5
Equipamiento para Redes

En el último par de años, el surgimiento de un interés sin precedentes en el equipamiento para redes inalámbricas ha traído una enorme variedad de equipos económicos al mercado. Tanta variedad, que resultaría imposible catalogar cada uno de los componentes disponibles. En este capítulo, nos enfocamos en clasificar la clase de características y atributos que son deseables en los componentes inalámbricos, y vemos varios ejemplos de herramientas comerciales y DIY (hágalo usted mismo) que han funcionado bien en el pasado.

Cableado Inalámbrico

Con un nombre como el de "inalámbrico", usted podría sorprenderse de cuántos cables están involucrados en el desarrollo de un simple enlace punto a punto. Un nodo inalámbrico está conformado por varios componentes que deben estar conectados entre sí con el cableado apropiado. Obviamente, se necesita al menos una computadora conectada a una red Ethernet, un enrutador inalámbrico, o un puente en la misma red. Los componentes de radio deben conectarse a las antenas, pero en el trayecto pueden requerir un amplificador, un protector contra rayos (es un dispositivo de tres terminales, uno conectado a la antena, el otro al radio y el tercero a tierra), u otro dispositivo. Muchos de éstos requieren energía, ya sea a través de otro cable AC, o utilizando un transformador DC. Todos estos componentes utilizan varias clases de conectores, sin mencionar una amplia variedad de tipos de cable de diferentes calibres.

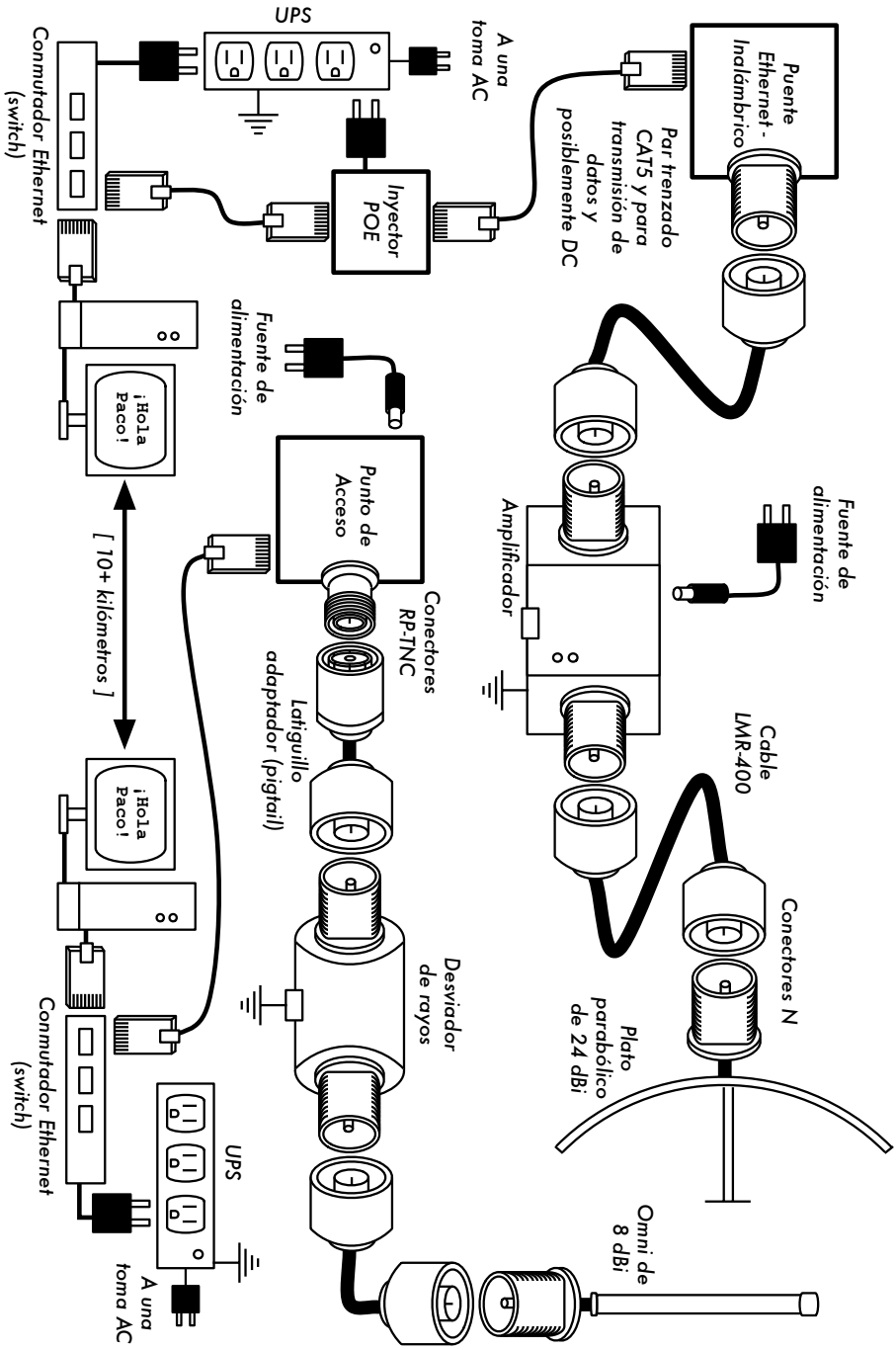

Figura 5.1: Interconexión de Componentes. .

Ahora multiplique esos cables y conectores por el número de nodos que va a instalar, y bien puede estar preguntándose porqué nos referimos a esta tecnología como "inalámbrica". El diagrama en la siguiente página le va a dar alguna idea del cableado requerido para un enlace típico punto a punto. Note que este diagrama no está a escala y no es necesariamente la mejor opción para el diseño de su red, pero le permitirá conocer en principio la variedad de conectores y componentes comunes que probablemente encontrará en el mundo real.

Aunque los componentes utilizados varían de nodo a nodo, toda instalación va incorporar estas partes:

1. Una computadora o una red conectada a un conmutador Ethernet (switch).
2. Un dispositivo que conecte esa red a un dispositivo inalámbrico (un enrutador inalámbrico, un puente o un repetidor).
3. Una antena integrada en el dispositivo inalámbrico, o conectada mediante un cable apropiado.
4. Componentes eléctricos consistentes en fuentes de alimentación, acondicionadores de energía, y protectores contra rayos.

La selección del equipamiento debe determinarse estableciendo los requerimientos del proyecto, el presupuesto disponible, y verificando que el proyecto sea viable utilizando los recursos disponibles (incluyendo provisiones para repuestos y costos de mantenimiento). Como discutimos en el capítulo uno, establecer el alcance de su proyecto es básico antes de tomar cualquier decisión de adquisiciones.

Eligiendo los componentes inalámbricos

Desafortunadamente, en un mundo de fabricantes de equipamiento que compiten entre sí y con una disponibilidad limitada de fondos, el tema del precio es el factor que generalmente recibe la mayor atención. El viejo dicho "tanto pagas, tanto obtienes" se cumple cuando compramos equipamiento de alta tecnología, pero no debe ser considerado como una verdad absoluta. Mientras que el precio es una parte importante de cualquier decisión de compra, es de vital importancia comprender precisamente qué es lo que puede obtener por su dinero, para que pueda hacer una elección que se ajuste a sus necesidades.

Cuando compare equipamiento inalámbrico para ser usado en su red, asegúrese de considerar estas variables:

- **Interoperabilidad.** ¿El equipamiento que está considerando funcionará con el de otros fabricantes? Si no es así, ¿es un factor importante para este segmento de su red? Si el equipo en cuestión soporta un protocolo abierto (como el 802.11b/g), entonces probablemente va a funcionar con equipamiento de otras fuentes.
- **Rango.** Como dijimos en el capítulo cuatro, el rango no es algo inherente a una pieza particular del equipo. El rango de un dispositivo depende de la antena conectada a él, el terreno que lo rodea, las características del dispositivo en el otro extremo del enlace, además de otros factores. En lugar de confiar en el valor del "rango" semi-ficticio provisto por el fabricante, es más útil conocer la ***potencia de transmisión*** del radio así como la ***ganancia de la antena*** (si está incluida la antena). Con esta información usted puede calcular el rango teórico como fue descrito en el capítulo tres.
- **Sensibilidad del radio.** ¿Cuán sensible es el dispositivo de radio a una tasa de transferencia dada? El fabricante debe proveer esta información, al menos a las velocidades más rápidas y más lentas. Esto puede utilizarse como una medida de la calidad del equipo, y le permite completar el cálculo del costo del enlace. Como vimos en el capítulo tres, mientras más bajo sea este valor mejor será la sensibilidad del radio.
- **Rendimiento.** Los fabricantes sistemáticamente ponen la tasa de transferencia más alta posible como la "velocidad" de su equipo. Tenga en mente que el valor de la tasa de transferencia del radio (ej. 54Mbps) nunca es el verdadero rendimiento del dispositivo (ej. aproximadamente 22Mbps para 802.11g). Si la información del rendimiento no está disponible para el dispositivo que usted está evaluando, un buen truco es dividir la "velocidad" del dispositivo por dos, y restar el 20% más o menos. Si tiene alguna duda, realice la prueba de rendimiento en una unidad de evaluación antes de comprometerse a adquirir una gran cantidad de equipamiento que no especifica una tasa de rendimiento oficial.
- **Accesorios requeridos.** Para mantener el precio inicial bajo, los vendedores a menudo quitan accesorios que se requieren para un uso normal. ¿El precio incluye todos los adaptadores de potencia? (Las fuentes DC generalmente se incluyen; pero los inyectores de potencia para Ethernet (POE) en general no. Del mismo modo, revise dos veces los voltajes de entrada, ya que el equipo normalmente viene con especificaciones de alimentación correspondiente a los estándares utilizados en los Estados Unidos. ¿Viene con los *pigtails*, adaptadores, cables, antenas, y las tarjetas de radio? Si piensa usarlo en exteriores, ¿incluye el dispositivo una caja impermeable?
- **Disponibilidad.** ¿Va a ser capaz de reemplazar los componentes que se rompan? ¿Puede ordenar esa parte en grandes cantidades? ¿Su proyecto va a requerir esas partes? ¿Cuál es el lapso de vida proyectado de este

producto en particular, en términos de tiempo de funcionamiento en el campo y probabilidad de que el vendedor lo siga suministrando?

- **Otros factores.** Asegúrese de que se provean otras características importantes para satisfacer sus necesidades particulares. Por ejemplo, ¿incluye el dispositivo un conector para una antena externa? Si lo hace, ¿de qué tipo es? ¿Existen limitaciones en número de usuarios o en el rendimiento impuestas por software, y si las hay, cuál es el costo de extender esos límites? ¿Cuál es la forma física del dispositivo? ¿Cuánta potencia consume? ¿Soporta POE como fuente de potencia? ¿Provee encriptación, NAT, herramientas de monitoreo de ancho de banda, u otras características críticas para el diseño de la red?

Contestando estas preguntas primero, va a poder tomar decisiones de compra inteligentes cuando sea el momento de elegir el equipamiento de la red. Es casi imposible que usted pueda contestar todas las dudas posibles antes de comprar el equipo, pero si le da prioridad a estas preguntas y presiona al vendedor para que las conteste antes de comprometerse a comprar, hará un mejor uso de su presupuesto y va a construir una red con componentes que se adecuen a sus necesidades.

Soluciones comerciales vs. Soluciones DIY (hágalo usted mismo)

Lo más seguro es que su proyecto de red incluya componentes adquiridos a través de proveedores externos así como otros conseguidos o fabricados localmente. Esta es una verdad económica en la mayor parte del mundo. En este estadio de la tecnología humana, la distribución global de la información es algo trivial en comparación a la distribución global de bienes. En muchas regiones, importar cada componente necesario para construir la red es prohibitivamente caro para la mayoría, aún para los grandes presupuestos. Se puede ahorrar mucho dinero a corto plazo encontrando fuentes locales para partes y mano de obra, e importar sólo aquellos componentes que lo ameriten.

Por supuesto que hay un límite a lo que puede ser hecho por una persona o un grupo en un tiempo determinado. Para ponerlo de otra forma, mediante la importación de tecnología, se intercambia dinero por equipamiento que le puede solucionar un problema particular en un periodo comparativamente inferior de tiempo. El arte de construir infraestructuras de comunicaciones locales está en encontrar el correcto balance entre el dinero y el esfuerzo que se necesita para resolver un problema dado.

Algunos componentes como las tarjetas de radio y los cables de antenas, son definitivamente muy complejos como para considerar fabricarlos local-

mente. Sin embargo, otros elementos como las antenas y las torres son relativamente simples y pueden hacerse a nivel local por una fracción del costo de importación. Entre estos dos extremos se encuentran los dispositivos de comunicación en sí.

Utilizando componentes disponibles como las tarjetas de radio, placas madre, y otros, se pueden construir dispositivos que provean características comparables (o aún superiores) a la mayoría de las implementaciones comerciales. Combinar plataformas de equipamiento abiertas con software de fuente abierta puede resultar en una verdadera ganga, porque provee soluciones robustas y a la medida por muy bajo costo.

Esto no quiere decir que el equipamiento comercial sea inferior a una solución "hágalo usted mismo". Al proveernos las conocidas "llave en mano", los fabricantes no sólo nos ahorran tiempo de desarrollo, sino que también permiten que personas relativamente no calificadas puedan instalar y mantener el equipamiento. La fortaleza principal de las soluciones comerciales es que ellas proveen ***soporte*** y ***garantía de equipamiento*** (usualmente limitada). También tienen una ***plataforma consistente*** que tiende a que las instalaciones de red sean muy estables y a menudo intercambiables.

Si una parte del equipamiento no funciona, es difícil de configurar, o tiene problemas, un buen fabricante lo va a asistir. Si en uso normal el equipamiento falla (excluyendo daños extremos, como los ocasionados por la caída de un rayo), el fabricante lo va a reemplazar. La mayoría ofrecen esos servicios por un tiempo limitado como parte del precio de compra, y otros brindan soporte y garantía por un período de tiempo extendido mediante el pago de una cuota mensual. Teniendo una plataforma consistente es sencillo tener los repuestos a mano y simplemente "cambiar" el equipo que falla sin la necesidad de un técnico que configure el equipo. Evidentemente esto viene de la mano de un costo inicial más alto si lo comparamos con los componentes disponibles localmente.

Desde el punto de vista de un arquitecto de red, los tres grandes riesgos ocultos al elegir soluciones comerciales son: ***quedar atrapado con un proveedor***, las ***líneas de productos descontinuadas***, y ***los costos de licenciamiento futuro***.

Puede ser muy costoso dejar que las mal denominadas nuevas "características" dirijan el desarrollo de su red. Los fabricantes frecuentemente van a ofrecerle características que son incompatibles por su diseño con los de la competencia, y luego usan elementos de mercadeo para convencerlo de que usted no puede vivir sin éstas, sin importar que la característica contribuya a solucionar sus problemas de comunicación o no. Al empezar a contar con esas características, probablemente en el futuro decidirá continuar comprando equipamiento del mismo fabricante. Esa es la esencia de quedar

atrapado con el proveedor. Si una gran institución utiliza una cantidad significante de equipamiento patentado, es improbable que simplemente vaya a abandonarlo para considerar un proveedor diferente. Los equipos de venta saben esto (y de hecho, algunos cuentan con ello) y utilizan esto como estrategia para la negociación de precios.

Un fabricante puede eventualmente decidir descontinuar una línea de productos sin importar su popularidad. Esto asegura que los clientes, que ya confiaban en las características del producto patentado del fabricante, van a comprar los nuevos modelos (casi siempre más caros). Los efectos a largo plazo de quedar atrapado con el proveedor y con los productos descontinuados, son difíciles de estimar cuando planificamos un proyecto de red, pero deben tenerse en mente.

Finalmente, si una pieza en particular del equipamiento utiliza un código de computadora patentado, usted va a tener que licenciar el uso de ese código en contratos futuros. El costo de esas licencias puede variar dependiendo de las características que brinda, el número de usuarios, la velocidad de la conexión u otros factores. ¡Si no se paga el costo de la licencia, algunos equipos están diseñados para simplemente dejar de funcionar hasta que se provea una licencia válida! Asegúrese de que comprende los términos de uso de cualquier equipamiento que adquiera, incluyendo las futuras cuotas de licenciamiento.

Usando equipamiento genérico que soporta estándares abiertos y software de fuente abierta, se pueden evitar algunos de estos riesgos. Por ejemplo, es muy difícil verse atrapado por un proveedor que utiliza protocolos abiertos (tales como TCP/IP sobre 802.11a/b/g). Si tiene un problema con el equipo o con el proveedor, siempre puede adquirirlo de otro proveedor, ya que va a funcionar con lo que usted ya compró. Es por estas razones que recomendamos utilizar protocolos patentados y espectro con licenciamiento **sólo** en casos donde el equivalente abierto (como el 802.11a/b/g) no es viable técnicamente.

Si bien los productos individuales pueden discontinuarse en cualquier momento, usted puede limitar el impacto que esto va a tener en su red utilizando componentes genéricos. Por ejemplo, si una *placa madre* particular ya no está disponible en el mercado, puede tener a mano varias *placas madre* de PC que van a desempeñarse efectivamente en la misma tarea. Más adelante en este capítulo vamos a ver algunos ejemplos de cómo utilizar esos componentes genéricos para construir un nodo inalámbrico completo.

Obviamente, no va a haber costos de licenciamiento en cuanto al software libre (con la excepción de un proveedor que ofrezca soporte u otros servicios sin cobrar por el uso del software en sí mismo). Ha habido ocasionalmente vendedores que se aprovechan indebidamente del regalo que los programa-

dores de fuente abierta le han dado al mundo, exigiendo el pago de licencias, violando de ese modo los términos de distribución acordados por los autores originales. Sería bueno evitar a dichos vendedores, y desconfiar de aquellas afirmaciones de "software libre" que, sin embargo, estipulan una cuota de licenciamiento a futuro.

La desventaja de utilizar software libre y equipamiento genérico es claramente una cuestión de soporte. Cuando lleguen los problemas a la red, va a tener que resolverlos por usted mismo. Esto a veces se logra consultando recursos gratuitos en línea y motores de búsqueda, y aplicando los parches al código directamente. Si no tiene ningún miembro de su equipo que sea competente en el tema y se dedique a diseñar soluciones a sus problemas de comunicación, entonces poner en marcha un proyecto de red puede tomar una cantidad considerable de tiempo. Por supuesto que tampoco hay garantías de que simplemente "a punta de dinero" se resuelva el problema. Si bien damos varios ejemplos de cómo hacer el trabajo usted mismo, seguramente le va a resultar un gran desafío. Necesita encontrar el balance entre el enfoque de las soluciones comerciales y las hechas por usted mismo, que funcionen de forma adecuada a su proyecto.

En resumen, siempre defina primero el objetivo de su red, identifique los recursos que puede tener para lidiar con el problema, y permita que la selección del equipamiento emerja naturalmente de esos resultados. Considere las soluciones comerciales así como los componentes abiertos, manteniendo siempre en mente los costos a largo plazo de ambas.

Productos inalámbricos profesionales

En el mercado existe equipamiento en abundancia para enlaces punto a punto (P2P) a larga distancia. La mayoría ya está listo para ponerse en funcionamiento al sacarlo de la caja; solamente debemos conectar y sellar los cables de la antena. Cuando pensamos en un enlace a larga distancia, existen tres factores principales que debemos considerar: la distancia total del enlace, los requerimientos de tiempo de puesta en funcionamiento, y por supuesto los requerimientos de velocidad.

La mayoría de los productos comerciales disponibles en la actualidad para enlaces de largo alcance, utilizan tecnología OFDM y operan en la banda ISM de 5800 MHz. Existen algunos productos que utilizan estándares abiertos, pero la mayoría tienen protocolos propietarios de algún tipo. Esto significa que para formar un enlace, las radios de ambos lados deben ser del mismo fabricante. Para el caso de un enlace crítico es una buena idea elegir un sistema que utilice equipamiento idéntico en ambos extremos del enlace. De esta forma se necesita tener almacenado solamente un repuesto, y si se tiene que usar puede reemplazarse en cualquier lado del enlace. Hay algu-

nos productos buenos en el mercado que usan diferentes equipamientos en los extremos del enlace. Los mismos pueden usarse en una red siempre que se haga con cuidado, de lo contrario se van a necesitar más repuestos para ambos tipos de radios.

Lo que sigue no intenta ser propaganda de venta de un radio, ni tampoco una queja acerca de otros. Son simplemente algunas notas generadas durante más de cinco años de experiencia de campo alrededor de todo el mundo, con productos comerciales sin licenciamiento. Desafortunadamente, no hay forma de considerar todos los productos, por esa razón sólo algunos de los favoritos se listan a continuación.

Redline Communications

Redline llegó al mercado en primera instancia con la línea de productos AN-50. Este fue el primer producto punto a punto disponible con tasas de transferencia de datos sobre los 50 Mbps, al alcance de los pequeños operadores. Sólo utiliza 20 MHz del espectro por canal. Hay tres modelos diferentes en la línea AN-50. Los tres tienen el mismo grupo de características básicas, sólo cambia el ancho de banda total. El modelo estándar tiene 36 Mbps de rendimiento, el modelo económico tiene 18 Mbps, y la versión completa 54 Mbps. Los controles del ancho de banda son a través de un programa y pueden acomodar la demanda de ancho de banda.

Los radios Redline están compuestos de una unidad interna, una externa y una antena. La unidad interna entra en un estante estándar de 19 pulgadas y ocupa 1U (1,5 pulgadas de altura). La unidad externa se monta en el mismo soporte que mantiene la antena en su lugar. Esta unidad es el radio. Las dos unidades están unidas por un cable coaxial. Se utiliza el cable Beldon RG6 o el RG11. Es el mismo que se utiliza para las instalaciones satelitales de TV. No es caro, se encuentra fácilmente y elimina la necesidad de adquirir cables caros de baja pérdida, como la serie de *Times Microwave LMR* o *Andrew Corporation Heliax*. El hecho de montar el radio tan cerca de la antena mantiene la pérdida del cable en un mínimo absoluto.

Debemos destacar dos características de los radios Redline. La primera es el ***Modo de Alineación General***, que utiliza una alarma sónica (*beeper*) que cambia el tono cuando cambia la técnica de modulación. Un beep más rápido significa una conexión más rápida. Esto permite un alineamiento mucho más sencillo porque el enlace puede ser alineado por los tonos únicamente. Sólo se necesita una sintonización final, y para ayudarnos tenemos una aplicación gráfica de Windows. Otra característica es el botón de ***Prueba***. Si realizamos cambios al radio, y no estamos seguros de que sean los correctos, presionando el botón de prueba en lugar del botón ***Guardar***, activará los nuevos cambios por cinco minutos. Después de esos cinco minutos, la configuración vuelve a la configuración anterior a apretar el botón

de ***Prueba***. Esto permite que se prueben los cambios, y si las cosas no funcionan y el enlace cae, el mismo se recobrará después de cinco minutos. Una vez que los cambios hayan sido probados, simplemente se confirma la nueva configuración, y se presiona el botón de guardar en lugar del de prueba.

Redline tiene otros modelos disponibles. El AN-30 tiene cuatro puertos T1/E1, además de una conexión a Ethernet de 30 Mbps. El AN-100 sigue el estándar 802.16a, y el próximo RedMax promete adherir a WiMax.

Por más información acerca de estos los productos vea *http://www.redlinecommunications.com/*

Alvarion

Una de las grandes ventajas de trabajar con los productos Alvarion es su bien establecida red de distribución mundial. También tienen una de las cuotas del mercado mundial más grande para toda clase de equipamiento de conectividad inalámbrica a Internet. Tiene distribuidores y revendedores en la mayoría de las regiones. Para los enlaces a larga distancia ofrece dos productos de interés: La serie VL, y el Link Blaster.

Si bien la serie VL es en realidad un sistema punto a multi-punto, un solo radio cliente conectado a un punto de acceso funcionará bien para establecer un enlace punto a punto. Lo único que debe considerarse es utilizar una antena con mayor direccionalidad en el punto de acceso, a menos que haya un enlace planeado a futuro que puede conectarse a ese punto de acceso. Hay dos velocidades disponibles para la serie VL, 24 Mbps y 6 Mbps. Los requerimientos de costo, tiempo de la señal y velocidad van a guiar la decisión de cuál CPE (*Customer Premises Equipment*- equipo de usuario) usar.

El Link Blaster se parece muchísimo al Redline AN-50. Esto se debe a que de hecho son el mismo aparato. Casi enseguida después de que el Redline AN-50 llegó al mercado, se firmó un acuerdo OEM (Original Equipment Manufacturer) entre las dos compañías y así nació el Link Blaster. A pesar de que la caja del modelo para interiores es diferente, y de que las antenas están marcadas de forma distinta, los componentes electrónicos internos de estos modelos son idénticos. El Link Blaster cuesta más que un Redline; este valor adicional se justifica por un diseño más robusto así como un nivel de soporte adicional. En muchos casos, a un revendedor de Alvarion le es sencillo conseguir productos de revendedores de Redline. Esto debe ser investigado a nivel local. Puede valer más la pena el dinero extra para tener un producto que esté disponible y tenga soporte local.

Alvarion tiene algunos productos para enlaces punto a punto de 2400 MHz. La mayoría de sus productos usan la banda ISM en los 2400 MHz con la

tecnología de espectro esparcido de salto de frecuencia (*FHSS por su sigla en inglés*) y generan mucho ruido que puede afectar otras aplicaciones sobre el espectro esparcido que usen secuencias directas (*DSSS por su sigla en inglés*) y que se encuentren en la misma torre. Si se está planeando una red basada en un sistema de distribución DSSS, un transporte (*backhaul*) FHSS no es una opción efectiva.

Para más información acera de los productos Alvarion, vea *http://www.alvarion.com/*

Rad Data Communications

La línea de productos Rad Airmux es relativamente nueva en el Mercado, y tiene un potencial grande. El Airmux 200 es una radio de 48 Mbps, usa el cable CAT5, y tiene uno de los mejores precios para cualquier solución comercial. Las unidades son pequeñas y fáciles de manipular en una torre. La única contra con la que nos podemos enfrentar es la falta de un sistema distribución local en el mundo en desarrollo. Tenemos dos modelos disponibles dentro de la línea Airmux. Uno usa antenas internas, y el otro externas.

La experiencia con los radios Airmux a principios del 2005 mostró la existencia de un problema con la temporización. Sólo se ve cuando la distancia del enlace es mayor a 12 millas, o 19 km. No importa qué tipo de antena se esté usando. Mientras que este problema no sea solucionado, esos radios sólo deberían utilizarse para enlaces de hasta 19 km. Si se sigue este consejo los radios van a desempeñarse muy bien, especialmente desde el punto de vista de su precio.

Para más información acerca de los productos Rad, vea *http://www.rad.com/*

Cisco Systems

Las soluciones inalámbricas de Cisco tienen dos grandes ventajas a su favor. Tienen una distribución muy bien establecida, soporte y entrenamiento en redes por casi todo el mundo. Esto puede ser de gran ayuda cuando debemos procurarnos el equipamiento, y aún más importante, si el mismo se rompe y necesitamos reemplazarlo. La siguiente gran ventaja es que utilizan estándares abiertos para la mayoría de las partes, siguiendo los estándares 802.11a/b/g.

La experiencia ha mostrado que sus herramientas de configuración vía web no son tan sencillas de comprender como las que encontramos en muchos otros productos, y el equipamiento tiende a tener un precio que hace que otras soluciones no comerciales de estándares abiertos sean más viables.

Más información acerca de Cisco se puede encontrar en *http://www.cisco.com/*

¿Algunas otras?

Actualmente hay muchas más soluciones disponibles en el mercado y siguen llegando otras todo el tiempo. Buenas soluciones se encuentran en compañías como Trango Broadband (*http://www.trangobroadband.com/*) y Waverider Communications (*http://www.waverider.com/*). Cuando consideremos qué solución utilizar, siempre debemos recordar los tres factores principales; distancia, tiempo de puesta en funcionamiento y velocidad. Debe chequear y asegurarse de que las radios operan en una banda sin licenciamiento donde usted las va a instalar.

Protectores profesionales contra rayos

La única amenaza natural del equipamiento inalámbrico son los rayos eléctricos. Hay dos formas diferentes mediante las cuales un rayo puede dañar el equipo: con un impacto directo o uno inducido. Los impactos directos son cuando el rayo realmente alcanza la torre o la antena. El impacto inducido se produce cuando el rayo cae cerca de la torre. Imagine un relámpago cargado negativamente. Como las cargas se repelen entre sí, hará que los electrones en el cable se alejen del rayo, creando corriente en las líneas. Esta es mucha más corriente de la que el sensible radio puede manejar. En general, cualquier tipo de rayo va a destruir el equipo que esté sin protección.

Proteger las redes inalámbricas de los relámpagos no es una ciencia exacta, y no hay garantías de que no vaya a caer un rayo, aún si se toman todas las precauciones. Muchos de los métodos utilizados van a ayudar a prevenir los impactos directos y los generados por inducción. Si bien no es necesario utilizar todos los métodos de protección contra rayos, tener más de uno va a ayudarnos a cuidar mejor el equipo. La cantidad de rayos observados históricamente en un área de servicio es la mejor guía para saber que debemos hacer.

Comience en la base misma de la torre. Recuerde que la base de la torre está bajo tierra. Después de colocados los cimientos de la torre, pero antes de que el pozo se llene nuevamente, se debe instalar un aro de alambre trenzado grueso para hacer tierra, extendido bajo la superficie y sobresaliendo de la misma cerca de la pata de la torre. El alambre debe ser por lo menos AWG #4 (*American Wire Gauge*) o más grueso. Adicionalmente, se debe enterrar una jabalina, y conectarla también a la torre en el mismo punto.

Figura 5.2: Torre con un cable de cobre grueso conectado a tierra.

Es importante tener en cuenta que no todos los metales conducen la electricidad de la misma forma. Algunos metales actúan como conductores eléctricos mejor que otros, y las diferentes capas existentes en la superficie también pueden afectar cómo el metal de la torre maneja la corriente eléctrica. El acero inoxidable es uno de los peores conductores, y las capas contra la herrumbre como los galvanizados o la pintura reducen la conductividad del metal. Por esta razón se coloca un alambre de tierra trenzado desde la base de la torre hasta la cima. La base necesita estar apropiadamente unida a los conductores provenientes del aro y de la jabalina. La cima de la torre debe tener una jabalina pararrayos, terminada en punta. Cuanto más fina y aguda sea la punta, más efectivo será el pararrayos. El alambre de tierra trenzado desde la base tiene que terminarse en esta jabalina. Es muy importante asegurarse de que el alambre de tierra esté conectado al propio metal. Cualquier tipo de capa, como la pintura, debe removerse antes de que se coloque el alambre. Una vez que se hizo la conexión, si es necesario, el área expuesta puede repintarse, cubriendo el alambre y los conectores para proteger a la torre de la herrumbre y la corrosión.

La solución anterior detalla la instalación de un sistema básico de tierra. El mismo provee protección para la torre contra los impactos directos, y representa el sistema de base al que se conectará todo lo demás.

La protección ideal para los impactos indirectos son protectores de gas contra rayos ubicados en ambos extremos del cable. Estos protectores contra rayos deben ser conectados directamente al alambre de tierra instalado en

la torre si este está en el extremo más alto. El extremo en la base debe también conectarse a una buena tierra, como una placa de tierra o una tubería metálica que esté llena de agua. Es importante asegurarse de que el protector contra rayos externo esté impermeabilizado. Muchos protectores contra rayos para los cables coaxiales son impermeables, mientras que los de cable CAT5 no lo son.

En el caso de que no se usen los protectores contra rayos, y el cableado esté basado en coaxiales, se conecta el revestimiento del cable coaxial al cable de tierra instalado en las torres, y de esta forma proveerá algo de protección. Esto proporciona un camino a tierra a las corrientes inducidas, y si la descarga no es muy fuerte no va a afectar el cable coaxial. Si bien este método no da una protección tan buena como la utilización de los protectores de gas, es mejor que nada.

Construyendo un AP con una PC

A diferencia de los sistemas operativos para consumidores (como Microsoft Windows), el sistema operativo GNU/Linux le brinda al administrador de red acceso completo a muchos elementos del trabajo en redes. Podemos acceder y manipular paquetes de red a cualquier nivel, desde la capa de enlace de datos hasta la capa de aplicación. Se pueden tomar decisiones de enrutamiento con base a cualquier información contenida en el paquete de red, desde la dirección de enrutamiento y puertos, hasta los contenidos de los segmentos de datos. Un punto de acceso basado en Linux puede actuar como enrutador, puente, corta fuego, concentrador VPN, servidor de aplicaciones, monitor de la red, o virtualmente cualquier otro rol de la red en el que usted pueda pensar. Es un software libre, y no requiere pagos de licenciamiento. Linux/GNU es una herramienta muy poderosa que puede ajustarse a una amplia variedad de roles en una infraestructura de red.

Agregar una tarjeta inalámbrica y un dispositivo Ethernet a una PC corriendo Linux le dará una herramienta muy flexible que puede ayudarlo a repartir el ancho de banda y administrar su red a un costo muy bajo. El equipamiento puede ser desde una computadora portátil reciclada, o una computadora de escritorio, hasta una computadora embebida, tales como un equipo de red Linksys WRT54G o Metrix.

En esta sección veremos cómo configurar Linux en las siguientes configuraciones:

- Como punto de acceso inalámbrico utilizando Masquerading/NAT y una conexión cableada a Internet (también denominada *gateway*).

- Como punto de acceso inalámbrico que actúa como puente transparente. El puente puede usarse tanto como un simple punto de acceso, o como un repetidor con dos radios.

Considere estas recetas como un punto de inicio. Construyendo estos ejemplos simples, puede crear un servidor que se ajuste de forma precisa a su infraestructura de red.

Pre-requisitos

Antes de comenzar, debe estar familiarizado con Linux desde la perspectiva del usuario, y ser capaz de instalar la distribución Linux/Gnu de su elección. También se requiere una comprensión básica de la interfaz de línea de comando (*terminal*) en Linux.

Va a necesitar una computadora con una o más tarjetas inalámbricas instaladas previamente, así como una interfaz Ethernet estándar. Estos ejemplos utilizan una tarjeta y un manejador (*driver*) específicos, pero hay varios tipos diferentes de tarjetas que pueden funcionar igualmente bien. Las tarjetas inalámbricas basadas en los grupos de chips Atheros y Prism lo hacen particularmente bien. Estos ejemplos se basan en la versión de Linux Ubuntu 5.10 (Breezy Badger), con una tarjeta inalámbrica soportada por los manejadores HostAP o MADWiFi.

Para más información acerca de estos manejadores vea *http://hostap.epitest.fi/* y *http://madwifi.org/*.

Para completar estas instalaciones se requiere del siguiente software, el cual debe estar incluido en su distribución Linux:

- Herramientas Inalámbricas (comandos iwconfig, iwlist)
- Cortafuego iptables
- dnsmasq (servidor cache DNS y servidor DHCP)

La potencia de CPU que se requiere depende de cuánto trabajo se tiene que hacer más allá de un simple enrutamiento y NAT. Para muchas aplicaciones una 486 de 133MHz es perfectamente capaz de enrutar paquetes a las velocidades inalámbricas. Si piensa usar mucha encriptación (como WEP o un servidor VPN), entonces necesita algo más rápido. Si también quiere correr un servidor de almacenamiento intermedio (como Squid, vea el capítulo tres) necesitará una computadora con mucha más rapidez, espacio de disco y memoria RAM. Un enrutador típico que solo esté realizando NAT puede operar con tan solo 64MB de RAM y almacenamiento.

Cuando armamos una máquina que está pensada para ser parte de una infraestructura de red, debemos tener en cuenta que los discos duros tienen una vida útil limitada en comparación con la mayoría de los otros componentes. A menudo puede utilizar almacenamiento de estado sólido, como un disco *flash*, en lugar de un disco duro. Este puede ser un manejador *flash* USB (suponiendo que su PC va a cargarse desde USB), o una tarjeta Compact Flash utilizando un adaptador de CF a IDE. Estos adaptadores son bastante económicos, y permiten que una tarjeta CF actúe en apariencia como un disco duro IDE. Pueden usarse en cualquier PC que soporte discos duros IDE. Como no tienen partes móviles, funcionarán por muchos años en un rango mucho más alto de temperaturas de las que puede tolerar un disco duro.

Escenario 1: punto de acceso con Enmascaramiento

Este es el más simple de los escenarios, y es especialmente útil en situaciones donde usted quiere un único punto de acceso para una oficina. Es el más fácil en una situación donde:

1. Existen un cortafuego y una pasarela (*gateway*) dedicados corriendo Linux, y usted sólo quiere agregar una interfaz inalámbrica.
2. Usted dispone de una vieja computadora común o portátil restaurada y prefiere utilizarla como un punto de acceso.
3. Requiere de más potencia en términos de monitoreo, registro y/o seguridad de lo que la mayoría de los puntos de acceso comerciales le proveen, pero no quiere derrochar en un punto de acceso empresarial.
4. Le gustaría que una única computadora actuara como dos puntos de acceso (y cortafuego) para poder ofrecer un punto de acceso seguro a la intranet, así como acceso abierto a los invitados.

Configuración inicial

Comience con una computadora ya configurada corriendo Linux/Gnu. Puede ser una instalación de Servidor Ubuntu, o Fedora Core. Para su funcionamiento, la computadora debe tener al menos dos interfaces, y al menos una de ellas debe ser inalámbrica. El resto de esta descripción supone que su puerto Ethernet (eth0) está conectado a la Internet, y que hay una interfaz inalámbrica (wlan0) que va a proveer la funcionalidad del punto de acceso.

Para saber si su grupo de chips soporta el modo maestro, pruebe con el siguiente comando en modo raíz (root):

```
# iwconfig wlan0 mode Master
```

...reemplazando wlan0 con el nombre de su interfaz.

Si obtiene un mensaje de error, su tarjeta inalámbrica no soporta el modo de punto de acceso. De todas formas puede probar la misma configuración en el modo ad hoc, que es soportado por todos los grupos de chips. Esto requiere configurar todas las computadoras portátiles que están conectadas al "punto de acceso" en el modo ad hoc, y puede que no funcione del modo que usted espera. En general es mejor encontrar una tarjeta inalámbrica que soporte el modo AP. Para obtener una lista de las tarjetas soportadas vea los sitios web HostAP y MADWiFi mencionados anteriormente.

Antes de continuar asegúrese de que dnsmasq está instalado en su computadora. Puede utilizar la herramienta de configuración gráfica de su distribución para instalarlo. En Ubuntu puede simplemente correr lo siguiente en modo raíz (root):

```
# apt-get install dnsmasq
```

Configurar las interfaces

Configure su servidor para que eth0 esté conectada a Internet. Utilice la herramienta de configuración gráfica que viene con su distribución.

Si su red Ethernet usa DHCP, puede probar con el siguiente comando como raíz:

```
# dhclient eth0
```

Debe recibir una dirección IP y una pasarela por defecto. Luego arranque su interfaz inalámbrica en el modo Maestro y póngale un nombre de su elección:

```
# iwconfig wlan0 essid "my network" mode Master enc off
```

El comando **`enc off`** desconecta la encriptación WEP. Para habilitar WEP agregue la clave hexagesimal del largo correcto:

```
# iwconfig wlan0 essid "my network" mode Master enc 1A2B3C4D5E
```

Como una alternativa, puede utilizar una clave legible comenzando con "**`s:`** "

```
# iwconfig wlan0 essid "my network" mode Master enc "s:apple"
```

Ahora déle a su interfaz inalámbrica una dirección IP en una sub red privada, pero asegúrese de que no sea la misma sub red de la de su adaptador Ethernet:

```
# ifconfig wlan0 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255 up
```

Configurar enmascarado en el kernel

Para ser capaces de traducir direcciones entre dos interfaces en la computadora, debemos habilitar el enmascarado (NAT) en el kernel linux. Primero cargamos el módulo kernel pertinente:

```
# modprobe ipt_MASQUERADE
```

Ahora vamos a desactivar todas las reglas del cortafuego existente para asegurarnos que las mismas no van a bloquearnos al reenviar paquetes entre las dos interfaces. Si tiene un cortafuego activado, asegúrese de que sabe cómo restaurar las reglas existentes antes de proceder.

```
# iptables -F
```

Habilite la funcionalidad de NAT entre las dos interfaces

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Finalmente tenemos que habilitar el kernel para reenviar paquetes entre las interfaces:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

En las distribuciones de Linux basado en Debian como Ubuntu, este cambio también puede hacerse editando el archivo **/etc/network/options**, y cambiando la línea

```
ip_forward=no
```

a

```
ip_forward=yes
```

y luego reiniciar las interfaces de red con:

```
# /etc/init.d/network restart
```

o

```
# /etc/init.d/networking restart
```

Configurar el servidor DHCP

En este momento deberíamos tener un punto de acceso en funcionamiento. Puede probarlo conectándose a la red inalámbrica “my network” desde otra

computadora a la que le haya asignado una dirección en el mismo rango de direcciones que su interfaz inalámbrica en el servidor (10.0.0.0/24 si siguió los ejemplos). Si ha habilitado WEP, tenga cuidado de utilizar la misma clave que especificó en el AP.

Para que sea más sencillo para las personas conectarse al servidor sin conocer el rango de direcciones IP, vamos a configurar un servidor DHCP para que maneje automáticamente las direcciones de los clientes inalámbricos.

Con este propósito utilizamos el programa dnsmasq. Como su nombre lo indica, provee un servidor DNS interino (*caching*) así como un servidor DHCP. Este programa fue desarrollado específicamente para el uso con cortafuegos que realizan NAT. Si su conexión a Internet tiene una alta latencia y/o un ancho de banda bajo, como conexión por discado (*dial-up*) o un VSAT, el tener un servidor DNS interino es de mucha utilidad. Esto significa que muchas consultas DNS pueden resolverse localmente, ahorrándole mucho tráfico a la conexión a Internet, y al mismo tiempo hace que la conexión se sienta notablemente más rápida.

Instale dnsmasq con el paquete de administración de la distribución. Si dnsmasq no está disponible como un paquete, descargue el código fuente e instálelo manualmente. Lo puede obtener en: *http://thekelleys.org.uk/dnsmasq/doc.html*.

Todo lo que necesitamos para correr dnsmasq es editar unas pocas líneas de su archivo de configuración, **`/etc/dnsmasq.conf`**.

El archivo de configuración está bien documentado, y tiene muchas opciones para varios tipos de configuración. Para tener el servidor básico DHCP en funcionamiento debemos quitar los comentarios y/o editar dos líneas.

Encuentre las líneas que comienzan de este modo:

```
interface=
```

...y asegúrese de que digan:

```
interface=wlan0
```

...cambiando wlan0 para que corresponda con el nombre de su interfaz inalámbrica. Luego encuentre las líneas que comienzan con:

```
#dhcp-range=
```

Quite el indicador de comentario de la línea y edítela para abarcar las direcciones pertinentes, por ej.

```
dhcp-range=10.0.0.10,10.0.0.110,255.255.255.0,6h
```

Luego salve el archivo e inicie dnsmasq:

```
# /etc/init.d/dnsmasq start
```

En este momento, debe ser capaz de conectarse al servidor como un punto de acceso, y obtener una dirección IP utilizando DHCP. Esto le debe permitir conectarse a Internet a través del servidor.

Agregando seguridad extra: Configurar un cortafuego

Una vez configurado y probado, se pueden agregar reglas de cortafuego utilizando la herramienta de cortafuego incluida en su distribución. Algunos gestores para configurar reglas del cortafuego son:

- ***firestarter*** – un cliente gráfico para Gnome, que requiere que su servidor corra en Gnome
- ***knetfilter*** – un cliente gráfico para KDE, el cual requiere que su servidor corra en KDE
- ***Shorewall*** – un conjunto de guiones y archivos de configuración que van a facilitar la configuración de los cortafuegos iptables. También hay gestores para shorewall, como el webmin-shorewall
- ***fwbuilder*** - una herramienta gráfica poderosa, pero ligeramente compleja que le permite crear guiones iptables en otra computadora, y luego transferirlos al servidor. Esto evita la necesidad de una interfaz gráfica en el servidor, y es una opción de seguridad aún más fuerte.

Una vez que todo está configurado de forma correcta, revise que todas las configuraciones estén reflejadas en el guión de arranque del sistema. De esta forma sus cambios seguirán funcionando aunque la computadora deba ser reiniciada.

Escenario 2: Hacer del punto de acceso un puente transparente

Este escenario puede utilizarse tanto para un repetidor de dos radios, o para un punto de acceso conectado a una Ethernet. Utilizamos un puente en lugar de un enrutador cuando queremos que ambas interfaces en el punto de acceso compartan la misma sub red. Esto puede ser particularmente útil en redes con múltiples puntos de acceso donde preferimos tener un único cortafuego central y tal vez un servidor de autentificación. Dado que todos los clientes comparten la misma sub red, pueden ser manejados fácilmente

con un único servidor DHCP y un cortafuego sin la necesidad de un relevador DHCP.

Por ejemplo, usted puede configurar un servidor como en el primer escenario, pero utiliza dos interfaces Ethernet cableadas en lugar de una cableada y una inalámbrica. Una interfaz sería su conexión a Internet, y la otra conecta a un conmutador. Luego conecte tantos puntos de acceso como sean requeridos al mismo conmutador, configurándolos como puentes transparentes, y cada uno pasará a través del mismo cortafuego y utilizará el mismo servidor DHCP.

La simplicidad de puentear tiene un costo en cuanto a eficiencia. Ya que todos los clientes comparten la misma sub red, el tráfico de difusión se repite a través de la red. Esto funciona bien con redes pequeñas, pero cuando el número de clientes se incrementa, se desperdicia mucho ancho de banda en el tráfico de difusión.

Configuración inicial

La configuración inicial para un punto de acceso puenteado es similar al del punto de acceso enmascarado, sin requerir de dnsmasq. Siga las instrucciones de configuración inicial del ejemplo anterior.

Además, para la función de puente se requiere el paquete *bridge-utils* (***utilidades*** puente). Este paquete está disponible para Ubuntu y otras distribuciones basadas en Debian, y también para Fedora Core. Asegúrese de que éste esté instalado y de que el comando **`brctl`** esté disponible antes del procedimiento.

Configurando las Interfaces

En Ubuntu o en Debian configuramos las interfaces editando el archivo **`/etc/network/interfaces`**

Agregue una sección como la que sigue, pero cambie los nombres de las interfaces y las direcciones IP que correspondan. La dirección IP y la máscara de red deben concordar con la de su red. Este ejemplo supone que está construyendo un repetidor inalámbrico con dos interfaces inalámbricas, wlan0 y wlan1. La interfaz wlan0 va a ser un cliente de la red "*office*", y wlan1 va a crear una red llamada "*repeater*".

Agregue lo siguiente a **`/etc/network/interfaces`**:

```
auto br0
iface br0 inet static
```

```
  address 192.168.1.2
  network 192.168.1.0
  netmask 255.255.255.0
  broadcast 192.168.1.255
  gateway 192.168.1.1
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid “office” mode Managed
  pre-up iwconfig wlan1 essid “repeater” mode Master
  bridge_ports wlan0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
```

Ponga una marca de comentario a todas las líneas que se refieran a wlan0, o a wlan1 para asegurarse de que no van a interferir con nuestra configuración.

Esta sintaxis para configurar los puentes mediante el archivo **interfaces** es específico para distribuciones basadas en Debian, y los detalles de la configuración del puente son manejados por un par de guiones: **/etc/network/if-pre-up.d/bridge** y **/etc/network/if-post-down.d/bridge**. La documentación para estos guiones se encuentra en **/usr/share/doc/bridge-utils/**.

Si dichos programas no existen en su distribución (como Fedora Core), aquí hay una configuración alternativa para **/etc/network/interfaces** que logrará lo mismo:

```
iface br0 inet static
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid “office” mode Managed
  pre-up iwconfig wlan1 essid “repeater” mode Master
  pre-up brctl addbr br0
  pre-up brctl addif br0 wlan0
  pre-up brctl addif br0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
  post-down brctl delif br0 wlan0
  post-down brctl delif br0 wlan1
  post-down brctl delbr br0
```

Arrancar el puente

Una vez que el puente esté definido como una interfaz, arranque el puente escribiendo:

```
# ifup -v br0
```

La "-v" significa salida verbosa y proporciona información acerca de lo que está pasando.

En Fedora Core (y otras distribuciones no Debian) también debe darle a su interfaz puenteada una dirección de IP y agregar una ruta por omisión al resto de la red:

```
#ifconfig br0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
#route add default gw 192.168.1.1
```

En este momento debería poder conectar a este nuevo punto de acceso una computadora portátil inalámbrica, y a través de ésta conectarse a Internet (o al menos con el resto de su red).

Si quiere más información sobre su puente y lo que está haciendo, utilice el comando ***brctl***. Intente por ejemplo:

```
# brctl show br0
```

Esto debería darle e información sobre lo que está haciendo el puente.

Escenarios 1 y 2 de la forma sencilla

En lugar de configurar su computadora como un punto de acceso desde cero, usted puede aprovechar una distribución Linux armada especialmente para este propósito. Estas distribuciones pueden hacernos la tarea tan simple como arrancar la computadora desde un CD preconfigurado con el sistema operativo para interfaz inalámbrica. Para más información diríjase a la sección, "Sistemas operativos amigables con la tecnología inalámbrica".

Como puede ver es fácil proveer servicios de punto de acceso desde un enrutador Linux estándar. Usar Linux le da un control mucho más significativo sobre cómo se enrutan los paquetes a través de su red, y tiene algunas características que simplemente son imposibles de encontrar en un equipamiento para consumidores.

Así, puede comenzar con cualquiera de los dos ejemplos anteriores e implementar una red inalámbrica privada donde los usuarios son autentificados utilizando un navegador web estándar. Mediante el uso de un portal cautivo como el ***Chillispot***, se pueden verificar las credenciales de los usuarios inalámbricos en una base de datos (por ejemplo, un servidor de dominios Windows accesible vía RADIUS). Este arreglo puede permitir un acceso preferencial a los usuarios existentes en la base de datos, al mismo tiempo que se permite un nivel de acceso muy limitado para el público en general.

Otra aplicación muy popular es el modelo comercial preparado. En el mismo, los usuarios deben adquirir un pase antes de acceder a la red. Este pase provee una contraseña que tiene validez por una cantidad de tiempo limitada (generalmente un día). Cuando el pase expira, el usuario debe comprar otro. Esta característica solamente está disponible en equipamientos de redes relativamente caros, pero puede implementarse usando un software libre como el Chillispot y el phpMyPrePaid. Vamos a ver más sobre la tecnología de portal cautivo y los sistemas de pase en la sección **Autentificación** del capítulo seis.

Sistemas operativos amigables con la tecnología inalámbrica

Existen varios sistemas operativos de fuente abierta que proveen herramientas muy útiles para trabajar en redes inalámbricas. Estos fueron pensados para utilizarse en PCs recicladas con otro propósito, o con otro equipamiento de red (en lugar de una computadora portátil o un servidor), y están bien afinados para trabajar en la implementación de redes inalámbricas. Algunos de estos proyectos incluyen:

- **Freifunk.** Basado en el proyecto OpenWRT (*http://openwrt.org/*), el *firmware* Freifunk brinda un soporte a OLSR para puntos de acceso tipo consumidor basados en MIPS, tales como Linksys WRT54G / WRT54GS / WAP54G, Siemens SE505, y otros. Simplemente sustituyendo el *firmware* estándar de uno de esos AP con el *firmware* de Freifunk, podrá construir rápidamente una red *mesh* OLSR auto-formada. En este momento Freifunk no está disponible para arquitecturas de computadoras x86. Es mantenido por Sven Ola del grupo inalámbrico Freifunk en Berlín. Puede descargar el *firmware* desde *http://www.freifunk.net/wiki/FreifunkFirmware* .
- **Metrix Pebble.** El projecto Linux Pebble fue iniciado en el 2002 por Terry Schmidt del grupo NYCwireless. Originalmente, fue una versión de la distribución Linux Debian que incluye herramientas inalámbricas, cortafuego, administración del tráfico, y enrutamiento. Desde 2004, Metrix Communication ha estado extendiendo Pebble para incluir manejadores actualizados, monitoreo de ancho de banda, y herramientas de configuración basadas en la web. El objetivo de Metrix Pebble es proveer una plataforma completa para el desarrollo inalámbrico. Trabaja con equipamiento x86 con al menos 64MB de memoria *flash* o almacenamiento de disco duro. Puede descargar Metrix Pebble desde *http://metrix.net/metrix/howto/metrix-pebble.html*.
- **m0n0wall.** Basado en FreeBSD, m0n0wall es un paquete cortafuego pequeño, pero muy completo, que provee servicios de AP. Se configura desde una interfaz web y la configuración completa del sistema es almacenada en un único archivo XML. Su reducido tamaño (menos de 6MB) lo

hace atractivo para el uso en sistemas embebidos pequeños. Su objetivo es proveer un cortafuego seguro, y como tal no incluye herramientas para el espacio del usuario (no es posible registrarse en la máquina desde la red). Más allá de esta limitación, es una buena elección para los administradores de redes inalámbricas, particularmente aquellos con un conocimiento previo en FreeBSD. Puede descargar m0n0wall desde *http://www.m0n0.ch/*.

Todas estas distribuciones están diseñadas para adecuarse a computadoras con un almacenamiento limitado. Si usted está utilizando un disco *flash* muy grande o un disco duro, ciertamente puede instalar un SO más completo (como Ubuntu o Debian) y utilizar la computadora como enrutador o punto de acceso. De todas formas le va a tomar cierta cantidad de tiempo de desarrollo asegurarse de que todas las herramientas necesarias estén incluidas, evitando instalar paquetes innecesarios. Por medio de la utilización de uno de estos proyectos como punto de inicio para construir un nodo inalámbrico, ahorrará considerable tiempo y esfuerzo.

El Linksys WRT54G

En el mercado actual uno de los puntos de acceso más popular es el Linksys WRT54G. Este punto de acceso tiene dos conectores de antena externos RP-TNC, un conmutador Ethernet con cuatro puertos, y un radio 802.11b/g. Se configura a través de una simple interfaz web. Si bien no está diseñado para exteriores, puede instalarse en una caja adecuada para tal fin, o en un tubo de plástico, a un costo relativamente bajo. En este momento el WRT54G cuesta aproximadamente U$S 60.

En el 2003, los *hackers* se dieron cuenta de que el *firmware* que se vendía con WRT54G en realidad era una versión de Linux. Esto lprodujo un tremendo interés en construir un *firmware* adaptable que extendiera las capacidades del enrutador de forma significativa. Algunas de esas nuevas características incluyen el soporte del modo cliente en el radio, portales cautivos, y redes *mesh*. Dos buenas alternativas de paquetes de *firmware* para WRT54G son OpenWRT (http://openwrt.org/) y Freifunk (*http://www.freifunk.net/wiki/FreifunkFirmware*).

Desafortunadamente, a fines del 2005, Linksys sacó la versión 5 de WRT54G. Esta nueva versión del equipamiento eliminaba algo de memoria RAM y de almacenamiento *flash* en la placa madre, haciendo prácticamente imposible correr Linux (se vende con VxWorks, un sistema operativo mucho más pequeño que no permite una fácil adaptación). Puesto que el WRT54G v5 no corre con el *firmware* adaptado basado en Linux, se volvió menos atractivo para los desarrolladores de redes. Linksys también desarrolló el WRT54GL, el cual es esencialmente el WRT54G v4 (que corre con Linux) con un precio ligeramente más alto.

Otros puntos de acceso Linksys corren Linux, incluyendo el WRT54GS y el WAP54G. Si bien también tienen unos precios relativamente bajos, las especificaciones de equipamiento pueden cambiar en cualquier momento. Sin abrir el paquete es difícil saber qué versión del equipamiento es usada, lo que hace riesgoso adquirirlos en una tienda y prácticamente imposible ordenarlos en línea. A pesar de que WRT54GL tiene garantía de correr con Linux, Linksys ha hecho saber que no espera vender este modelo en grandes volúmenes, y no queda claro por cuánto tiempo el mismo va a estar en venta.

Si puede encontrar una revisión anterior de WRT54G, o de WRT54GL, estos enrutadores son versátiles y baratos. Con un *firmware* de código abierto, pueden configurarse para funcionar como una *mesh* OLSR o en el modo cliente, y trabajan muy bien como una solución económica del lado del cliente. Aunque el nuevo modelo v5 funciona como punto de acceso, no puede ser configurado como cliente, y los usuarios que han publicado sus opiniones respecto a estos equipos han expresado reservas en comparación con el v4 y modelos anteriores.

Para más información, diríjase a uno de estos sitios web:

- *http://linksysinfo.org/*
- *http://seattlewireless.net/index.cgi/LinksysWrt54g*