. 802.11m**

Estándar propuesto para el mantenimiento de las redes inalámbricas.

### **1.7. PROTOCOLOS DE TRANSMISION DE DATOS**

#### **1.7.1. Protocolo TCP/IP**

Es un protocolo de red independiente del nivel físico y que soporta múltiples sesiones entre múltiples ordenadores, esta construido en capas, lo que permite adaptarlo a nuevas tecnologías y requerimientos sin necesidad de modificar el conjunto.

Soporta sesiones confirmadas, asegurando que los datos llegan a su destino y lo hacen en el mismo orden en que se enviaron.<sup>10</sup>

La arquitectura abierta de TCP/IP permite construir sobre el protocolo de aplicación de muy diversa índole y funcionalidad, muchos de los cuales son estándares muy conocidos, los objetivos principales son:

---

<sup>10</sup> Douglas Comer, Redes Globales de Información con Internet y TCP/IP, México, Prentice-Hall, 1999

- Tener conectividad universal a través de la red.
- Estandarización de protocolos.
- Independencia de tecnología de conexión y arquitectura de la computadora.

TCP (Protocolo de Control de Transmisión) e IP (Protocolo Internet), esta familia de protocolos es la base de la red Internet, la mayor red de ordenadores del mundo. Por lo cual se ha convertido en el más extendido.

#### **1.7.1.1. Características de TCP/IP**

Protocolo de Control de Transmisión, sus características fundamentales se resumen en que es orientado a conexión y proporciona mecanismos que ofrecen seguridad acerca de la entrega de los paquetes a su destino; así como su capacidad de ordenación y no duplicación.

- Protocolo estándar, abierto, amigable, útil para el desarrollo de aplicaciones distribuidas o que utilizan un entorno de red, en forma independiente del computador o su sistema operativo.
- Es independiente del hardware de la red, lo que permite integrar varios tipos de redes. TCP/IP puede correr sobre una red ethernet, token ring, X.25, FDDI, en redes sobre líneas telefónicas, y sobre redes que utilicen cualquier medio de transmisión de datos.
- Posee un esquema de direcciones que permite asignar una dirección única a cada dispositivo de la red.

- Posee un conjunto de protocolos estandarizados, que permiten la amplia disponibilidad de servicios en red para el usuario<sup>11</sup>.

#### **1.7.1.2. Direccionamiento**

El servicio de direccionamiento de IP determina rápidamente si una dirección IP dada por la capa de transporte pertenece a la red local o a otra red.

Las direcciones IP son números de 32 bits divididos en 4 octetos. Cada dirección es la combinación del identificador único de la red y el identificador único de la máquina.

El problema inmediato con las direcciones IP es que son difíciles de memorizar. Por esta razón, las computadoras también pueden ser identificadas con nombres particulares. El DNS fue implementado para facilitar el uso de las direcciones IP a los seres humanos.

#### **a) Direcciones IP**

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes

---

<sup>11</sup> [www.tcpi.com](http://www.tcpi.com)

independientes entre sí (sin ningún camino posible que las comunique), las direcciones IP se clasifican en:

- **Direcciones IP Públicas.**

Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

- **Direcciones IP Privadas (reservadas).**

Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o *Proxy*) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- **Direcciones IP Estáticas (fijas).**

Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

- **Direcciones IP Dinámicas.**

El protocolo Internet mueve datos entre hosts en forma de datagramas. Cada datagrama es enviado a la dirección contenida en la Dirección Destinataria de la cabecera del datagrama. La Dirección del Destinatario es una dirección IP estándar de 32 bits (4 bytes) que contiene suficiente información para identificar únicamente a una red y a un host específico dentro de dicha red. Ejemplo:

xxxxxxxx . xxxxxxxx . xxxxxxxx . xxxxxxxx    (x= 0 o 1)  
 1<sup>er</sup> byte    2<sup>do</sup> byte    3<sup>er</sup> byte    4<sup>to</sup> byte

Una dirección IP contiene una "parte de red" y una "parte de host", pero el formato de estas partes es diferente para cada tipo de dirección IP. El número de bits de dirección usado para identificar la red, y el número de bits usado para identificar al host, varía de acuerdo a la clase de dirección.

Las tres principales clases de red son clase A, clase B, y clase C estas letras es un número comprendido entre el 0 y el 255, cuyas estructuras se observan en la siguiente tabla. (Equivalencias: R = red; N = nodos; 24 bits de red).

Clase de red	bits del 1er Byte	Rango del 1er. Byte	Formato de la dirección	Nº de redes	Nº de hosts por red
A	0XXXXXXXX	1 – 126 *(0 y 127) uso especial	R.N.N.N	$2^7 - 2$	$2^{24} - 2$
B	10XXXXXXXX	128 – 191	R.R.N.N	214	$2^{16} - 2$
C	110XXXXXX	192 – 223	R.R.R.N	221	$2^8 - 2$
D	1110XXXX	224 - 239			
E	11110XXX	240 - 247			

Tabla 3. Clases de Direcciones

- **Direcciones IP Especiales y Reservadas**

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host, algunas de ellas tienen significados especiales. Su interpretación depende del host desde el que se utilicen.

- **Direcciones de Broadcast.**

Una dirección IP con todos los bits de la parte de máquina puestos a uno (1) es una "dirección de broadcast". Una dirección de broadcast es usada para direccionar simultáneamente a todas las máquinas dentro de una red. La dirección de broadcast para la red 128.66 es 128.66.255.255. Un datagrama enviado a esta dirección es entregado a todas y cada una de las máquinas individuales dentro de la red 128.66.

IP utiliza la parte de red de la dirección para encaminar el datagrama entre redes. La dirección completa, incluyendo la información del host, es usada para hacer la entrega final cuando el datagrama alcanza la red de destino.

### **1.7.1.3. Máscara de Red.**

Existe el término "máscara", muy utilizado en redes TCP/IP; para obtener la máscara se debe poner unos (1s) en todos los bits de la parte de red, y ceros (0s) en todos los bits de la parte de máquina. La máscara permite determinar el número de subredes que contiene una red.

La máscara para una red de clase A es 255.0.0.0, para una red de clase B es 255.255.0.0 y para una red de clase C es 255.255.255.0; estas máscaras se refieren a redes que no contienen subredes. La siguiente tabla muestra las máscaras de red correspondientes a cada clase:

<b>Clase</b>	<b>Máscara de red</b>
<b>A</b>	255.0.0.0
<b>B</b>	255.255.0.0
<b>C</b>	255.255.255.0

Tabla 4. Mascará de red

#### **1.7.1. 4. Subredes (Subneting)**

La estructura estándar de una dirección IP puede modificarse localmente para usar bits de la dirección del host como bits de direcciones de redes adicionales. Esencialmente, la “línea de división” entre los bits de dirección de red y los bits de dirección del host es movida con la creación de subredes, esto se logra reduciendo el número de hosts que pueden pertenecer a una red. Esta definición de redes dentro de una red más grande es conocida como subred.

Para conocer como definir una dirección de subred, debe tomarse en cuenta el número de subredes que se desea obtener y de acuerdo a esto, tomar un número exponencial de base 2 elevado a la n, tal que el resultado del cálculo anterior cubra el número de subredes requeridas. Este número n servirá posteriormente

para realizar un desplazamiento de la línea de división entre los bits de la parte de red y los bits de la parte de host.

#### **1.7.1.5. Familia de Protocolos TCP/IP**

**a) UDP (User Datagram Protocol).**- Protocolo de Datagramas de Usuario, es un protocolo no orientado a conexión. No garantiza que los datagramas sean entregados en destino.

**b) CMP (Internet Control Message Protocol).**- Protocolo de Mensajes de Control en Internet, utilizado para gestionar la comunicación de mensajes de error entre distintos puntos de la red.

**c) IP (Internet Protocol).**- Protocolo Internet, es el protocolo que proporciona el servicio de envío de paquetes para los protocolos soportados TCP, UDP e ICMP.

**d) ARP (Address Resolution Protocol).**- Protocolo de Resolución de direcciones, permite mantener asignaciones de pares formados por direcciones Internet direcciones físicas de dispositivos de comunicación.

**e) RARP (Reverse Address Resolution Protocol).** - Protocolo de Resolución Inversa de direcciones, al Contrario del anterior, permite mantener asignaciones de direcciones físicas-Internet.

## **1.7.2. Protocolo de Aplicaciones Inalámbricas**

### **1.7.2.1. (WAP) Wireless Application Protocol**

En la evolución de las redes de telecomunicaciones, una reciente estrategia de actuación es la de dotar a los usuarios de "**movilidad**", de tal manera que éstos puedan establecer una comunicación independientemente del lugar donde se encuentren. Ello es posible gracias a la utilización de la tecnología inalámbrica entre los elementos que desean comunicarse.

En el mundo de la tecnología inalámbrica se está escuchando mucho **el término WAP**, cuyo significado es el protocolo de aplicaciones inalámbricas. Algunos entendidos manifiestan que posee una amplia gama de aplicaciones (multimedia) que permiten la comunicación de datos bajo tecnología inalámbrica.

**WAP** es un estándar que permite ofrecer a usuarios móviles con dispositivos inalámbricos fácil acceso a toda la información disponible en el Internet y a las aplicaciones y servicios que la misma ofrece.

#### **a) Componentes de la arquitectura WAP**

La arquitectura WAP provee un ambiente escalable y extensible para el desarrollo de aplicaciones para dispositivos de comunicaciones móviles. Esto se logra a través de un diseño de capas de la pirámide completa del protocolo. Cada una de

las capas de la arquitectura es accesible por las capas superiores, así como por otros servicios y aplicaciones.<sup>12</sup>

- Capa de aplicaciones (WAE)
  - Capa de sesión (WSP)
  - Capa de transición (WTP)
  - Capa de seguridad (WTLS)
  - Capa de transporte (WDP)
- **Ambiente de Aplicación Inalámbrico (WAE)**

Es una combinación de las tecnologías WWW y de telefonía móvil. El objetivo primario es establecer un ambiente inter operable que permitirá a los operadores y a los proveedores de servicio construir aplicaciones y servicios que puedan alcanzar una amplia.

▪ **Protocolo de Sesión Inalámbrica (WSP)**

El protocolo de sesión inalámbrica (WSP) provee la capa de aplicación del WAP con una interfaz consistente para dos servicios de sesión. El primero es un servicio orientado a la conexión que opera sobre el protocolo de capa de transición (WDP).

▪ **Protocolo de Transición Inalámbrica (WTP)**

El protocolo de transición inalámbrica (WTP) corre en el tope de un servicio de datagrama. WTP opera eficientemente sobre redes de datagramas inalámbricos seguros y no seguros.

---

<sup>12</sup> <http://neutron.ing.ucv.ve/revista-e/No8/JLPerez%5CWAP.HTM>

- **Seguridad de Capas de Transporte Inalámbricas (WTLS)**

WTLS es un protocolo de seguridad basado en el protocolo de seguridad de capas de transporte estándar de la industria (TLS), antiguamente conocido como SSL. WTLS se desarrolla para usarse con los protocolos de transporte WAP y ha sido optimizado para usar sobre canales de comunicación de banda angosta.

- **Protocolo de Datagrama Inalámbrico (WDP)**

El protocolo de capa de transporte en la arquitectura WAP está referido como WDP. Como un servicio de transporte general, WDP ofrece un servicio consistente a los protocolos de capas superiores del WAP.

#### **b) Servicio de Portadores**

El protocolo WAP fue diseñado para operar sobre una gran variedad de servicios portadores, incluyendo los de mensajes cortos, datos conmutados por circuitos y paquetes de datos. Los servicios portadores ofrecen diferentes calidades de servicio dependiendo de la cantidad de información total de salida, tasa de error y los retardos.

El protocolo WAP esta diseñado para compensar con cierto grado de tolerancia estas variaciones del grado de servicio.

La arquitectura de capas WAP permite habilitar otros servicios y aplicaciones que utilicen las características de las especificaciones de este protocolo, mediante un conjunto de interfaces bien definidas. Aplicaciones externas pueden estar en la

capacidad de acceder a las capas de sesión, transporte, transacción y seguridad directamente.

La clave del crecimiento de servicios de localización inalámbricos se basa en la capacidad de la tecnología para ubicar un equipo móvil con una precisión de 50m o menos. Los operadores móviles cuentan con un rango de opciones tecnológicas tales como la identificación de celdas, redes basadas en triangulación, dispositivos manuales basados en triangulación, incluyendo GPS.

#### **1.7.2.2. Protocolo de Seguridad WEP (*Wired Equivalent Privacy, Privacidad Equivalente al Cable*)**

Es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.<sup>13</sup>

##### **a) Estándar**

El estándar IEEE 802.11 proporciona mecanismos de seguridad mediante procesos de autenticación y cifrado. En el modo de red Ad Hoc o conjunto de servicios avanzados, la autenticación puede realizarse mediante un sistema abierto o mediante clave compartida. 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.

---

<sup>13</sup>. Applying known techniques to WEP Keys , Tim Newsham, Cracking WEP Keys

El estándar 802.11 especifica una capacidad opcional de cifrado denominada WEP (Wireless Equivalent Privacy); su intención es la de establecer un nivel de seguridad similar al de las redes cableadas. WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire.

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.<sup>14</sup>

WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación.

---

<sup>14</sup> <http://documentos.shellsec.net/otros/SeguridadWireless.pdf>  
Seguridad en redes inalámbricas.

Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional.

#### **b) 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.

### c) 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*. 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.

#### **d) Algoritmos**

El algoritmo de encriptación utilizado es RC4 con claves principal, según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo,

por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

A continuación se detalla el algoritmo de encriptación de WEP:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).
2. Se concatena la clave secreta a continuación del IV formado el *seed*. \*
3. El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del *seed*, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el *seed* y con ello podrá generar el *key stream*. Realizando el XOR entre los datos recibidos y el *key stream* se obtendrá el mensaje sin cifrar (datos y CRC-32), luego se comprueba que el CRC-32 es correcto.

#### e) Algoritmo de encriptación RC4

Funciona a partir de una clave de 1 a 256 bytes (8 a 1024 bits), inicializando una tabla de estados. Esta tabla se usa para generar una lista de bytes

pseudoaleatorios, los cuales se combinan mediante la función XOR con el texto en claro; el resultado es el texto cifrado.

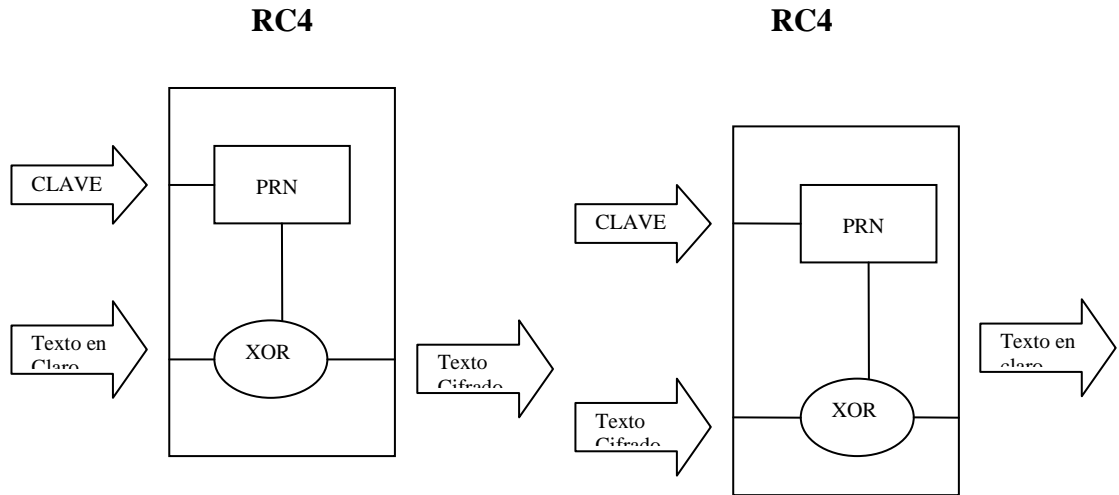


Gráfico 15 Encriptación del WEP

## 1.8. SEGURIDADES DE REDES INALÁMBRICAS

Como sabemos, la seguridad en redes tipo inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

Aunado a ello, la falta de una recomendación que permitiera la interoperabilidad entre equipos de diferentes productores, contuvo el despliegue masivo de las WLANs. No fue sino hasta mediados de la década pasada que se publicó el estándar que dictaba las especificaciones y criterios que debían aplicarse

consistentemente en la fabricación y aprovisionamiento de productos inalámbricos.

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle.

Existe el término “wardriving”, que se refiere a la acción de recorrer una ciudad para buscar la existencia de redes inalámbricas y ganar acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes.

El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable). Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica.

La seguridad WLAN abarca dos elementos: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente). Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquéllos instalados sin el conocimiento de los administradores de la

red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Estos “hoyos” en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red alámbrica a la cual se conecta. La tabla siguiente contiene los mecanismos de seguridad usados en redes WLAN, así como las ventajas y desventajas de cada uno de ellos.

#### **1.8.1. Mecanismos de seguridad para redes WLAN:**

**a) Especificación original 802.11.** Utiliza tres mecanismos para proteger las redes WLAN:

- **SSID (Identificador de Servicio):** es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para acceder a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía (beacon).
- **Filtrado con dirección MAC (Control de Acceso al Medio):** restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN.

Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico.

- WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.

- b) **802.1X.**- Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autenticación remota de usuarios

entrantes (RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes).

- c) **WPA (Wi-Fi Protected Access).**- Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de Llaves Integras –Seguras Temporales). TKIP fue construido tomando como base el estándar WEP, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación.

Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi.

Esta especificación proporciona una mayor encriptación de datos para corregir las vulnerabilidades de seguridad WEP, además de añadir autenticación de usuarios que no se habían contemplado

**CAPITULO II**  
**ESTUDIO DE FACTIBILIDAD Y DISEÑO DE LA RED**  
**INALÁMBRICA**

**2.1. INTRODUCCIÓN**

El presente estudio tiene el propósito de explorar una tecnología económica de comunicación inalámbrica, para utilizarla como posible solución de conexión de red inalámbrica en la Universidad Técnica de Cotopaxi. Según sondeos iniciales, la única alternativa técnicamente probada y ampliamente disponible que ofrece el mercado hoy en día para las redes informáticas inalámbricas es la conexión con un dispositivo llamado Access Point, claro si se lo realiza en un edificio pero si es más extenso se lo realizará con antenas.

Hoy en día la Universidad Técnica de Cotopaxi en su edificio central cuenta con una red de datos la misma que esta distribuida en laboratorios y dependencias administrativas esta infraestructura esta funcionando correctamente pero una parte de esta no esta cumpliendo las normas que se rigen para brindar seguridad a la información que allí se genera, por lo que algún instante puede colapsar la red.

Basta dar un vistazo a algunas dependencias en las cuales tienen guindados los cables en las paredes los cuales dan un pésimo aspecto a lo estético del edificio.

Pero la evolución de las formas de intercambiar información (voz datos video) han ido cambiado en una forma vertiginosa, es así que gracias a la electrónica y a

la informática se han desarrollado dispositivos con los cuales se facilita la comunicación entre equipos electrónicos, para la que no se utiliza medios físicos “cables”, por eso a esta tecnología se la ha denominado wireless “inalámbricos”.

Con el inicio de la construcción del campus universitario bloques académicos y administrativo, El Alma Mater se vería beneficiada con la utilización de una red inalámbrica ya que no necesitaría la utilización de materiales empleados para el funcionamiento de cableados estructurado. En la actualidad los costos de una red inalámbrica están a la par de una red física.

Al usar esta tipo de tecnología la Universidad se beneficiaría notablemente ya que sus puntos de datos no se los ubicaría en forma estática, al contrario se los iría desplazando de acuerdo a las necesidades de los usuario. Los equipos se comunican mediante la emisión de frecuencias electromagnéticas, las cuales no son nocivas para la salud.

## **2.2. Análisis e Interpretación de resultados de las encuestas realizadas.**

La interpretación de los resultados de las encuestas aplicadas al Personal Administrativo, Estudiantes y Docentes, determinan las necesidades prioritarias en lo que respecta a la implementación, interconexión y beneficios de una red inalámbrica.

Después de revisar y analizar los resultados obtenidos en las encuestas podemos decir que la implementación de las redes inalámbricas, la Universidad Técnica de

Cotopaxi beneficiaría en el aspecto administrativo, académico y de estética ya que estaría acorde a los avances tecnológicos y lo que es mejor se podría optimizar el tiempo y las funciones de todas las personas involucradas en esta institución.

En la estética todos los encuestados afirman que actualmente la estética e infraestructura de cableado que posee la Universidad no es presentable, ya que se pueda ver los cables por todos lados desprotegidos y siempre en constante peligro de accidentes tanto humano como de los equipos.

En relación a lo académico el cuerpo docente y los estudiantes afirman que sería mejor ya que podrían trabajar desde cualquier lugar sin tener que hacer las tediosas filas para adquirir una máquina o ingresar al Internet, con las redes inalámbricas estaría más cómodo ya que podrían utilizar sus propias laptops.

En general las redes Inalámbricas al ser utilizadas darían a la Universidad una oportunidad de mejorar, aunque no hay que olvidarse que para tener una aplicación de las bondades que ofrece las redes inalámbricas se debería dar una capacitación a los empleados y a los estudiantes se deberá implementar una materia de redes y comunicaciones, logrando así que los estudiantes se adentren a esta tecnología y logren ser competitivos con las otras Universidades del país, por lo cual las autoridades deberían tomar en cuenta dicha tecnología.

## **2.3 Diseño de la Wireless en la Universidad Técnica Cotopaxi.**

### **2.3.1 Parámetros de Diseño.**

El objetivo fundamental de este proyecto es el de proporcionar a los usuarios un medio inalámbrico adecuado y versátil para la integración de los servicios brindados por los diferentes sistemas de telecomunicaciones (datos), independientemente de tipo de equipos que los conforman y adaptables a nuevas tecnologías.

La red inalámbrica, brindará un enlace confiable, seguro y con capacidad de habilitar a todas las estaciones de trabajo los diferentes servicios de comunicaciones (datos) previstos en la entidad.

Esta red cumplirá con los conceptos de wireless propuestos por la IEEE permitiendo en forma fácil, sencilla y rápida efectuar cambios de reubicación de equipos de cómputo.

### **2.3.2 Descripción general de la red inalámbrica**

El sistema wireless básicamente consiste en lo siguiente:

- El acceso a la información se lo realizara mediante la no utilización de cables para el enlace entre las pcs y los puntos de acceso.
- La comunicación se lo realizara por medio de radiofrecuencia la misma que no es nociva para la salud ni el medio ambiente.
- El hardware adicional: impresoras, plotter, scanner también estará dentro de la comunicación inalámbrica

- El hardware que se utilizara para que entre en funcionamiento la wireless es tarjetas PCI Inalámbrica, Access Point, Antenas Direccionales, Antenas Parabólicas, Antenas Yagui.

#### **2.4. Diseño de red**

La Universidad Técnica de Cotopaxi dentro de su planificación para la construcción de su Campus Universitario cuenta con dos bloques, Bloque A para las dependencias administrativas (actual edificio matriz) y el Bloque B para las dependencias académicas "Aulas" en construcción, en cada una de ellas esta planificado que posea cuatro plantas. A continuación se detallan la distribución de los distintos departamentos que están presentes en dichos bloques.

Bloque Administrativo "A"

Primera Planta Alta

- Recursos Humanos
- Rectorado
- Vicerrectorado
- Secretaria General
- Procuraduría
- Contabilidad
- Tesorería
- Presupuesto
- Departamento Financiero
- Auditoria
- Dirección Administrativa

- Proveeduría
- Construcción y Mantenimiento

#### Segunda Planta Alta

- Planeamiento
- Consejo Académico

#### Tercera Planta Alta

- Centro de Investigaciones
- Direcciones Académicas

#### Bloque Académico “B”

#### Planta Baja

- Salas de Computo
- Asociación de Empleados
- Asociación de Estudiantes
- Asociación de Profesores
- Laboratorio de Idiomas

## **2.5 Especificaciones Técnicas de Diseño de la red inalámbrica en la Universidad Técnica de Cotopaxi.**

### **Información general**

La Universidad Técnica de Cotopaxi se encuentra ubicada al sur-este de la ciudad de Latacunga en la Parroquia Eloy Alfaro, Barrio San Felipe. Es una entidad de derecho público con plena autonomía para organizarse y cumplir sus altas

finalidades de servicio al desarrollo regional, nacional. Sus fundamentales propósitos constituyen la formación de profesionales útiles a la sociedad.

El Alma Mater de la provincia en su Campus Universitario cuenta con diferentes bloques en los que se encuentra distribuidos, la parte académica y la parte administrativa, considerando el notable crecimiento de usuarios (empleados, estudiantes, profesores) además del avance tecnológico en el mundo de la computación y las comunicaciones (pcs, laptop, palms, telefonía celular). Las mismas que necesitan disponer de una red móvil para optimizar su desenvolvimiento y los recursos con los que cuentan, además de compartir información entre los equipos existentes con los nuevos dispositivos que ofrecen una tecnología de comunicación en la cual no se necesita la utilización de cables o sea la tecnología inalámbrica .

La aplicación de esta tecnología beneficiara a las actividades que se desarrollan en la Universidad; por lo que se hace necesario la instalación de una wireless.

### **Descripción general**

El diseño de la red inalámbrica, se lo ha realizado para todos los bloques, como se muestran en los planos del anexo 3.1, 3.2 ,3.3, 3.4 y 3.5 se tendrán varios puntos de acceso a los cuales se enlazarán los puntos de datos inalámbricos, en este caso las computadoras de escritorio como las portátiles con tarjetas inalámbricas. Los APs estarán ubicados en un punto donde brinden una mejor emisión de

frecuencia para que el acceso a la información sea de una manera confiable y segura.

### **Alcance de los trabajos**

#### **Objetivo General**

El alcance del proyecto comprende el análisis, diseño y una propuesta para la instalación, de la red inalámbrica en la Universidad Técnica de Cotopaxi, además se realizara la factibilidad del uso de la tecnología de transmisión inalámbrica basada en el estándar 802.11 (2.4 GHz.) como alternativa para una posible implementación en la Universidad Técnica de Cotopaxi.

#### **Específicos**

- Los puntos de acceso APs se ubicaran de acuerdo a las especificaciones técnicas con las cuales se logre una mejor emisión de la señal de radio frecuencia que emiten estos equipos, de acuerdo al esquema de la propuesta.
- Los puntos de datos los que se enlazarán a los puntos de acceso, en este caso las computadoras de escritorio como las portátiles, con tarjetas inalámbricas estarán ubicados en un punto donde brinden una mejor recepción de frecuencia para que el acceso a la información sea de una manera confiable.
- La comunicación entre los distintos pisos se los realizara mediante el enlace entre el access point principal de cada planta a un switch general.

- La instalación de los elementos inalámbricos Aps, tarjetas wireless, antenas se lo realizaran en base a la norma internacional de la IEEE 802.11
- Realizar pruebas de señal dentro del establecimiento para confirmar resultados esperados según el método de análisis geográfico propuesto.

### Normas

Las normas en las cuales nos basaremos para el diseño e instalación serán:

IEEE 802.11. ISO/IEC 11801 Código Eléctrico Nacional.

### 2.6 Requerimientos de los puntos de datos de los usuarios, en función de la ubicación en el Campus Universitario.

#### Bloque Administrativo “A”: Primera Planta Alta

<b>Dependencia</b>	<b># Puntos Inalámbricos</b>
Recursos Humanos	2
Rectorado	2
Vicerrectorado	2
Secretaria General	2
Procuraduría	2
Contabilidad	2
Tesorero	2
Presupuesto	2
Departamento Financiero	2
Auditor	2
Dirección Administrativa	2
Proveeduría	2
Construcción y Mantenimiento	1
Hacienda	1
<b>Total</b>	<b>14</b>

Tabla 5. Bloque Administrativo “A”; Planta alta

### Segunda Planta Alta

<b>Dependencia</b>	<b># Puntos Inalámbricos</b>
Planeamiento	<b>6</b>
Consejo Académico	<b>3</b>
<b>Total</b>	<b>9</b>

Tabla 6. Bloque Administrativo “A”; Segunda Planta Alta

### Tercera Planta Alta

<b>Dependencia</b>	<b># Puntos Inalámbricos</b>
Centro de Investigaciones	<b>2</b>
Direcciones Académicas	<b>10</b>
<b>Total</b>	<b>12</b>

Tabla7. Bloque Administrativo “A”; Tercera Planta Alta

### Bloque Académico “B”

### Planta Baja

<b>Dependencia</b>	<b># Puntos Inalámbricos</b>
Salas de Computo	<b>52</b>
Asociación de Emplea	<b>2</b>
Asociación de Estudiantes	<b>2</b>
Asociación de Profeso	<b>2</b>
Laboratorio de Idiomas	<b>1</b>
<b>Total</b>	<b>59</b>

Tabla 8. Bloque Administrativo “B”; Planta Baja

## 2.7. Requerimientos de elementos Inalámbricos para la red.

En base al análisis realizado en los planos del campus universitario y de acuerdo a los requerimientos de puntos inalámbricos se necesitara los siguientes equipos de wireless.

<b>Lista Equipos Wireless</b>	
<b>Can</b>	<b>Descripción</b>
100	Tarjetas de red PCI Inalámbrica WIFI DWL-G520+
10	Access Point Inalámbrica DWL-2100 AP
5	Adaptador de red PCMCIA Inalámbrica Wi-Fi DWL-G650+
2	Antenas Yagui : ANT24-2101 / 50 grados C/ Supre
2	Antenas parabólica HG5824D : 24dBi / V / 5.8Ghz / N-H / 11000 m
2	Antenas Direccional ANT24-0801 : 08dBi / V /2.4Ghz/ 1000m

Tabla 9. Requerimientos de elementos Inalámbricos para la red.

## Estimación de Costos de Recursos y Equipamiento.

### 2.8. Análisis de Costos.

Se realizó el análisis de costos de acuerdo a las proformas obtenidas de las empresas proveedores de dispositivos inalámbricos. Se ha seleccionado a dos que son las más razonables en costos y calidad de los equipos. Ver anexo (3.6).

Resultando favorecida Martel Cablecom ya que es una empresa proveedora de dispositivos para redes físicas como inalámbricas a nivel nacional, además proporcionan garantía en los equipos que comercializan y lo que es más tienen un buen precio.

Dado que el proyecto de una red inalámbrica como la estudiada es viable.

El costo total del proyecto de Factibilidad de una Red Inalámbrica en la Universidad Técnica de Cotopaxi es de 6270.40 dólares. Ver anexo (3.7)

### **Estimación de Costos de un Prototipo de una Red WiFi.**

Con el objeto de tener un valor referencial, se muestra en la tabla 10 el costo de un Prototipo de red inalámbrica para demostración práctica del proyecto de factibilidad de una red inalámbrica en la Universidad Técnica de Cotopaxi la misma que consta de dos computadores y un Access Point.

En esta red se contempla la instalación de 2 tarjetas inalámbricas, interconectadas entre sí, y que se constituirían en los puntos de enlace al Access Point.

<b>PUNTOS DE CONEXIÓN</b>	<b>DISPOSITIVOS</b>	<b>CANT.</b>	<b>TOTAL</b>
servidor	Pc tarjeta inalámbrica	1	41,86
cliente	Pc tarjeta inalámbrica	1	41,86
enlace	Access Point	1	90,35
<b>TOTAL DEL PROTOTIPO</b>			<b>174,07</b>

Tabla10. Costos estimados de de un Prototipo de una Red WiFi.

El valor del prototipo WiFi obtenido en la tabla 10, es el costo de la instalación mínima, puesto que este valor no considera la instalación de tarjetas, antenas, además de los costos del equipamiento, para la implantación de esta tecnología se deben considerar costos adicionales por concepto de:

- Mano de obra que realice la instalación.
- Soporte y mantenimiento de las instalaciones.

## **2.9. Diseño Físico**

El diseño físico de la wireless se refiere a la configuración activa o ubicación geográfica en los lugares donde van a estar posicionados los equipos inalámbricos (planos) en este caso serán las tarjetas inalámbricas y los Access Point. En cada planta del bloque A y B estarán representados los puntos de datos inalámbricos con su símbolo que será un triángulo azul circunscrito a una circunferencia del mismo color con unas medias circunferencias en el exterior que simbolizan dispositivos wireless, así como también el Access Point tendrá su símbolo el mismo que es un círculo de color azul circunscrito a una circunferencia del mismo color. Ver anexos (planos 3.1, 3.2, 3.3, 3.4 y 3.5).

## **2.10. Diseño Lógico**

Es la forma como se van a conectar o enlazar los distintos equipos inalámbricos, tanto el Access Point con las tarjetas inalámbricas (puntos de datos inalámbricos), así como también entre Access Point. Esto se lo hará basándose en las normas 802.11 utilizadas para las Wireless, Ver Anexos (3.1.1, 3.2.1, 3.3.1, 3.4.1, 3.5.1).

## **2.11. Exploración Técnica de Equipamiento WiFi**

### **2.11.1. La Tecnología de Transmisión WIFI**

Hace mucho tiempo que comenzaron a utilizarse las tecnologías inalámbricas, sin embargo, pocas son las instituciones públicas, privadas y usuarios que utilizan mencionada tecnología, en el mundo del mercado están apareciendo dispositivos para redes locales que podían competir en velocidad y prestaciones con las

alternativas de cableado tradicional. Esto se debe a la incorporación de una nueva tecnología de transmisión por ondas de radio.

Esta nueva tecnología de transmisión inalámbrica permite lograr velocidades de hasta 11 Mbps, que es incluso mayor a la de una red Ethernet 10BaseT, que transmite a 10 Mbps.

Además, junto con aumentar la velocidad varios órdenes de magnitud respecto de dispositivos de transmisión inalámbrica antiguos, se dispusieron algunos métodos de seguridad en la transmisión de los datos, hecho que le dio el nombre de WiFi (Wireless Fidelity) a esta tecnología.

Por estas ventajas en velocidad y seguridad, muchas compañías (Cisco, 3Com, D-Link, Trendware, Orinoco, entre otras) vieron una gran oportunidad de negocios en estas nuevas tecnologías y comenzaron a desarrollar una serie de productos orientados a diversos mercados. Esto provocó una significativa disminución en los precios de tales dispositivos y, por lo tanto, hoy en día se están distinguiendo como alternativas reales a las redes de cableado tradicionales.

Actualmente existen compañías que están trabajando en el desarrollo del protocolo 802.11n que aumenta la velocidad de transmisión a 54 Mbps y utiliza la frecuencia de 5 Ghz, menos usada que la de 2.4 Ghz del estándar 802.11b.

### 2.11.2. Funcionamiento de las WiFi

La tecnología WiFi permite crear, desde pequeñas redes inalámbricas tipo LAN (Local Área Network) para el hogar o la oficina, hasta redes tipo WAN (Wide Área Network) que abarquen grandes distancias. Para implementar éstas últimas, se utiliza equipamiento especial que permite ampliar la cobertura alcanzada por los productos básicos para redes locales (tarjetas de red y hubs inalámbricos), mediante antenas externas (direccionales y omnidireccionales), Access Points (hubs) más sofisticados y amplificadores de señal. Con esta tecnología se pueden alcanzar distancias superiores a 70 Km. en una conexión. El grafico16 muestra la configuración de un set de comunicación básico de tecnología WiFi.

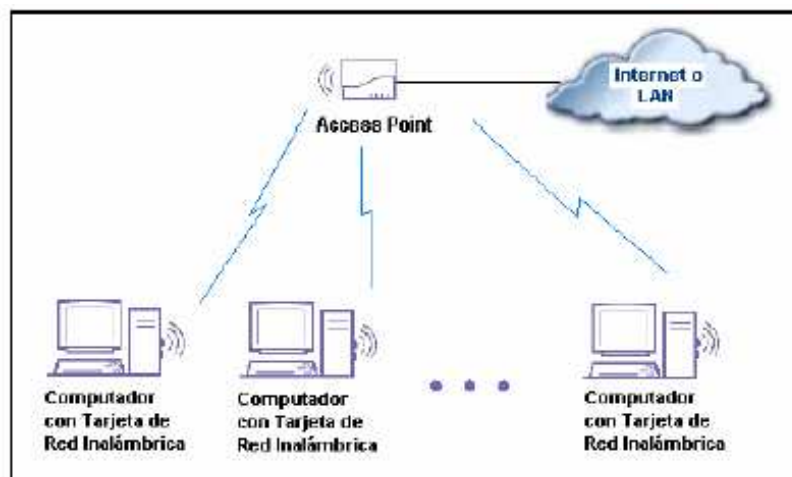


Gráfico 16: Modelo de set de comunicación inalámbrica básico.

Como se aprecia en el grafico 16, el equipamiento necesario para conformar el set básico de comunicación es llamado comúnmente *Celda*, y está compuesto por computadores con tarjetas de red inalámbrica (clientes) y un Access Point, que cumple el rol de Hub inalámbrico, y que puede estar conectado a una red de cableado tradicional, como Internet o la red corporativa o local.



## **2.12. Especificaciones Técnicas de los elementos Wíreless.**

### **2.12.1. Equipamiento Básico.**

#### **2.12.1.1. Access Point APs**

Los APS a utilizarse serán: Access Point Inalámbrica DWL-2100 AP; Los mismos que se utilizarán para el enlace entre estaciones inalámbricas de datos.

##### **Características**

- Crea una red inalámbrica de alto rendimiento.
- Hasta 108 Mbps con otros productos inalámbricos AirPlus Xtreme G.
- Funciona con otros dispositivos inalámbricos 802.11g, compatible hacia atrás con 802.11b.
- Soporta cinco modos distintos de funcionamiento: punto acceso, bridge PtP, Bridge PtMP, cliente inalámbrico y repetidor inalámbrico.
- Características del sistema de distribución inalámbrico (WDS, features Wireless Distribution) en modos PtP, / PtMP /repetidor.
- Mayor seguridad gracias a WPA y autenticación del usuario 802.1x.

#### **2.12.1.2. Tarjetas Inalámbricas**

Las Tarjetas de red a utilizarse serán: PCI Inalámbrica WIFI DWL-G520+.

Los mismos que se utilizaran para la conexión entre los PCs Desk con los Aps.

## Características

- Trabajo inalámbrico en red más rápido con velocidades de hasta 108 Mbps en modo turbo.
- Compatible con dispositivos 802.b y 802.11g.
- Mejor seguridad con 802.1x y WPA1 / WPA2.
- Prestaciones PCI 32-bit/ conectividad Plug And Play.

### 2.12.1.3. Adaptadores Inalámbricos

Adaptador de red PCMCIA Inalámbrica Wi-Fi DWL-G650+

Los mismos que se utilizaran para la conexión entre las Laptop con los APs y compartición de información.

### 2.12.2. Equipamiento de Amplificación de Señal.

#### 2.12.2.1. Antena Direccional 1

La antena a utilizarse es: D link ANT24-0801: 08dBi / V / 2.4GHz

Apta para interiores	NO
Apta para exteriores	SI
Herrajes incluidos	SI
Ganancia	12 dBi
Cobertura vertical	50 grados
Cobertura horizontal	50 grados
Alcance	7000 metros
Dimensiones: Alto	28 cm
Dimensiones: Ancho	8 cm
Dimensiones: Profundo	4 cm

Tabla 11. Características de Antena Direccional 1.

### 2.12.2.2. Antenas Direccional 2

La antena a utilizarse es: HG5824D: 24dBi / V / 5.8GHz / Direc / N-H

Apta para interiores	NO
Apta para exteriores	SI
Herrajes incluidos	SI
Ganancia	24 dBi
Cobertura vertical	9 grados
Cobertura horizontal	9 grados
Alcance	1100 metros
Dimensiones: Alto	43 cm
Dimensiones: Ancho	43 cm
Dimensiones: Profundo	12 cm

Tabla12. Características de Antena Direccional 2.

### 2.12.2.3. Antenas Yagui

La antena a utilizarse es: Ant24-1201. Yagui Ant / 12dBi /

Apta para interiores	NO
Apta para exteriores	SI
Herrajes incluidos	SI
Ganancia	12 dBi
Cobertura vertical	53 grados
Cobertura horizontal	50 grados
Alcance	1100 metros
Dimensiones: Alto	280cm
Dimensiones: Ancho	87 cm
Dimensiones: Profundo	48 cm

Tabla13. Características de Antena Yagui.

## 2.13. Escenarios de Configuración de Puntos de Acceso

### 2.13.1. Escenario 1: Configuración del Punto de Acceso del hardware

Esta es la configuración típica de instalación, utilizando el Acces Point como Hub, lo que permite una red compartida, el AP (hardware) emite la señal a los demás PCs. Es una configuración más sencilla y la que requiere menos equipamiento.

Cada computadora con un interfaz, redes inalámbricas puede comunicarse directamente con otras. Wireless conectó computadoras que usan un Punto de acceso del Hardware.

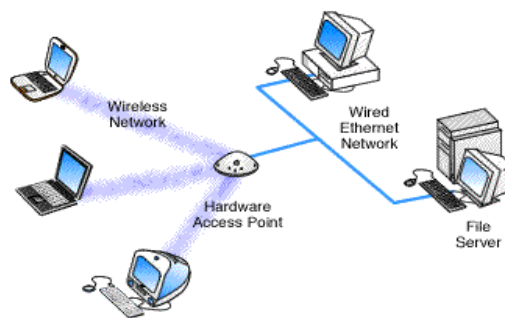


Gráfico 18: El Punto de Acceso del hardware.

### 2.13.2. Escenario 2: Configuración del Punto de Acceso del software.

Un punto de acceso del software no limita el tipo o el número de los interfaces de la red que usted utiliza. Puede también permitir flexibilidad considerable en el abastecimiento del acceso a diversos tipos de la red, tales como diversos tipos de redes de Ethernet, de la radio y del token ring. Tales conexiones son limitadas solamente por el número de ranuras o de interfaces en la computadora usada para esta tarea.

Wireless conectó computadoras que usan un Punto de acceso del Software.

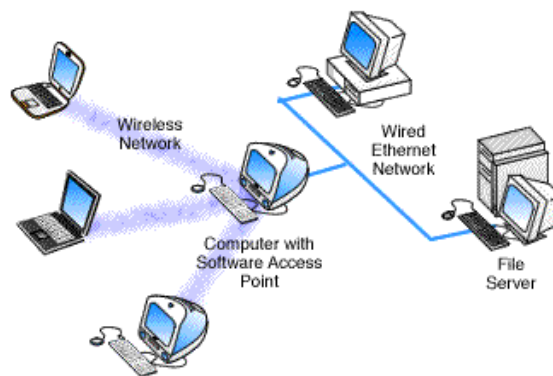


Gráfico19: El Punto de acceso del software.

### 2.13.3. Escenario 3: Configuración con redes inalámbricas para interconectar dos LANs.

Sí, el establecimiento de una red inalámbrica ofrece una solución rentable a los usuarios con las instalaciones físicas difíciles tales como campus, hospitales o negocios con más de una localización en proximidad inmediata pero separada por la carretera pública. Este tipo de instalación requiere dos puntos de acceso. Cada punto de acceso actúa como un puente o rebajadora que conecta su propio LAN con la conexión inalámbrica. La conexión de redes inalámbricas permite que los dos puntos de acceso se comuniquen uno con otro, y por lo tanto interconecta las dos LAN's.

Ahora se puede tener más de un punto de acceso, sí los puntos de acceso múltiples se pueden conectar con un LAN con cable, o iguales a veces a LAN de redes inalámbricas si el punto de acceso apoya esto.

En la mayoría de los casos, los puntos de acceso separados se interconectan vía una LAN con cable, proporcionando conectividad con redes inalámbricas en áreas

específicas, tales como oficinas o salas de clase, para el acceso a los recursos de la red, tales como servidores de archivo.

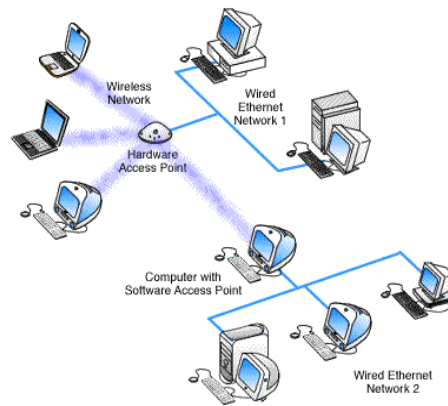


Gráfico 20: LAN a LAN las Comunicaciones Inalámbricas.

#### 2.13.4. Escenario 4: Configuración con la Access Point.

Si una sola área es demasiado grande para ser cubierta por un solo punto de acceso, entonces los puntos de acceso múltiples o los puntos de la extensión pueden ser utilizados. Observe que un "punto de la extensión" no está definido en el estándar de redes inalámbricas, pero han sido convertidos por algunos fabricantes. Al usar puntos de acceso múltiples, cada área de redes inalámbricas del punto de acceso debe traspasar sus vecinos. Esto proporciona un área inconsistente para los usuarios al movimiento alrededor, al usar una característica llamada el "vagar" (a partir de un punto de acceso a otro). Algunos fabricantes producen los puntos de la extensión, que actúan como relays inalámbricos, prolongando la gama de un solo punto de acceso. Los puntos múltiples de la extensión se pueden encadenar juntos para proporcionar el acceso a redes inalámbricas, a las localizaciones lejos ausentes del punto de acceso central.

Wireless conectó computadoras que usan un Punto de acceso con un Punto de la Extensión.

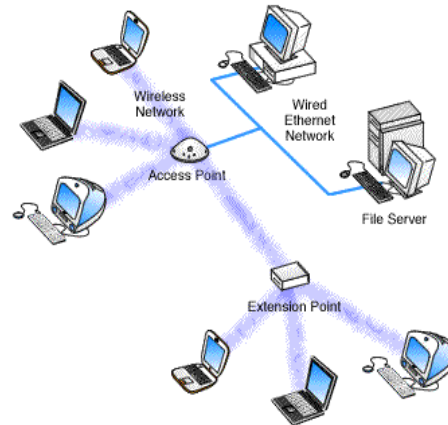


Gráfico 21: La extensión Point.

### 2.13.5. Escenario 5: El punto de Acceso múltiple.

Wireless conectó computadoras que usan los Puntos de acceso Múltiples.

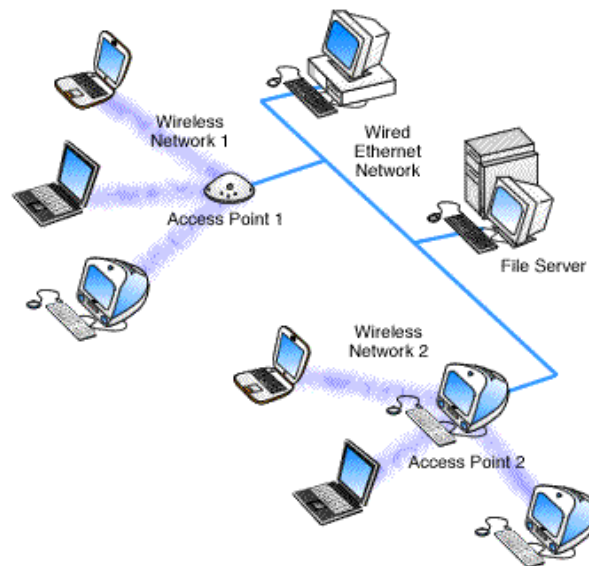


Gráfico 22: El punto de Acceso múltiple.

#### **2.14. Actividades Previas a la Instalación**

Las actividades previas a la instalación de una Red Inalámbrica, consisten principalmente en analizar, revisar y establecer los puntos donde existe comunicación de datos en el Campus Universitario para determinar la existencia de visibilidad entre el punto de acceso y las estaciones trabajo. Más detalladamente, las tareas a realizar son las siguientes:

- Hacer un análisis, técnico y crítico, para detectar posibles obstáculos entre las estaciones de trabajo y el punto de acceso.
- Luego realizar la ubicación de los puntos de Acceso en lugares estratégicos tomando en cuenta los posibles obstáculos.
- Seguidamente se procederá a la instalación del software y hardware requeridos para poner a funcionar de una manera eficiente la red.
- Posteriormente configuramos los protocolos de transmisión (TCP/IP), acorde a las norma internacionales IEEE 802.11 b.
- Finalmente realizar pruebas de conectividad para el funcionamiento óptimo de la red.

Cuando las pruebas de comunicación desde las estaciones de trabajo al punto de acceso resultan infructuosas, es necesario, saber si ello se debe a problemas de conexión, o simplemente a que no existe visibilidad entre ellos. Por esta razón es importante comprobar el buen funcionamiento del set de pruebas (configuraciones, dispositivos, Internet).

## **2.15. Pruebas de funcionalidad**

Una vez terminada la instalación de todos los elementos inalámbricos se realizarán pruebas de funcionalidad para verificar el correcto desempeño de los equipos, al mismo tiempo se verificará la calidad en la transmisión de la señal en este caso será la información.

Mediante la aplicación de la Intranet Inalámbrica los usuarios podrán acceder a todos los registros, hojas de datos, al ejemplo de la página Web e información obtenida durante la ejecución de las pruebas.

## **2.16. Proyecciones**

### **802.11v Simplificará la Gestión de WLAN.**

IEEE está desarrollando el estándar 802.11v para simplificar la gestión de redes inalámbricas. Cuando este finalizando, la nueva norma permitirá además dotarse de un mayor control sobre los clientes wireless y equilibrar automáticamente las cargas de trabajo entre los distintos puntos de acceso.

IEEE espera que el estándar, cuyo desarrollo comenzó a principios de 2005, este finalizado en 2008. Aunque muy probablemente sus primeras plasmaciones comerciales aparecerán un año antes. Mayoritariamente, el soporte de 802.11v se implementará en software en los nuevos productos, así como para actualizar los anteriores a su aparición comercial. Para que el estándar sea efectivo, su soporte tendrá que estar garantizado tanto en los clientes (los adaptadores y las tarjetas WLAN) como en la infraestructura (conmutadores WLAN y puntos de acceso).

802.11v permitirá controlar a los clientes, seleccionar y optimizar las redes a las que estos se conectan, así como monitorizar y recuperar estadísticas. El control de clientes wireless implica varios aspectos, como el balanceo de cargas, que distribuye los clientes entre los puntos de acceso en función de su volumen de tráfico.<sup>15</sup>

### **Reducción de los costos de despliegue.**

EN 802.11, cuando un dispositivo cliente se une a la red se identifica por el Service Set Identifier (SSID), pero no existe ningún mecanismo que le avise automáticamente de que red debería conectarse sin configurar manualmente el dispositivo con el SSID y las credenciales de seguridad. Sin embargo, 802.11v permite realizar configuraciones de clientes seguras desde la infraestructura, lo que reduce drásticamente el tiempo de despliegue en entornos a gran escala.

### **802.11n**

La IEEE anunció que había formado un nuevo grupo de trabajo dentro del 802.11 llamado TGn (Task Group n) y cuyo objetivo es desarrollar un nuevo modo para el estándar 802.11. Se espera que este nuevo modo sea unas 40 veces más rápido que el 802.11b y 10 veces más rápido que el 802.11a y 802.11g, llegando a una velocidad real de transferencia de información de 100 Mbps.

Uno de los requisitos iniciales para este nuevo modo de operación es que debe ser compatible con los tres anteriores (a, b, g) y para esto tiene que funcionar con ambas bandas: la de 2.4GHz y la de 5 GHz, por lo tanto sería una tecnología “dual-band / quad-mode”.

---

<sup>15</sup>. <http://computerworld.com.ec/anónimo/> 2006

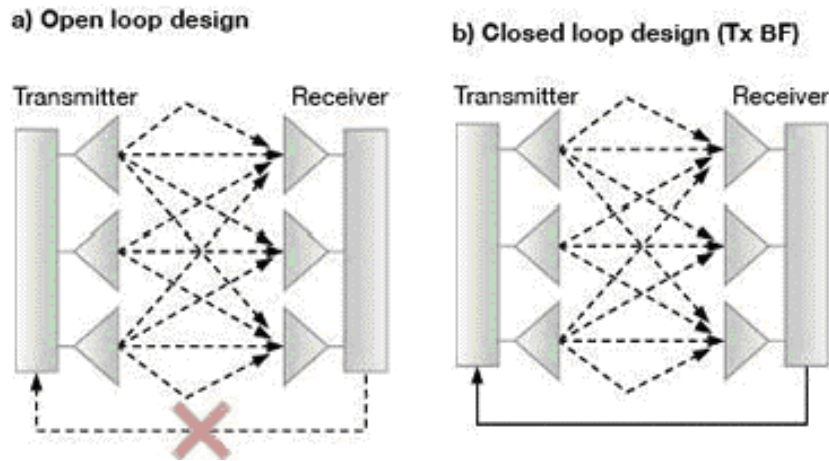


Gráfico 23. Tecnología “dual-band / quad-mode”.

La base del 802.11n es la tecnología MIMO (Multiple-input / Multiple-Output). Las versiones anteriores han sido desarrolladas para una sola antena en los equipos transmisor y receptor, aunque algunos fabricantes han puesto dos antenas para mejorar la comunicación, sin embargo sólo funciona la antena con mejor recepción -una a la vez- lo que implica que el circuito asociado a ambas antenas sea el mismo.

**WWiSE** se ha enfocado en la simplicidad de los circuitos y prefiere un diseño de lazo abierto: el transmisor envía los datos directamente hacia el receptor sin esperar ningún tipo de información de parte de éste.



Gráfico 24. Tecnología WWiSE

Cada una de las alternativas tiene sus ventajas y desventajas. Por ejemplo, WWiSE es capaz de manejar sin problemas comunicaciones con receptores en movimiento, pero debido a que no tiene una retroalimentación por parte del receptor, transmite utilizando siempre la misma potencia lo que se traduce en una pobre eficiencia en el uso de la energía en la transmisión.

Al contrario, TGnSync tiene una alta eficiencia en la transmisión y una optimización en el consumo de energía, pero la necesidad de que exista un envío de información por parte del receptor hacia el transmisor, hace que no sea muy apropiado su uso para terminales que estén en movimiento.<sup>16</sup>

### **PRE N O SUPER G**

Algunos fabricantes como [Belkin](#), [Linksys](#) y [Netgear](#) ya han sacado al mercado sus productos llamándolos pre-N o Super G. Estos son routers y adaptadores que emplean la tecnología MIMO pero con esquemas propietarios, las ventajas de estos equipos es un mejor rendimiento de la red y tasas de transferencia de datos más rápidos, pero por utilizar tecnologías propietarias sólo se asegura una compatibilidad entre elementos del mismo fabricante.



Gráfico 25. PRE N O SUPER G

---

<sup>16</sup>. <http://www.Mouse.cl/2005/productos/12/06.index.asp>

## CAPITULO III

### DEMOSTRACIÓN DE UNA RED INALÁMBRICA

#### 3.1. INSTALACIÓN DE LOS DISPOSITIVOS DE UNA RED INALÁMBRICA

##### 3.1.1. Pasos para la instalación de una tarjeta inalámbrica

Antes de comenzar la instalación de las tarjetas inalámbricas debe fijarse que estas sean compatibles con el AP caso contrario no funcionarán:

1. Encender el ordenador e introducir el CD con el controlador Air Plus Xterm G DWL-G520 D-Link En la Unidad de CD-ROM



Gráfico 26. Instalación de la tarjeta Inalámbrica

2. A continuación si la función Autorun del CD no se ejecuta automáticamente en el ordenador, debe escribirse "D:/Drivers/setup.exe. Si se ejecuta

automáticamente, seleccionar de la pantalla Install Drivers continuar con la pantalla siguiente:

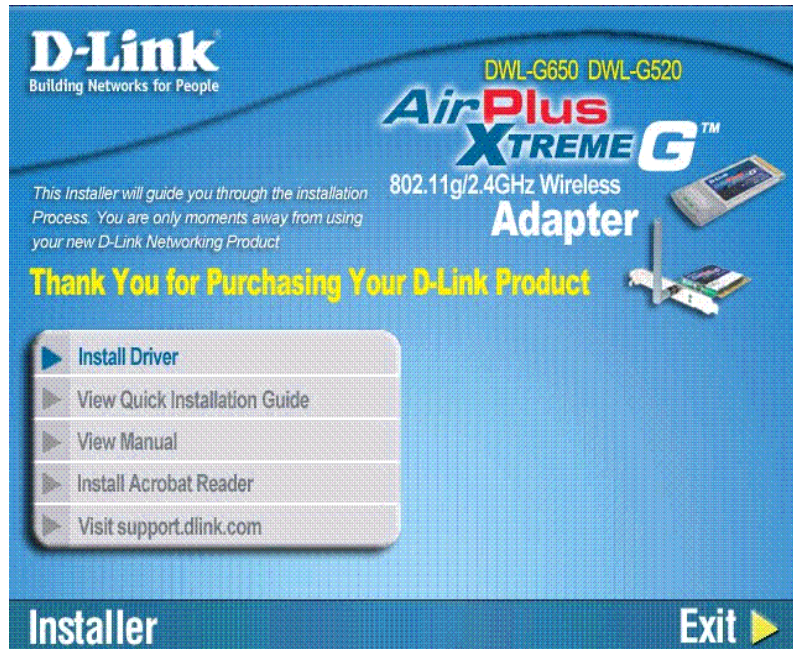


Gráfico 27. Auto Run del CD.

3. Luego aparecerá la siguiente pantalla

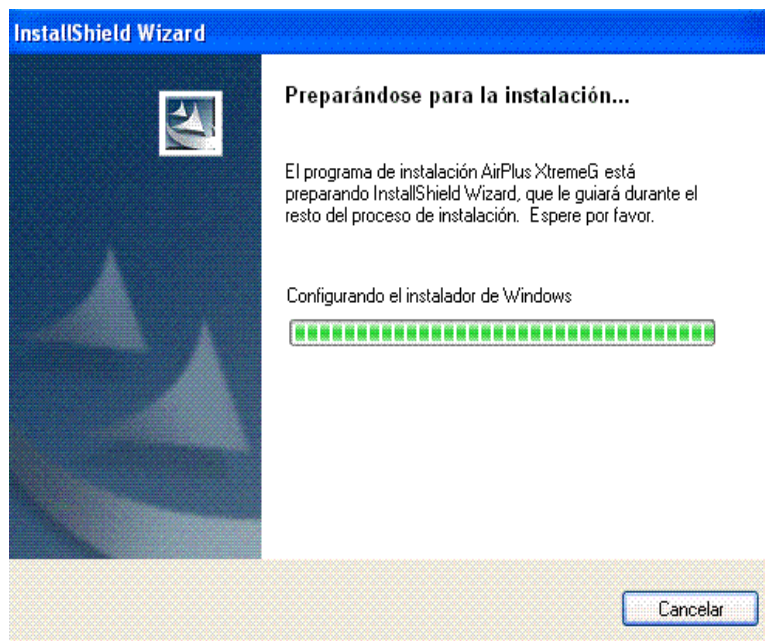


Gráfico 28. Preparando la Instalación

4. Pulse Clic en Next (Siguiete)

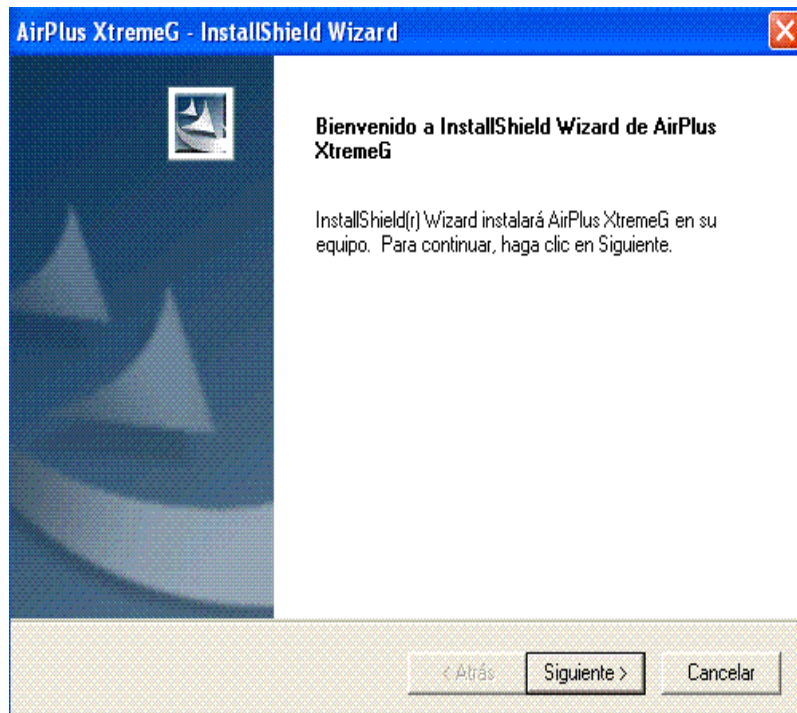


Gráfico 29. Installshield Wizard

5. Pulse Clic en Next (Siguiete)

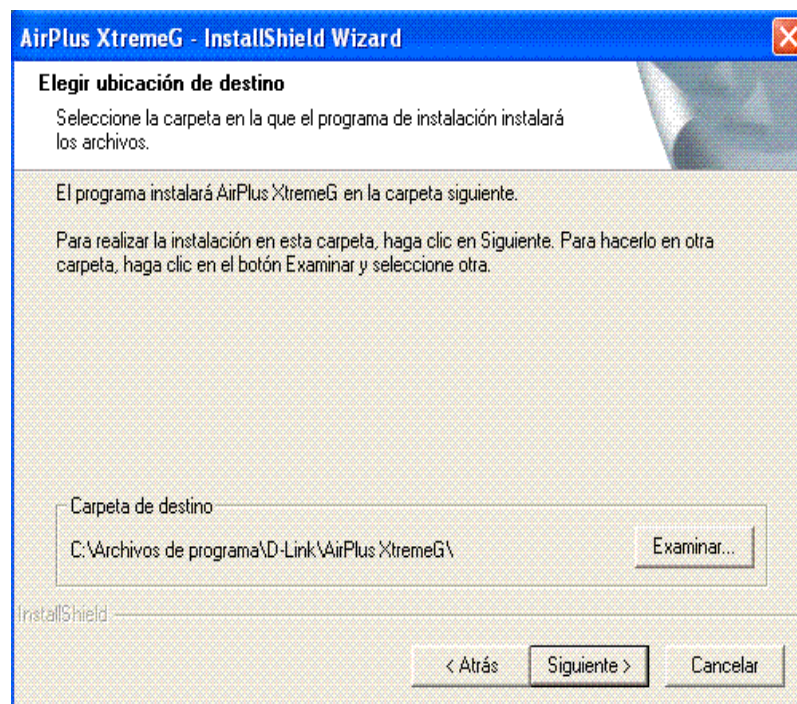


Gráfico 30. Ubicación de destino

## 6. Hacer Clic en siguiente

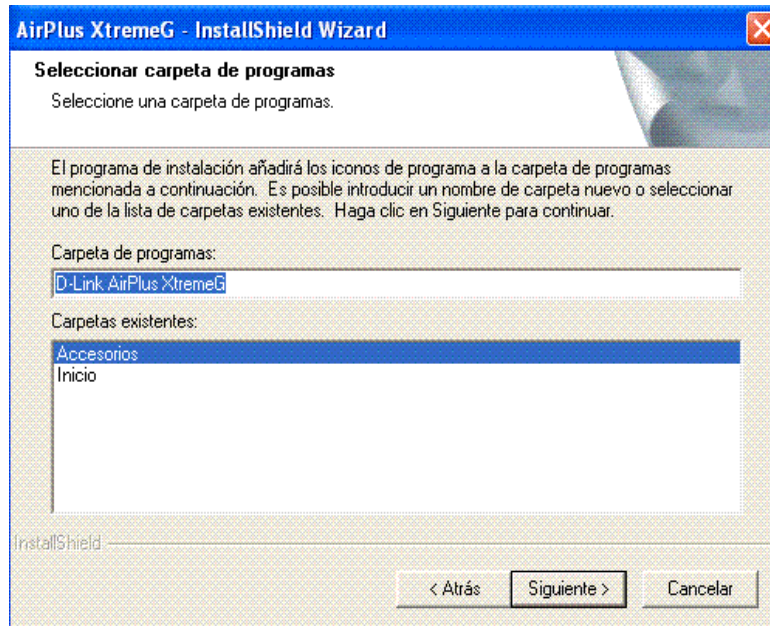


Gráfico 31. Seleccionar carpetas de programas

## 7. A continuación aparecerá la siguiente pantalla

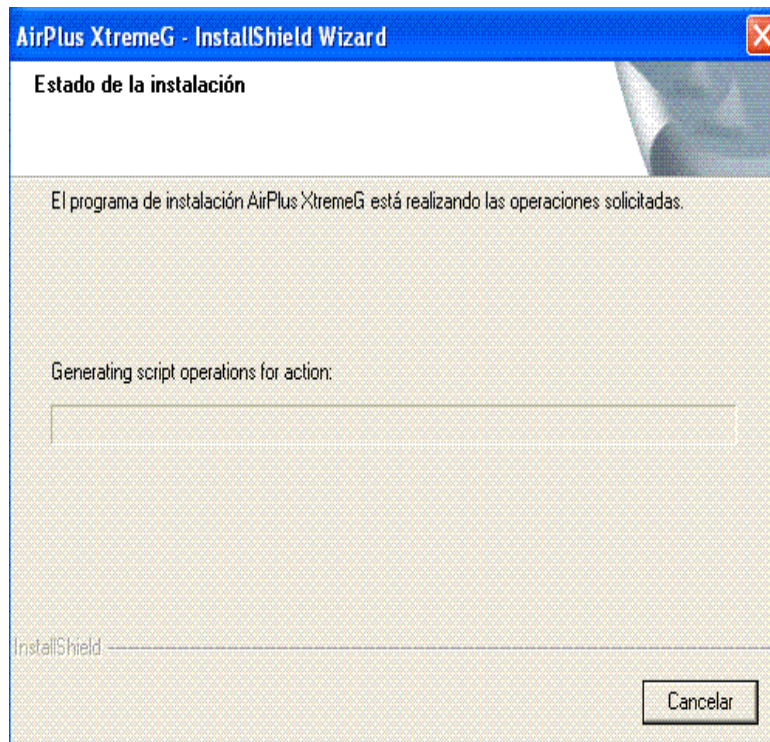


Gráfico 32. Estado de instalación

8. Por último hacemos clic en Finalizar para terminar la instalación

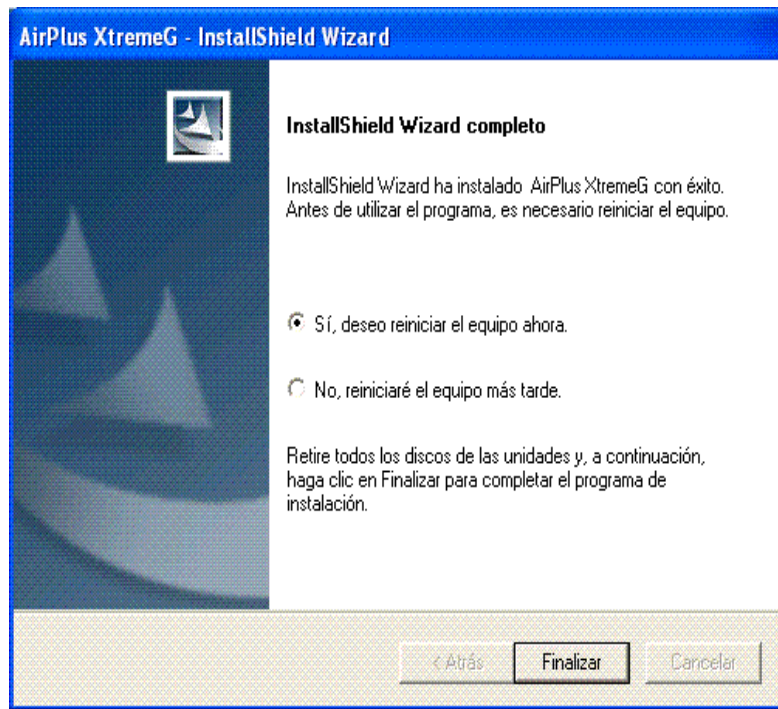


Gráfico 33. Fin de la instalación

9. Apagar el ordenador, para lo cual no se debe sacar el CD DWL-G520 de la unidad de CD-ROM.



Gráfico 34. Apagado el ordenador

**10.** Asegurarse de que el ordenador este apagado y que el cable de poder este desenchufado de la toma de poder.

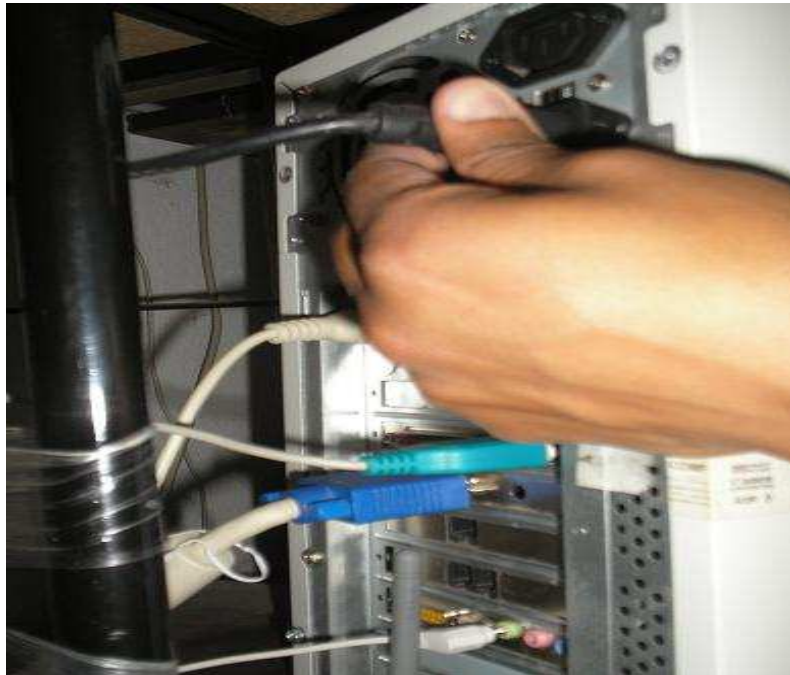


Gráfico 35. Ordenador apagado y cable desenchufado

**11.** Se procede a destapar la cubierta del PC, para la cual utilizaremos destornilladores.



Gráfico 36. Destapar la cubierta del PC

**12.** Antes de manipular cualquier dispositivo de la Pc se debe tocar el case de la misma para que de esta manera quitarse la energía estática que todo ser humano la posee.



Gráfico 37. Quitarse la energía estática

**13.** Seleccionar una ranura PCI vacía para allí instalar la tarjeta.

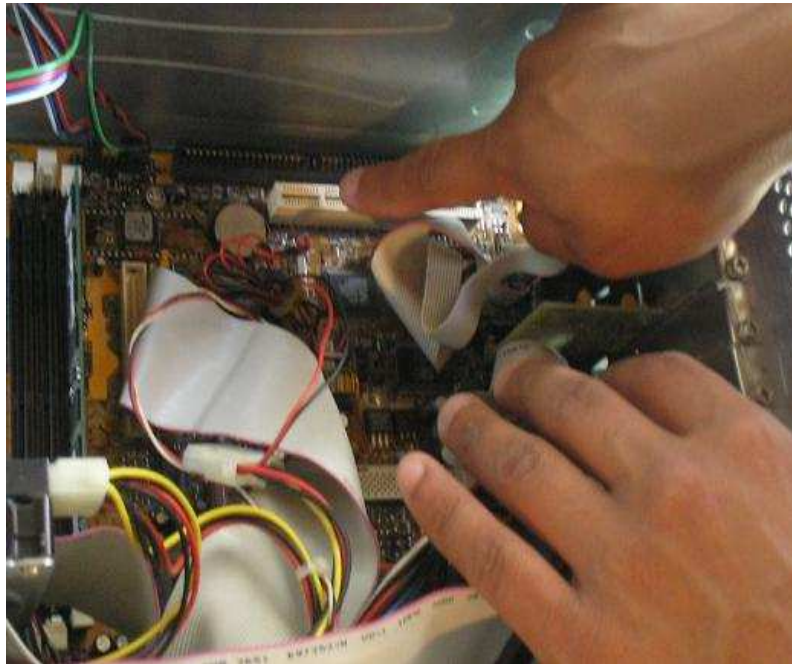


Gráfico 38. Seleccionar una ranura PCI

**14.** Coger la tarjeta inalámbrica por los bordes para no topar ningún circuito

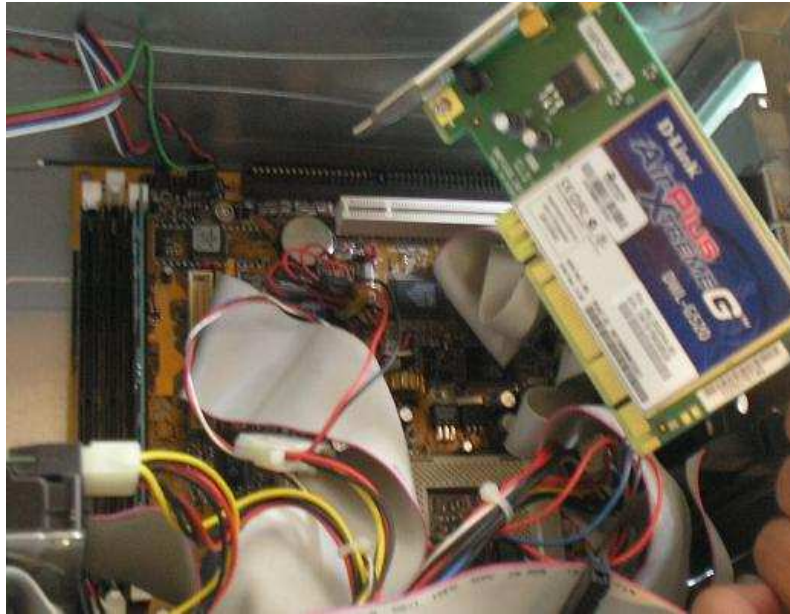


Gráfico 39. Instalación de la tarjeta Inalámbrica

**15.** Colocar la tarjeta encima de la ranura.

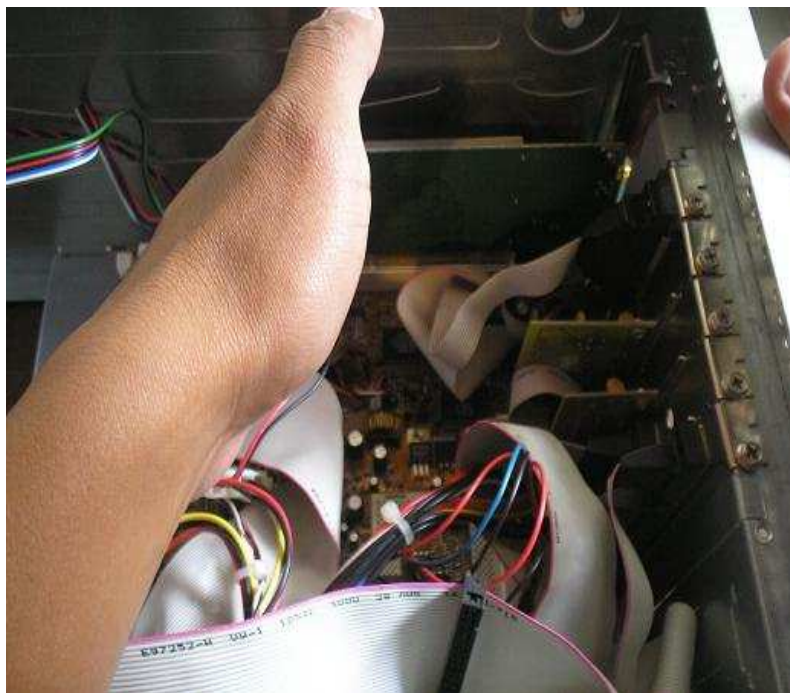


Gráfico 40. Colocación de la tarjeta Inalámbrica

**16.** Empuje hacia abajo firmemente para que se asiente en la ranura.



Gráfico 41. Colocación de la tarjeta Inalámbrica

**17.** Asegurar con un tornillo el revestimiento del panel trasero de la tarjeta.

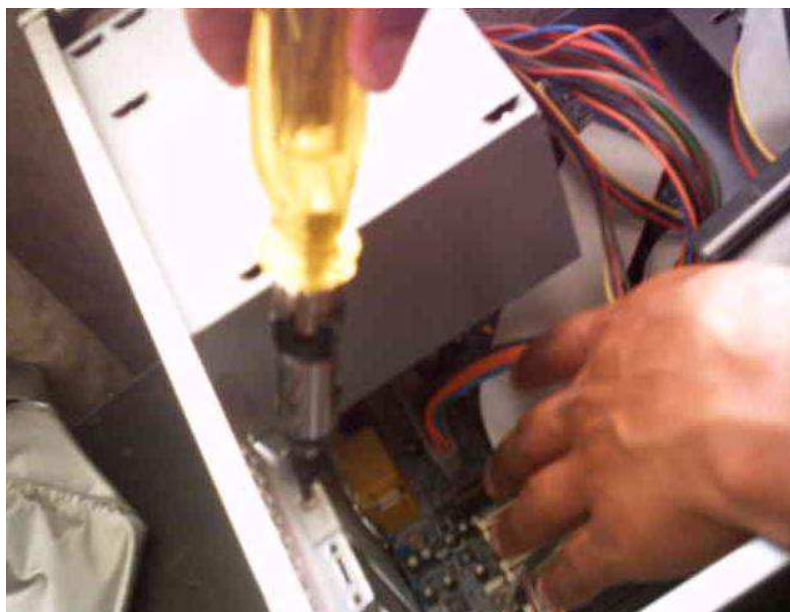


Gráfico 42. Aseguramiento del tornillo en panel de la tarjeta Inalámbrica

**18.** Proceda a tapan el case del PC.



Gráfico 43. Tapan el case del PC

**19.** Conecte todos los dispositivos del computador (mouse, teclado, monitor, etc) además, enchufe el cable de alimentación.

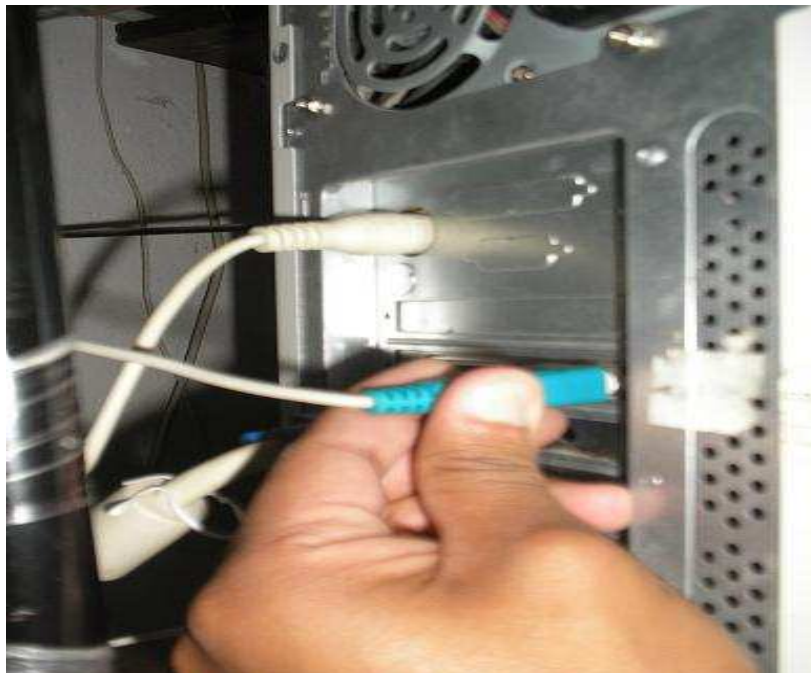


Gráfico 44. Conectar los dispositivos del computador

**20.** Conecte la antena en la tarjeta inalámbrica.



Gráfico 45. Conexión la antena de la tarjeta

**21.** Ponga en funcionamiento la computadora (Encender).



Gráfico 46. Encendida del Pc

### 3.1.2. Pasos para la configuración de una tarjeta inalámbrica

1. Como tenemos controladores de las tarjetas inalámbricas procedemos. Hacer click derecho en mis sitios de red, en propiedades click.



Gráfico 47. Configuración de la Tarjeta Inalámbrica

2. Aparecerá la siguiente pantalla en la que cogeremos redes inalámbricas.



Gráfico 48. Configuración de red inalámbrica

3. Como se va a emplear la utilidad Air Plus Xtreme G para Windows XP, Se debe seguir los siguientes pasos:

### 3.1 Ir a inicio clic en D link - Air Plus Utility, hacer Click



Gráfico 49. Escoger D link - Air Plus Utility.

### 3.2 Se mostrará la siguiente ventana.



Gráfico 50. Ventana del D link - Air Plus Utility, opción información del enlace.

**3.3** Elegiremos, Configuración y procederemos a habilitar la Pci card, en la red, para lo cual llenaremos SSID, Modo Inalámbrico, Encriptación, longitud de clave.

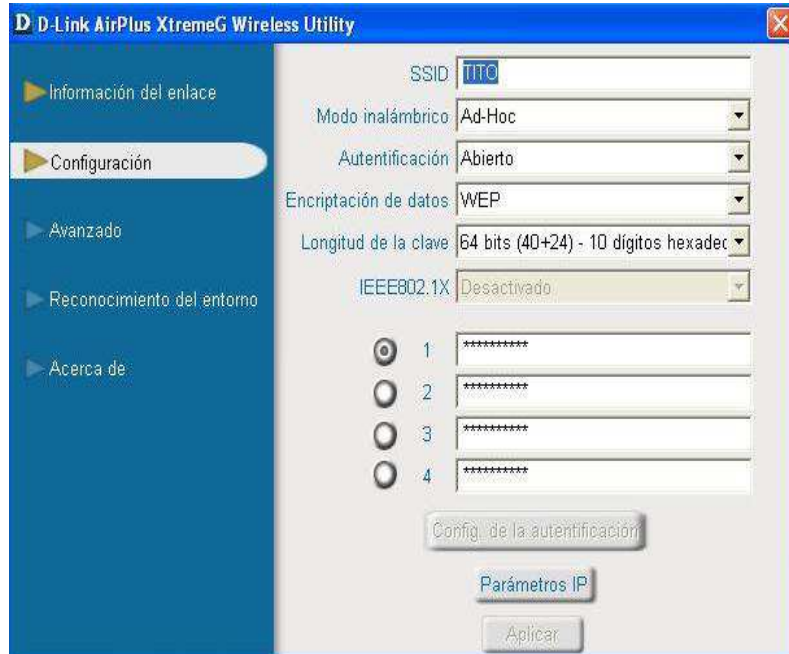


Gráfico 51. Opción configuración.

**3.4** Como vamos a utilizar la propiedad Air plus Xtreme G seleccionamos avanzado y elegiremos los parámetros que consideremos necesarios.

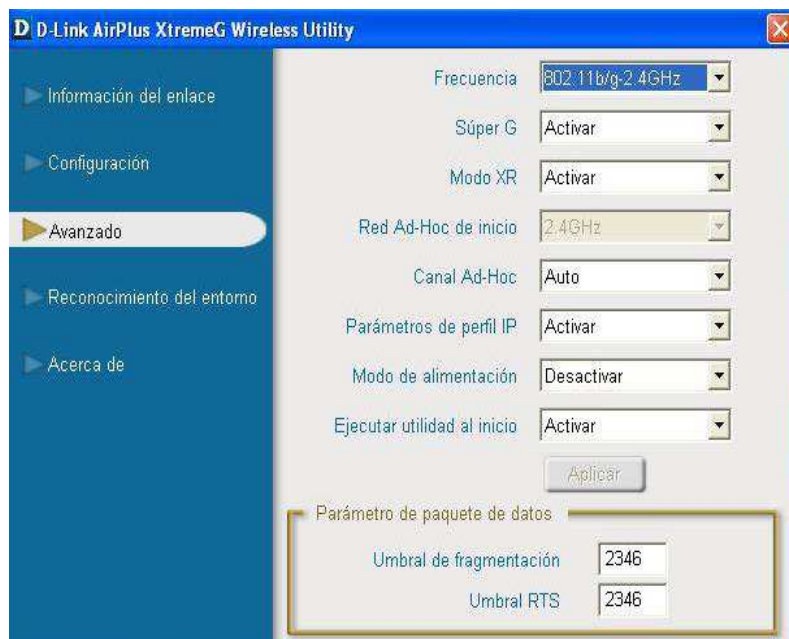


Gráfico 52. Opción avanzada.

3.5 En el reconocimiento del entorno se muestra el SSID, MAC, Señal de la tarjeta. Así también el perfil de la tarjeta.

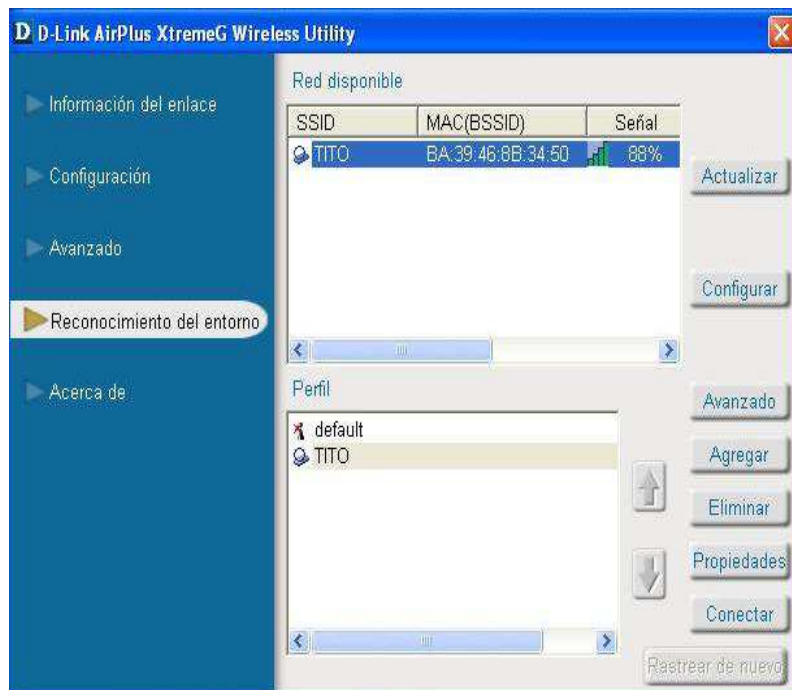


Gráfico 53. Opción Reconocimiento del entorno.

### 3.1.3. Pasos para la configuración de una IP, para Windows XP.

1. Hacer click derecho en mis sitios de red, en propiedades click.

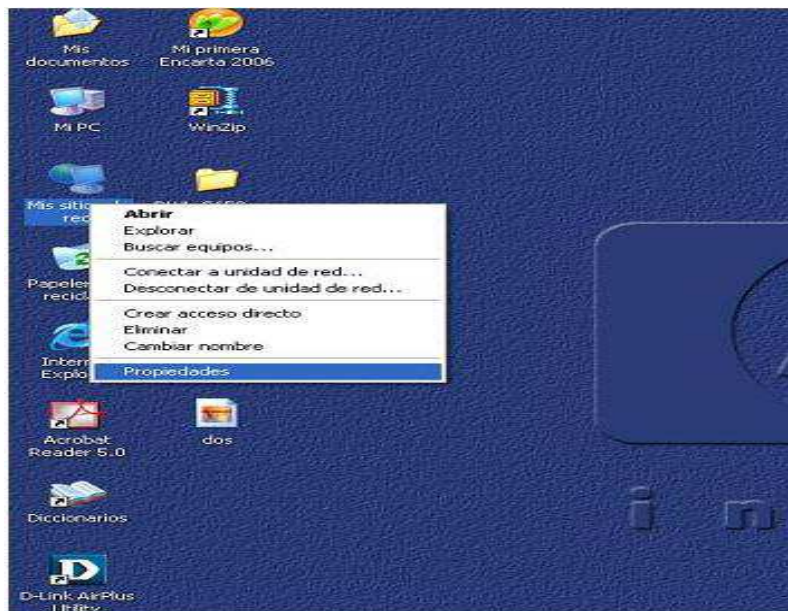


Gráfico 54. Mis sitios de red y propiedades.

2. Aparecerá la siguiente pantalla, en la que debemos posicionar el cursor sobre el icono de conexiones inalámbricas para hacer clic.

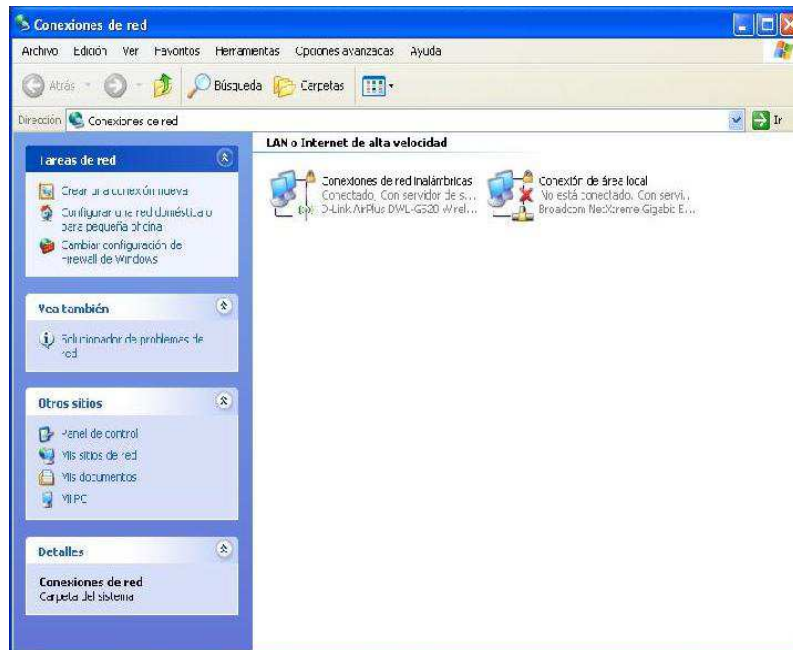


Gráfico 55. Hacer click conexiones inalámbricas.

3. Hacer click en propiedades

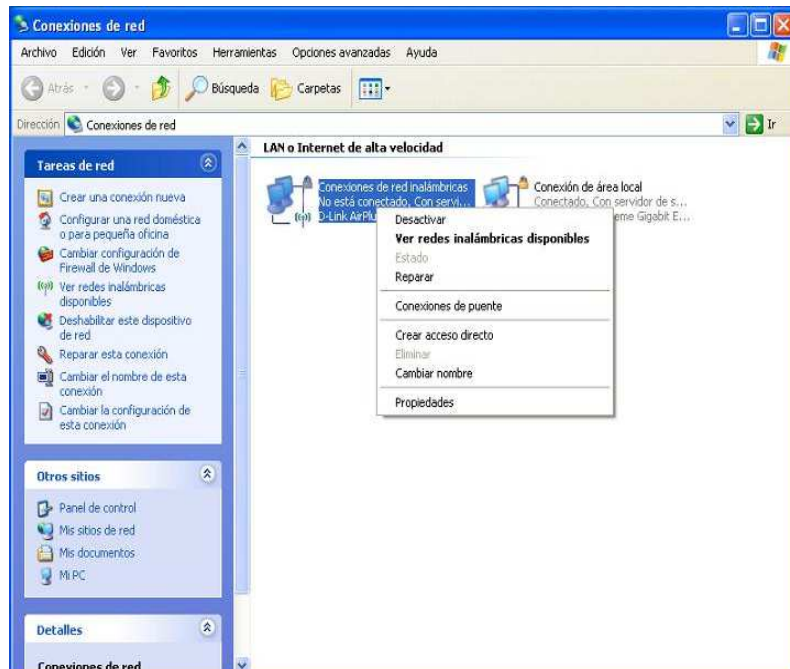


Gráfico 56. Hacer click en propiedades.

4. Se mostrara la siguiente Pantalla en la cual escogeremos, redes inalámbricas, protocolo TCP/IP, posesionamos clic en propiedades.



Gráfico 57. Seleccionar Protocolo Internet (TCP/IP).

5. Como vamos a utilizar una dirección IP estática, seleccionar Usar la siguiente dirección IP, ingresaremos la Dirección IP con la máscara de Subred y aceptar.

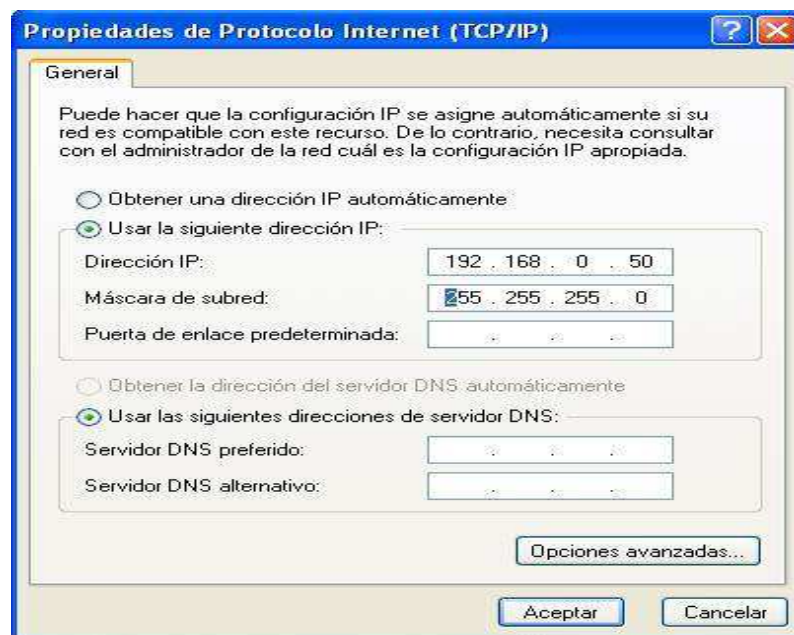


Gráfico 58. Ingreso de la Dirección IP.

### 3.1.4. Pasos para la configuración de un punto de acceso.

1. Conectar al alimentador al receptor situado en la parte posterior del DW 2100Ap y después conectar el otro extremo de alimentación en una base de pared o regleta de alimentación, el led de poder se pondrá en ON para indicar que la operación ha sido correcta.



Gráfico 59. Conectar el alimentador al receptor.

2. Conectar el adaptador de energía al AP así como también la antena.



Gráfico 60. Conectar el AP y la antena.

3. Introducir el extremo del cable en el puerto Ethernet del panel trasero del AP y el otro extremo del cable en el puerto para RJ 45 del PC. El led se prendera para indicar que la conexión Ethernet es correcta.



Gráfico 61. Conectar el AP y la antena.

4. Abra su Navegador de web y teclee: [Http://10.10.1.13](http://10.10.1.13) en la barra de direcciones URL. Pulse ENTER. Aparecerá la pantalla de conexión.



Gráfico 62. Navegador de web.

5. En el campo de usuario digite **admin.** y deje el campo de la contraseña en blanco. Haga clic en OK



Gráfico 63. Ingreso del usuario y contraseña.

6. Una vez que se haya conectado aparecerá la pantalla de inicio, haga click en Run Wizard.



Gráfico 64. Pantalla de inicio.

7. Aparecerán la siguiente pantalla, haga click en next.



Gráfico 65. Inicio del setup del Access point.

8. Introduzca una nueva contraseña y un nuevo password, clic continuar



Gráfico 66. Ingreso el Set Password.

9. Introduzca el SSID y el Canal.



Gráfico 67. Ingreso del SSID.

10. Habilite la encriptación y seleccione uno de los niveles de encriptación para que la comunicación sea más segura.



Gráfico 68. Seleccionar el Security Level.

11. Como seleccionamos WPA, aparecerá la siguiente pantalla. En la cual ingresaremos una frase que se encriptará para la seguridad.

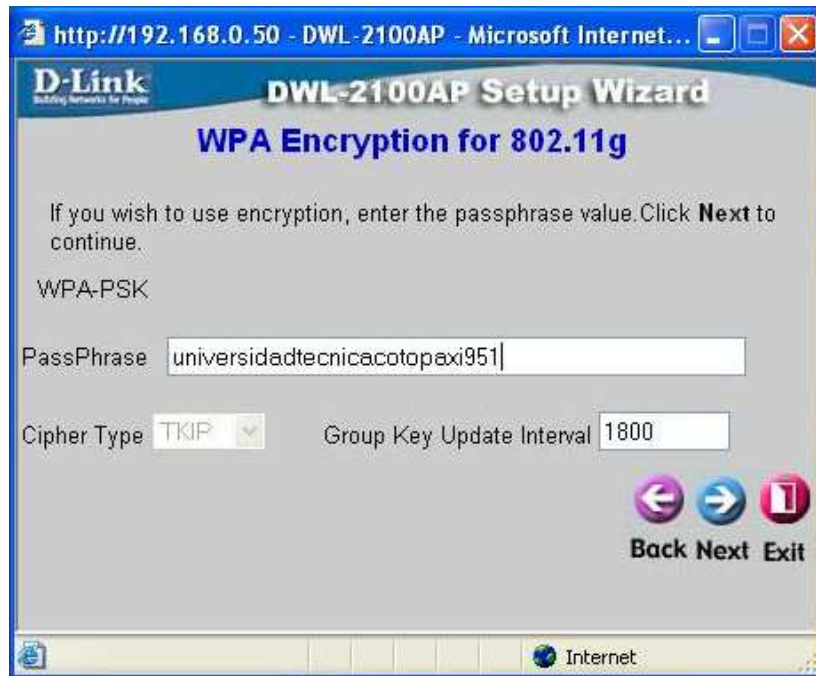


Gráfico 69. Encriptación del WPA.

12. Selecciones restarar (reiniciar), Finalmente Cerrar y volverá a la ventana de Inicio, haga clic en X.

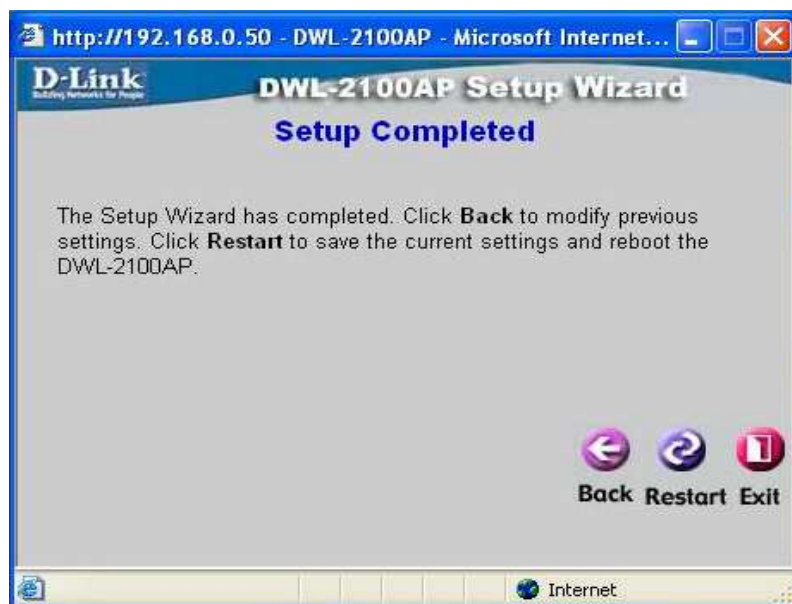


Gráfico 70. Fin del Setup.

## 3.2 PRUEBAS DE ENLACE INALAMBRICO

### 3.2.1. Red Ad-Hoc (Dos Computadores)

1. Abrimos los controladores de las tarjetas inalámbricas las cuales despliegan información de fábrica como son información de enlace, configuración, avanzado, reconocimiento del entorno como lo demuestran el siguiente gráfico, esto es para las dos maquinas a utilizar.



Gráfico 71. Red Ad-Hoc, opción información del enlace.

2. Para configurar la red. En ambas computadores, el SSID se llamará PRUEBA, el modo será Ad Hoc. La autenticación estará abierta y la encriptación estará desactivada.

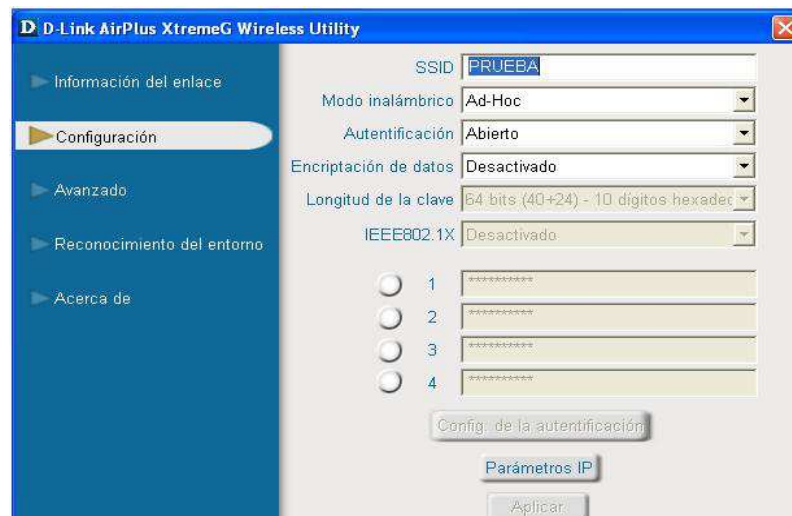


Gráfico 72. Red Ad-Hoc, opción configuración

3. Continuando la configuración de la red. En ambos computadores, en el Ítem avanzado, todas las opciones que poseen las tarjetas se utilizarán las que vienen de fábrica

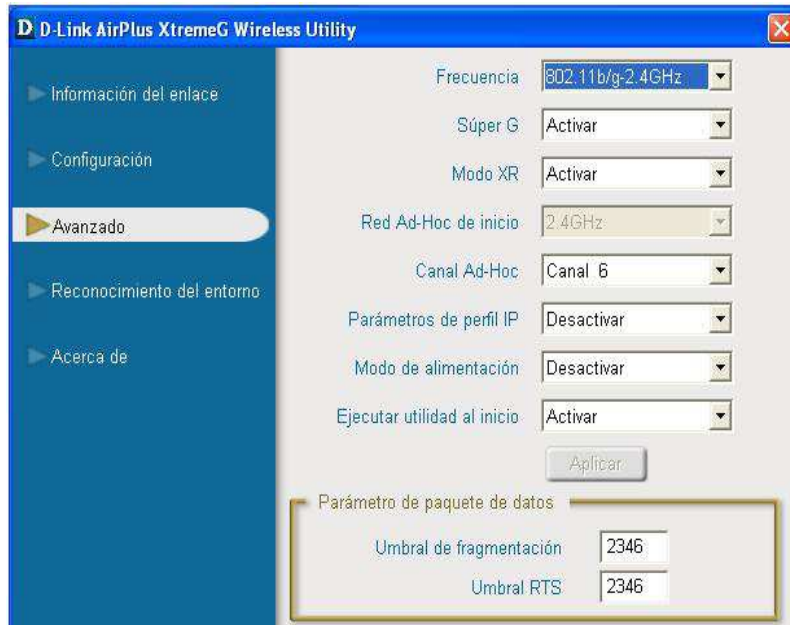


Gráfico 73. Red Ad-Hoc, opción Avanzada.

4. En lo que respecta al reconocimiento del entorno en las maquinas se mostrara el siguiente gráfico. Esto se debe a que estamos configurando las tarjetas y la señal será 0.

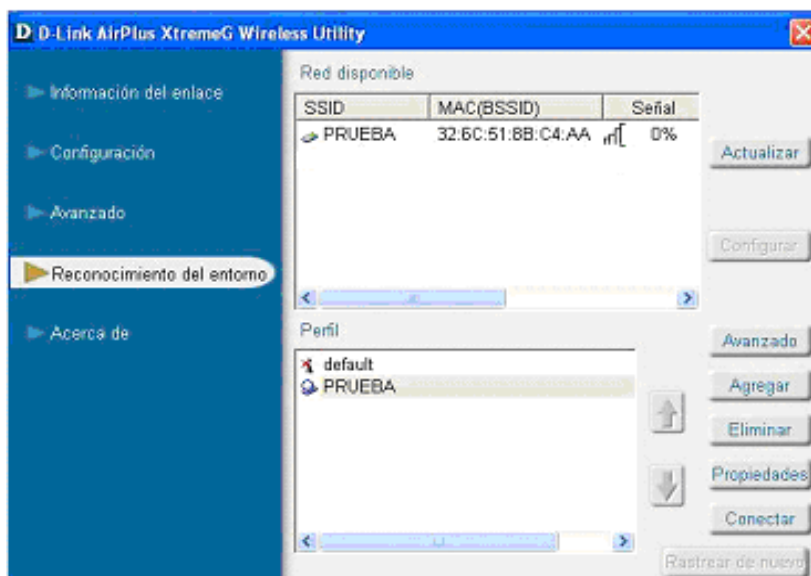


Gráfico 74. Red Ad-Hoc, opción Reconocimiento del Entorno.

5. En lo que respecta ítem **Acerca de**, es información de los fabricantes en este caso de la empresa Dlink. Finalizada la configuración iremos a Información de enlace y se mostrara toda la configuración que se ha realizado en ambas PCs.



Gráfico 75. Red Ad-Hoc, configuración realizada.

Procedemos a realizar pruebas de enlace entre los dos PCs, para lo cual nos iremos nuevamente a reconocimiento del entorno.

6. En la PC uno se muestra la siguiente pantalla, en la cual indica que hay conexión

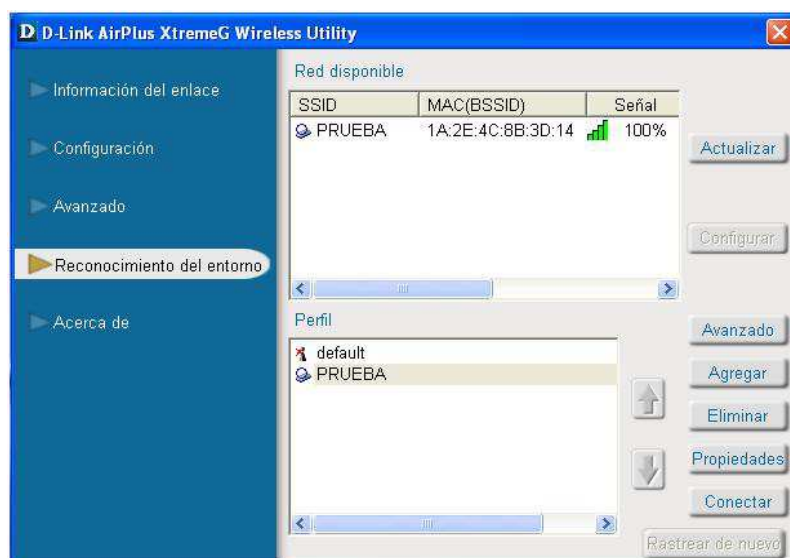


Gráfico 76. Red Ad-Hoc, demostración del la conexión

En la PC dos se muestra la siguiente pantalla, en la cual indica que hay conexión.

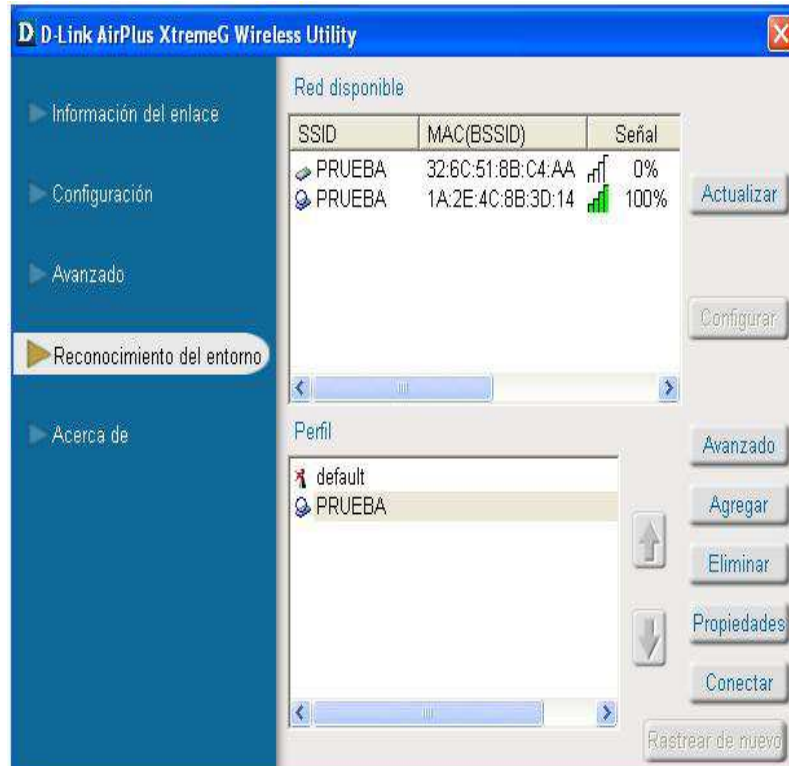


Gráfico 77. Red Ad-Hoc, demostración del la conexión en las dos PCS.

Finalmente cerramos la pantalla de configuración.

7. Nos vamos a la parte inferior derecha de la pantalla de la PC y vemos que el icono de conexión de redes inalámbricas esta activado (verde) damos doble click y se nos aparece la siguiente pantalla en ambas computadoras de prueba. Lo cual indica que ya se están en funcionamiento inalámbrico mediante emisión de frecuencias.

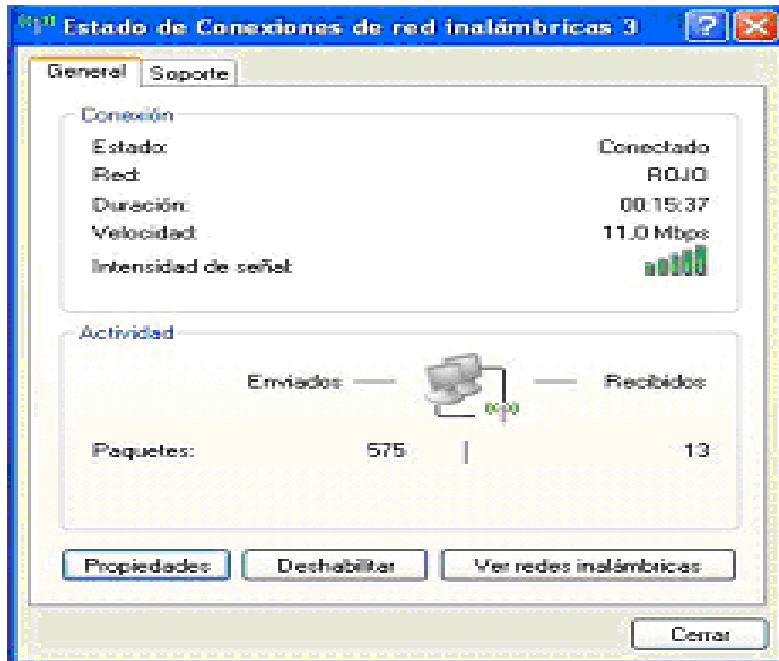


Gráfico 78. Red Ad-Hoc, estado de la conexión en la PC.

Utilizaremos la máquina dos para ver si se tienen acceso a la red con lo que vamos al icono de entorno de red damos doble click y se nos desplegará las dos maquinas que estamos utilizando para la práctica.

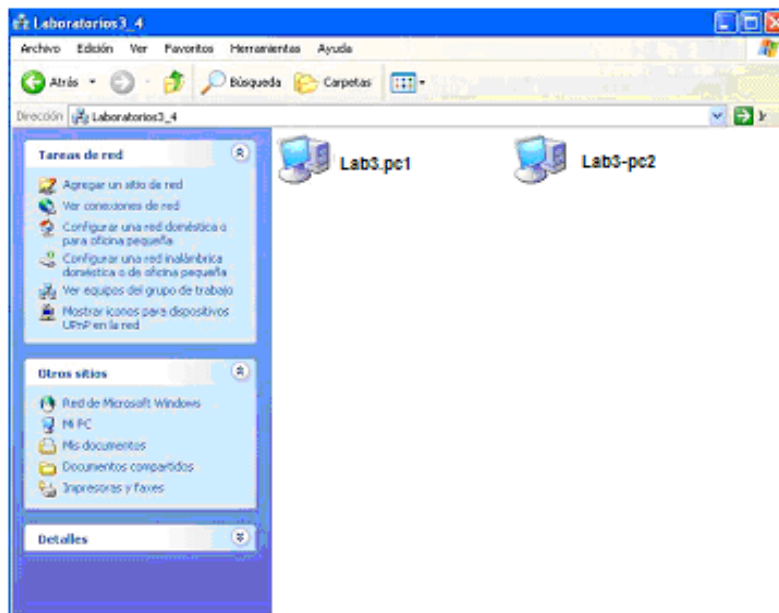


Gráfico 79. Red Ad-Hoc, comprobación de conexión entre las PCs.

8. Seleccionaremos la máquina uno daremos doble click para que se muestren los dispositivos compartidos.

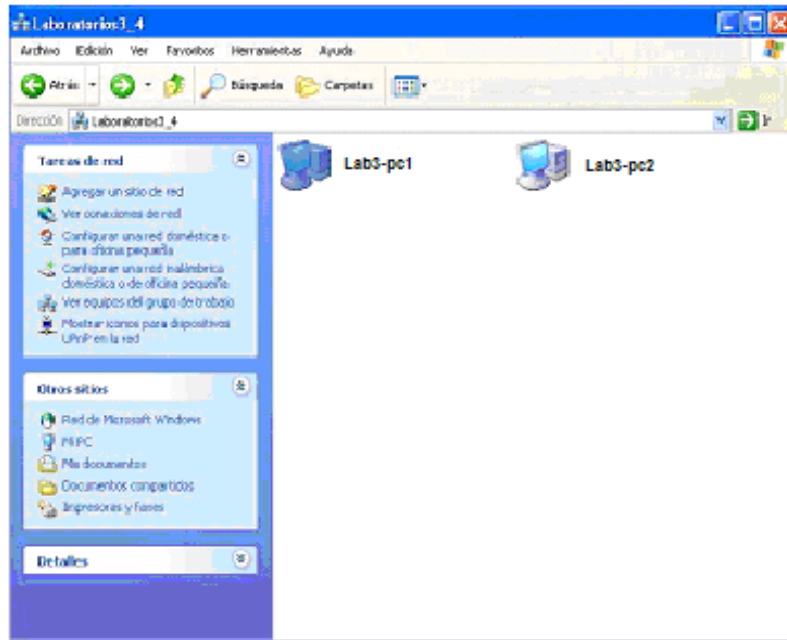


Gráfico 80. Red Ad-Hoc, estado de la conexión en la PC.

9. En este caso la máquina uno permite el acceso y están compartidos las unidades A, C, las impresoras y faxes. Seleccionamos la unidad C.

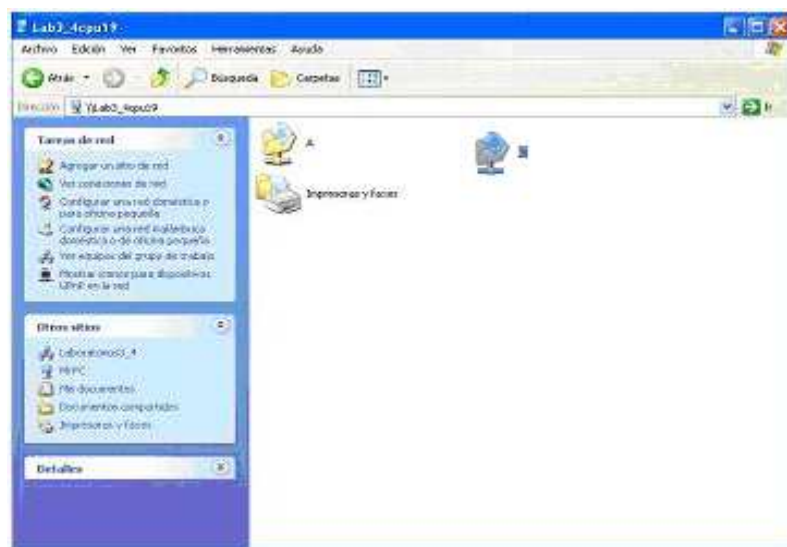


Gráfico 81. Red Ad-Hoc, compartir las unidades y archivos de las PCs.

Se muestra todo el contenido existente en ella.

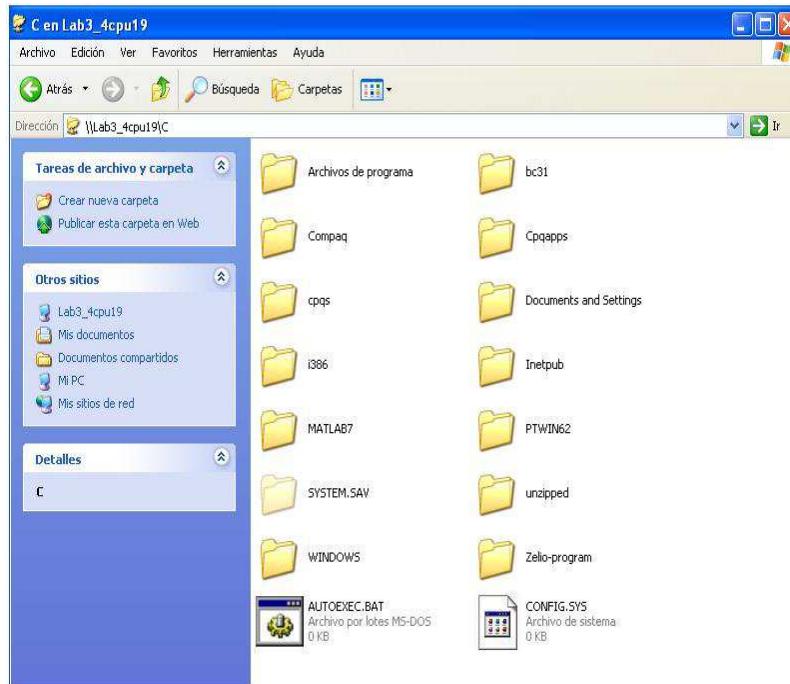


Gráfico 82. Red Ad-Hoc, contenido de la PC.

10. En el caso de la máquina uno para ver si se tienen acceso a la red seguimos los mismo pasos anteriores en las maquinas que estamos utilizando para la práctica.

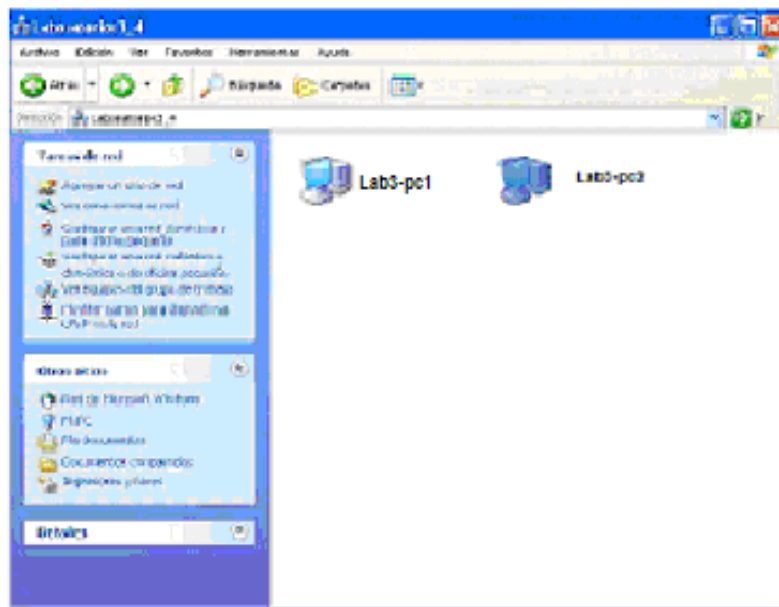


Gráfico 83. Red Ad-Hoc, estado de la conexión en la PC 2.

En este caso la máquina dos permite el acceso y esta compartidos la unidades C, las impresoras y faxes. Seleccionamos la unidad C.

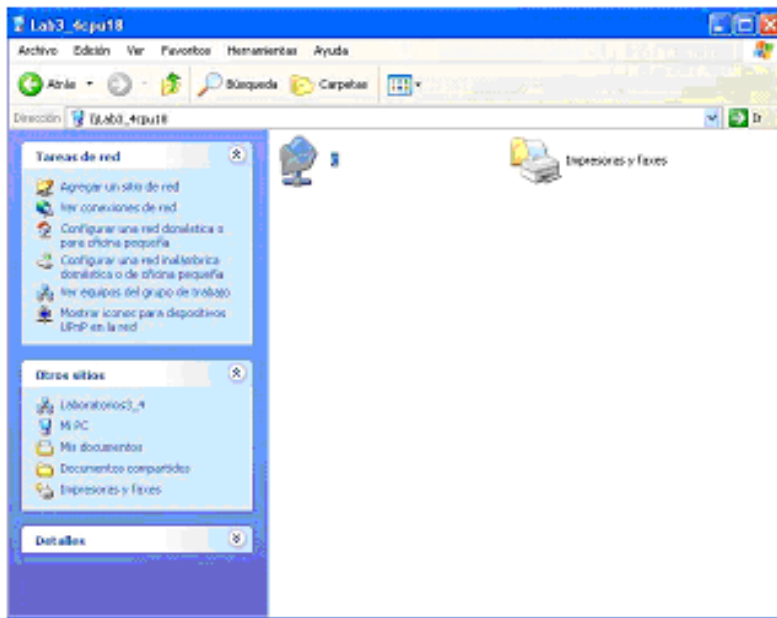


Gráfico 84. Red Ad-Hoc, compartir las unidades y archivos de las PCs.

Se muestra todo el contenido existente en ella.

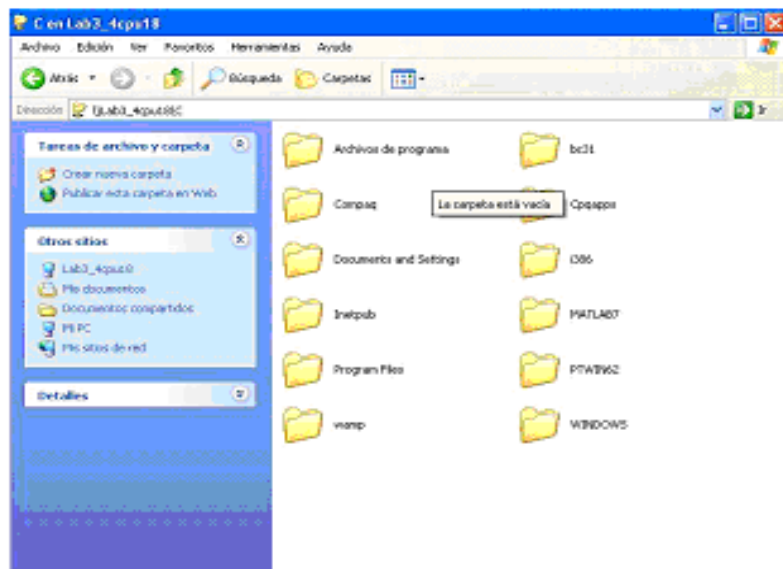


Gráfico 85. Red Ad-Hoc, contenido de la PC 2.

### 3.2.2. Modo Infraestructura

1. Utilizaremos en parte la configuración del modo Ad Hoc, en este caso las direcciones IPS y el SSID, con la diferencia que en este modo entra en funcionamiento un elemento adicional como es el Access Point, el cual debe estar configurado con el SSID que tienen las tarjetas como identificador de red inalámbrica, para que entre en funcionamiento.

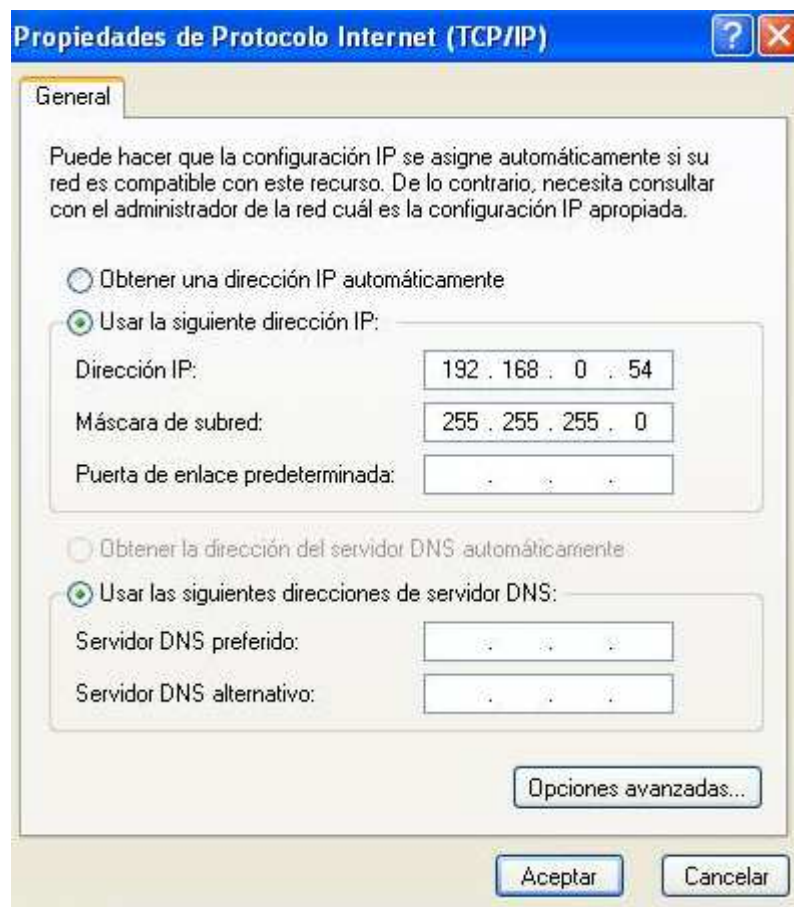


Gráfico 86. Direcciones IPS y el SSID de la máquina 1.

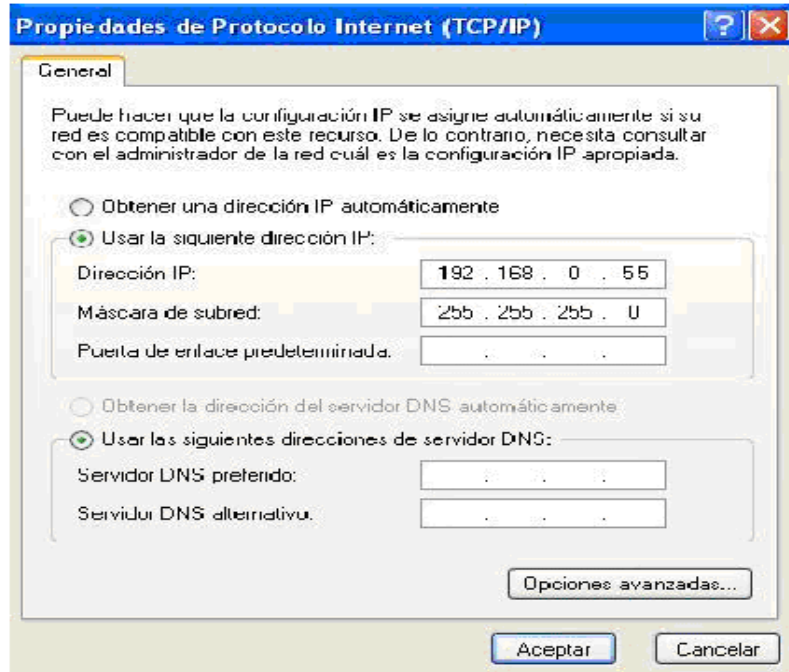


Gráfico 87. Direcciones IPS y el SSID de la máquina 2

2. Así también como el SSID, como en este caso es PRUEBA.

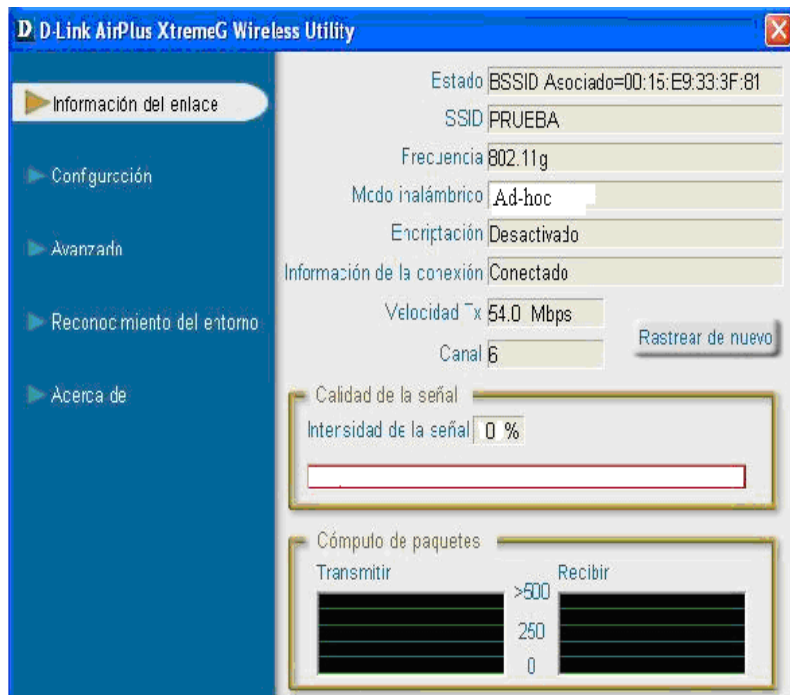


Gráfico 88. SSID en las dos PCS similar a la Red Ad-Hoc.

3. Ahora se dará doble click en el icono de la tarjeta Dlink, de la pantalla

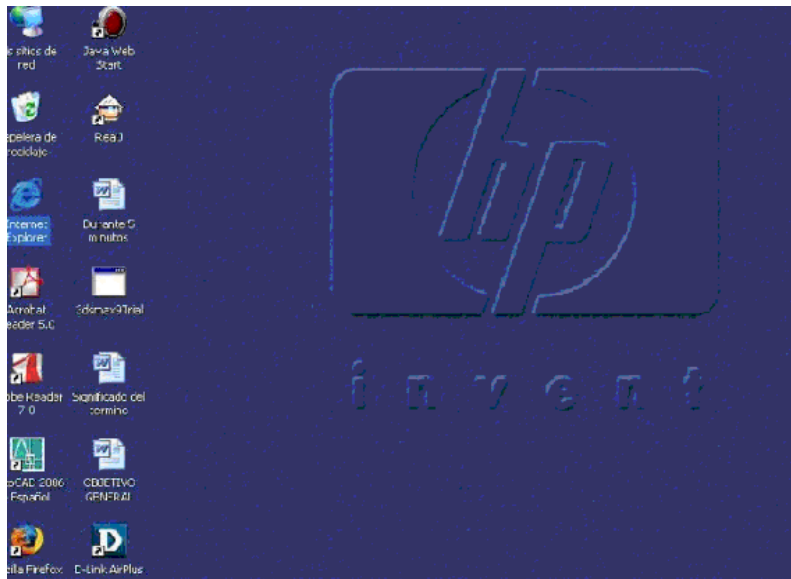


Gráfico 89. Icono de la tarjeta Dlink.

4. Aparecerá la siguiente pantalla en las cuales se encuentran los ítems de configuración. En este caso el Modo Inalámbrico a ser ingresado será el de INFRAESTRUCTURA daremos click en aplicar para que se grave los cambios y cerraremos la pantalla

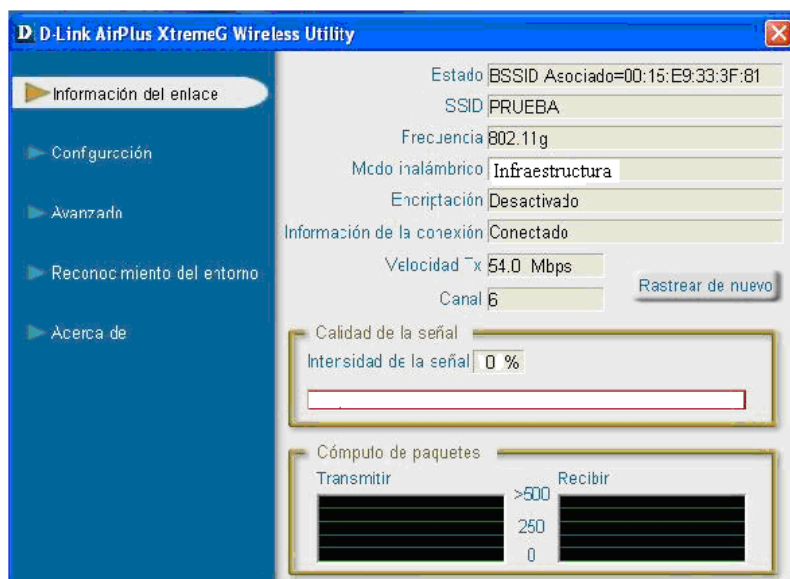


Gráfico 90. Modo infraestructura, opción información del enlace.

5. Luego abriremos nuevamente la pantalla de configuración y veremos que los cambios se han gravado.

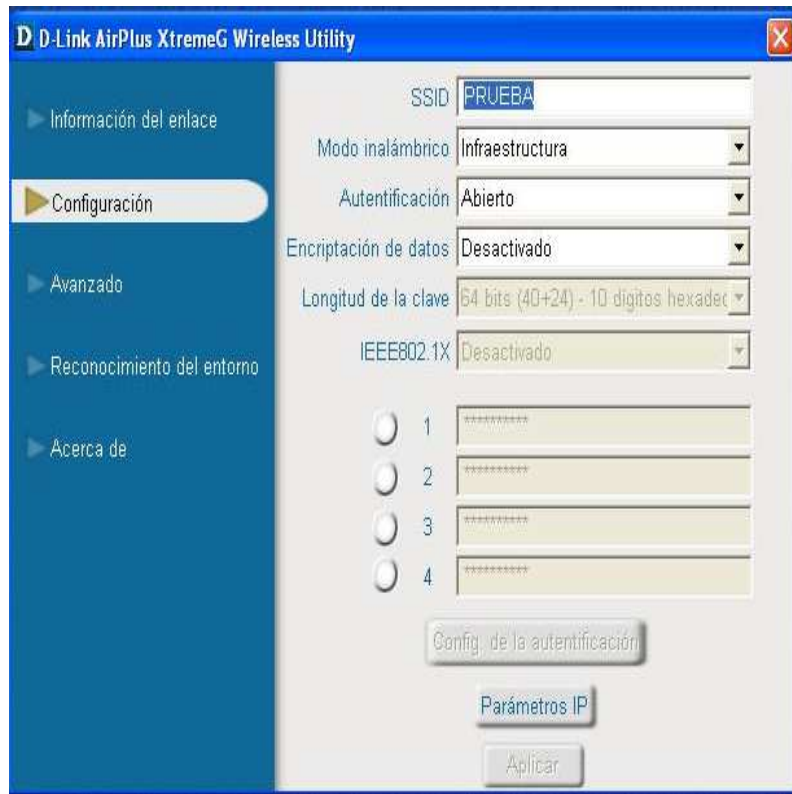


Gráfico 91. Modo infraestructura, opción configuración.

6. El siguiente paso se procederá a poner en funcionamiento el Access Point (encenderlo y conectarlo a la red física). Previamente el AP ya debe estar configurado como se demostró en la parte de configuración. Por defecto el Access Point viene con el IP 192.168.0.50, con la máscara 255.255.255.0, por lo cual no habrá problemas al utilizarlo para que sea el nexo de conexión de las dos máquinas a la wireless.

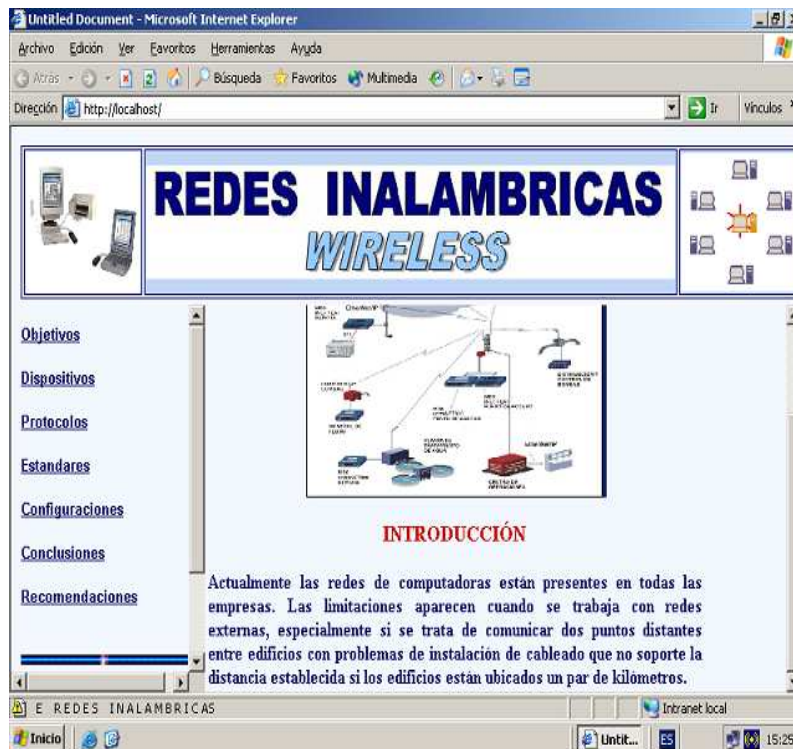


Gráfico 92. Modo infraestructura, pantalla Internet.

7. Luego verificaremos que el SSID de las tarjetas sea el mismo del Access Point en este caso el SSID de AP y de las tarjetas es PRUEBA.



Gráfico 93. Modo infraestructura, verificación del SSID.

8. A continuación verificaremos que haya conexión de las maquinas con el AP para lo cual miramos en la parte inferior derecha del monitor que el icono de redes inalámbricas esta activado, al igual que el icono de la tarjeta esta en verde (Letra D).



Gráfico 94. Modo infraestructura, verificación de la conexión.

9. Del mismo modo observaremos que si entramos a la parte de protocolo TCP/IP para redes inalámbricas existirá conexión.



Gráfico 95. Modo infraestructura, verificación del TCP/ IP.

**10.** En lo que respecta a soporte de conexión inalámbrica se despliega información sobre el IP, máscara y si existe o no conexión.



Gráfico 96. Modo infraestructura, despliegue del TCP/IP y máscara.

**11.** De nuevo abriremos la pantalla de Utilidades de la tarjeta y miramos que ya esta en funcionamiento con una calidad de señal óptima.

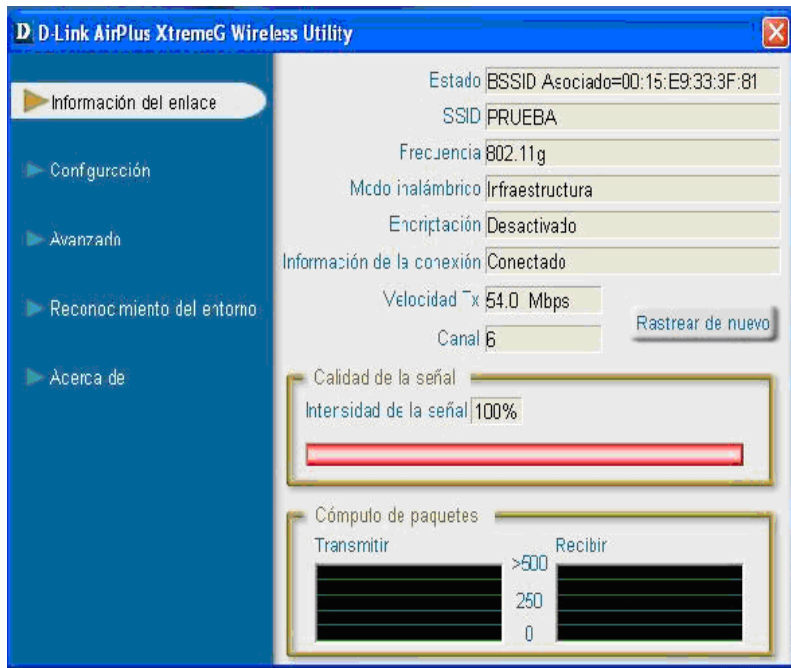


Gráfico 97. Modo infraestructura, opción Información del enlace

12. En lo que respecta al reconocimiento del entorno la señal esta en un 100% de calidad, transmisión recepción. Lo que demuestra que estamos listos para ingresar a trabajar en la red. Cerramos la ventana.

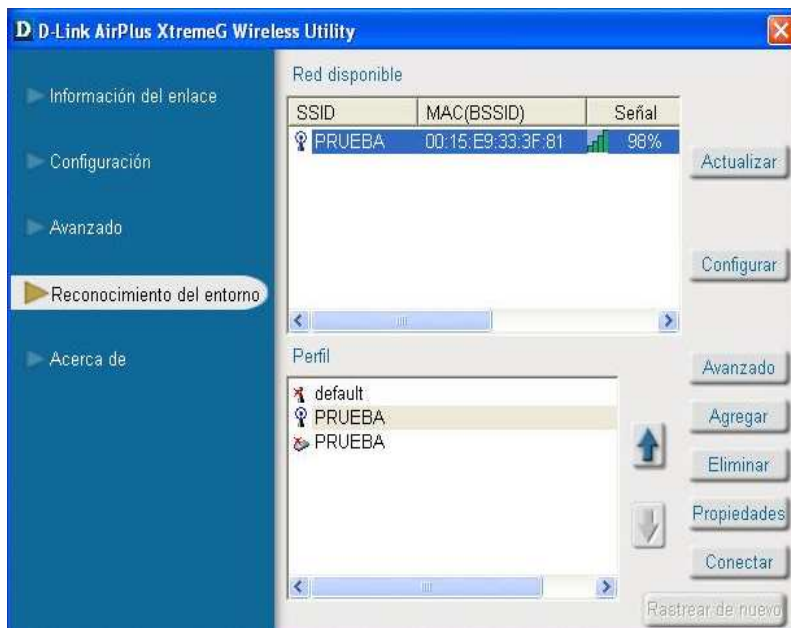


Gráfico 98. Modo infraestructura, Reconocimiento del entorno.

13. Para darse cuenta si hay conexión a la red, se dará doble click en Mis sitio de red



Gráfico 99. Modo infraestructura, verificación en mis sitios de red.

14. Aparecerá la siguiente pantalla, en la cual muestra las redes existentes, en nuestro caso la wireless, que esta en funcionamiento.

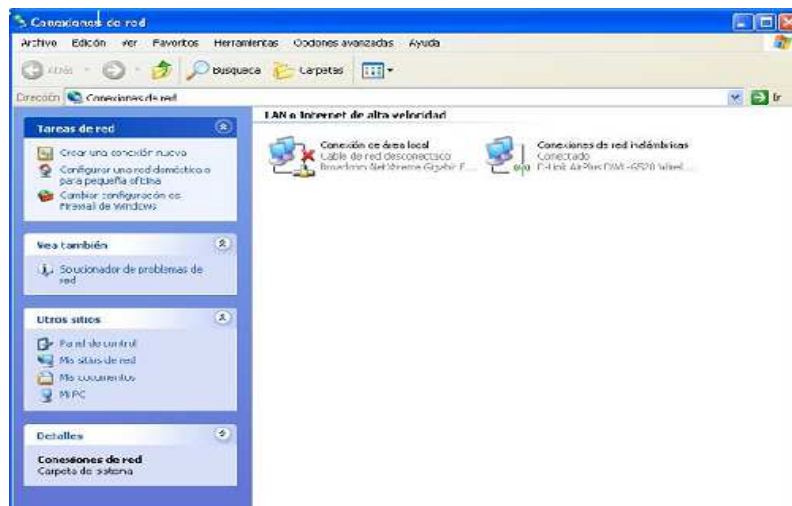


Gráfico 100. Verificación de la conexión.

15. Abriremos mis sitios de red y veremos que nuestra red se llama PRUEBA

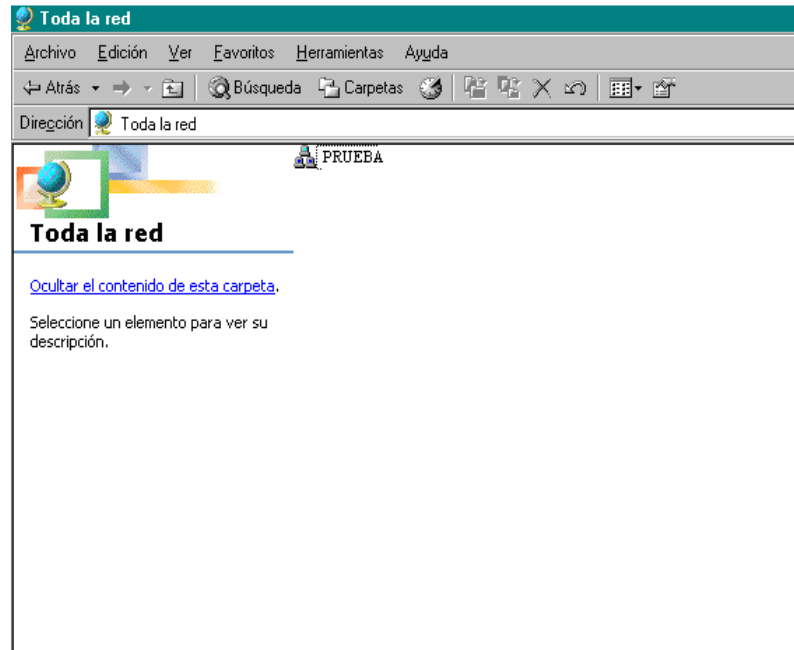


Gráfico 101. Red prueba.

16. Se mostrarán las PCs existentes en la wireless y la red Lan.

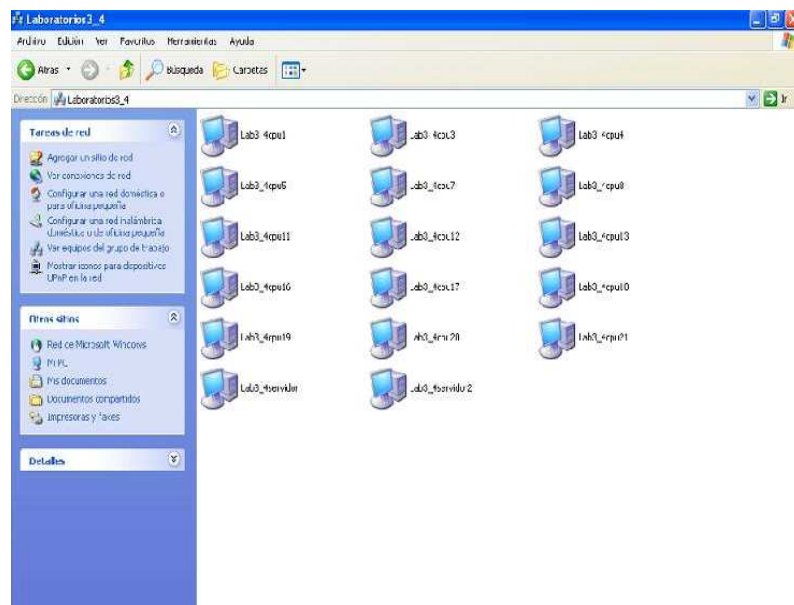


Gráfico102. PCs existentes en la wireless y la red Lan.

17. Seleccionamos una computadora de la red para comprobar que esta compartiendo su información

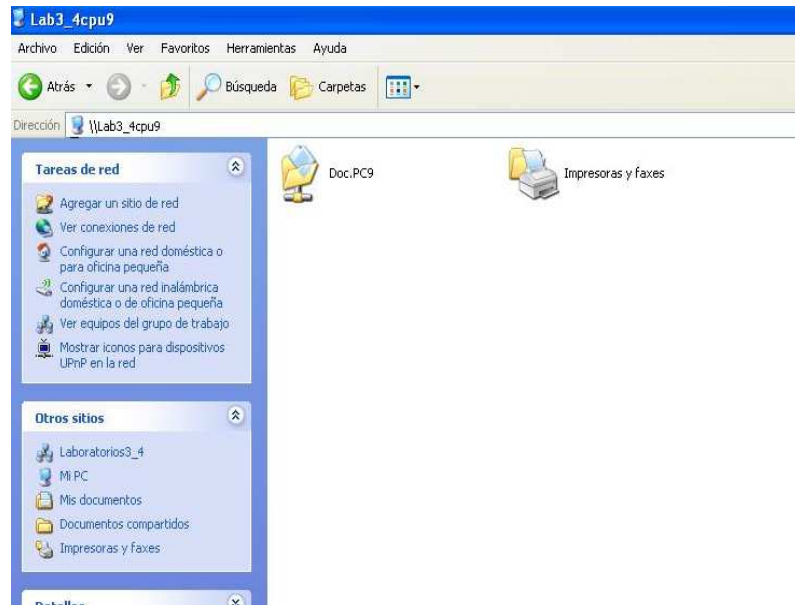


Gráfico 103. Compartiendo su información

18. Abrimos su contenido y copiamos un archivo al azar, para ver la transmisión de información.

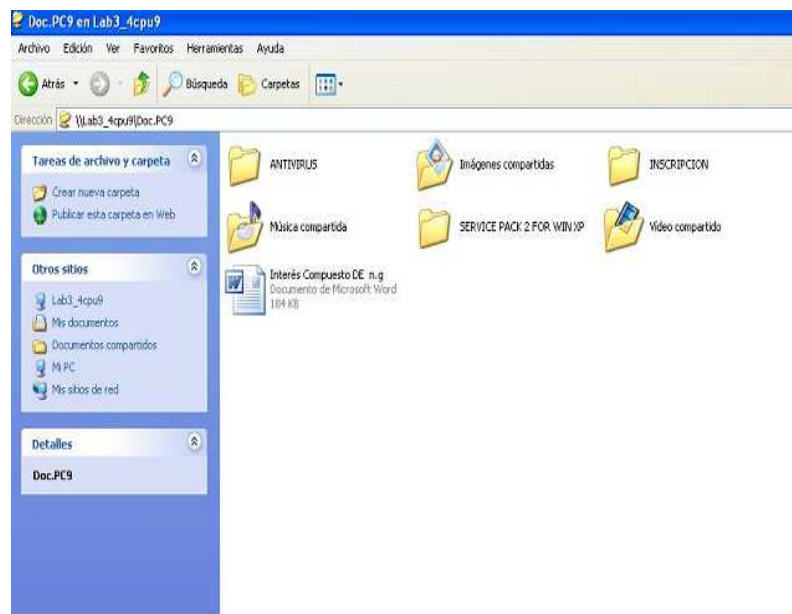


Gráfico104. Compartiendo su información

19. En este caso copiaremos en la máquina uno el contenido de la carpeta portada de la máquina dos.

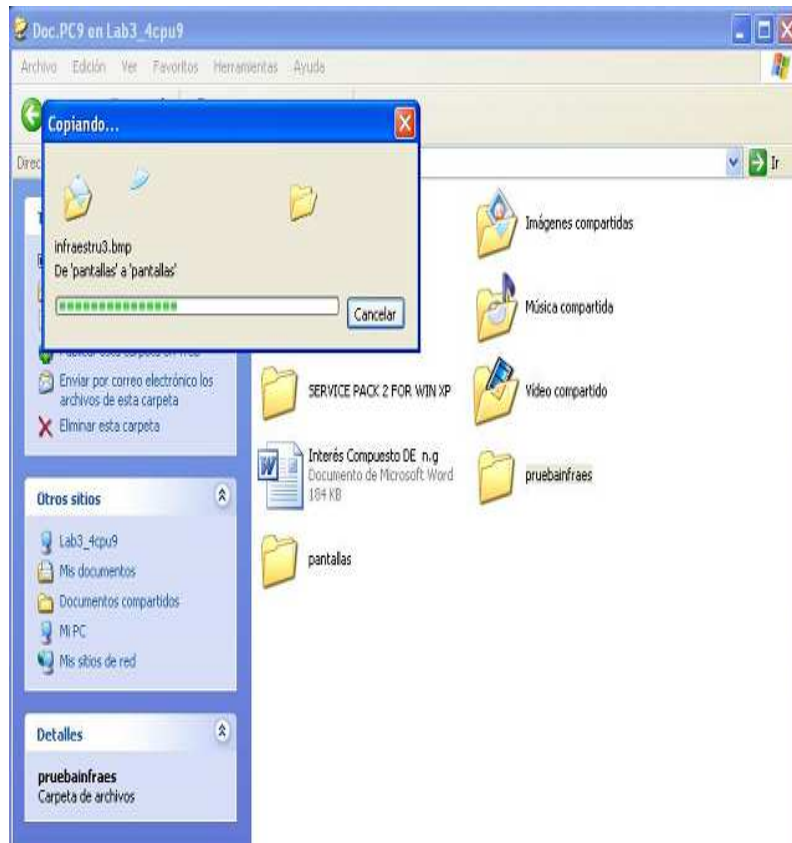


Gráfico105. Copiando información de una Pc a Otra.

20. Luego de que ya hemos configurado, las tarjetas de red, el AP, realizado pruebas de emisión de señal, probado el funcionamiento de las maquinas en modo ad-hoc e infraestructura y que trabajan normalmente. Finalmente vamos a conectar las maquinas a Internet, para lo cual nos damos click en Internet Explorer.



Gráfico 106. Selección de Internet.

21. Se observara que hay acceso al mismo y que la página se esta descargado.

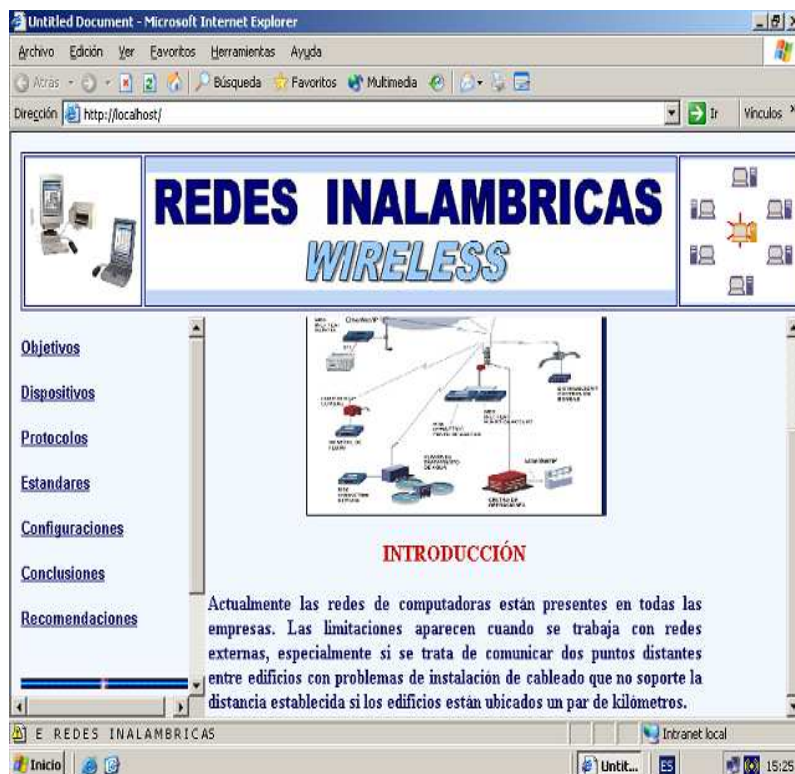


Gráfico107. Ventana de Internet abierta.

### 3.3. DEMOSTRACIÓN DE UNA INTRANET

#### 3.3.1 Configuración de servicios y servidor en Windows 2003

Para realizar la demostración hemos escogido el sistema operativo Windows 2003 ya que cuenta con los servicios básicos para establecerle como servidor que facilitará la implementación de la Intranet.

1. Después de instalar el sistema operativo Windows 2003, procedemos a configurar el servidor y sus servicios.



Gráfico108. Asistente para configurar el servidor.

2. Damos click en siguiente, aparece la siguiente pantalla.

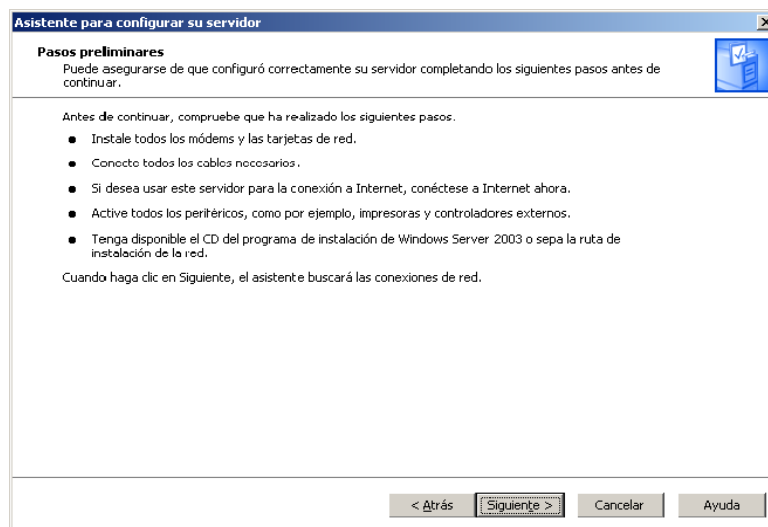


Gráfico109. Pasos preliminares para configurar el servidor.

3. Hacemos click en siguiente, aparece la siguiente pantalla.

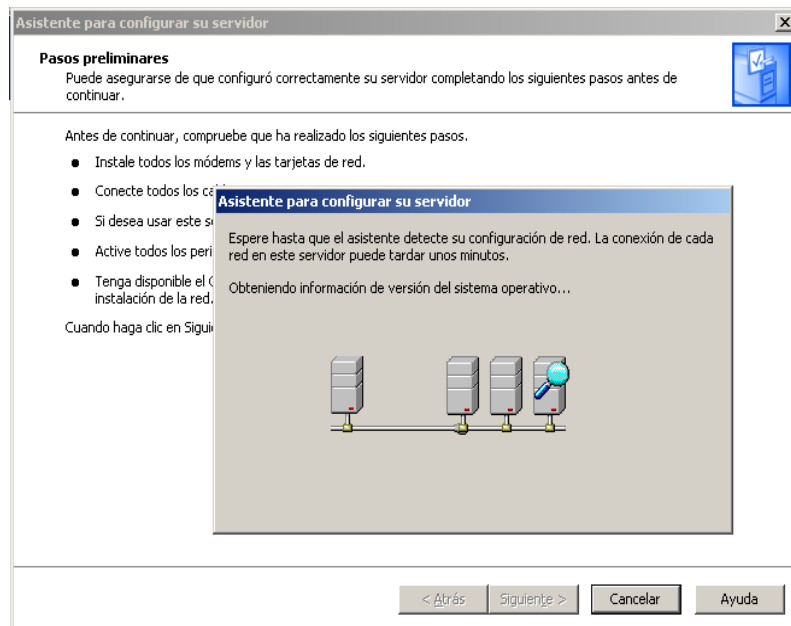


Gráfico 110. Pasos previos para configurar el servidor.

4. Hacemos click en siguiente, aparece la siguiente pantalla.

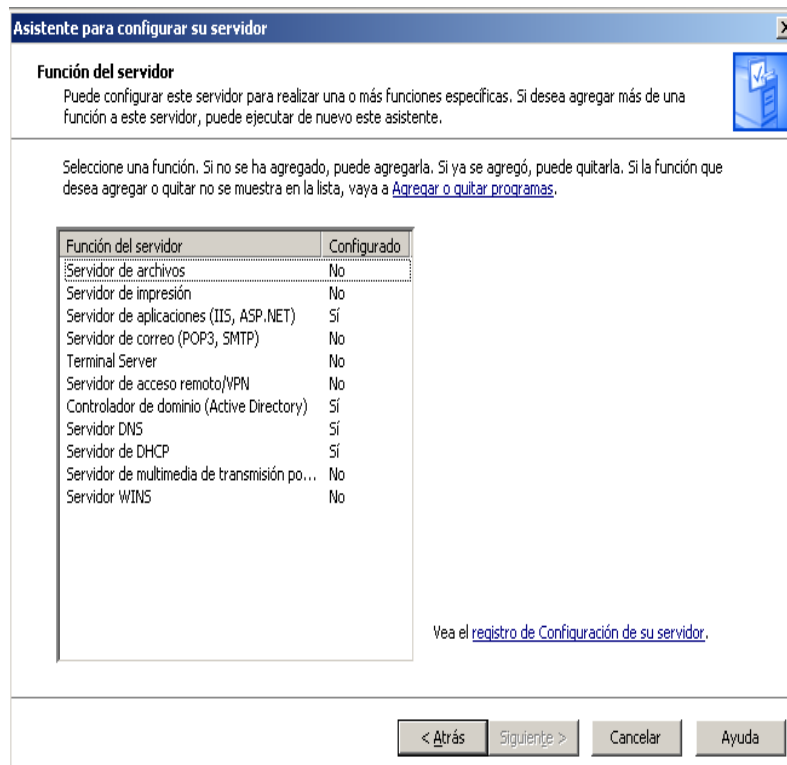


Gráfico 111. Funciones del servidor

5. Si los servicios no están agregados los servicios, seleccionamos Inicio, Herramientas administrativas, Administre su servidor.

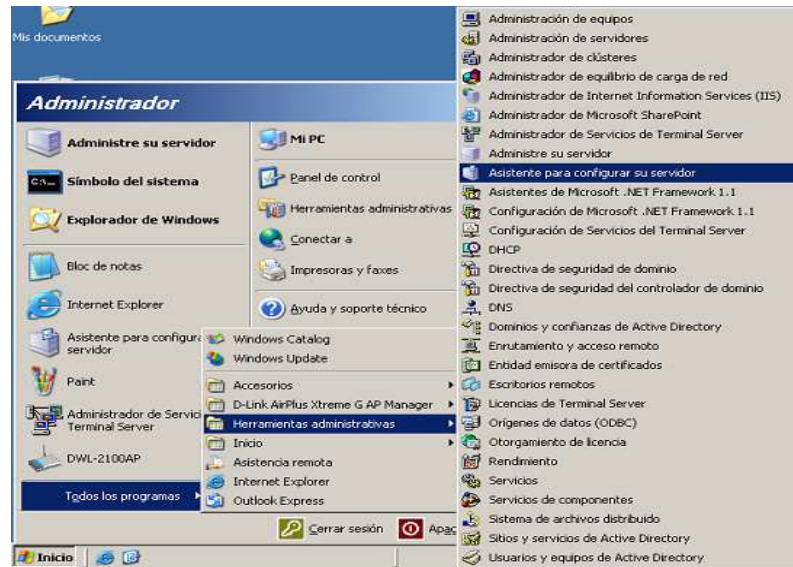


Gráfico112. Inicio, Herramientas administrativas, Administre su servidor

6. Aparece la siguiente pantalla, en la que vamos agregando uno a uno los servicios como Active Directory, DNS, Internet Information Server y DHCP.



Gráfico 113. Administre su servidor.

7. El DHCP es un servicio en donde podemos establecer seguridades a nuestra red mediante direcciones IP, las mismas que pueden ser dinámicas o estáticas. Para la configuración de DHCP seguimos los siguientes pasos:



Gráfico 114. Nombre de ámbito para acceder a la red

8. Una vez ingresado el ámbito, damos click en siguiente apareciéndonos la ventana Intervalo de direcciones IP, especificamos la clase de IP a utilizar.

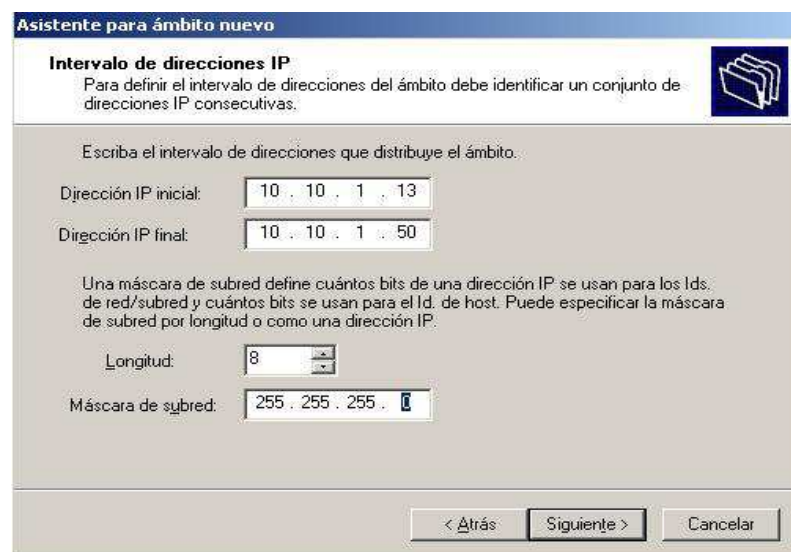


Gráfico 115. Intervalo de direcciones IP

9. En esta ventana podemos excluir a IPs que no van hacer parte del dominio la misma que puede ser opcional.



Gráfico 116. Exclusiones de direcciones IP

10. Se establece la duración de la conexión (días, horas, minutos).

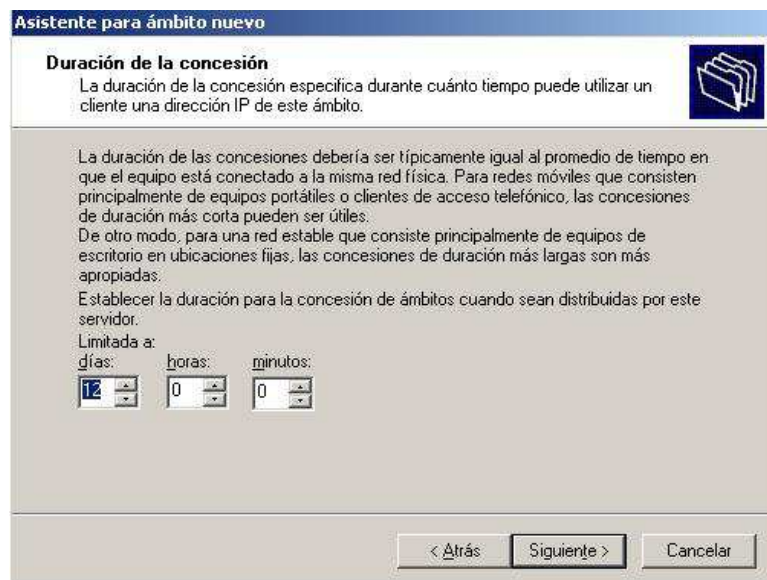


Gráfico 117. Duración de conexión.

11. En la siguiente ventana especificamos el dominio, el nombre del servidor damos click en Resolver y nos aparece la IP finalmente agregamos.



Gráfico 118. Nombre de dominio y servidores DNS.

12. Una vez concluido la configuración de DHCP aparece la Finalización.



Gráfico 119. Finalización DHCP.

13. Una vez agregado los servicios, damos click en Inicio, Herramientas administrativas y podemos visualizar como se ve en la figura los servicios marcados.

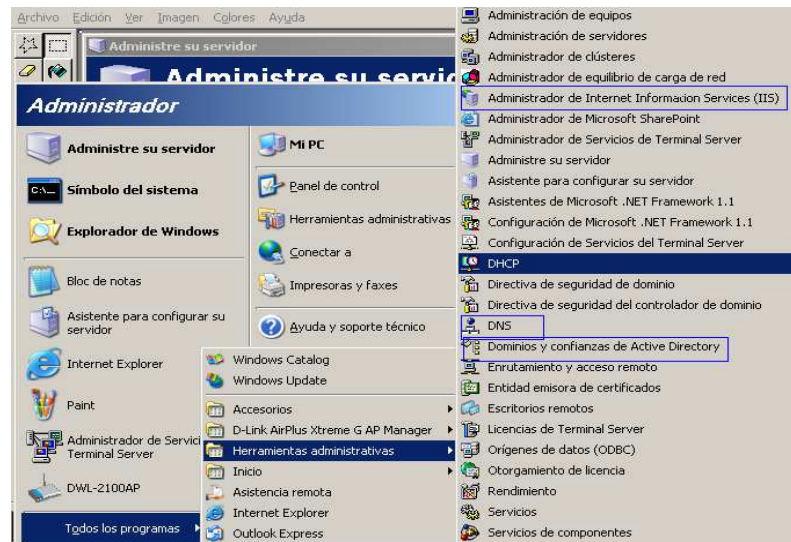


Gráfico 120. Servicios en funcionamiento

14. Luego seleccionamos administrador de Internet Information Server en donde procedemos configurar la página Web, haciendo referencia al nombre del equipo que en este caso es **Oficina**, damos click en el servidor, que nos presenta varias carpetas escogemos Sitios Web.

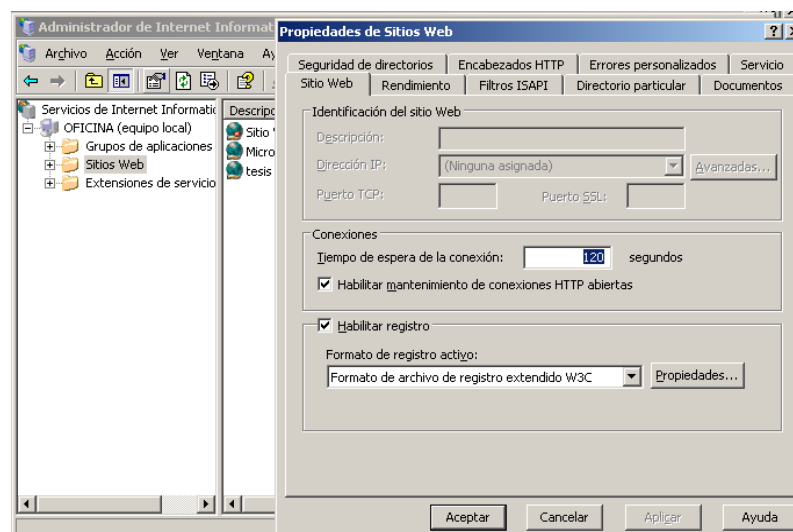


Gráfico 121. Sitios Web y sus Propiedades

15. Seleccionamos propiedades del Sitio Web, click en documentos y nos presenta una lista en la que seleccionamos el nombre de nuestra página Web.

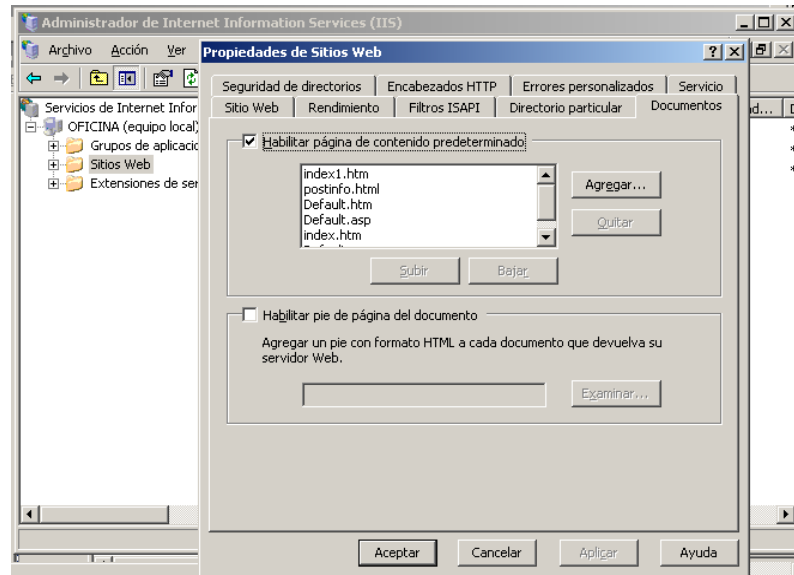


Gráfico 122. Selección de la Página Web.

16. Posteriormente, accedemos al Internet y comprobamos si podemos ver la página escribiendo la dirección IP del servidor, el nombre del equipo, el nombre de página predeterminada.

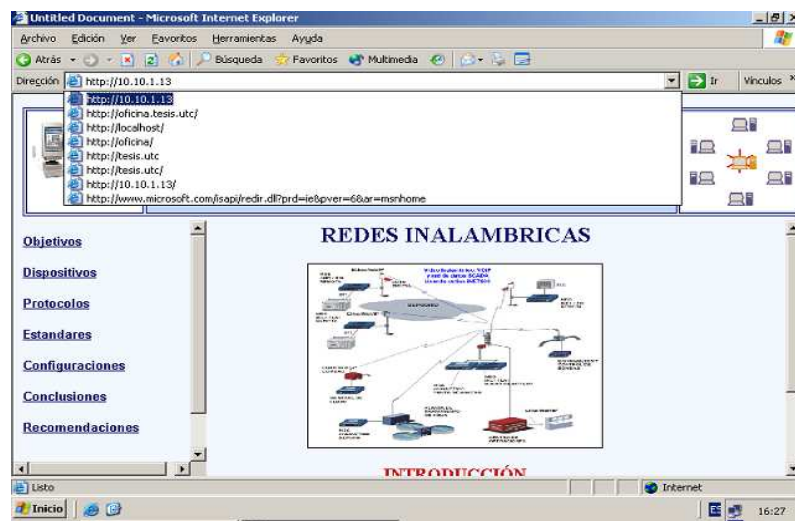


Gráfico 123. Visualización de la Página Web.

## **CAPITULO IV**

### **CONCLUSIONES, RECOMENDACIONES**

#### **4.1. VERIFICACIÓN DE HIPOTESIS.**

La hipótesis planteada en el plan de tesis ha sido comprobada de acuerdo al análisis, encuestas, factibilidad, y la demostración de la red inalámbrica para la Universidad Técnica de Cotopaxi, de tal manera que la hipótesis planteada es verdadera.

Con la demostración de la funcionalidad de Redes Inalámbricas se optimiza recursos tales como tiempo, dinero, espacio, además brinda servicios de transmisión de datos dando una comunicación rápida con otras PCs y mejorando la estética en la Universidad Técnica de Cotopaxi.

#### **4.2. VERIFICACIÓN DE OBJETIVOS**

El problema que existe en el alma mater de Cotopaxi, en cuanto a la infraestructura de la red de datos existente la cual no brinda las seguridades que exponen en los estándares de cableado estructurado se resolverá si en la misma pone en marcha el funcionamiento una wireless “red inalámbrica de datos”, lo cual permite optimizar los recursos existentes en dicha Institución.

Los objetivos han sido cumplidos en su totalidad, lo que permitió el análisis, diseño y propuesta de una Red Inalámbrica en la Universidad Técnica de Cotopaxi.

### 4.3. CONCLUSIONES

- Antes de instalar una red inalámbrica es preciso realizar un análisis previo el lugar donde se va a instalar la red de manera que se pueda determinar la ubicación correcta de los equipos para su óptimo funcionamiento.
- El presente trabajo investigativo cumplió los objetivos propuestos tales como realizar un Estudio Factibilidad y la demostración de la funcionalidad de una red inalámbrica para la Universidad Técnica de Cotopaxi.
- Se comprueba la hipótesis planteada en el anteproyecto dándonos como verdadera, ya que con la práctica realizada se optimiza recursos.
- Para el desarrollo del proyecto se utilizó los métodos inductivo (particular - general), deductivo (general – particular) y observación directa.
- Las técnicas realizadas para el Estudio de Factibilidad fueron las encuestas ya que permitió la recopilación de información que nos permita conocer la necesidad de implementar la tecnología Wireless en la Universidad.
- Los equipos utilizados en el prototipo y en la propuesta como tarjetas inalámbricas y Access Point es en base al rendimiento que posee cada uno de ellos para lo cual elegimos una banda radio de frecuencia 2.4 GHz ya que es una banda destinada a uso libre y esta dentro de la zona de las

microondas y porque la mayor parte de dispositivos inalámbricos viene incorporados esta frecuencia.

- También se cumplió con las normas internacionales de estándares de redes inalámbricas como es el 802.11b y 802.11g para nuestra demostración ya que estos estándares son compatibles con los demás, y ofrecen garantías y confiabilidad en la transmisión de información ya que se transmite a una velocidad de 11Mbps.
- Desarrollado el Estudio de Factibilidad se obtiene información de los requisitos como son ubicación de equipos (visibilidad entre ellos), dispositivos acordes a la institución en que se vaya implementar esta tecnología en este caso en la Universidad Técnica de Cotopaxi.
- El dispositivo Access Point debe estar en la zona radio frecuencia para tener un enlace con las tarjetas inalámbricas, no se puede aislar a una distancia exagerada ya que ellos funcionan a una distancia de 100 metros a la redonda.
- Se instalaron puntos de acceso en áreas estratégicas para asegurar una cobertura de servicio en la mayor parte de áreas geográficas de la Universidad.
- Las medidas de seguridad que ayudan a proteger el tráfico de la red incluyendo el acceso a la red y a la protección de datos se lo pudo hacer

con la autenticación y encriptación, para nuestro estudio utilizamos el SSID y el WEP.

- Realizamos una Intranet Inalámbrica con un servidor de Windows Server 2003 el mismo que permitió configurar servicios tales como DHCP, DNS, Internet Information Server y Active Directory, dichos servicios nos permitieron dar dominios, direcciones IP las mismas que pueden ser dinámicas o estáticas de esta manera poder visualizar una página Web de una manera segura.
- Para simplificar la instalación, la detección de problemas y para obtener el máximo desempeño de los componentes de WIFI deben ser del mismo tipo de tecnología, preferiblemente del mismo fabricante.
- Una red inalámbrica puede ser utilizada por cualquier dispositivo (Laptop, PDA, etc), que cuente con tarjeta de red compatible con el estándar 802.11b WiFi para acceder a servicios.
- Estudiantes, Docentes y Administrativos contarán con el acceso a la red en cualquier lugar de la Universidad Técnica de Cotopaxi.
- En la Universidad Técnica de Cotopaxi existe una red cableada, por lo que para una implementación de este sistema de red inalámbrico no reemplaza al sistema alámbrico actual, solo sirve de un complemento como medio de

conexión alternativa y como extensión de servicios de la red de datos a la comunidad académica y administrativa.

#### **4.4. RECOMENDACIONES**

- Se recomienda tomar en cuenta el espacio físico, interferencias y la ubicación de los dispositivos a instalar como se realizó en los planos.
- Si es factible implementar una red inalámbrica en la Universidad Técnica de Cotopaxi por lo que se recomienda implementar a futuro.
- Para el desarrollo de futuros proyectos se recomienda tomar en cuenta los conceptos de hipótesis, técnicas, y métodos ya que estos permiten encaminar a la culminación del proyecto.
- Se recomienda utilizar equipos con las mismas características ya que de esa manera se aprovechará todos los beneficios (velocidad y seguridad) de los mismos.
- Tomar en cuenta para implementación los estándares más adecuados según los requerimientos que tenga el lugar donde vaya a ser instalado sin dejar a un lado la compatibilidad con los dispositivos a utilizar.
- Para conseguir el mejor alcance de su Access Point hay que considerar seriamente la ubicación del mismo. El desempeño inalámbrico baja

drásticamente cuando se reduce la fuerza de señal ud. debe ubicar su Access Point en un lugar donde todas sus computadoras reciban una señal potente.

- Para probar la cobertura haga una instalación preliminar de su Access Point entonces conecte una portátil inalámbrica y camine alrededor de la oficina para probar la fuerza de la señal en el software de administración del adaptador inalámbrico.
- Asegúrese que la tarjeta adaptadora y el enrutador estén configurados con el mismo SSID, el mismo modo cifrado (WEP, WAP) y clave cifrado, un error en cualquiera de estos parámetros impedirá entrar en la red y dando seguridad para que no puedan acceder a la misma .
- Debe tener un sistema operativo acorde con la exigencia a la que va estar sometida la Red Inalámbrica para la eficiencia en la transmisión de información.
- Las comunicaciones inalámbricas en el futuro nos pueden ahorrar muchas configuraciones y lo que es más importante dinero y tiempo. No tenemos que disponer de complicadas infraestructuras cableadas para transmisión de datos ya que la tecnología inalámbrica es muy fiable y cada vez rápida alcanzando mayores distancias.

## **BIBLIOGRAFIA**

### **BIBLIOGRAFIA CITADA.**

- Applying known techniques to WEP Keys , Tim Newsham,  
Cracking WEP Keys
- Douglas Comer, Redes Globales de Información con Internet y  
TCP/IP, México, Prentice-Hall, 1999
- GIBBS, Mark .redes para todos. Editorial Prentice Hall  
Hispanoamericana, S.A. Naucalpan de Juárez, México, 1995
- <http://computerworld.com.ec> /anónimo / 2006
- <http://documentos.shellsec.net/otros/SeguridadWireless.pdf>  
.Seguridad en redes inalámbricas.
- <http://neutron.ing.ucv.ve/revista-e/No8/JLPerez%5CWAP.HTM>
- <http://www.Mouse.cl/2005/productos/12/06.index.asp>
- <http://www.conocimientosweb.net/portal/article246.html>,  
Anónimo, 1999
- <http://www.e-advento.com/soluciones/wlan.htm> , Anónimo, 2003
- <http://www.intel.com/es/home/trends/wireless/nw/transition.htm>,  
anónimo, 2000
- José A. Carballar Falcón, WI-FI. CÓMO CONSTRUIR UNA  
RED INALÁMBRICA, 2ª EDICIÓN
- Reid Neil & Seide Ron, MANUAL DE REDES  
INALÁMBRICAS, Editorial McGraw-Hill.
- [http://www.wl0.org/~sjmudd/wireless/network-  
structure/english/article.html](http://www.wl0.org/~sjmudd/wireless/network-structure/english/article.html), Anónimo, 2002

- Rob Flickenger, WIRELESS. LOS MEJORES TRUCOS, (Ed. Anaya Multimedia)
- www.ieee.com, 2005
- www.ProyectoExtremaduraWireless.htm,2005
- www.tcpi.com

## **BIBLIOGRAFIA CONSULTADA**

### **Libros**

- Abad Domingo, Alfredo, Redes de área local / Alfredo Abad Domingo, Madrid: McGraw-Hill, c1997.
- Cobb, Stephen, Manual de seguridad para PC y redes locales / Stephen Cobb, Madrid: McGraw-Hill, c1994.
- Comer, Douglas, TCP/IP: redes globales de información con internet / Douglas Comer, México: Prentice Hall, c1996.
- COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. Editorial Prentice Hall Hispanoamericana, S.A Naucalpan de Juárez, México,1996
- Dyson, Peter, Diccionario de redes / Peter Dyson Bogotá: McGraw-Hill, c1997.
- Ford, Merilee, Tecnologías de interconectividad de redes: Una referencia concisa y esencial para todo profesional en redes / Ford,
- GIBBS, Mark .redes para todos. Editorial Prentice Hall Hispanoamericana, S.A. Naucalpan de Juárez, México,1995

- Gibbs, Mark, Redes para todos / Mark Gibbs. -- 2ª. Ed, México: Prentice-Hall.
- Rodríguez, Jorge, Introducción a las redes de áreas local / Jorge Rodríguez, México: McGraw-Hill, c1996.
- Tanenbaum, Andrew S., Redes de ordenadores / Andrew S.
- Tanenbaum. -- 2ª. Ed, México: Prentice- Hall, 1991.

### **Revistas**

- Colección de Revistas de Redes Inalámbricas (PCWORLD),Ecuador, enero del 2005
- Colección de Revistas de Redes Inalámbricas (PC-PLUS), España. Septiembre 2004
- Colección de Revistas de Redes Inalámbricas (PCMAGAZINE), Ecuador, mayo del 2005.
- Colección de Revistas de Redes Inalámbricas (COMPUTER WORLD)  
Ecuador, febrero del 2006.

### **BIBLIOGRAFÍA DE INTERNET**

#### **Redes inalámbricas, Aplicaciones y Estándares Para Redes Inalámbricas.**

- <http://www.wl0.org/~sjmudd/wireless/network-structure/english/article.html>, Anónimo, 2002
- [http://lat.3com.com/lat/technology/technical\\_papers/wireless.htm](http://lat.3com.com/lat/technology/technical_papers/wireless.htm)  
l Anónimo, 2000
- <http://www.madridwireless.net>, Anónimo, 2003

- <http://www.wapforum.org/what/technical.htm> Anónimo, 2002
- [http://www.wirelessmundi.com/Dealer\\_02.shtml](http://www.wirelessmundi.com/Dealer_02.shtml), Anónimo, 2003
- <http://www.cisco.com/warp/public/44/jump/wireless.shtml>,  
Anónimo, 2003
- <http://www.monografias.com/trabajos14/wi-fi/wi-fi.shtml>,  
Anónimo, 2003
- <http://www.hispazone.com/conttuto.asp?IdTutorial=54>
- [http://www.consulintel.es/html/Tutoriales/Lantronix/guia\\_et\\_p1.html](http://www.consulintel.es/html/Tutoriales/Lantronix/guia_et_p1.html)

### **Antenas Inalámbricas**

- <http://dlink/wiFiAntenas.htm>
- <http://www.acri.ws/antenas.cfm>
- <http://34t.com/Unique/wiFiAntenas.asp>
- <http://www.servinet-tecnologias.com/antenasomnidireccionales.htm>
- [http://www.dlinkla.com/home/productos/descrip\\_c.jsp?id=3&sm=4](http://www.dlinkla.com/home/productos/descrip_c.jsp?id=3&sm=4)
- <http://www.sincables.net/modules.php?name=News&file=article&sid=202>
- <http://www.todoantenas.cl/antenas-parabolicas.html>

### **Teoría Inalámbrica.**

- [http://lat.3com.com/lat/technology/technical\\_papers/wireless.htm](http://lat.3com.com/lat/technology/technical_papers/wireless.htm)  
l Anónimo, 2000
- <http://www.wapforum.org/what/technical.htm> Anónimo, 2002
- <http://wifiepcc.unex.es/modules.php?op=modload&name=Textos&file=index&serid=38>.

- [http://www.arturosoria.com/eprofecias/art/wireless\\_seguridad.as](http://www.arturosoria.com/eprofecias/art/wireless_seguridad.as)
- <http://www.spitzer.caltech.edu/espanol/edu/ir/discovery.html>
- <http://www.zonablutooth.com/documentacion.htm>
- <http://lmds.donde-es.net/internet/index.htm>
- [http://es.wikipedia.org/wiki/IEEE\\_802.16](http://es.wikipedia.org/wiki/IEEE_802.16)
- <http://blogwimax.com/>
- <http://www.wimaxforum.org/home>
- [http://www.radioptica.com/Radio/caracteristicas\\_estandar\\_wimax.asp](http://www.radioptica.com/Radio/caracteristicas_estandar_wimax.asp)
- <http://www.adslayuda.com/index.php>

#### **Información Frecuencias**

- [www.conatel.gov.ec](http://www.conatel.gov.ec)
- <http://www.zonablutooth.com/documentacion.htm>
- [www.microsoft.com/help/wifi.html](http://www.microsoft.com/help/wifi.html)

#### **REDES DE BANDA ANCHA:**

- <http://www.ts.es/doc/area/produccion/ral/BANDA.HTM> 8 de enero del 2002

#### **Laboratorio de Redes:**

- <http://ccdis.dis.ulpgc.es/ccdis/laboratorios/redes.html>

#### **Interconexión :**

- <http://www.ts.es/doc/area/produccion/ral/CABLE.HTM>