



Unidad 05: Configuración de Estaciones

Autores: Tomas B. Krag <t@wire.less.dk> (Linux), Bruno Roger, ESMT (Windows) ,IT +46 .
Basado en el trabajo original de: Onno W. Purbo and Sebastian Buettrich. Clientes Inalámbricos.
Traducido por Colnodo. Editado por: Alberto Escudero Pascual , IT + 46.

Tabla de contenido

| | |
|--|----|
| 1. Sobre este documento..... | 3 |
| 1.1 Información sobre propiedad intelectual..... | 3 |
| 1.2 Grados de dificultad..... | 3 |
| 1.3 Información sobre los iconos..... | 3 |
| 2. Introducción..... | 3 |
| 3. Configuración de puntos de acceso..... | 4 |
| 3.1 Antes de comenzar..... | 4 |
| 3.2 Instalando el hardware y el firmware..... | 5 |
| 3.2.1 Instalación física..... | 5 |
| 3.2.2 Actualizando el firmware..... | 7 |
| 3.2.3 Conectando su computadora al dispositivo | 7 |
| 3.3 Configuración del hardware siguiendo el modelo OSI..... | 8 |
| 3.3.1 La capa física..... | 9 |
| 3.3.1.1 Número de canal..... | 9 |
| 3.3.1.2. Potencia de transmisión..... | 9 |
| 3.3.1.3 Tasa o velocidad de transmisión | 10 |
| 3.3.2 La capa de enlace..... | 10 |
| 3.3.2.1 Modos de operación..... | 10 |
| 3.3.2.2 SSID (Service Set Identifier)..... | 11 |
| 3.3.2.3 Control de acceso al medio | 12 |
| 3.3.2.6 Restricción de acceso a través de autenticación..... | 15 |
| 3.3.3 La capa de red..... | 17 |
| 3.3.4 Capa de aplicación..... | 17 |
| 4. Instalación de clientes: Parte A - Linux..... | 18 |
| 4.1 Seleccionando el hardware inalámbrico..... | 18 |

| | |
|--|----|
| 4.1.1 Tipos de hardware..... | 18 |
| 4.1.2 Chipsets inalámbricos..... | 19 |
| 4.1.3 Hardware soportado..... | 20 |
| 4.1.4 Hardware no soportado..... | 20 |
| 4.1.5 Diferencias entre drivers..... | 21 |
| 4.2 Instalando el dispositivo inalámbrico..... | 21 |
| 4.2.1 Preparando la instalación..... | 22 |
| 4.2.2 Insertando la tarjeta..... | 22 |
| 4.2.3 Identificando el chipset..... | 23 |
| 4.3 Configurando el dispositivo inalámbrico..... | 28 |
| 4.3.1 Ejemplo 1: Ubuntu con Gnome..... | 28 |
| 5. Parte B: Instalación de clientes Windows XP..... | 30 |
| 5.1 Seleccionando el hardware inalámbrico..... | 30 |
| 5.2 Instalación del dispositivo inalámbrico..... | 31 |
| 5.3 Configuración del dispositivo inalámbrico..... | 31 |
| 5.3.1 Paso 1: Seleccione la red..... | 32 |
| 5.3.2 Paso 2: configuración IP | 35 |
| 6. Conclusiones..... | 36 |
| 7. Ejercicios..... | 37 |
| 7.1 Configuración de puntos de acceso..... | 37 |
| 8. Recursos Adicionales..... | 39 |
| 8.1 Puntos de acceso..... | 39 |
| 8.1.1 En línea..... | 39 |
| 8.1.2 Libros/artículos..... | 40 |
| 8.2 Parte A: Instalación de clientes - Linux..... | 40 |
| 8.2.1 En línea..... | 40 |
| General..... | 40 |
| Drivers inalámbricos..... | 40 |
| Software..... | 41 |
| 8.2.2 Libros/artículos..... | 43 |
| 8.3 Parte B: Instalación de clientes - Windows..... | 43 |
| 8.3.1 En línea..... | 43 |
| 8.3.2 Libros/artículos..... | 44 |
| 9. Declaración de Derechos de Propiedad Intelectual..... | 45 |

1. Sobre este documento

Este material es parte del paquete de materiales del proyecto TRICALCAR. Para información sobre TRICALCAR consulte el módulo de introducción de estos materiales, o www.wilac.net/tricalcar/. Este material fue traducido del inglés de los materiales desarrollados para el proyecto "Capacity Building for Community Wireless Connectivity in Africa" de APC <<http://www.apc.org/wireless/>>. El material fue actualizado y adaptado para el contexto de América Latina.

1.1 Información sobre propiedad intelectual






Esta unidad temática se ha hecho disponible bajo los términos de la licencia **Atribución-No Comercial-Licenciamiento Recíproco 3.0 Genérica**. Para ver los términos completos de esta licencia: http://creativecommons.org/licenses/by-nc-sa/3.0/deed.es_MX

1.2 Grados de dificultad

El grado de dificultad de esta unidad es "básico" con algunas partes adicionales consideradas "avanzadas". Todas las secciones "avanzadas" están dentro de un recuadro de fondo gris, para indicarle al lector el grado de dificultad del contenido.

1.3 Información sobre los iconos

En los contenidos encontraremos 5 tipos de iconos, cuyo significado se describe a continuación:

| Concepto teórico clave | Recomendación práctica importante | Ejercicio | Propiedad intelectual | Propiedad intelectual |
|---|---|---|---|---|
|  |  |  |  |  |

2. Introducción

En esta unidad se aborda la configuración de estaciones inalámbricas. Denominamos así a los equipos configurados para tener acceso a una red inalámbrica. Dichos equipos pueden estar configurados como puntos de acceso o como clientes de la red inalámbrica. Esta misma diferenciación es considerada para estructurar los contenidos de esta unidad.

En la primera parte se provee una metodología general para instalar y configurar puntos de acceso y enrutadores inalámbricos. En lugar de enfocarnos en “qué botón presionar”, nuestro propósito es brindar la comprensión de *qué* implica cada una de las opciones y *cuándo* y *por qué* se requiere cierta configuración. La metodología sigue el modelo **OSI**, enfocándose principalmente en la capa física y la de enlace.

Adicionalmente, en la Práctica 1 se provee el proceso paso a paso para la configuración de un punto de acceso a través de una interfaz gráfica en web.

La segunda parte de la unidad trata sobre la instalación de clientes inalámbricos para redes IEEE 802.11. Consta de dos partes independientes de acuerdo con el sistema operativo utilizado. La parte **A** cubre aspectos referentes a Linux, mientras que la parte **B** describe aspectos referentes a Microsoft Windows.

Independientemente de la plataforma seleccionada, el proceso de instalación de los clientes se puede describir en 3 fases diferentes: (1) Selección del hardware inalámbrico, (2) instalación y (3) configuración.

Este documento hace énfasis en diferentes asuntos dependiendo del sistema operativo, como resultado, en la sección sobre clientes Linux (Parte A) nos enfocamos en las dos primeras fases, mientras que al discutir sobre Windows (Parte B), nos enfocamos principalmente en problemas de configuración, pues la selección de hardware y su instalación no “debería” presentar problemas.

Si usted está interesado en Linux, no deje de consultar la sección de Recursos adicionales que incluye muchos enlaces útiles.

3. Configuración de puntos de acceso

3.1 Antes de comenzar

Independientemente de cuál hardware está usando o cuál es la topología de red que desea utilizar, hay un conjunto de pautas generales que siempre debería tener en mente:



1. Lea el manual del punto de acceso y conozca el dispositivo y su configuración por defecto
2. Considere las condiciones del lugar físico de la instalación (acceso a fuente de alimentación, antenas, temperatura, humedad, etc.). Vea “Estudio del sitio” para mayor información.



3. Antes de comenzar, planee la red (TCP/IP) y realice un dibujo de la topología. La planeación incluye el conocimiento de la configuración del proveedor de servicios de internet (ISP) o de la red de área local (LAN) incluyendo DNS, etc.
4. Asegúrese de tener toda la documentación y material (físicamente, no sólo en línea), de manera que pueda trabajar aún si está desconectado durante el proceso.
5. Tome nota sobre cada paso que realice durante el proceso de configuración, especialmente cuando cambie direcciones IP, opciones de red y contraseñas.
6. Asegúrese de tener todo el hardware necesario (computador de escritorio o portátil con interfaces inalámbrica y de Ethernet)
7. Asegúrese de tener todo el software necesario, como:
 - Herramientas TCP/IP (ping, route)
 - Software específico del vendedor (actualizaciones de firmware, manejadores *-drivers-*, etc.)
 - Software para medir/detectar señales inalámbricas (Kismet, Netstumbler)

3.2 Instalando el hardware y el firmware

El primer paso del proceso de configuración es instalar el hardware, conectar el punto de acceso a su computador y (opcionalmente) actualizar el firmware. Esta sección le da una visión general de la capa física de un punto de acceso y de cómo instalar el dispositivo físicamente.

3.2.1 Instalación física

Típicamente existen dos diferentes partes de los puntos de acceso a las que debería poner atención:

1. LEDs de estado (diodos emisores de luz).¹
2. Interfaces de Radio y de Ethernet.

Normalmente, en la parte superior del punto de acceso encontrará un conjunto de LEDs que indican el estado del dispositivo. Típicamente estos LEDs indican con luz intermitente o sostenida (verde o roja) los siguientes parámetros:

1. Alimentación del punto de acceso.
2. Puertos activos.

1. LED= Diodo emisor de luz

3. Errores internos.
4. Conexión Ethernet (conexión a la red).

Los LEDs pueden darle información muy valiosa cuando localiza los problemas de su red. Le recomendamos estudiar cuidadosamente el significado de cada diodo en el manual de referencia de su punto de acceso antes de iniciar el proceso de configuración.

Las interfaces básicas de un punto de acceso inalámbrico son:



1. **Ethernet:** llamada a menudo WAN (conexión a una red de área amplia - WAN) o LAN (conexión a una red de área local - LAN). Un punto de acceso “transparente” (puente inalámbrico) tiene únicamente un puerto Ethernet. Un punto de acceso con más de un puerto Ethernet es normalmente un enrutador/pasarela(gateway) inalámbrico.
2. **Radio/Antena(s):** conexión inalámbrica a clientes.

Los dispositivos inalámbricos más avanzados pueden estar equipados con dos o más interfaces inalámbricas (dos o más radios) .

En uno de los lados posteriores, generalmente podemos encontrar las interfaces Ethernet junto a algunas otras funcionalidades:

1. Entrada de alimentación (12V, 5 V o 3.5 V DC): conectada a una fuente de alimentación DC.
2. Botón de restablecimiento (Reset): Usado para restablecer la configuración por defecto.
3. Conectores LAN (RJ45): para conectar a una LAN.
4. Puerto WAN (RJ45): permite conectar a DSL, cable modem o cualquier otra interfaz que utilice el proveedor de servicios de Internet para conexión a una red.

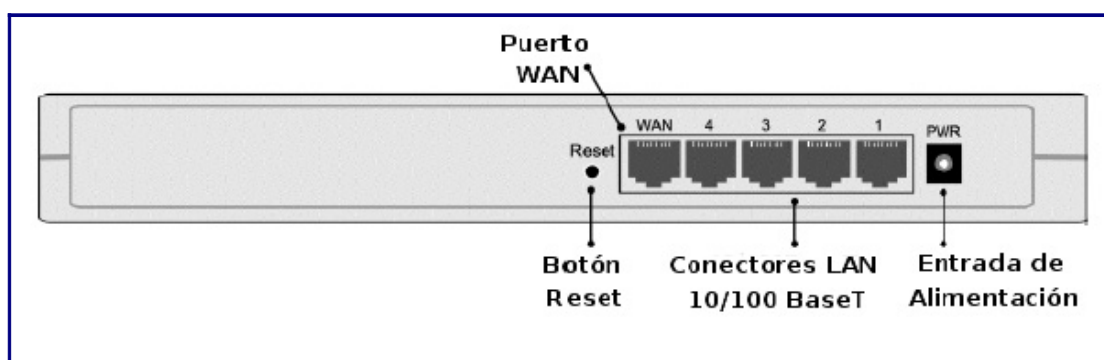


Figura 1: Una configuración típica de conectores y adaptadores en la parte posterior de un punto de acceso (enrutador inalámbrico).

Además, un punto de acceso está equipado con una o un par de antenas que pueden estar dentro del punto de acceso o fijadas a la cubierta. Las antenas externas normalmente se pueden orientar para concordar con una implementación específica.

3.2.2 Actualizando el firmware

El microcódigo o firmware es un software que ha sido escrito dentro de la ROM (memoria de sólo lectura) y es una parte permanente del dispositivo. Podríamos decir que el firmware es un hardware.

El firmware permanecerá en la memoria ROM después de que se haya apagado el dispositivo. Hay que utilizar un procedimiento especial para modificar el firmware y tener cuidado porque una interrupción de energía que ocurra cuando se está realizando el procedimiento puede causar daños irreparables. El programa BIOS que controla el inicio de todas las computadoras es también un “firmware”.


Los fabricantes actualizan el firmware de sus productos continuamente para ofrecer la última configuración y corregir problemas reportados. Actualice siempre el punto de acceso con el último firmware “estable” antes de empezar a configurarlo y revise periódicamente las actualizaciones.

3.2.3 Conectando su computadora al dispositivo

Para configurar el punto de acceso, debe conectar éste a su computadora de escritorio o portátil. Puede hacer esta conexión por cable o de forma inalámbrica.

Es muy recomendable comenzar la configuración usando conexión por cable y, una vez que la configuración básica esté lista y usted sienta más seguridad con el proceso de configuración, cambiar a conexión inalámbrica.

La conexión por cable puede realizarse usando:



1. Cable Ethernet por HTTP.
2. Ethernet usando software específico del fabricante basado en SNMP.
3. Puerto serial (null modem) usando HyperTerminal u otro programa de comunicación serial (si el punto de acceso tiene un puerto serial).

Entre las tres opciones, la más común es conectarse a través de un cable Ethernet usando HTTP. Esta forma de configuración del punto de acceso es independiente de la plataforma y sólo requiere un navegador web. Tenga en cuenta que la interfaz de usuario (UI) lucirá diferente de fabricante en fabricante y de modelo en modelo. Ellos cambian constantemente y usted nunca encontrará dos del

mismo tipo. Sin embargo, todas ellas siempre contienen los mismos elementos básicos. Sepa también que no todos los fabricantes se refieren a los mismos “conceptos” con las mismas palabras.

A continuación se introducen los conceptos básicos:

Para lograr comunicarse con el punto de acceso:

- El cliente debe pertenecer a la misma subred IP.
- Busque en el manual de referencia la dirección IP por defecto del punto de acceso y
- Cambie la dirección IP de su computador como corresponda.
- Después de esto, abra una ventana del navegador y proceda con la configuración a través de la interfaz web.

También existen utilidades “privativas” (*Proprietary*), es decir, exclusivas de un fabricante particular, para la configuración de puntos de acceso que podrá instalar en su computador con el fin de montar un dispositivo inalámbrico. Ellas se basan normalmente en un protocolo conocido como SNMP. (*Ver la unidad de Solución de problemas*).

La tercera opción, usando un cable serial, se puede considerar como un plan de reserva cuando las cosas han salido mal. Esta opción implica que usted deba tener acceso físico al dispositivo y por lo tanto no puede ser hecho por “cualquier persona”. El cable serial es generalmente el mecanismo utilizado para reconfigurar el punto de acceso cuando se ha olvidado la contraseña y no se desea restablecer la configuración por defecto. Normalmente, usted puede acceder al punto de acceso a través de la interfaz serial sin necesidad de conocer la contraseña.

3.3 Configuración del hardware siguiendo el modelo OSI

A primera vista, la configuración de un punto de acceso podría lucir muy compleja, juzgando por el grosor del manual de referencia. Normalmente, una gran cantidad de opciones están disponibles y puede ser difícil distinguir las opciones básicas de las de modo avanzado.

Para un punto de acceso “transparente”² solo se requiere ajustar dos opciones:

1. Nombre o SSID (Service Set Identifier -Identificador de la red-).
2. Número de canal.

Sin embargo, a menudo es conveniente fijar otros parámetros. Muchos parámetros opcionales se refieren a seguridad en términos de la cifrado y restricciones de acceso, los cuales son importantes para evitar intrusos en su red.

A continuación se da una aproximación teórica a la configuración del hardware siguiendo el modelo **OSI** y haciendo énfasis en qué hace cada ajuste y por qué es necesario. Creemos seriamente que

2. Por “transparente” nos referimos a un punto de acceso que actúa como un puente inalámbrico que NO tiene capacidades de enrutamiento. El punto de acceso no provee NAT, DHCP etc.

entender, **POR QUÉ** es importante cierta configuración y **QUÉ** implica cierto parámetro, es esencial para construir redes inalámbricas de alta calidad.



Como sabemos hasta ahora, la conexión de redes inalámbricas se restringe a las dos primeras capas del modelo **OSI**, es decir los niveles **físico** y de **enlace**. Cuando un punto de acceso es un dispositivo inalámbrico, nada más que un “concentrador inalámbrico”, todos los ajustes sobre las opciones inalámbricas afectan las primeras dos capas del modelo OSI.

Si el punto de acceso soporta enrutamiento y enmascaramiento (NAT), entonces también incluirá opciones relativas a la capa 3 del modelo OSI: capa de **red**.

3.3.1 La capa física

Los parámetros de un punto de acceso que afectan la capa física son:

3.3.1.1 Número de canal

Cuando fija el canal de un punto de acceso, usted determina la gama de frecuencias (GHz) en que operará el dispositivo. Antes de fijar el canal, usted debería escanear el rango de frecuencias con un software como “Netstumbler” u otro similar, para evitar usar el mismo canal de otras redes (si están presentes). Haciendo esto se minimiza la probabilidad de interferencia.



- Para redes IEEE 802.11b, use los canales 1, 6 u 11 para asegurar suficiente separación de frecuencias y evitar conflictos.
- Para redes 802.11a no hay riesgo de que los canales se traslapen, sólo debe asegurar que los puntos de acceso IEEE 802.11a que se encuentren alrededor estén operando en canales diferentes al que usted ha seleccionado.

Algunos puntos de acceso nuevos tienen una característica que define automáticamente el canal basado en la frecuencia ociosa escaneando el espectro y encontrando cuáles ya están en uso.

3.3.1.2. Potencia de transmisión



A mayor potencia de transmisión, el punto de acceso tendrá un mayor rango de cobertura. Si desea alcanzar la mayor cobertura posible, la potencia de transmisión debería fijarse en el valor más alto

Para muchos países el máximo límite legal es 100mW (20dBm), mientras en otros (EEUU, Canadá) el límite es 1W. Sin embargo, debe evitarse usar más potencia de la necesaria pues aumenta la probabilidad de interferir con otros usuarios.

No todos los puntos de acceso le permitirán fijar la potencia de salida. Note que la potencia máxima debe ser calculada considerando la ganancia de la antena que está utilizando. La suma de la potencia de salida en dBm y la ganancia de la antena en dBi es lo que se conoce como PIRE (Potencia Isotrópica Radiada Equivalente, o en inglés EIRP (*Equivalent Isotropic Radiated Power*) y su valor máximo también está limitado por disposiciones legales (Vea Cálculo de Radio Enlaces).



Tome en cuenta también que a veces es posible mediante software aumentar la potencia de salida de un dispositivo por encima del valor especificado por el fabricante, pero generalmente esto deteriora el espectro transmitido y aumenta la interferencia producida en canales adyacentes, por lo que no es aconsejable.

Si en cambio, se busca incrementar la capacidad total de la red inalámbrica adicionando puntos de acceso ubicados cerca uno de otro, entonces la potencia debería ser fijada en el valor más bajo posible, esto para disminuir el solapamiento y la interferencia potencial. Además usted deberá disponer adecuadamente las antenas para minimizar la interferencia entre puntos de acceso.

3.3.1.3 Tasa o velocidad de transmisión

En algunos puntos de acceso, es posible seleccionar la tasa de transmisión preferida (11, 5.5, 2 o 1 Mbps para IEEE 802.11b). Al hacer esto, está cambiando la técnica de modulación para la transmisión de datos.

Por defecto, defina la velocidad al mayor valor posible. Si está construyendo un enlace muy largo y experimenta problemas de pérdida de paquetes, puede intentar reducir la velocidad para tener una señal más robusta.

3.3.2 La capa de enlace

Los parámetros de un punto de acceso que afectan la capa de enlace son los siguientes:

3.3.2.1 Modos de operación

El modo del punto de acceso no debe ser confundido con los dos modos básicos “de radio” de cualquier tarjeta inalámbrica, que son infraestructura y *ad hoc*.

El modo de un punto de acceso se refiere al tipo de tareas que éste realiza. La denotación de “modo” puede ser confusa en muchos casos ya que los fabricantes usan diferentes nombres para describir el modo de operación de un producto. Todo punto de acceso funciona como puente entre la red cableada y la inalámbrica, y cuando se limita a esta tarea se dice que funciona como puente. Si,

además, realiza funciones adicionales como enrutamiento y enmascaramiento (NAT), entonces estamos hablando de un enrutador inalámbrico. Los modos se diferencian principalmente en cuándo el punto de acceso actúa como puente o enrutador/NAT.

En la siguiente sección se describe el conjunto típico de “modos” que usted encontrará en los puntos de acceso (o enrutadores inalámbricos). Note que el nombre del modo puede diferir de vendedor en vendedor.

Punto de acceso (*Access Point Bridging / Access Point Mode*)

El punto de acceso trabaja como un puente transparente entre el enrutador y los clientes inalámbricos. El punto de acceso no realiza labores de enrutamiento o NAT. Este es el modo de configuración más simple de un punto de acceso inalámbrico.

Pasarela (*Gateway*)

El punto de acceso actúa como un enrutador inalámbrico entre una LAN y un grupo de clientes inalámbricos llevando a cabo el enrutamiento o el enmascaramiento (NAT) para esos clientes. El punto de acceso puede obtener del proveedor de acceso a la Red una dirección IP a través de DHCP (Dynamic Host Configuration Protocol). El punto de acceso puede entregar direcciones IP a sus clientes usando DHCP.

Puente punto a punto (*Point-to-Point bridge / Repeater mode*)

Se usan dos puntos de acceso para tender un puente entre DOS redes cableadas. No se realiza NAT en los puntos de acceso ya que el enmascaramiento simplemente pasa sobre los paquetes de datos.

Enrutamiento punto a punto (*Point-to-Point routing / Wireless Bridge Link*)

El punto de acceso es usado como un enrutador inalámbrico entre dos LAN separadas.

Adaptador inalámbrico Ethernet (*Wireless Ethernet adapter / Wireless Client mode*)

Este modo se usa para conectar un computador que no soporta adaptadores inalámbricos. Conectando un punto de acceso como un dispositivo a través de los puertos Ethernet o USB, el punto de acceso se puede usar “como un adaptador inalámbrico”.

3.3.2.2 SSID (*Service Set Identifier*)

El SSID es el nombre de la LAN inalámbrica y también se incluye en todos los paquetes “beacon” (baliza) enviados por el punto de acceso³. El SSID es una cadena de texto sensible a mayúsculas y minúsculas, que acepta hasta 32 caracteres alfanuméricos y es usada durante el proceso de “asociación” a una red inalámbrica. El proceso de asociación es equivalente a la acción de “enchufar” el dispositivo.

Los clientes que quieren comunicarse con un determinado punto de acceso, deben usar el SSID durante el proceso de asociación (ver Instalación de clientes, para más información).

3. Más información sobre SSID: http://www.issa-uk.org/downloads/presentations/issa-uk/wp_ssid_hiding.pdf.

El SSID de un punto de acceso se difunde por defecto en el “beacon” para anunciar su presencia. Esto significa que cualquiera con un adaptador inalámbrico puede “ver” su red en términos de su SSID. Si en el punto de acceso de una red no se ha implementado un mecanismo extra de seguridad en términos de cifrado (WPA) o autenticación (filtro de MAC, portal cautivo), cualquiera puede asociarse a su punto de acceso y conectarse a la red que se encuentra detrás de él.

Muchos puntos de acceso ofrecen la posibilidad de desactivar la difusión del SSID para “ocultar” la red al público. Este truco se puede usar para mejorar la seguridad de la red inalámbrica frente a usuarios con conocimientos intermedios sobre computadores. Sin embargo, para usuarios avanzados ese es un mecanismo de seguridad débil pues con las herramientas adecuadas, es posible monitorear y capturar ciertos paquetes de la red inalámbrica y así encontrar el SSID.

3.3.2.3 Control de acceso al medio

En los puntos de acceso hay algunas opciones avanzadas que pueden ser particularmente relevantes para redes congestionadas. Esos parámetros son, por ejemplo, intervalos de *beacon*, RTS/CTS y fragmentación.

Intervalo de Beacon

El intervalo de beacon es la cantidad de tiempo entre la transmisión de tramas beacon de un punto de acceso. El valor por defecto de este intervalo es generalmente 10ms, lo que implica que cada segundo se envían 10 beacons. Este valor proporciona soporte suficiente en términos de movilidad en un ambiente de oficina. Si necesita soporte para una movilidad más alta, puede incrementar el intervalo de beacon. Al disminuir el intervalo de beacon se obtiene como resultado una reducción de la tara (overhead) en la red, pero es probable que la itinerancia (roaming) entre estaciones base no trabaje correctamente. Le recomendamos no cambiar este valor a menos que tenga muy buenas razones para hacerlo.

RTS/CTS (Request-to-send / Clear-to-send)

RTS/CTS es el método usado por las redes inalámbricas del estándar IEEE 802.11 para reducir colisiones causadas por “nodos ocultos” (Ver “Conexión avanzada de redes inalámbricas”). En breve, este es un método para conceder el acceso al medio que involucra un proceso de “apretón de manos” entre un punto de acceso y un nodo inalámbrico. RTS/CTS introduce mecanismos para evitar colisiones mediante el método CSMA/CA y por lo tanto, hace al método de acceso más robusto, pero incrementa la tara (overhead) en la red.

El RTS/CTS funciona como sigue: Un nodo que desea enviar datos inicia el *apretón de manos* con el punto de acceso enviando una trama RTS. El punto de acceso recibe el RTS y responde con una trama CTS si el medio está libre. Cuando el nodo recibe el CTS, este comienza a

enviar sus datos. Ya que todos los nodos deben ser capaces de escuchar al punto de acceso, la trama CTS alcanzará a todos los nodos conectados a él. La trama CTS incluye un valor del tiempo que los otros nodos deberán esperar para enviar otras tramas RTS. Un *apretón de manos* RTS/CTS completo, asegurará que el nodo pueda enviar sus datos sin ser estorbado por tramas enviadas por los otros nodos.

Si en la red inalámbrica hay sólo unos pocos clientes y todos ellos pueden “verse” unos a otros, la opción RTS/CTS debería apagarse. En este caso, usar RTS/CTS solo introduciría tara debido a la adición de tramas RTS/CTS y disminuiría el rendimiento total.

Si existen nodos ocultos en la red, usted debería considerar usar RTS/CTS. En este caso, tanto RTS como CTS introducirán tara en términos de tramas RTS/CTS, pero podrían también reducir la tara total debido a la disminución de la retransmisión de tramas de datos.

Las preguntas son ¿cuál factor es más importante? ¿se introduce más tara de la que se reduce? Para responder a esto, usted deberá medir la tasa de pérdida de paquetes (en el nivel de transporte) para las dos opciones.

Fragmentación

El estándar IEEE 802.11 incluye una característica opcional que permite a tarjetas de red basadas en radio y a puntos de acceso fragmentar tramas de datos en pequeñas piezas para mejorar el rendimiento en presencia de interferencia o en áreas mal cubiertas.

Enviando tramas pequeñas, el riesgo de colisión con otras tramas es menos probable. Esto conlleva al incremento de la confiabilidad de transmisión de las tramas (pero también a una alta tara).

El valor de fragmentación, que normalmente se encuentra entre 256-2048 bytes, puede ser controlado por el usuario. El mecanismo de fragmentación ocurre cuando el punto de acceso o los nodos inalámbricos intentan enviar una trama de un tamaño mayor que el umbral de fragmentación.

Igual que la función de RTS/CTS, usted primero debería monitorear la red y estimar la cantidad de retransmisiones ocasionadas por colisiones. Si el nivel de colisiones es alto, entonces considere modificar el umbral de fragmentación.

En caso de que el porcentaje de colisiones sea inferior al **5%**, no utilice la opción de fragmentación ya que la sobrecarga de las tramas de fragmentación introduciría más taras que la reducción de colisiones no existentes.

3.3.2.4 Control de acceso a través de filtrado MAC

El filtrado MAC implica que sólo un grupo limitado de direcciones MAC conocidas puedan conectarse al punto de acceso. Esta es una medida de seguridad muy débil pero se puede usar en combinación con otras soluciones más avanzadas.

Un usuario avanzado puede capturar fácilmente los paquetes que vienen de la red y encontrar a cuáles direcciones MAC se les ha concedido el acceso. Después, puede cambiar su propia dirección MAC a una de las aceptadas y “engañar” al punto de acceso fingiendo ser uno de los usuarios autorizados.

3.3.2.5 cifrado (WEP, WPA)



WEP (Wired Equivalent Privacy – Privacidad equivalente a la cableada) es un **viejo** protocolo de cifrado implementado hoy en día en la mayoría de los puntos de acceso. Aunque WEP ha demostrado tener grandes debilidades y no es considerada como una opción segura de cifrado, es frecuentemente usada entre los usuarios de conocimientos intermedios.

WEP usa el algoritmo de cifrado RC-4 de 40-bits para encriptar todos los datos antes de la transmisión entre el punto de acceso y los clientes. Muchos vendedores adicionan funciones de cifrado privativas a su software y alcanzan niveles de cifrado hasta de 128 bits.



La configuración WEP hecha en el punto de acceso siempre se debe reflejar en el lado del cliente. Asegúrese de que su dispositivo cliente soporta el protocolo de cifrado, el tipo de autenticación y la longitud de la clave que usted configuró en el punto de acceso.

Si selecciona habilitar WEP, elimine siempre las claves WEP que provee el fabricante por defecto y defina sus propias claves privadas. Si está usando una clave de 64-bits nominales (Clave real de 40-bits), debe ingresar una clave de 10 caracteres hexadecimales (0-9, a-f, o A-F). La clave de 128-bits, que provee mayor seguridad, consiste en una larga cadena hexadecimales de 26 caracteres.



!Recuerde! La alternativa actual a WEP es WPA (Wi-Fi Protected Access por sus siglas en inglés), que es un protocolo de cifrado que fue diseñado para manejar los problemas de WEP. WPA2 es la segunda generación de WPA basado en el estándar 802.11i (enmienda).

Aún hoy (2007), muchos puntos de acceso en el mercado soportan sólo WEP por defecto. Normalmente encontrará que está disponible la actualización a WPA del *firmware* de puntos de acceso y clientes inalámbricos. Revise el sitio web del vendedor para saber si hay actualizaciones disponibles del firmware. Para mejorar la seguridad de la red utilizando cifrado WPA, debe actualizar el firmware de los siguientes componentes:

- Puntos de acceso inalámbrico.
- Adaptadores de red inalámbrica.
- Programas de cliente inalámbrico (manejadores o *drivers*, herramientas de gestión, etc.).

3.3.2.6 Restricción de acceso a través de autenticación

El acceso restringido a una red a través de autenticación, se puede hacer utilizando un servidor de autenticación Radius (Remote Dial-Up Service). Al implementar un servidor de autenticación Radius, el punto de acceso actúa como un “Cliente Radius” y debe estar al tanto de los ajustes definidos en la base de datos del Servidor Radius. Como parte de las funciones MAC del estándar IEEE 802.11, los puntos de acceso ofrecen Autenticación en sistemas abiertos (Open system authentication) y también en algunos casos Autenticación por clave compartida. Puesto que ninguno de dichos sistemas de autenticación han demostrado ser seguros, hoy en día muchos puntos de acceso incluyen mecanismos IEEE 802.1x para permitir la autenticación de usuarios a través de un servidor de autenticación externo. El tema de autenticación está fuera del alcance de esta unidad y no se discutirá más a fondo.

3.3.2.7 cifrado punto a punto

El cifrado punto a punto es la forma más segura de proteger la transferencia de datos valiosos. Una VPN (Red Privada Virtual) ofrece servicio de cifrado punto a punto y hoy en día es soportada por muchos puntos de acceso.

En caso de implementar una VPN, el punto de acceso permite el paso a través de PPTP/IPSec. VPN está más allá del alcance de esta unidad y no se discutirá más a fondo.

El cifrado punto a punto es la forma más segura de proteger la transferencia de datos valiosos. Una VPN (Red Privada Virtual) ofrece servicio de cifrado punto a punto y hoy en día es soportada por muchos puntos de acceso. En caso de implementar una VPN, el punto de acceso permite el paso a través de PPTP/IPSec.

VPN está más allá del alcance de esta unidad y no se discutirá más a fondo.

3.3.2.8 Sistema de Distribución Inalámbrico WDS (Wireless Distribution System)

Este sistema permite la conexión inalámbrica entre puntos de acceso, haciendo puenteo a Nivel de la capa 2 entre todas las estaciones registradas en los puntos de acceso conectados mediante WDS.

En WDS un punto de acceso puede comportarse como AP o Puente, facilitando que la red se extienda sin necesidad de cables. Todos los AP de la red deben utilizar el mismo canal de radiofrecuencia y deben compartir la clave WEP, aunque pueden usar SSID diferentes.

La conexión de las estaciones se realiza en la capa 2 ya que se utiliza las direcciones MAC de las tarjetas inalámbricas de origen y destino, que gracias a WDS se conservan en dos campos adicionales dentro de los paquetes transferidos.

WDS puede ser usado para proveer dos modos de conexión inalámbrica entre puntos de acceso:

- Puento inalámbrico que solo permite la comunicación entre dos puntos de acceso sin que otro cliente inalámbrico pueda acceder
- Repetidor inalámbrico que permite que un Punto de Acceso se comuniquen con otros puntos de acceso y estaciones cliente

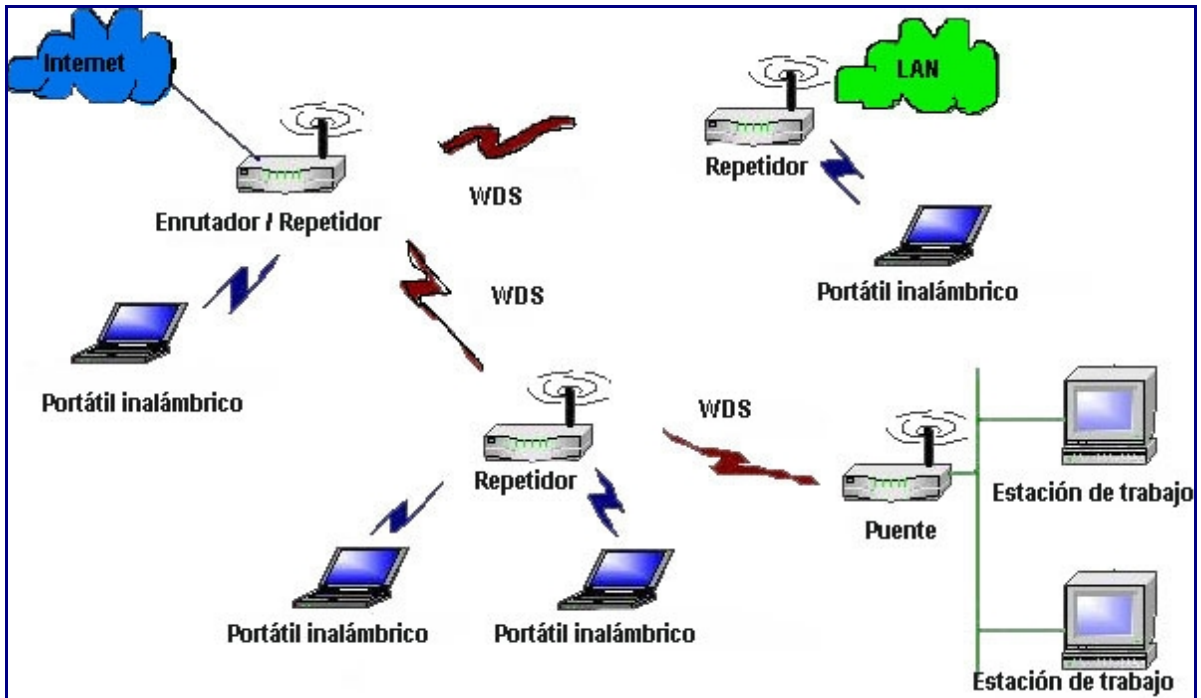


Figura 2: Sistema de Distribución Inalámbrico WDS (Wireless Distribution System)

3.3.3 La capa de red

Estrictamente hablando, la capa de Red no es parte de las redes inalámbricas de comunicación. Sin embargo, muchos puntos de acceso no son “transparentes” e incluyen funcionalidades adicionales como enrutamiento y enmascaramiento (NAT).

La siguiente tabla describe brevemente cada uno de los parámetros involucrados en la capa de red:

| Opción | Descripción |
|----------------|--|
| Dirección IP | La dirección IP de un punto de acceso no es necesaria para realizar sus tareas básicas (actuar como concentrador inalámbrico). La dirección IP se usa para acceder al dispositivo desde una aplicación web y facilitar el proceso de configuración. Si el punto de acceso es usado como un enrutador inalámbrico, su dirección IP debería estar en la misma subred del enrutador al que está unido y se deben definir las reglas apropiadas de enrutamiento. |
| Máscara de red | <i>Netmask</i> . Ver “Conexión de redes inalámbricas avanzadas” |
| Pasarela | <i>Gateway</i> . Dirección IP de la conexión de salida de su red. |
| DNS | Dirección IP del servidor de DNS que se anuncia por DHCP a los clientes inalámbricos. |

Tabla 1: Opciones de un punto de acceso relativas a la capa de Red.

3.3.4 Capa de aplicación

Los ajustes más importantes de todo el proceso de configuración se encuentra en la capa de aplicación. Estos ajustes están protegidos mediante la “contraseña de administración” del punto de acceso. El dispositivo viene normalmente con una contraseña por defecto (usuario:admin contraseña:admin) que le recomendamos encarecidamente cambiar inmediatamente por una más segura.



Evite las contraseñas que pueden relacionarse con usted como una persona u organización ya que pueden ser adivinadas fácilmente

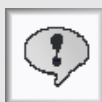
Si una persona “indeseada” accede a la contraseña de admin, él o ella pueden “secuestrar” su punto de acceso y cambiar la contraseña de modo que no pueda acceder a él. En este caso la única solución es reiniciar (resetear) manualmente el punto de acceso o conectarlo a través de la interfaz serial y cambiar la contraseña.

4. Instalación de clientes: Parte A - Linux

4.1 Seleccionando el hardware inalámbrico

Uno de los desafíos de utilizar Linux en una estación de trabajo (computadora portátil o de escritorio) es que muchos de los vendedores de hardware solo suplen manejadores (drivers) para su hardware que funcionan en los principales sistemas operativos privativos. Por lo tanto a menudo se deja a desarrolladores voluntarios la tarea de hacer que esos dispositivos de hardware trabajen bajo Linux, esto frecuentemente con muy poco o ningún soporte de los vendedores. Esto significa sobre todo que el nuevo hardware podría no ser soportado en los primeros meses de aparición en el mercado y en algunos casos, nunca ser soportado. Además, lograr que un dispositivo de hardware específico funcione bajo Linux a menudo requiere mayor trabajo que hacer que funcione bajo Windows.

Por estas razones es recomendable tomar un tiempo para investigar sobre el mejor hardware para su distribución de Linux, y dependiendo de su habilidad y experiencia con Linux, definir cuál hardware es soportado por las utilidades gráficas que son suplidas con su distribución.



Para seleccionar el hardware inalámbrico para Linux hay que tomar en cuenta: tipos de hardware; chipsets inalámbricos; hardware soportado; hardware no soportado y diferencias entre drivers.

4.1.1 Tipos de hardware

Las tarjetas inalámbricas para clientes a menudo vienen en uno de los siguientes factores de forma:

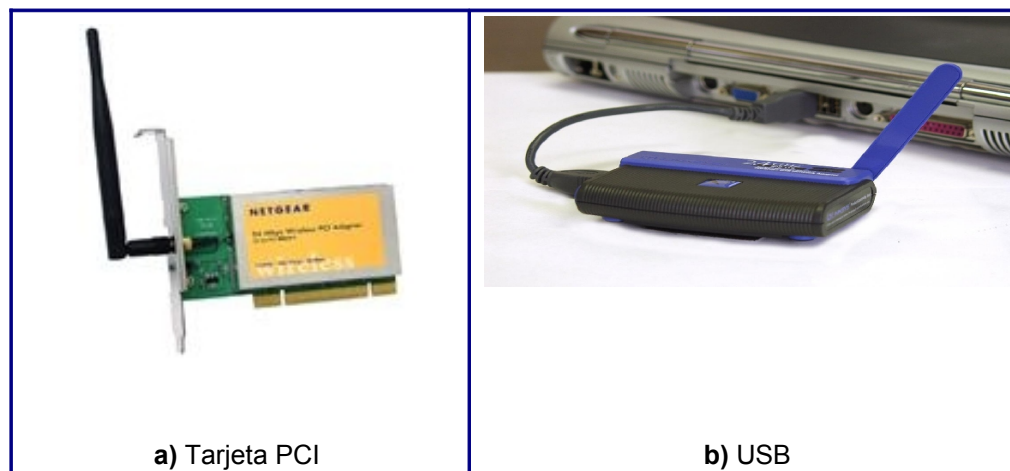


Figura 3: Tipos de hardware

Tarjetas PCI

Las tarjetas PCI se encuentran a menudo dentro de computadores de escritorio o servidores. Se requiere abrir la carcasa del computador por lo que su instalación podría ser un poco más difícil que la de otras opciones.

Adaptadores USB

Los adaptadores USB funcionarán en la mayoría de computadores de escritorio y portátiles (los computadores más modernos soportan el conector USB estándar). Estos adaptadores son pequeños, no se requiere abrir el computador y se pueden colocar y remover de forma muy sencilla. Sin embargo, bajo Linux, no todos los adaptadores USB son soportados, y la mayoría de manejadores empiezan por soportar PCMCIA (PC Card) y PCI antes de incluir el soporte para USB.

PCMCIA o PC Card

Estas tarjetas son hechas específicamente para computadoras portátiles, que tienen puertos PCMCIA. Estas tarjetas ocupan poco espacio y no se requiere abrir la computadora para instalarlas. Los computadores de escritorio no tienen ranuras PC Card, pero existen adaptadores PC Card a PCI y PC Card a ISA que pueden utilizarse para aprovechar hardware existente.

Mini-PCI

Las tarjetas Mini-PCI son esencialmente versiones de factor de forma pequeño de las tarjetas tipo PCI, que a menudo están incorporadas a las computadoras portátiles o en dispositivos dedicados al acceso inalámbrico. Aunque es posible instalarlas en algunos portátiles, esto muy probablemente anularía la garantía. Muchos computadores portátiles modernos vienen con tarjetas mini-PCI pre instaladas. En términos de instalación de manejadores son equivalentes a las tarjetas PCI.




Figura 4: Una tarjeta PC Card (PCMCIA)

4.1.2 Chipsets inalámbricos

Aunque hay cientos de fabricantes que producen hardware inalámbrico para computadoras, solo unas 10 compañías hacen los *chipsets* (conjunto de circuitos integrados utilizados para el acceso inalámbrico) que utilizan las tarjetas. Y debido a que a menudo los drivers para Linux no son desarrollados por los fabricantes, cada controlador trabajará generalmente para un chipset específico,

y por lo tanto para varias tarjetas de diferentes fabricantes. Es importante conocer cuál chipset está en una tarjeta específica antes de comprarla, ya que esto dice más sobre su soporte en Linux que la información sobre la marca del fabricante. Por ejemplo, hay varias compañías que producen tarjetas con el chipset prism2 o prism2.5, y todas ellas trabajan con los mismos controladores. Vea *“Dispositivos inalámbricos, sus chipsets y manejadores”* en los *Recursos adicionales para más información*.


Algunos de los chipset más comunes son:



- Atheros (driver recomendado: madwifi).
- Intel Pro/Wireless 2100 & 2200 (driver ipw2100/ipw2200).
- Prism2/2.5/3 (driver hostap o wlan-ng).
- Orinoco (orinoco_cs).
- Broadcom (actualmente no cuenta con controlador nativo de Linux).

4.1.3 Hardware soportado

La mayoría de las distribuciones de Linux tienen en sus sitios web una lista del hardware soportado. Algunas listas son muy extensas, mientras otras solo muestran el hardware de demostrada compatibilidad. Para utilizar Linux es recomendable revisar primero esta lista. Si su tarjeta no está en la lista, quizá considere usar una distribución diferente, o comprar una tarjeta diferente. Es conveniente revisar si se ofrece soporte para otra tarjeta basada en el mismo chipset, pues esto es lo que en definitiva importa.



También puede usar Google (www.google.com) para buscar una tarjeta específica con una distribución específica, esto a menudo le mostrará si hay problemas conocidos con esa combinación.

4.1.4 Hardware no soportado

Si usted termina con una tarjeta que no es soportada por su distribución, todavía hay algunas opciones disponibles. Primero que todo, generalmente es posible compilar los drivers en la versión del kernel usada por su distribución, y cargarlos como módulos del kernel. Mire los sitios web individuales de los drivers para tener mayor información sobre esto. Algunos fabricantes proveen drivers binarios (no de fuente abierta) para su hardware, y podrían ayudarle directamente. También hay dos proyectos que están implementando una capa de compatibilidad que permite a Linux usar los manejadores para Windows XP provistos para casi todas las tarjetas. Estos proyectos son “ndiswrapper” que es software

libre y “Driverloader” solución comercial de “Linuxant”. Ver “Drivers inalámbricos” en Recursos Adicionales para mayor información.

4.1.5 Diferencias entre drivers

Vale la pena notar que no todos los drivers son creados iguales. Mientras que la mayoría de los drivers de tarjetas inalámbricas para Linux soportan las funcionalidades básicas para permitirle conectarse a un Punto de Acceso con o sin cifrado WEP básica, puede haber diferencias en cuanto al soporte de funcionalidades más avanzadas.



Esto puede ser importante si usted está buscando hacer algo como lo siguiente:

- Usar la tarjeta en modo *ad hoc*.
- Usar su caja Linux como un punto de acceso inalámbrico.
- Usar cifrado y autenticación avanzada WPA y WPA2.
- Usar una herramienta de escaneo inalámbrico para encontrar redes inalámbricas existentes.

Además algunos chipsets son soportados por varios drivers cada uno de los cuales ofrece diferentes características, de manera que vale la pena examinar las alternativas, aún cuando su tarjeta tenga el soporte básico en su distribución.



Aquí están algunos ejemplos de diferencias entre drivers:

- El driver linux-wlan-ng no soporta *wireless-tools*, y no es soportado por muchas utilidades inalámbricas.
- El driver orinoco_cs no soporta el escaneo para redes a menos que sea parchado y recompilado.
- Madwifi (chipset Atheros) es el único driver que soporta multi banda (802.11a/b/g) bajo linux.
- Los drivers hostap y madwifi tienen buen soporte para montar un punto de acceso inalámbrico (802.11 modo maestro).

4.2 Instalando el dispositivo inalámbrico

Esta sección dará una breve introducción acerca de la instalación de manejadores de dispositivos inalámbricos bajo Linux.

4.2.1 Preparando la instalación



Antes de empezar, busque siempre el sitio web de su distribución para conseguir información sobre la instalación inalámbrica en general y su hardware particular. De esta manera puede conocer de antemano detalles y problemas específicos. También use Google u otro buscador para buscar el nombre de su tarjeta y distribución (p.e. “Linksys WPC54G Fedora Core” y también “Problemas Linksys WPC54g Fedora Core”).

Si encuentra una guía oficial o no oficial para la instalación de su tarjeta inalámbrica bajo esa distribución específica, úsela y salte el resto de este capítulo.

Si es posible, tenga la tarjeta insertada cuando instale la distribución, ya que muchas distribuciones tienen una excelente detección de hardware durante la instalación.

Puede hacerlo utilizando el comando ***iwconfig***.

Abra una ventana de terminal y teclee: **# which iwconfig**

Si ve la ruta del programa ***iwconfig***, usted tiene el paquete instalado. Si no, busque un paquete llamado “wireless-tools” usando el administrador de paquetes de su distribución.

Las distribuciones más modernas deberían tener el paquete disponible, si no instalado por defecto. Si no, usted necesita instalar el paquete wireless-tools (herramientas de red inalámbrica).

Vea “*Herramientas para redes inalámbricas*” en los Recursos Adicionales, para mayor información.

4.2.2 Insertando la tarjeta

Si la tarjeta aún no está insertada o conectada, este es un buen momento para hacerlo. Entonces debemos comprobar si la tarjeta fue detectada automáticamente por su distribución. Para esto abra la interfaz del Gestor de red inalámbrica (Network manager) que su distribución utiliza por defecto (figura 5). El siguiente ejemplo es de la versión “Warty Warthog” de Ubuntu, usando el administrador de redes inalámbricas que trae por defecto Gnome.

En este punto su tarjeta debería estar lista para ser usada, y todas las opciones de red inalámbrica pueden fijarse usando el gestor de redes inalámbricas gráfico de su distribución. En la sección 4.2 encontrará más información sobre cómo configurar su tarjeta.

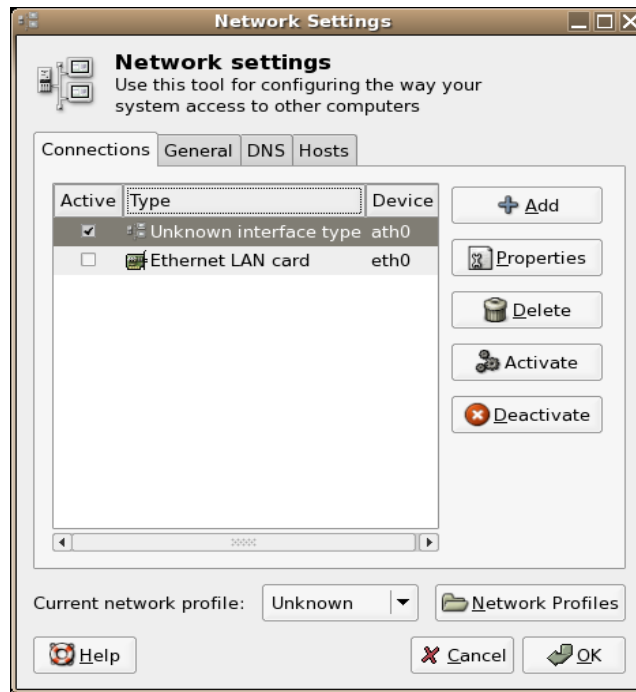


Figura 5: Gestor de red inalámbrica de Gnome

4.2.3 Identificando el chipset



Si su tarjeta no es detectada automáticamente por su distribución, usted debe identificar el chipset y el driver pertinente.

Algunos de los comandos y herramientas más importantes para identificar el hardware son:

lspci

Este comando lista todos los dispositivos PCI conectados a la computadora, y por lo tanto es útil para dispositivos PCI y mini-PCI.

cardctl ident

El comando cardctl es usado para controlar los dispositivos PCMCIA de los computadores portátiles. Al usarlo con el parámetro "ident" retornará información sobre el hardware en los puertos PCMCIA de las computadoras.

usbview

usbview es una utilidad gráfica que está incluida (o cuenta con paquetes disponibles para fácil instalación) en muchas distribuciones. Proporciona una vista en estilo de árbol de todos los dispositivos USB conectados al computador.

hal-device-manager

Esta utilidad gráfica reemplaza el comando usbview en las distribuciones que basan su hardware en HAL (Hardware Abstraction Layer) y dbus. Esta muestra el mismo tipo de información, pero referente a todo el hardware conectado al computador, incluyendo dispositivos USB, PCMCIA, PCI y mini-PCI.

dmesg

Este comando imprime el buffer de anillo del kernel, que contiene mensajes generados por el kernel cuando este inicia y detecta los dispositivos de hardware conectados a la computadora.

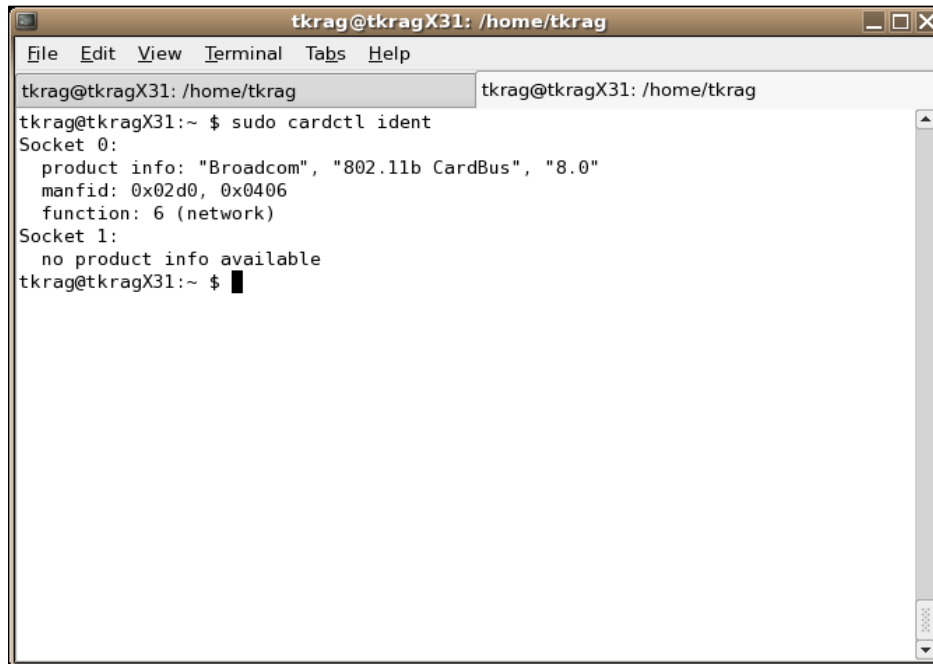
Alternativamente al uso de estos comandos puede buscar en Internet información sobre dispositivos inalámbricos y sus chipsets. Vea *“Dispositivos inalámbricos, sus chipsets y manejadores” en Recursos Adicionales, para más información*. Sin embargo, se ha sabido que algunos fabricantes cambian los chipsets sin cambiar el número del modelo de sus tarjetas, de manera que esta información no siempre es exacta.

4.3.2.1 Ejemplo: Identificar el chipset de un Linksys WPC54G en Ubuntu

La Linksys WPC54G es una tarjeta inalámbrica PCMCIA que usa un chipset que no es soportado automáticamente por Ubuntu, ya que actualmente no hay un driver nativo para Linux. En este ejemplo, nosotros usamos un IBM Thinkpad x31 corriendo el release “Warty Warthog” de Ubuntu Linux.

Después de insertar la tarjeta en el puerto PCMCIA, probamos con alguno de los comandos mencionados anteriormente para identificar correctamente el chipset.

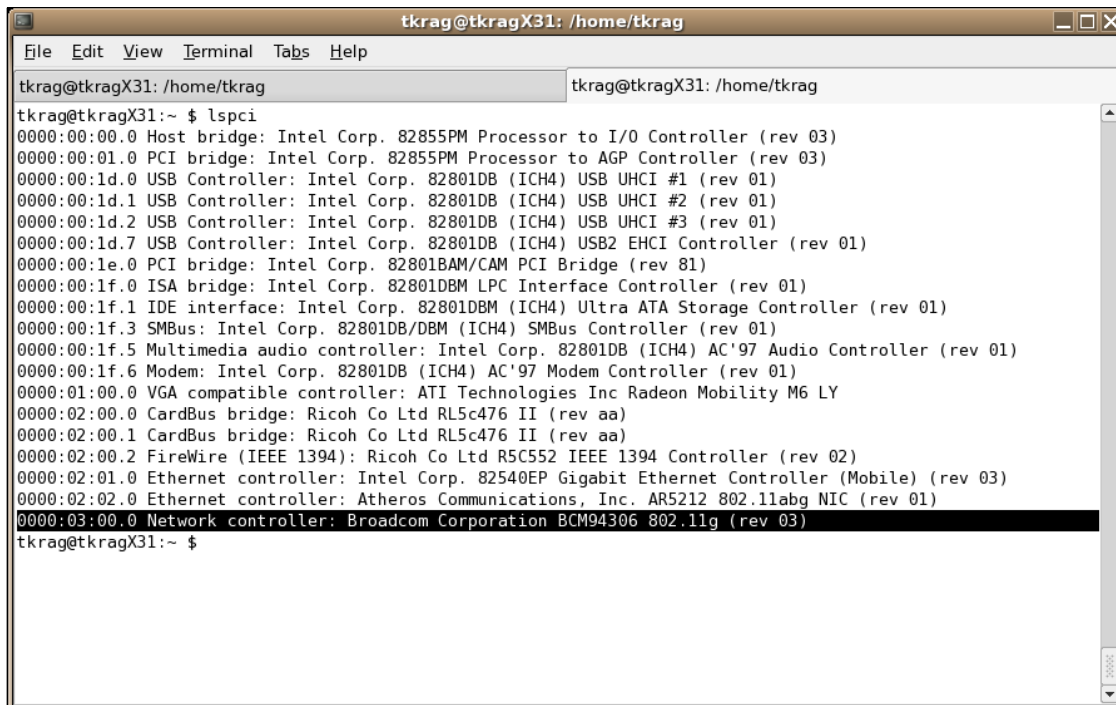
Comando 1: # sudo cardctl ident



```
tkrag@tkragX31: /home/tkrag
tkrag@tkragX31: /home/tkrag
tkrag@tkragX31:~ $ sudo cardctl ident
Socket 0:
  product info: "Broadcom", "802.11b CardBus", "8.0"
  manfid: 0x02d0, 0x0406
  function: 6 (network)
Socket 1:
  no product info available
tkrag@tkragX31:~ $
```

Figura 6: *cardctl ident* muestra el hardware está actualmente en los sockets PCMCIdel computador portátil.

Comando 2:# lspci



```
tkrag@tkragX31: /home/tkrag
tkrag@tkragX31: /home/tkrag
tkrag@tkragX31:~ $ lspci
0000:00:00.0 Host bridge: Intel Corp. 82855PM Processor to I/O Controller (rev 03)
0000:00:01.0 PCI bridge: Intel Corp. 82855PM Processor to AGP Controller (rev 03)
0000:00:1d.0 USB Controller: Intel Corp. 82801DB (ICH4) USB UHCI #1 (rev 01)
0000:00:1d.1 USB Controller: Intel Corp. 82801DB (ICH4) USB UHCI #2 (rev 01)
0000:00:1d.2 USB Controller: Intel Corp. 82801DB (ICH4) USB UHCI #3 (rev 01)
0000:00:1d.7 USB Controller: Intel Corp. 82801DB (ICH4) USB2 EHCI Controller (rev 01)
0000:00:1e.0 PCI bridge: Intel Corp. 82801BAM/CAM PCI Bridge (rev 81)
0000:00:1f.0 ISA bridge: Intel Corp. 82801DBM LPC Interface Controller (rev 01)
0000:00:1f.1 IDE interface: Intel Corp. 82801DBM (ICH4) Ultra ATA Storage Controller (rev 01)
0000:00:1f.3 SMBus: Intel Corp. 82801DB/DBM (ICH4) SMBus Controller (rev 01)
0000:00:1f.5 Multimedia audio controller: Intel Corp. 82801DB (ICH4) AC'97 Audio Controller (rev 01)
0000:00:1f.6 Modem: Intel Corp. 82801DB (ICH4) AC'97 Modem Controller (rev 01)
0000:01:00.0 VGA compatible controller: ATI Technologies Inc Radeon Mobility M6 LY
0000:02:00.0 CardBus bridge: Ricoh Co Ltd RL5c476 II (rev aa)
0000:02:00.1 CardBus bridge: Ricoh Co Ltd RL5c476 II (rev aa)
0000:02:00.2 FireWire (IEEE 1394): Ricoh Co Ltd R5C552 IEEE 1394 Controller (rev 02)
0000:02:01.0 Ethernet controller: Intel Corp. 82540EP Gigabit Ethernet Controller (Mobile) (rev 03)
0000:02:02.0 Ethernet controller: Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01)
0000:03:00.0 Network controller: Broadcom Corporation BCM94306 802.11g (rev 03)
tkrag@tkragX31:~ $
```

Figura 7: *lspci* lista todos los dispositivos PCI en el computador (incluyendo PCMCIA).

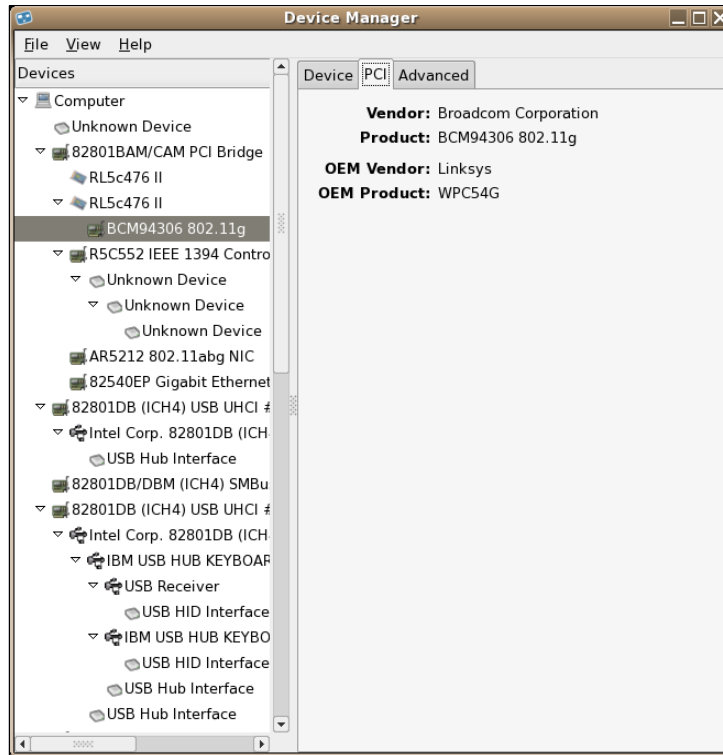


Figura 8: El *hal-device-manager* da una vista en estilo de árbol de todo el hardware en la máquina

Con esta información es muy fácil identificar la tarjeta como un *chipset* de *Broadcom*.



Algunas búsquedas en Google y sabremos que ese chipset *no tiene un driver nativo bajo Linux*, y por lo tanto debemos utilizar la utilidad *ndiswrapper* para instalar el driver de Windows. Buscando un *How-To* encontraremos varias páginas que describen como instalar la tarjeta bajo diferentes distribuciones.

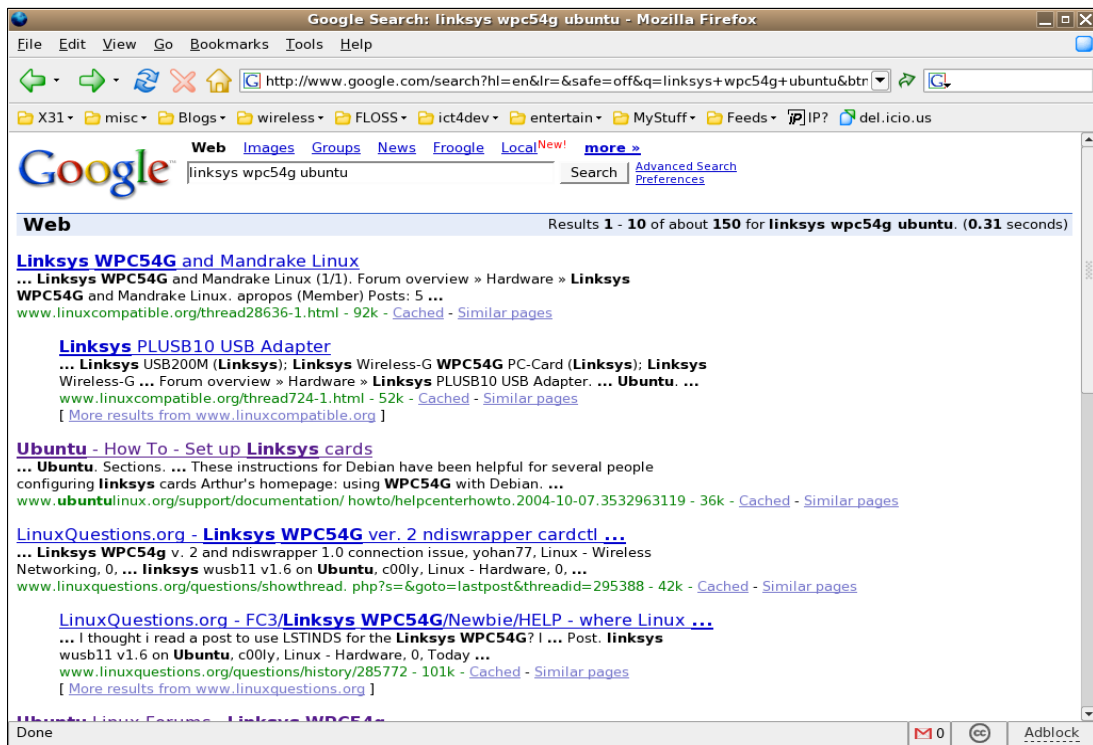


Figura 9: Google es nuestro mejor amigo cuando intentamos instalar hardware bajo Linux.

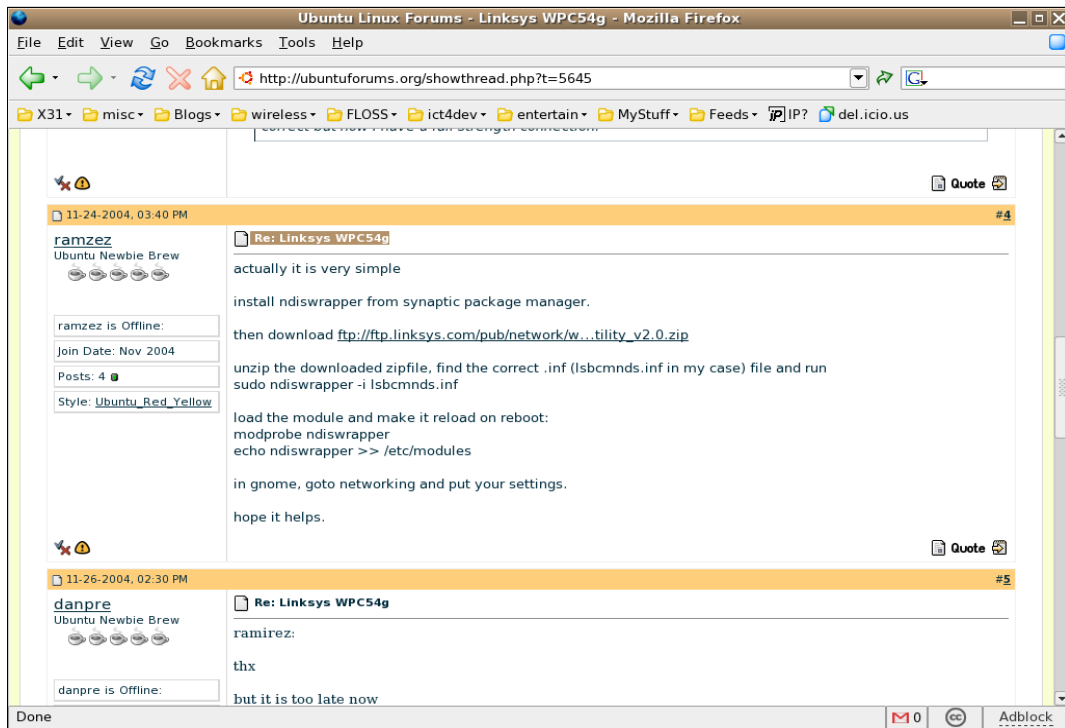


Figura 10: En este caso hay un buen manual para la tarjeta Linksys en los foros de Ubuntu.

De hecho, este caso es muy simple y se puede resumir como sigue:

```
# instalar ndiswrapper desde el administrador de paquetes synaptic
# descargar ftp://ftp.linksys.com/pub/network/wpc54g\_v2\_driver\_utility\_v2.0.zip
# descomprimir el archivo .zip descargado, encontrar el archivo .inf adecuado (en mi caso
lsbcmnds.inf) y correrlo
# sudo ndiswrapper -i lsbcmnds.inf
# cargar el módulo y reiniciar para recargarlo
# modprobe ndiswrapper
# echo ndiswrapper >> /etc/modules
# en gnome, ir a networking y definir su configuración
```

Esto debería ser suficiente para definir una interfaz inalámbrica llamada wlan0 que puede ser configurada usando las herramientas gráficas típicas para conexión de redes.

4.3 Configurando el dispositivo inalámbrico

Una vez que la tarjeta ha sido instalada exitosamente, debemos preparar la red para conectarla al punto de acceso inalámbrico de nuestra elección, conseguir una dirección IP y así sucesivamente.

Los pasos básicos requeridos para la mayoría de las redes son:

1. Configurar el SSID (nombre de la red inalámbrica).
2. Seleccionar DHCP o dirección IP estática.
3. Habilitar o deshabilitar la clave de seguridad WEP.
4. Activar la red.

4.3.1 Ejemplo 1: Ubuntu con Gnome

Esta sección muestra cómo montar la interfaz inalámbrica bajo Ubuntu (Warty Warthog) corriendo Gnome 2.08. El procedimiento debería ser el mismo para todas las distribuciones modernas basadas en Gnome.

Debemos iniciar el Gestor de Redes de Gnome que es una utilidad gráfica usada por Gnome para configurar la información de la Red.

Vaya a : > Menú de la computadora> Configuración del sistema > Conexión a redes

El sistema le pedirá su contraseña para poder continuar.

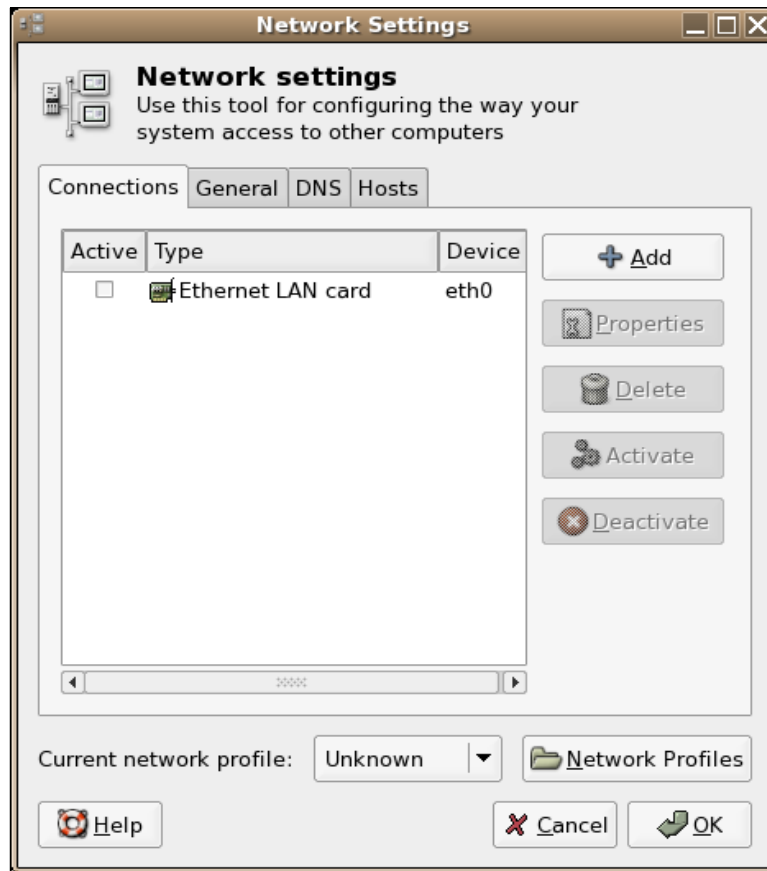


Figura 11: La red inalámbrica no es visible en la herramienta de configuración.

Si su tarjeta de red inalámbrica fue reconocida durante la instalación de la computadora portátil, o automáticamente reconocida por Ubuntu, debería haber una entrada con la interfaz de red en el menú. Sin embargo, en este caso, hemos acabado de instalar el ndiswrapper y el manejador de windows, y Ubuntu no ha reconocido e instalado automáticamente el dispositivo.

Pulse el botón **+ Add** para iniciar un instructivo que le ayudará a instalar la interfaz. Después de registrar toda la información relevante y completar el instructivo, la interfaz de red será incluida en la lista, y usted debería tener una conexión con su Punto de Acceso.



Figura12: La interfaz inalámbrica ha sido añadida al Gestor de Redes de Gnome.

5. Parte B: Instalación de clientes Windows XP

La instalación de clientes inalámbricos en Windows es un proceso sencillo, sin embargo hay dos cosas que lo/la pueden poner en apuros:

- Normalmente la tarjeta inalámbrica viene con una herramienta de Gestión de configuración y Windows tiene su propio gestor. Si los dos programas están activados habrá un conflicto que puede echar a perder las cosas. Simplemente seleccione uno de ellos y desactive el otro.
- La interfaz de radio que se encuentra en la mayoría de las nuevas computadoras portátiles se puede cambiar de encendida a apagada (on/off). Cuando empiece a configurar su dispositivo asegúrese que la interfaz esté encendida (On).

5.1 Seleccionando el hardware inalámbrico

Realmente no es un desafío seleccionar hardware inalámbrico con soporte para Windows. Cualquier hardware podrá utilizarse aquí. Es interesante comprobar la potencia de salida, la sensibilidad y la posibilidad de conectar una antena externa cuando compre una tarjeta externa.

5.2 Instalación del dispositivo inalámbrico

Para quienes usan Windows XP o Windows 2000, encontrar el driver necesario debería ser muy sencillo. Sin embargo, para versiones anteriores de Windows puede requerir un poco más de esfuerzo. Vea “Instalación de clientes inalámbricos en Windows 98” como ejemplo.

Windows XP tiene integradas herramientas para redes inalámbricas, y tendrá disponibles los drivers de la mayoría de equipos PCMCIA o USB sin que se requiera medios externos.

Conecte la tarjeta PCMCIA o dispositivo USB (las tarjetas PCI internas solo se usan en computadores de escritorio y se requieren herramientas para su instalación). Windows XP detectará el nuevo software e instalará el driver más apropiado. Si ya cuenta con acceso a Internet a través de cable, incluso podría descargar la versión más reciente del driver desde Internet.

En el caso de tarjetas específicas de modelo muy nuevo, refiérase a la instalación manual del driver en el documento “Instalación de clientes inalámbricos en Windows 98”.

Instale su adaptador de red inalámbrica en Windows XP con SP2. Este proceso incluye la instalación de los drivers apropiados para que su adaptador de red inalámbrica aparezca como una conexión inalámbrica en Conexiones de Red.

5.3 Configuración del dispositivo inalámbrico

A menos que diga algo diferente, Windows XP siempre seleccionará conectar a la red inalámbrica que provea la mejor señal, pero le pedirá confirmar antes de conectar a una red no cifrada. Cuando el cliente esté dentro del rango de un punto de acceso inalámbrico, en el área de notificación de su barra de tareas aparecerá un mensaje diciendo “Redes inalámbricas detectadas”.

Un clic izquierdo sobre el icono de conexión inalámbrica en la barra de tareas (imagen 12) le permitirá seleccionar entre las redes inalámbricas disponibles.

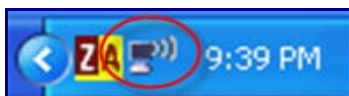


Figura 13: Icono en la barra de tareas mostrando que hay redes inalámbricas disponibles.

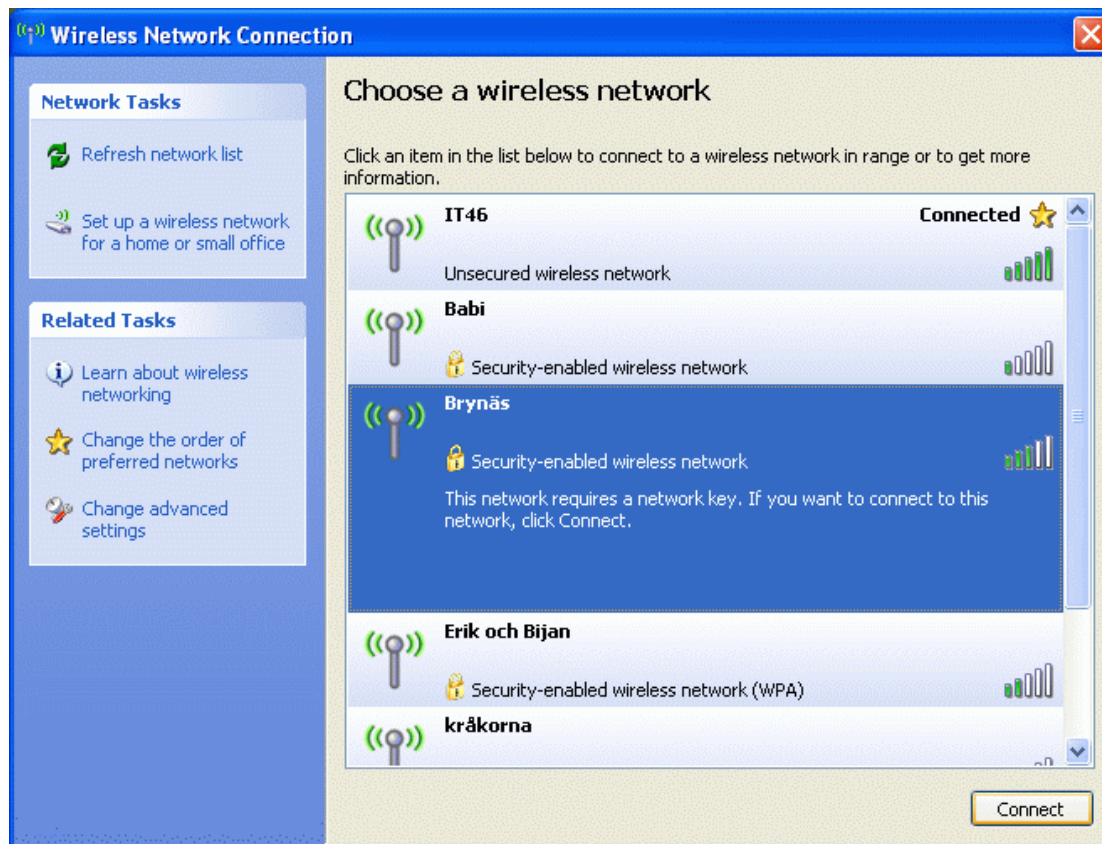


Figura 14: Listado de redes inalámbricas. El candado dorado identifica las redes cifradas.

5.3.1 Paso 1: Seleccione la red

Puede seleccionar una red escogiendo el SSID de la red con la que desea conectarse. El SSID (Identificador de conjunto de servicio - Service Set Identifier-) es el nombre de la red. Cuando más de un punto de acceso usa el mismo SSID, es llamado ESSID (Identificador de conjunto de servicio extendido - Extended Service Set ID).

Si usted escoge conectarse a una red que no está usando cifrado (WEP/WPA), simplemente seleccione el SSID y acepte que desea conectarse a una red no protegida. Después de esto, el cliente intentará conectarse a la red seleccionada.

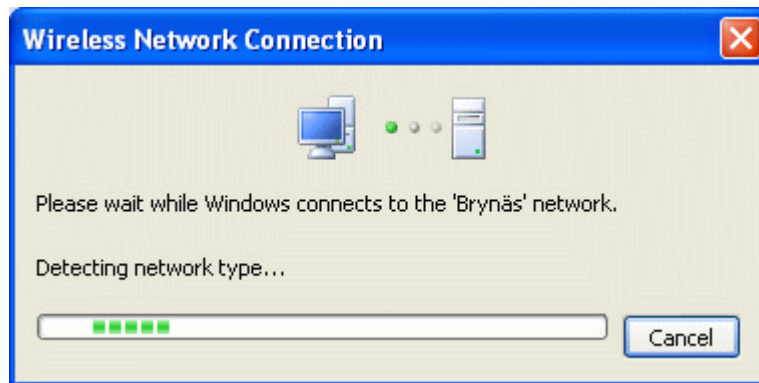


Figura 15: Iniciando la conexión a la red inalámbrica seleccionada.

Si su red usa cifrado (configurado en el punto de acceso) usted requerirá una clave de cifrado antes de que pueda conectarse. La clave de cifrado (encriptación) debería ser la misma con la que configuró el punto de acceso a utilizar.

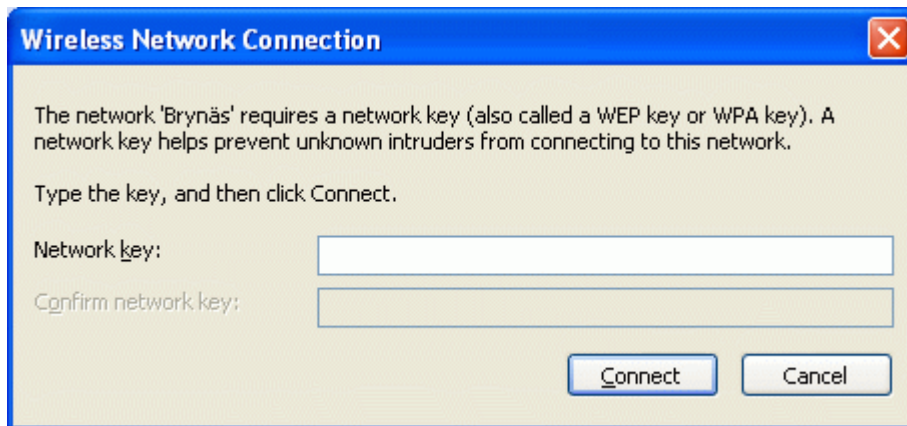


Figura 16: Para las redes cifradas, se comparte la clave entre el punto de acceso y sus clientes.

Si el mensaje de estado (desplegado en la esquina superior derecha del recuadro que corresponde a la red que usted ha seleccionado) es “*Conectado*”, usted ha logrado conectarse exitosamente al punto de acceso (ver Figura 14).

Si, en cambio, el mensaje de estado es “*Autenticación no exitosa*”, haga lo siguiente:

- Seleccione Cambiar el orden de las redes preferidas (en la lista de Tareas relacionadas).
- Seleccione la pestaña Redes Inalámbricas, que encontrará en las Propiedades de su adaptador de red inalámbrica y pulse el nombre de su red inalámbrica en Redes preferidas. Entonces pulse Propiedades y visualizará la pantalla siguiente:

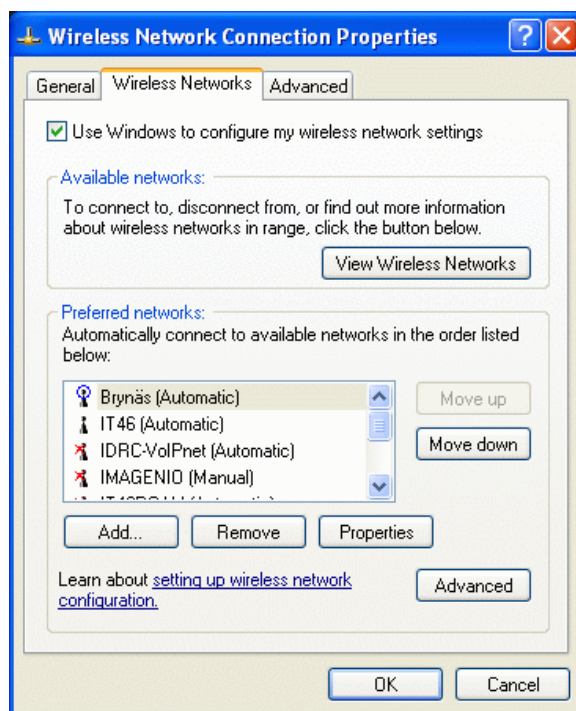


Figura 17: Seleccione la red que desea configurar manualmente.

- En Autenticación de red, seleccione Abierta (en la lista de Tareas relacionadas).
- En cifrado (encriptación) de datos seleccione WEP.
- En Clave de red (y Confirmar clave de red) teclee la clave de cifrado WEP (idéntica a la clave que registró en el punto de acceso).
- En Índice de clave, seleccione el índice de la clave principal que corresponde a la posición en memoria de la clave de cifrado en el punto de acceso.
- Seleccione OK para guardar los cambios (Redes inalámbricas).
- Seleccione OK para guardar los cambios (Adaptador de redes inalámbricas).

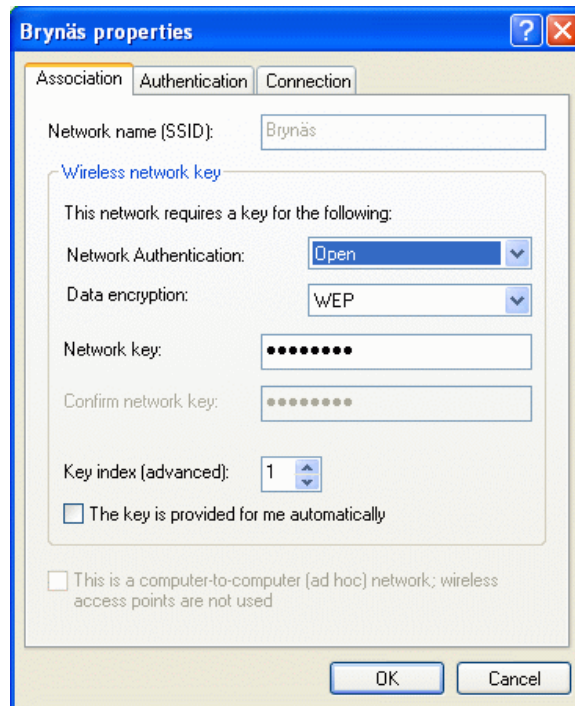


Figura18: Configuración manual de la clave WEP

5.3.2 Paso 2: configuración IP

Ahora es momento de ajustar las opciones de TCP/IP. Dependiendo de cómo ha configurado su punto de acceso, puede obtener una IP dinámica a través de DHCP o fijar manualmente una dirección IP estática.

Si el punto de acceso está configurado para DHCP, ya debería tener una dirección IP. Verifique su configuración IP desde la línea de comandos:

ipconfig

Si a pesar de que se supone que los puntos de acceso le dan una dirección IP (por DHCP), no la ha obtenido, intente lo siguiente:

ipconfig /release all

ipconfig /renew

Si necesita configurar manualmente los parámetros TCP/IP, pregunte a su administrador de red los parámetros de red a usar. Luego haga lo siguiente:

Inicio > Panel de Control > Conexiones de red

Déle un clic derecho sobre Conexiones de red inalámbrica y seleccione Propiedades.

Seleccione la pestaña General y desplácese hacia abajo en el menú hasta que encuentre Protocolo de Internet (TCP/IP), luego seleccione Propiedades y registre manualmente los parámetros de red.

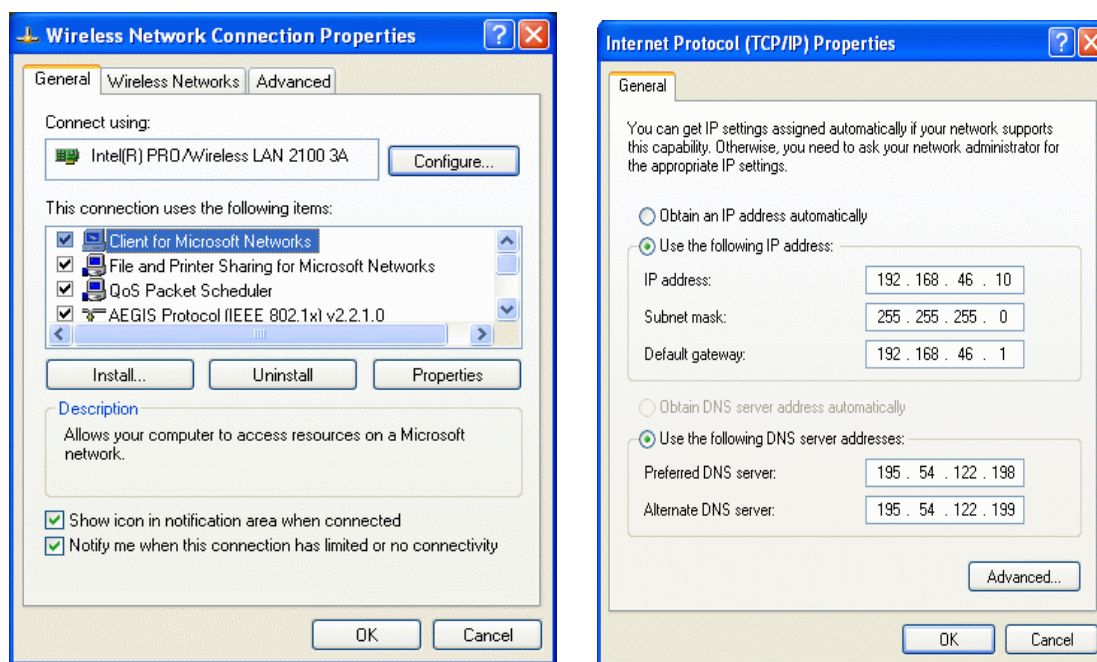


Figura 19: a) Seleccione Propiedades para configurar Protocolo Internet (TCP/IP).

b) Ajuste los parámetros IP manualmente incluyendo el servidor DNS preferido.

Le recomendamos usar la última versión del Service Pack para Windows XP. Las herramientas inalámbricas han sido mejoradas para SP2, especialmente en lo referente a la elección de la red a la que se desea conectar, y al firewall definido por defecto.

6. Conclusiones

Considerando lo visto en la primera parte de esta unidad referente a la Instalación de Puntos de Acceso, podemos decir que la configuración de un punto de acceso o un enrutador inalámbrico se puede resumir en los siguientes grandes pasos:

1. Entender el hardware y la solución que desea implementar.
2. Definir los parámetros inalámbricos relativos a la capa física como canal, SSID, potencia de transmisión y velocidad.
3. Definir los parámetros inalámbricos relativos a la capa de enlace como cifrado o control de acceso MAC.
4. Si quiere usar las funcionalidades de red de su punto de acceso definir los parámetros relativos a la capa de red como enrutamiento/NAT o servidor DHCP.

El desafío no es sólo aprender los menús de la herramienta de configuración, sino comprender mejor qué hace cada uno de los parámetros. Cada fabricante tendrá una configuración diferente para la interfaz, pero los “conceptos” van a ser los mismos.

Por otro lado, podemos concluir que el principal desafío que debemos afrontar en la Instalación de Clientes Inalámbricos, es determinar si el producto es soportado (hardware o software) por el sistema operativo que desea usar. En Windows esto casi nunca es un problema ya que los vendedores de hardware diseñan sus productos para trabajar con Windows. Para distribuciones Linux, esto puede volverse un desafío si el hardware inalámbrico está basado en un nuevo chipset para el que actualmente no hay drivers disponibles.



¡Si ese es el caso, sólo debe ser paciente y puede estar seguro de que la comunidad Linux le proveerá una solución en unos meses!

Los cinco asuntos principales a recordar de la segunda parte de esta unidad, con respecto a la instalación de clientes inalámbricos, se pueden resumir de la siguiente forma:

1. El éxito en la instalación de un cliente inalámbrico para Linux depende en gran medida de qué tan bien hizo el pre estudio sobre el driver y el soporte del chipset.
2. Si desea evitar problemas, antes de comprar el hardware para el cliente inalámbrico asegúrese de que esté soportado por su distribución.
3. Use Internet (Google) para averiguar sobre experiencias al realizar la misma tarea.
4. Asegúrese de conocer la configuración de red y radio (SSID, WEP, configuración IP) del punto de acceso al que desea conectarse.
5. Cuando trabaje con Windows, asegúrese de que sólo una Herramienta de gestión de configuración está corriendo pues de otro modo pueden ocurrir conflictos.

7. Ejercicios

7.1 Configuración de puntos de acceso

Se sugiere que los siguientes ejercicios sean realizados en grupo. Esta sugerencia se puede ajustar a las necesidades y habilidades específicas de los participantes del taller.

Imagine una situación típica:

- Existe una conexión a Internet, que puede ser una línea fija, DSL o conexión satelital.
- Usted desea permitir que muchos usuarios compartan la línea a través de un punto de acceso inalámbrico conectado a dicha línea.

¿Qué necesitará?: Una computadora, navegador, un mecanismo para conectar el punto de acceso (red inalámbrica o por cable).

Realice los siguientes pasos:

¡Restablezca (reset) el dispositivo!

¿Cómo lo va a hacer? _____

Conecte el punto de acceso. Requerirá conocer la configuración por defecto. Por favor registre los datos a continuación.

IP WAN: _____

IP LAN: _____

SSID: _____

Canal: _____

¿Tiene habilitado cifrado WEP? _____

¿Tiene habilitado DHCP? _____

Asigne una nueva clave al punto de acceso !Ahora! :)

Escríbalo aquí: _____

Cambie los parámetros de red –¡defina que el extremo del punto de acceso inalámbrico trabaje en la subred 10.11.12.x!

Si es necesario, ajuste las opciones de su computadora para reconectar el punto de acceso.

Escriba a continuación los datos de la configuración actual de red de su computadora:

Cambie el canal a 14 – si está permitido en su país.

Ajuste los parámetros de su computadora; si es necesario, reconecte.

Cambie el SSID a un nombre de su selección:

Escríbalo aquí:

Ajuste los parámetros de su computadora. Si es necesario, reconecte.

Use el control de direcciones MAC, de manera que el punto de acceso sólo le permita el acceso a usted y a su vecino.

Escriba a continuación su dirección MAC:

¿Cómo encontró su dirección MAC?

8. Recursos Adicionales

8.1 Puntos de acceso

8.1.1 En línea

Puntos de partida esenciales para la implementación de redes comunitarias:

<http://www.seattlewireless.net>

<http://www.freenetworks.org>

Libro en línea de Onno W. Purbo:

<http://sandbox.bellanet.org/~onno/the-guide/wifi>

Practicallynetworked tiene algunas guías referentes al montaje de Puntos de Acceso y redes:

http://practicallynetworked.com/networking/alternative_net_examples.htm

Actualización de firmware para soporte de WPA:

<http://support.microsoft.com/?kbid=815485#E0LB0ACAAA>

Montando un Linksys con cifrado WPA:

<http://www.stanford.edu/group/networking/lnaguide/docs/linksys/>

8.1.2 Libros/artículos

Flickenger. Rob. 2nd Edition June 2003. **Building Wireless Community Networks**. O'Reilly.

Standard introduction to all aspects of wireless community networking. I

SBN: 0-596-00502-4

Gast. Matthew. 1st Edition April 2002. **802.11 Wireless Networks: The Definitive Guide**. O'Reilly.

ISBN: 0-596-00183-5

Chapter 14 deals with Access Point Setup

8.2 Parte A: Instalación de clientes - Linux

8.2.1 En línea

General

[Roger Weeks](#), [Edd Dumbill](#), [Brian Jepson](#): "Linux Unwired" O'Reilly Associates

<http://www.oreilly.com/catalog/lnxunwired/>

Dispositivos inalámbricos, sus chipsets y manejadores:

http://www.linux-wlan.org/docs/wlan_adapters.html.gz

Drivers inalámbricos

hostap para prism2/2.5/3: <http://hostap.epitest.fi/>

Madwifi: <http://www.mattfoster.clara.co.uk/madwifi-faq.htm>

Orinoco: <http://www.nongnu.org/orinoco/>

ndiswrapper: <http://ndiswrapper.sourceforge.net/>

Linuxant: <http://www.linuxant.com/driverloader/>

Intel wireless/PRO 2100: <http://ipw2100.sourceforge.net/>

Intel wireless/PRO 2200:<http://ipw2200.sourceforge.net/>

prism54:<http://www.prism54.org/>

Cisco airo: <http://sourceforge.net/projects/airo-linux/>

More info: <http://www.seattlewireless.net/index.cgi/LinuxDrivers>

Software

Ubuntu Linux

<http://www.ubuntulinux.org/>

Mandrake Linux

<http://www.mandrakelinux.com/>

Red-Hat NetworkManager

<http://people.redhat.com/dcbw/NetworkManager/>

Usando la impresionante potencia y flexibilidad de [dbus](#) y [hal](#), NetworkManager provee facilidades para que otras aplicaciones de escritorio como navegadores y clientes de correo puedan mantenerse enterados del estado de la red y ajustar sus operaciones de acuerdo con características como la operación fuera de línea .

KwifiManager

<http://kwifimanager.sourceforge.net/>

Con la aplicación KWiFiManager usted puede configurar y monitorear su tarjeta de red bajo Linux/KDE.

Wifi Radar

http://www.bitbuilder.com/wifi_radar/

WiFi Radar es una utilidad de [Python/PyGTK2](#) para la administración de perfiles WiFi.

Herramientas para redes inalámbricas (iwconfig etc)

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

Linux Wireless Extension y *Wireless Tools* son un **proyecto de Software libre** patrocinado por [Hewlett Packard](#) (con mi contribución) desde 1996, y construido con la **colaboración de muchos usuarios de Linux** alrededor del mundo.

WPA sobre Linux (WPA_Supplicant)

http://hostap.epitest.fi/wpa_supplicant/

wpa_supplicant es un solicitante de WPA para Linux, BSD y Windows con soporte para WPA y WPA2 (IEEE 802.11i / RSN). Un Solicitante es el componente IEEE 802.1X/WPA que es usado en las estaciones cliente. Este implementa negociación de claves con un autenticador de WPA y controla el roaming y la autenticación/asociación IEEE 802.11 del driver de WLAN.

OpenSSH

<http://www.openssh.com/>

OpenSSH es una versión **LIBRE** del conjunto de aplicaciones para conexión a la red usando el protocolo SSH que incrementa el número de personas que confían en Internet.

IPSec

<http://www.ipsec-howto.org/>

El *how-to* oficial de IPSec para Linux

Linux PPTP Client

<http://pptpclient.sourceforge.net/>

PPTP Client es un cliente para Linux, FreeBSD, NetBSD y OpenBSD para el protocolo propietario de Microsoft Point-to-Point Tunneling Protocol, PPTP. Permite conectarse a una Red Privada Virtual (VPN por sus siglas en inglés) basada en PPTP y es usada por algunos proveedores de servicio por Cable o ADSL.

OpenVPN

<http://openvpn.net/>

OpenVPN es una solución con características completas para SSL VPN que puede adecuarse a una amplia gama de configuraciones, incluyendo acceso remoto, VPNs punto a punto, seguridad WiFi, y soluciones de acceso remoto para empresas, con balance de cargas, sistema de recuperación de fallos y controles de acceso bien definidos.

GPS Drive website

GpsDrive es un sistema de navegación para vehículos (carro, bicicleta, barco, avión). GpsDrive despliega su posición provista por un receptor GPS que utiliza el protocolo NMEA en un mapa ampliable, el archivo del mapa se puede seleccionar de acuerdo con la posición y escala preferidas.

<http://www.gpsdrive.cc/>

prismstumbler

<http://prismstumbler.sourceforge.net/>

Prismstumbler es una herramienta para descubrir redes inalámbricas para tarjetas basadas en Prism2.

Wellenreiter

<http://www.wellenreiter.net/>

Wellenreiter es una herramienta para descubrir y auditar redes inalámbricas. Soporta tarjetas basadas en Prism2, Lucent, y Cisco.

WDS

http://www.wikilearning.com/sacando_el_jugo_al_wireless_interconexion_de_redes_con_wds-wkc-779.htm

http://en.wikipedia.org/wiki/Wireless_Distribution_System

8.2.2 Libros/artículos

[Edd Dumbill](#), [Brian Jepson](#), [Roger Weeks](#).

“Linux Unwired”

Abril de 2004, O'Reilly *Linux Unwired* es una fuente de información inalámbrica muy completa para aquellos usuarios activos de Linux. Cuando usted esté considerando Wi-Fi como un suplemento o alternativa al cable DSL, usar Bluetooth en dispositivos de su casa u oficina, o quiere usar el plan de su celular para acceder a datos desde casi cualquier lugar, este libro le dará una visión completa de las posibilidades de redes inalámbricas con Linux , y cómo obtener ventaja de ellas.

Rob Flickenger

Wireless Hacks

Septiembre de 2003, O'Reilly

Escrito para usuarios intermedios a avanzados, *Wireless Hacks* está lleno de soluciones ingeniosas, directas y prácticas a los problemas reales de las redes. Cuando su red inalámbrica deba ir más allá del límite de su oficina o al otro lado de la ciudad, esta colección de no obvias, técnicas “desde campo” le mostrarán como realizar el trabajo.

8.3 Parte B: Instalación de clientes - Windows

8.3.1 En línea

¿Cómo configurar su computadora para conectarse a una red inalámbrica con Windows XP?

<http://support.microsoft.com/default.aspx?scid=kb;en-us;314897&sd=tech>

Último acceso 6 de Noviembre 2005.

¿Cómo instalar un cliente para redes Microsoft?

<http://compnetworking.about.com/cs/windowsnetworkin1/ht/client4msnet.htm>

Último acceso: 6 de Noviembre de 2005.

Instalar drivers de Windows 2000 y utilidades para adaptadores de clientes Cisco de la serie Aironet 340/350

http://www.cisco.com/en/US/products/hw/wireless/ps458/products_tech_note09186a0080094cf9.shtml

Cómo instalar tarjeta CISCO Aironet en Windows 2000

Último acceso: 6 de Noviembre de 2005.

Instrucciones de instalación/configuración de la tarjeta inalámbrica ORiNOCO

<http://www.willamette.edu/wits/resources/docs/network/wireless/orinoco.htm>

Manajadores y procedimiento para instalar tarjetas ORINOCO en Windows

Último acceso 6 de Noviembre de 2005.

Montaje de redes: Instalación de una simple red inalámbrica punto a punto

http://www.utexas.edu/its/wireless/install/install_peer.html

Guía de cómo montar una red inalámbrica punto a punto para intercambio de archivos o juegos de red en casa. Último acceso: 6 de Noviembre de 2005.

Conexión de redes Ethernet e inalámbricas para Windows NT

http://www.cmu.edu/computing/documentation/wireless_nt/Wire_WinNT.html

Documentación de la Universidad Carnegie Mellon sobre conexión a redes con plataforma WinNT.

Último acceso: 6 de Noviembre de 2005.

8.3.2 Libros/artículos

Wireless Home Networking for Dummies

Welcome to Wireless Home Networking For Dummies

por Danny Briere, Pat Hurley, Walter Bruce

Publicado: For Dummies (Mayo 27 de 2003)

ISBN: 0764539108

802.11 Wireless Networks: The Definitive Guide

Creating and Administering Wireless Networks

por Matthew Gast

Publicado: O'Reilly; 1ra edición (Abril de 2002)

ISBN: 0-596-00183-5

Building Wireless Community Networks, 2nd Edition

por Rob Flickenger

176 páginas

Publicado: O'Reilly; 2da edición (Junio 23 de 2003)

ISBN: 0596005024

Windows XP Home Networking

por Paul Thurrott

480 páginas

Publicado: Wiley; 1ra edición (Julio 17 de 2002)

ISBN: 0764536753

9. Declaración de Derechos de Propiedad Intelectual

Los materiales desarrollados en el marco del proyecto TRICALCAR utilizan una versión resumida del formato MMTK – Multimedia Training Kit. Han sido desarrollados para ser utilizados y compartidos libremente por instructores/as vinculados a proyectos de nuevas tecnologías para el desarrollo.

Todos los materiales están disponibles bajo una de las licencias Creative Commons <<http://creativecommons.org/>>. Estas licencias han sido desarrolladas con el propósito de promover y facilitar que se compartan materiales, pero reteniendo algunos de los derechos del autor sobre la propiedad intelectual.

Debido a que las organizaciones del Proyecto TRICALCAR que usan el formato MMTK para el desarrollo de sus materiales tienen diversas necesidades y trabajan en contextos diferentes, no se ha desarrollado una licencia única que cubra a todos los materiales. Para mayor claridad sobre los términos y condiciones en las que usted puede utilizar y redistribuir cada unidad temática, por favor verifique la declaración de derechos de propiedad intelectual incluida en cada una de ellas.

Provisiones de derechos de propiedad intelectual para esta unidad: Esta unidad temática se ha hecho disponible bajo los términos de la licencia **Atribución- No Comercial -Licenciamiento Recíproco**, bajo los siguientes términos:

- **Atribución.** Reconocer la autoría del material en los términos especificados por el propio autor o licenciante.
- **No comercial.** No puede utilizarse este material para fines comerciales.
- **Licenciamiento Recíproco.** Si altera, transforma o crea un material a partir de este, solo podrá distribuir el material resultante bajo una licencia igual a ésta.

Documento preparado para el taller de comunicaciones inalámbricas de Tshwane en Sudáfrica (c) 7th September 2005, Creative Commons Deed. Attribution-NonCommercial-ShareAlike 2.0 (c) 21 Abril 2007.

Este módulo integra la traducción y ajuste de dos de los módulos originales Puntos de Acceso y Clientes Inalámbricos:

Puntos de Acceso. Desarrollado por: IT +46. Basado en el trabajo original de: Onno W. Purbo and Sebastian Buettrich

Clientes Inalámbricos. Desarrollado por: Tomas B. Krag <t@wire.less.dk> (Linux) Bruno Roger, ESMT (Windows). Editado por: Alberto Escudero Pascual IT + 46. Traducido por Colnodo.