Windows y Macintosh

Introducción a las Redes Inalámbricas

802.11a, 802.11b, AirPort y AirPort Extreme de Apple

Adam Engst
Glenn Fleishman

ANAYA MULTIMEDIA

1. ¿Por qué inalámbrico?

Inalámbrico, la palabra evoca aquella emocionante época en que la radio dominaba el mundo del entretenimiento y las familias se reunían alrededor de un aparato de radio del tamaño de una mesa camilla y se maravillaban ante una tecnología que emitía voces incorpóreas desde la lejanía. Aunque ahora vemos la radio como algo usual, en aquellos días era pura magia que se oyeran palabras y música, sin ni siquiera necesitar cables entre el receptor y un transmisor que podía estar a kilómetros de distancia.

Volviendo al presente, un tipo de radio diferente está poniendo el mundo de los ordenadores patas arriba. Ahora las radios son minúsculos chips encastrados en dispositivos del tamaño de una tarjeta de crédito que se conectan en ordenadores que a su vez no son mucho más grandes que un cuaderno. Estas radios no transmiten ni reciben ásperas voces y efectos de sonido, sino pequeños paquetes de ceros y unos: datos informáticos. En el pasado, la radio conectó a la gente e hizo posible la primera cultura de masas; en la actualidad, la radio conecta nuestros ordenadores con redes inalámbricas y la inmensa Internet.

Lo más llamativo de las redes inalámbricas es la potencia del concepto, teniendo en cuenta la simplicidad subyacente. No hay muchas novedades en las redes inalámbricas, pero la conexión de los distintos aspectos de la informática con los de la transmisión las convierten en una opción atractiva e inclu-

so insinúa la raíz de una revolución social, pues la gente puede comunicarse de formas nuevas y más flexibles que nunca.

Las redes convencionales con cables hace tiempo que ofrecen el mismo tipo de comunicación que pueden ofrecer las redes inalámbricas y, lo que es más, los datos generalmente fluyen por las redes de cable mucho más rápido y de forma más barata. Pero velocidades mayores y hardware más barato resultan no ser lo importante; el atractivo de las redes inalámbricas está en la combinación de flexibilidad, ubicuidad de la red y distancia entre nodos de red que hace que las redes inalámbricas superen al prosaico mundo cableado. Conectando algunas baratas piezas de equipamiento y activando una conexión podemos vagabundear por nuestra casa u oficina, salir al patio o visitar un café manteniendo el acceso a la red todo el tiempo. De repente estamos utilizando las redes de una forma que hace una década parecía ciencia ficción.

Desenchufar, sintonizar, encender

Mire detrás de su ordenador de mesa. Si es un ordenador normal, ahí detrás encontrará un follón de cables. El monitor y el teclado están conectados al ordenador, el monitor y el ordenador están enchufados a tomas eléctricas en una regleta que, a su vez, está conectada a una toma de pared; y después están los cables que se arrastran hasta la impresora, el ratón y demás. Ahora, imagine un ordenador completamente libre de cables. Puede resultarle difícil si está pensando en un ordenador de mesa con un gran monitor, pero no tanto si piensa en un portátil, con su pantalla, teclado y ratón integrados, todos recibiendo energía de una batería interna. No necesita ningún cable, al menos mientras aguante la batería.

Con un portátil podemos trabajar donde queramos: en la cama, el sofá, un avión o una cafetería. Y con los portátiles actuales, que combinan veloces procesadores con hermosas pantallas en un esbelto paquete de sólo algunos kilos, ni siquiera renunciamos a demasiadas cosas a cambio de liberarnos del escritorio. Pero hasta hace poco, había una cosa que nos obligaba a renunciar: el acceso a Internet.

No vamos a entrar en lo emocionante que es Internet porque es de sobra conocido lo útil que es intercambiar mensajes de correo electrónico, navegar por la Web, especialmente para la juventud, confiar en la mensajería instantánea para permanecer en contacto constante con los amigos... Pero emocionante es, y hemos estado utilizándola y escribiendo sobre Internet desde antes que se convirtiera en el fenómeno cultural que es hoy. (De hecho, Adam escribió uno de los primeros libros sobre Internet en 1993 y en unos pocos años, cientos de

miles de personas habían utilizado su serie de libros Internet Starter Kit para entrar en Internet por primera vez. Glenn fundó una temprana empresa de desarrollo Web en 1994 y utilizar un módem le parece como intentar chupar la pulpa de una sandía a través de una pajita.) Los ordenadores actuales son dispositivos de comunicación y, para establecer esa comunicación, necesitan acceso a Internet.

Esta necesidad de acceder a Internet perjudicó a los portátiles durante un tiempo, pues aunque se podía trabajar en un portátil sin tener que conectarlo a nada mientras duraba su batería, si ese trabajo exigía el uso de Internet, se necesitaba un cable de módem o de Ethernet amarrando el ordenador a la pared. Y una vez que debía estar amarrado a la pared, lo más sencillo era enchufar el ordenador a la toma de corriente para conservar la carga de la batería. Y como es una molestia tener que cargar con el adaptador de corriente de un lado a otro, lo más probable era que estuviera al lado del escritorio. Antes de darnos cuenta, el portátil estaba anclado al escritorio igual que cualquier ordenador de mesa.

Entonces aparecieron las redes inalámbricas. De pronto, añadiendo dos baratas piezas de hardware (una tarjeta de red inalámbrica para conectarla al ordenador y un punto de acceso) de nuevo podíamos usar el portátil en cualquier parte dentro del alcance del punto de acceso disfrutando de conectividad con Internet. La cama, el sofá, el jardín trasero estaban otra vez a nuestro alcance. Y la libertad que ofrecen las redes inalámbricas no se acaba cuando salimos de casa. Muchas oficinas han cogido el tren y han preparado salas para que los empleados puedan acceder a archivos compartidos y recursos de información de Internet. (Y una ventaja añadida es comprobar el correo electrónico durante una aburrida reunión, pero no hemos dicho eso.) Los viajantes pueden contar con acceso inalámbrico a Internet en aeropuertos, ferias comerciales e incluso cafeterías y campos de deporte.

Y las redes inalámbricas también funcionan en parques. Gente que piensa en la comunidad en muchas ciudades del mundo ha levantado grandes redes inalámbricas que cubren barrios enteros, de modo que si está en Bryant Park en New York City o en casi cualquier parte en Ashland, Oregón (sede del Oregon Shakespeare Festival anual), para acceder a Internet no tiene más que abrir el portátil, aunque seguro que no piensa en ello en mitad de la representación de Romeo y Julieta.

En román paladino, la red inalámbrica es uno de los desarrollos más increíbles en la informática de los últimos años, no sólo por las muchas nuevas proezas técnicas, sino porque permite que los ordenadores estén en nuestras vidas más cómodamente. La gente no precisa estar sentada en el mismo sitio día sí y día también, y aunque aquellos de nosotros que hemos dedicado nues-

tro tiempo a trabajar con ordenadores hemos hecho ese sacrificio durante años, la combinación de un esbelto portátil con las redes inalámbricas que proporcionan acceso a Internet desde cualquier parte es tremendamente liberadora.

En resumen, una maravilla.

Raíces de las redes inalámbricas

¿Qué queremos decir exactamente cuando hablamos de redes inalámbricas? Para el propósito de este libro, casi siempre estamos hablando de una tecnología de radio de corto alcance sin patente llamada IEEE 802.11b, también conocida como Wi-Fi (es una abreviatura de *Wireless Fidelity,* creada por una asociación comercial). Aunque a veces hablaremos de redes para Macintosh y para Windows por precisión, utilizaremos principalmente Wi-Fi a lo largo del libro para evitar confusiones. Wi-Fi no es ni mucho menos la única tecnología de redes inalámbricas, pero es de lejos la más común (veremos las otras tecnologías principales en el próximo capítulo). Veamos brevemente el desarrollo de las redes inalámbricas.

La primera red inalámbrica fue desarrollada de la University of Hawaii en 1971 para enlazar los ordenadores de cuatro islas sin utilizar cables de teléfono. Las redes inalámbricas entraron en el mundo de los ordenadores personales en los 80, cuando la idea de compartir datos entre ordenadores se estaba haciendo popular. Algunas de las primeras redes inalámbricas no utilizaban las ondas de radio, sino que empleaban *transceptores* (transmisores-receptores) de infrarrojos. Desgraciadamente, los infrarrojos no terminaron de despegar porque ese tipo de radiación no puede atravesar los objetos físicos. Por tanto, requieren un paso libre en todo momento, algo difícil de conseguir en la mayoría de las oficinas. (Además, incluso los infrarrojos modernos siguen teniendo un ancho de banda muy bajo, cuando funcionan.)

Las redes inalámbricas basadas en radio despegaron a principios de los 90 cuando la potencia de procesamiento de los chips llegó a ser suficiente para gestionar los datos transmitidos y recibidos a través de conexiones de radio. Sin embargo, estas primeras implementaciones eran caras y eran productos de marca: no se podían comunicar unas con otras. Las redes incompatibles están abocadas al fracaso, de modo que, a mediados de los 90, la atención se centró en torno al naciente estándar IEEE 802.11 para las comunicaciones inalámbricas. Las primeras generaciones del IEEE 802.11, ratificado en 1997,

eran relativamente lentas, ejecutándose a entre 1 y 2 megabits por segundo (Mbps). Se utilizaron a menudo en logística: operaciones de almacén e inventario en las que no era viable el uso de cableado o resultaba muy caro mantenerlo.

Estaba claro que la tecnología podía ir mucho más allá y, en 1999, el IEEE finalizó el estándar 802.11b, aumentando el rendimiento de las redes inalámbricas a 11 Mbps (como comparación, la red Ethernet del estándar 10BaseT va a 10 Mbps).

Aunque hubo muchas compañías implicadas en la creación de la especificación 802.11b, Lucent Technologies y Apple Computer abrieron el camino para producir dispositivos de red inalámbrica asequibles para los pequeños consumidores. (Otras compañías como BreezeCOM y Aironet Wireless Communications ya estaban vendiendo caros equipamientos dirigido al mercado corporativo.)

Nota

El IEEE ratificó antes un estándar 802.11a mucho más rápido. Sin embargo, la realidad técnica y política retrasó su desarrollo. El primer equipamiento 802.11a salió a mediados de 2002. Veremos con más detalle el estándar 802.11a en el capítulo 3.

El momento decisivo para las redes inalámbricas llegó en julio de 1999, con el lanzamiento por parte de Apple de su tecnología AirPort. AirPort era una versión del IEEE 802.11b ajustada al estándar de la industria y Apple puso en marcha el mercado cobrando sólo 100$ por una tarjeta de red inalámbrica que encajaba en distintos modelos del Macintosh y 300$ por un punto de acceso (que Apple llamaba una Estación Base AirPort). Costó más de un año que otras compañías bajaran sus precios al nivel que había establecido Apple, pero introduciendo las redes inalámbricas en el mayor mercado de los PC, estas otras compañías pudieron continuar reduciendo los precios. En el momento de escribir este libro, el coste de equipar un solo ordenador PC o Macintosh con una tarjeta Wi-Fi está entre 50 y 100€ y un punto de acceso cuesta menos de 150€.

A lo largo de los últimos años, las capacidades han aumentado y los precios han bajado y la facilidad de uso ha mejorado para que cualquiera que pueda configurar un ordenador pueda también configurar una red inalámbrica, complementada con una conexión compartida con Internet. Hemos recorrido un largo camino en poco tiempo y, con la popularidad de las redes inalámbricas, el futuro parece igual de brillante que el reciente pasado. Si quiere saber qué podemos esperar del futuro de lo inalámbrico, vea el capítulo 11.

¿Quién debe leer este libro?

Teníamos en mente un público determinado al escribir este libro. Sacará el máximo provecho del libro si alguno de los siguientes casos se corresponde con el suyo.

- Acabo de comprar un portátil y quiero compartir la conexión de Internet de mi ordenador de mesa. ¿Cómo puedo compartir mi conexión de forma barata y sencilla?
- Tengo una pequeña red con cables para compartir archivos y una conexión con Internet en dos ordenadores de mesa, pero ahora quiero añadir mi portátil a la red sin utilizar más cables de red. ¿Qué debo comprar para añadirlo a mi portátil?
- Acabo de mudarme y desplegar todos los cables de Ethernet hasta donde necesito acceso de red sería demasiado caro y daría mucho trabajo. Quiero que todos mis ordenadores compartan una conexión con Internet sin utilizar cables. ¿Resolverá una red inalámbrica mis problemas?.
- Tengo en funcionamiento una red inalámbrica, pero no puedo recibir la señal en algunas habitaciones. ¿Cómo puedo ampliar el alcance de mi red?
- He comprado todo lo que necesito y he configurado mi red inalámbrica, pero no consigo que funcione mi conexión con Internet. ¿Puede este libro decirme qué he hecho mal?
- Viajo mucho. ¿Qué necesito en cuanto a hardware, software y cuentas para obtener acceso a Internet inalámbrico desde cualquier sitio?
- No puedo conseguir una DSL (Línea de suscriptor digital) ni acceso por cable de módem a Internet, pero he oído que quizá pueda obtener acceso inalámbrico de alta velocidad en mi localidad. ¿Cómo puedo hacerlo?
- Estoy intentando comprender cómo funcionan las redes inalámbricas para poder aconsejar a mi departamento si invertir o no en esta tecnología. ¿Puede este libro explicarme lo básico de las redes inalámbricas, decirme cuáles van a ser los próximos avances y señalar sitios Web útiles en los que pueda aprender más?
- Mis amigos y colegas me consideran su gurú sobre temas de ordenadores e Internet y todos están interesados en las redes inalámbricas. ¿Qué

información necesito para empezar a configurar redes para usuarios particulares?

- Me preocupa que los *crackers* entren en mi red inalámbrica y roben los sensibles planes de productos de mi empresa. ¿Cómo puedo garantizar que mi red es segura?

Estamos seguros que si sus necesidades entran en alguno de estos puntos, encontrará la información que necesita en este libro. O, si ha habido algún cambio desde el momento en que se editó el libro, habremos tratado el tema en el sitio Web del libro en www.wireless-starter-kit.com o en el sitio de Glenn 802.11b Networking News, en http://80211b.weblogger.com/. También encontrará que le resultan de utilidad los sitios Web aludidos a lo largo del libro.

Nuestro objetivo es proporcionar información práctica y consejos para cualquiera que intente trabajar con una red inalámbrica, aunque debemos señalar que este libro no es adecuado para lectores totalmente inexpertos. Si todavía no conoce lo básico del uso de sistemas Windows o Macintosh, por ejemplo, le recomendamos que lea primero un libro para principiantes y después vuelva a este libro.

En el otro extremo del espectro, no examinamos las redes inalámbricas en el nivel de protocolos, diseccionamos las cabeceras de paquete, comentamos la física implicada en la recepción de ondas de radio ni entramos en ningún tema verdaderamente técnico. Ese tipo de información es útil principalmente para aquellas personas que diseñan hardware para redes inalámbricas, escriben software para redes inalámbricas o establecen mallas de red para comunidades, y queremos que este libro esté centrado en temas prácticos experimentados por grupos de personas más grandes.

Redes inalámbricas de la vida real

Antes de entrar en los elementos básicos de las redes inalámbricas, queremos mostrar de dónde venimos para que pueda ver que no somos tecnólogos de sillón, hemos vivido todo esto. Hemos estado implicados con la tecnología durantes más de 20 años y, en los últimos 12, hemos dedicado gran parte de nuestro tiempo a escribir sobre las tecnologías que nos fascinaban porque nos encanta explicar temas complejos.

Desde 1990, Adam ha publicado TidBITS, un boletín de noticias electrónico semanal dedicado a temas que interesan a los usuarios de Macintosh e

información necesito para empezar a configurar redes para usuarios particulares?

- Me preocupa que los *crackers* entren en mi red inalámbrica y roben los sensibles planes de productos de mi empresa. ¿Cómo puedo garantizar que mi red es segura?

Estamos seguros que si sus necesidades entran en alguno de estos puntos, encontrará la información que necesita en este libro. O, si ha habido algún cambio desde el momento en que se editó el libro, habremos tratado el tema en el sitio Web del libro en www.wireless-starter-kit.com o en el sitio de Glenn 802.11b Networking News, en http://80211b.weblogger.com/. También encontrará que le resultan de utilidad los sitios Web aludidos a lo largo del libro.

Nuestro objetivo es proporcionar información práctica y consejos para cualquiera que intente trabajar con una red inalámbrica, aunque debemos señalar que este libro no es adecuado para lectores totalmente inexpertos. Si todavía no conoce lo básico del uso de sistemas Windows o Macintosh, por ejemplo, le recomendamos que lea primero un libro para principiantes y después vuelva a este libro.

En el otro extremo del espectro, no examinamos las redes inalámbricas en el nivel de protocolos, diseccionamos las cabeceras de paquete, comentamos la física implicada en la recepción de ondas de radio ni entramos en ningún tema verdaderamente técnico. Ese tipo de información es útil principalmente para aquellas personas que diseñan hardware para redes inalámbricas, escriben software para redes inalámbricas o establecen mallas de red para comunidades, y queremos que este libro esté centrado en temas prácticos experimentados por grupos de personas más grandes.

Redes inalámbricas de la vida real

Antes de entrar en los elementos básicos de las redes inalámbricas, queremos mostrar de dónde venimos para que pueda ver que no somos tecnólogos de sillón, hemos vivido todo esto. Hemos estado implicados con la tecnología durantes más de 20 años y, en los últimos 12, hemos dedicado gran parte de nuestro tiempo a escribir sobre las tecnologías que nos fascinaban porque nos encanta explicar temas complejos.

Desde 1990, Adam ha publicado TidBITS, un boletín de noticias electrónico semanal dedicado a temas que interesan a los usuarios de Macintosh e

Internet. También ha sido editor colaborador de MacUser, MacWEEK y Macworld. Junto con la exitosa serie Internet Starter Kit, Adam ha escrito y colaborado en otros libros, incluyendo Internet Explorer Kit for Macintosh (con Bill Dickson), Eudora for Windows & Macintosh: Visual QuickStart Guide, The Race for Bandwidth (escrito sin firmar con Steve Manes para nuestro viejo amigo Cary Lu), Crossing Platforms: A Macintosh/Windows Phrasebook (con David Pogue) y, más recientemente, iPhoto 1.1 for Mac OS X: Visual QuickStart Guide.

Durante gran parte de ese tiempo, Glenn ha sido un escritor autónomo, fundador de Point of Presence Company en 1994, una de las primeras empresas de desarrollo de sitios Web; Peachpit fue uno de sus primeros clientes, para el que desplegó un sistema de cesta de compras para venta de libros en 1995. También pasó un periodo de seis meses como administrador del catálogo de Amazon.com, se tomó un tiempo para derrotar a la enfermedad de Hodgkin y fue coautor (con el editor ejecutivo de TidBITS, Jeff Carlson) de tres ediciones de Real World Adobe GoLive. Glenn escribe actualmente para publicaciones como The Seattle Times, Wired, The New York Times y la O'Reilly Network. También dirige el popular sitio Web 802.11b Net working News y goza de amplio reconocimiento como escritor de artículos de fondo dedicados a las redes inalámbricas.

Nos conocemos desde hace más de diez años, después de contactar a través del correo electrónico a principios de los 90 y hacernos amigos cuando los dos vivíamos en Seattle. Desde que Adam dejó Seattle para volver a su ciudad natal de Ithaca, New York, nos vemos generalmente en ferias comerciales y otros eventos del campo, manteniéndonos en contacto el resto del tiempo a través del teléfono, el correo electrónico y la mensajería instantánea.

Una vez hecho este resumen estilo curriculum del camino que hemos seguido, nos gustaría explicar de otra forma de dónde venimos, esta vez contando anécdotas de los eventos de las redes inalámbricas que nos cautivaron y nos hicieron convertirnos en sus defensores. Por cada anécdota, fíjese en la nota final; con estas historias no sólo intentamos relacionar los sucesos importantes que hemos experimentado, sino también ilustrar puntos importantes sobre cómo se pueden usar las redes inalámbricas.

La presentación de AirPort (Adam)

El hito que presentó las redes inalámbricas ante el mundo tuvo lugar en julio de 1999. El lugar fue el Jacob Javits Convention Center de New York City y el evento era la feria semestral Macworld Expo. Steve Jobs había vuelto

a Apple no hacía mucho y, al menos desde el punto de vista de los medios, la compañía estaba resurgiendo de sus cenizas.

Para aquellos que nunca han asistido a ellas, una charla para establecer la tónica de la feria de Steve Jobs es una maravilla. La mayoría de las charlas de la industria informática son áridas y las dan personas cualificadas por el puesto de su compañía en la industria, no por sus capacidades comunicativas. Pero en la jerga de la industria, Jobs hizo una buena demo y esa presentación sería recordada durante mucho tiempo.

Tenga en cuenta que, aunque las redes inalámbricas ya llevaban años existiendo, siempre habían sido caras, lentas y poco fiables, y se puede decir que la mayoría de la gente ni siquiera conocía su existencia. (Glenn agrega: "Tenía tantas reservas cuando supe por primera vez de ellas, que tontamente dejé pasar otro año sin ni siquiera probarlas".)

Cuando Jobs mostró los primeros iBooks, los portátiles de Apple orientados al pequeño consumidor, y anunció que añadiendo una tarjeta de 100$ podría trabajar en red con otros ordenadores e incluso acceder a Internet a través de un punto de acceso de 300$, el público quedó anonadado. Apple llamó a la tecnología AirPort, pero Jobs tuvo mucho cuidado en señalar que era una implementación del estándar de la industria IEEE 802.11b para las redes inalámbricas.

Aunque todos los que estábamos entre el público creímos lo que dijo Jobs (cuando estás ante su presencia es casi imposible no creer todo lo que dice, gracias a su bien conocido Campo de Distorsión de la Realidad), Apple remachó la libertad que permitían las redes inalámbricas cuando Jobs presentó al vicepresidente de marketing de la compañía, Phil Schiller, que apareció en una plataforma a 25 pies por encima del suelo. Sosteniendo un nuevo iBook que reproducía una película QuickTime recibida a través de la red inalámbrica, Schiller saltó desde la plataforma a una gran alfombra de espuma que había debajo para demostrar que no había ningún cable. Mientras Schiller se ponía en pie y alzaba triunfante el iBook, una cámara de vídeo hizo un zoom para mostrar que la película seguía reproduciéndose en la pantalla del iBook. Para que luego hablen de magia.

Nota

Si intenta mostrar el funcionamiento de las redes inalámbricas a alguien que no entiende qué tienen de bueno (como un jefe recalcitrante o quizá su esposa), piense en algo que pueda hacer con la red inalámbrica pero que sea absolutamente imposible con una red convencional, como dar un paseo mientras navega por la Web. Las redes inalámbricas se demuestran por sí solas.

Llevar una red inalámbrica a casa (Adam)

Después de la atractiva demostración de Apple de las redes inalámbricas en julio del 99, se presentó la solución para un problema que teníamos mi esposa Tonya y yo. Habíamos tenido un hijo y, aunque Tonya estaba pensando en tomarse un año sabático en su trabajo como escritora y editora autónoma, no habíamos tenido en cuenta hasta qué punto nuestro hijo iba a querer estar en brazos todo el tiempo. Inicialmente habíamos trasladado su escritorio y el Power Mac 7600 al comedor para que pudiera navegar por la Web o leer el correo electrónico mientras cuidaba de Tristan. Funcionó, pero no resultaba muy atractivo, especialmente por el cable Ethernet azul de 50 pies que se arrastraba por el suelo de la cocina y el comedor. Además, cuando Tristan empezó a gatear, el cable se convirtió en un juguete muy atractivo.

Como tempranero regalo de Navidad, compramos un iBook con una tarjeta AirPort y una de las estaciones base AirPort tipo OVNI de Apple. Conecté la Estación Base AirPort a nuestra red Ethernet interna, puse en marcha el asistente de configuración de AirPort y, en un momento, el nuevo iBook de Tonya podía acceder a Internet desde casi todos los lugares de la casa (vea el capítulo 5). Tonya encontró algunos puntos ciegos en los que la señal quedaba bloqueada por tener que atravesar demasiadas paredes, pero no eran zonas críticas. Y sí, tan pronto como empezó a funcionar, dimos un paseo por la casa sosteniendo el iBook abierto, vigilando el indicador de fuerza de la señal y navegando por páginas Web al azar sólo para comprobar que podía hacerse. Incluso llevamos fuera el iBook y paseamos hasta el porche de la casa de nuestros vecinos antes de perder la señal. De nuevo, magia pura. El iBook demostró ser una potente máquina para Tonya, activando la red inalámbrica sin esfuerzo durante largas sesiones de lactancia. Le encantaba poder sentarse en una silla cómoda y disponer del portátil durante los poco frecuentes momentos de sueño de Tristan. ¿Quién iba a imaginar que lo que necesitaba de verdad una madre era un portátil y una conexión inalámbrica con Internet?

Nota *Es fácil y barato configurar una red inalámbrica que permita a un ordenador portátil compartir una conexión con Internet. Puede hacerlo en su casa u oficina por sólo 200 euros y no más de una hora de trabajo (con la ayuda de este libro, ¡por supuesto!). Y si piensa en ello, seguro que encuentra situaciones en que su vida sería más fácil disponiendo de una conexión inalámbrica en su casa o jardín.*

Evolucionar de red con cables a red inalámbrica (Adam)

Cada año, asisto a una convención verdaderamente poco usual. Se llama MacHack, y es una convención de desarrolladores puesta en marcha por miembros de la comunidad de desarrolladores de Macintosh para sus colegas programadores. A diferencia de la mayoría de las convenciones, organizadas como están por empresas de gestión de ferias comerciales para usuarios estereotipo, MacHack está diseñada por programadores para otros programadores: la convención comienza a medianoche con pizza ilimitada y una conferencia para establecer la tónica de la reunión que es conocido por durar hasta las 6 de la mañana; los programadores permanecen despiertos durante 72 horas escribiendo código para mostrarlo en el Hack Contest y las bebidas con cafeína fluyen sin freno. Naturalmente, se proporciona acceso total a Internet y, durante los primeros años que asistí, la escena usual en el salón era unas quince mesas redondas, cada una ocupada por programadores encorvados sobre sus PowerBooks, con cables Ethernet reptando hasta un concentrador Ethernet en cada mesa.

(No suponga que eso significa que los asistentes a MacHack son antisociales. De hecho, es más cierto lo opuesto y a menudo colaboran en la escritura de código para el Hack Contest. La belleza de disponer de acceso inalámbrico a Internet constantemente es que las cuestiones que surgen en una conversación pueden resolverse inmediatamente y aquellas personas que no han podido asistir permanecen en contacto con sus amigos que sí están en la convención.)

En el 2000, primera celebración de MacHack después de que Apple presentara AirPort, los concentradores no habían desaparecido, pero se necesitaron menos, pues mucha gente se había comprado inmediatamente tarjetas AirPort para sus PowerBooks e iBooks. Yo disponía de una tarjeta Farallon SkyLINE compatible con Wi-Fi para mi PowerBook G3 ese año, que era un poco lenta pero funcionaba bien para el acceso a Internet. El CompUSA al otro lado del parking del hotel hizo su agosto vendiendo tarjetas de red inalámbrica cuando la gente que no había venido preparada para aprovechar la red inalámbrica de MacHack descubrió sus ventajas. Para el 2001, ya había cambiado mi ordenador por uno de los iBooks blancos de Apple, complementado con una tarjeta AirPort interna, y usar la red inalámbrica de MacHack iba como la seda. Todavía quedaban algunos concentradores Ethernet para los rezagados que todavía no habían abrazado la revolución inalámbrica y también para aquellos cuyos Titanium PowerBook G4 todavía tenían problemas para ver la red inalámbrica (no me irás a decir que recubrir una antena de radio con titanio perjudica a la recepción de la señal).

En el 2002, las únicas máquinas que no tenían instaladas tarjetas de red inalámbricas eran las que alguien había comprado por razones históricas y el vecino CompUSA vendió una sola tarjeta, a una persona cuyo portátil se había estropeado justo antes del congreso y que había olvidado la tarjeta del viejo PowerBook que le había prestado un amigo. Una vez que se cae en ella, la adición a las redes inalámbricas es difícil de abandonar.

Aunque seguramente los administradores de red del congreso tenían preparados un par de concentradores Ethernet por si acaso, queda claro que, al menos para MacHack, los cableados Ethernet han seguido el mismo camino que los disquetes: todavía se pueden comprar si es necesario, pero no suelen ser la opción elegida.

Nota *Las redes inalámbricas funcionan muy bien en situaciones en las que desplegar cables es difícil o resulta caro, especialmente cuando sólo se necesita la red durante un corto tiempo. Además, en ciertas comunidades, las redes inalámbricas son casi omnipresentes; estas personas creen que podrán encontrar una red inalámbrica allá donde vayan. Si conoce a alguien así, seguramente se sentirá encantado de ayudarle a configurar una red inalámbrica.*

Reemplazar el cableado por lo inalámbrico (Glenn)

Hace algunos años, un puñado de articulistas informáticos y diseñadores gráficos que compartían ideas, incluyendo el autor, se mudó al piso superior de un viejo edificio del barrio Green Lake de Seattle. El edificio de dos pisos había sido renovado a medias y también tenía nuevos arrendatarios en el piso de abajo: un grupo de entrenadores que habían instalado aparatos de gimnasia y organizaban carreras para aficionados y profesionales.

Cuando entablamos relaciones con nuestros vecinos de abajo, empezamos a mostrarles cómo conectar con nuestra Estación Base AirPort del piso de arriba para poder compartir nuestra rápida conexión con Internet y después taladramos un agujero en el suelo para poder desplegar un cable Ethernet para conectar también sus máquinas de red convencional.

Cuando los entrenadores alquilaron algo más de espacio para oficinas en el edificio de al lado, se encontraron con un problema: no había una forma fácil de extender un cable desde un edificio a otro. La red inalámbrica tampoco era

la solución, pues el edificio vecino estaba principalmente en el subsuelo por la parte de atrás, rodeado de grueso cemento que bloqueaba la señal excepto en la parte delantera.

Buscamos varias alternativas y por fin encontré una forma fácil de enlazar nuestras redes: un dispositivo del fabricante de equipamiento de red Linksys que tenía el poco atractivo nombre de WAP11. Linksys había diseñado el WAP11 como punto de acceso barato, pero tenía un extra especial: podía ser establecido en un modo distinto con el que servir de puente para conectar dos redes Ethernet.

Compramos dos WAP11, que entonces costaban alrededor de 150$ cada uno (ahora han bajado a unos 100$) dirigiendo cada uno hacia el otro a través de ventanas que proporcionaban una línea de visión directa desde un edificio al otro. Después de mucho trastear y de meses de chapuzas (el equipo original del WAP11 era un poco tosco, pero no cesa de mejorar) terminamos con una conexión fiable constante que unió nuestras dos oficinas y les permitió ahorrarse 60$ mensuales adicionales en una suscripción de Internet.

Si tuviéramos que resolver este problema hoy, sólo necesitaríamos una pieza de equipamiento, también de Linksys: el Puente Ethernet inalámbrico WET11 de 130$, del que hablaremos en el capítulo 5.

Nota

A veces una red inalámbrica puede ayudar a resolver un problema que sería peliagudo o caro en caso de usar cables. Los baratos puentes inalámbricos que pueden aceptar antenas externas facilitan la conexión de edificios con redes inalámbricas.

Creación de redes ad hoc (Adam)

No asuma la falsa impresión de que las redes inalámbricas precisan todo tipo de hardware. De hecho, si no necesita más que transferir archivos de un lado a otro, puede crear una rápida red entre dos portátiles utilizando tarjetas de red inalámbrica estándar, sin necesidad de un punto de acceso. Y con las capacidades incorporadas en el sistema operativo Macintosh (Mac OS 9 y Mac OS X, desde la versión 10.2), incluso puede compartir una conexión con Internet entre esos dos portátiles.

Utilicé las redes inalámbricas por primera vez para compartir una conexión con Internet entre dos ordenadores cuando compartía una habitación de hotel con mi amigo y colega Jeff Carlson durante la Macworld Expo del 2000. Jeff tenía un bonito dispositivo, llamado módem Ricochet, que en esencia era un

módem de radio de marca que permitía a un ordenador acceder a Internet sin cables a baja velocidad (a unos 33 kilobits por segundo, casi igual que un módem normal conectado a una línea telefónica) en varias ciudades de los EE.UU., incluyendo Seattle, donde vive Jeff, y San Francisco, donde se celebraba la Macworld Expo. Los dos teníamos tarjetas de red inalámbrica estándar 802.11b en nuestros PowerBooks, de modo que en lugar de sufrir las caras tarifas telefónicas locales y las frecuentes desconexiones endémicas de los hoteles, Jeff utilizó el software de la Estación Base AirPort de Apple para compartir su conexión con Internet basada en Ricochet con mi PowerBook.

Y allí estábamos, sentados en nuestras camas de la habitación del hotel a cientos de millas de casa, comprobando el correo electrónico y navegando por la Web sin usar un solo cable. Incluso nosotros, que comprobamos cada nueva tecnología en cuanto sale, lo consideramos una hazaña impresionante. Además, no habíamos necesitado ningún hardware poco usual ni conocimientos esotéricos, estábamos usando tarjetas de red tal como habían salido de la caja y capacidades incorporadas en el Mac OS. Cualquiera podría haberlo hecho. Y usted también podrá, después de leer el capítulo 4.

Nota *Las redes inalámbricas ad hoc se configuran fácilmente y funcionan bien para compartir archivos o incluso conexiones de Internet durante los viajes.*

Acceso a Internet durante los viajes (Adam)

Desgraciadamente, el servicio Ricochet, que Jeff utilizó durante varios años para acceder a Internet en numerosas cafeterías de Seattle, cayó entre las víctimas de la explosión de la burbuja de las punto com a mediados de 2001. Curiosamente, después de los ataques terroristas a New York City del 11 de septiembre de 2001, la red Ricochet de New York City volvió a la vida para ayudar a la gente que trabajaba en las labores de rescate a comunicarse. (En agosto de 2002, Aerie Networks, la compañía que compró los activos de Ricochet a precio de ganga, empezó a reactivar parte de la red.)

Afortunadamente, los lugares desde los que es posible acceder a Internet a través de una red inalámbrica Wi-Fi han proliferado en los últimos años y se ha vuelto fácil obtener acceso a Internet a través de una red inalámbrica en muchas partes del mundo (vea el capítulo 7). Glenn y yo hemos encontrado

personalmente redes inalámbricas que podíamos utilizar para acceder a Internet en cafeterías, aeropuertos, ferias comerciales y parques. Quizá la demostración más atractiva de lo bien que pueden funcionar las redes inalámbricas para acceder a Internet la tuvimos mi mujer y yo en una visita a Ithaca buscando casa en mayo de 2001. Teníamos algunos minutos libres en un centro comercial en Ithaca, de modo que abrí mi iBook y encontré no una sino dos redes inalámbricas a las que podía acceder. Un minuto o dos después, había comprobado mi correo electrónico.

Más tarde ese mismo día, teníamos que comprar comida y, como nuestro hijo Tristan estaba dormido en su asiento del coche, me ofrecí voluntario para quedarme en el coche con él trabajando en el iBook mientras Tonya compraba. Me sorprendió descubrir una red inalámbrica a la que podía acceder desde el mismo aparcamiento y, como era el día en que tenía que publicar el tema semanal de TidBITS, la conectividad con Internet fue muy bien recibida. Allí estaba, sentado en un coche en el aparcamiento de una tienda de comestibles, descargando archivos, verificando sitios Web y respondiendo a mensajes de correo de otros editores acerca del tema, todo mientras Tristan dormitaba en el asiento trasero. No pretendo decir que merezca la pena volver a ese aparcamiento sólo para entrar en Internet, pero en aquel momento, fue magnífico saber que no necesitaba conducir hasta algún lugar para conectar mi portátil a una línea de teléfono para sufrir con una lenta conexión por módem.

Nota

Transferir el correo electrónico durante los viajes solía ser una propuesta difícil, pero gracias a la proliferación de las redes inalámbricas, ahora es probable que pueda obtener acceso inalámbrico a Internet desde la mayoría de los destinos.

¿Tomar un atajo o robar? (Glenn)

Durante Macworld 2002 en New York City, me encontré en uno de los mejores hoteles baratos de New York: el Hotel Pennsylvania, justo enfrente del Madison Square Garden, a un cómodo paseo o viaje en autobús desde el Javits Convention Center. Aunque mi habitación se encontraba en una extraña esquina del edificio, cuando colocaba mi iBook en el alfeizar de la ventana podía encontrar una red inalámbrica abierta.

La conexión de red inalámbrica era lo bastante rápida para obtener mi correo y navegar por la Web, pero cuando mi móvil sonó a las once y media una de las noches en que estaba en mi habitación, me alarmé. La voz preguntó por

mí dando mi nombre completo y proporcionando el suyo. Colgué. Pensé, "Por Dios, alguien controlando su conexión ha visto mi sesión segura de correo y la ha seguido hasta mis servidores de correo de Seattle y después ha utilizado mi registro de dominio InterNIC para encontrar mi número de teléfono".

La persona no volvió a llamar, la conexión siguió funcionando y me calmé. Pero la experiencia puso en evidencia que había utilizado la conexión de alguien sin su conocimiento o permiso.

Nota *¿Estás robando los recursos de alguien cuando usas inconscientemente su red no segura o es como seguir el camino asfaltado a través de un jardín privado para llegar a tu destino? Es un asunto peliagudo y lo examinaremos con más detalle en el capítulo 10.*

Sin alambres en los mares profundos (Glenn)

En las zonas verdaderamente remotas del mundo, lejos del sonido incesante de los teléfonos móviles, las conexiones de cable y los equipos de TV, uno podría pensar que llega el momento de relajarse y olvidarse de Internet. Nada de eso: somos fanáticos, y fanáticos inalámbricos nada menos. En mayo de 2002, Adam y yo nos encontramos (con nuestras familias) en el crucero ms Volendam durante la convención MacMania, pero a pesar de encontrarnos en lugares remotos (y flotantes) por las costas de Canadá y Alaska, seguíamos disponiendo de acceso a Internet casi continuo.

La idea había nacido en la cabeza de Neil Bauman, capitán y jefe ejecutivo de Geek Cruises, y había reunido a muchos gurús de Macintosh para hablar de temas relacionados con los ordenadores Mac. De forma bastante apropiada, Adam y yo estábamos mostrando en colaboración el funcionamiento de las redes inalámbricas en una sesión de medio día, aunque teníamos que competir con los sorprendentes paisajes de Glacier Bay, que, de manera desconcertante, nosotros podíamos ver pero el público tenía a su espalda.

Afortunadamente, tanto para nuestra sesión como para el resto de la convención, Geek Cruises había acordado proporcionar acceso inalámbrico a Internet. La conexión con Internet provenía de un satélite que ofrecía sólo unos 100 Kbps, nos encontrábamos tan al norte que la señal del satélite llegaba casi tangente a la Tierra, reduciendo mucho la velocidad de la conexión. Pero aunque era lenta, funcionaba bastante bien y pudimos utilizarla a través de la red

inalámbrica interna que había preparado Geek Cruises. Inicialmente, Geek Cruises quería proporcionar acceso en todo el barco, pero debido a cuestiones políticas (los oficiales del barco no veían con buenos ojos que se utilizarán tantos cables para conectar puntos de acceso en las distintas cubiertas) y técnicas (todo el metal del barco bloqueaba las señales rápidamente), el acceso termino centrándose en la biblioteca del barco.

El hecho de que el acceso a Internet sólo estuviera disponible en la biblioteca resultó ser una bendición, pues convirtió esa parte del barco en el centro de conferencias, donde la gente se reunía, obtenía su correo electrónico, navegaba por la Web, intercambiaba anécdotas y se calentaba a la luz digital de la conexión de Internet. Era un poco como la descripción que ha dado Adam del salón del hotel en la convención de desarrolladores MacHack.

Nuestra celebridad local, John de Lancie, que representó el papel de "Q" en la serie de televisión Star Trek: La Próxima Generación, es un fanático confeso de los Mac y, durante una sesión en la biblioteca, observó cómo varios expertos desmontaban su PowerBook para instalar una tarjeta inalámbrica para que pudiera tomar parte en la acción.

Fue una respuesta humana antigua aunque no prevista. Si la conexión a Internet hubiera estado disponible en todo el barco, los asistentes nos habríamos dispersado. Al estar centrada en un lugar, nos ayudó a reunirnos.

Nota

En un espacio público, crear un lugar en el que la gente se pueda reunir físicamente para compartir una conexión inalámbrica con Internet es una magnífica forma de ayudar a formar grupos.

Conexiones inalámbricas de Internet de largo alcance (Adam)

Aunque principalmente pensamos en las redes inalámbricas como un útil reemplazo de las pequeñas redes convencionales, no hay una razón particular para que esto sea cierto. Las redes inalámbricas pueden reemplazar a las redes convencionales en prácticamente cualquier situación, incluso aunque la conexión principal se establezca con un proveedor de servicios de Internet. Obtener acceso inalámbrico a Internet tiene más sentido aún si se vive en algún lugar con malas conexiones telefónicas que no admiten DSL o donde la televisión por cable todavía no ha llegado. El truco está en la antena, la mayoría de las tarjetas de red inalámbrica pueden establecer la comunicación en un rango

de unos 50 metros porque sus antenas son un pequeño cable enrollado en la propia tarjeta o desplegado dentro del ordenador. Conectando una antena grande del tipo correcto a una tarjeta de red inalámbrica, se pueden enviar y recibir señales a distancias de más de 30 kilómetros. Es como en los antiguos tiempos de la televisión en que podías ver casas con grandes antenas en el tejado dirigidas a lejanas estaciones repetidoras.

Naturalmente, sólo es posible obtener acceso inalámbrico a Internet si lo proporciona un ISP (Proveedor de servicios de Internet) o si se está dispuesto a poner dinero y esfuerzo en ambos lados de la conexión. Cuando me mudé de Seattle, Washington, a Ithaca, New York, en 2001, mi búsqueda de opciones de Internet dio como resultado que encontré un ISP en Ithaca llamado Lightlink que ofrecía conexión inalámbrica con Internet a precios razonables. Y, más importante, una de sus torres de antenas estaba a la vista de mi nueva casa. Lightlink no prometía fiabilidad absoluta (nadie quiere trepar a una torre de transmisiones para arreglar una antena durante una tormenta de hielo), pero estaba intrigado e inicié el proceso de investigar seriamente qué se necesitaría para conectar una red casera a una conexión inalámbrica de Internet de Lightlink. También contraté un servicio de cable de módem con Road Runner, un gran proveedor de Internet por cable, pero como había escuchado informes esporádicos de la poca fiabilidad de Road Runner en Ithaca, supuse que entre la conexión de cable de módem y la conexión inalámbrica de alto alcance podría mantener una conectividad con Internet fiable pasara lo que pasara.

Establecer mi conexión inalámbrica con Internet resultó más complicado de lo previsto (y de lo que es ahora, sólo un año después). Tuve que encontrar una antena correcta, sacar por el exterior un cable Ethernet (para no tener que desplegar un cable azul de Ethernet 150 metros por todas las escaleras) y configurar todos los detalles de la red. No voy a profundizar más aquí, pero tenga por seguro que todo lo que aprendí lo encontrará en el capítulo 8.

En la práctica, el funcionamiento de mi conexión inalámbrica de largo alcance ha sido impecable. Bueno, no es del todo cierto, estuve sin conexión alrededor de una hora el año pasado. Pero esa fiabilidad es más que aceptable. Y una vez sucedió algo realmente inusual. El transmisor que utilizo está a unas dos millas de distancia y necesito una antena parabólica bastante grande para recibir la señal con normalidad. Sin embargo, una noche de invierno en que nevaba mucho, algo en los cristales de nieve afectó a la señal de modo que todos mis ordenadores podían recibir la señal de la torre sin necesidad de usar la gran antena.

La moraleja de la anécdota es que hay muchas variables que pueden afectar a la potencia de una señal de radio. Algunas personas pierden totalmente una señal fuerte cuando los árboles dejan caer sus hojas.

Nota

Añadiendo una antena al hardware de red inalámbrica, podemos aumentar el alcance de la red hasta 50 kilómetros (suponiendo que hay una línea de visión). Eso podría hacer que fuera posible obtener acceso inalámbrico a Internet de un ISP local o, configurando los dos lados de la conexión inalámbrica, proporcionar acceso a Internet a una ubicación remota.

Redes inalámbricas comunitarias (Glenn)

Poco después de que el equipamiento de red inalámbrica entrará en el mundo de los aficionados serios, la gente empezó a intentar ampliar el alcance de las redes más allá de los cientos de metros utilizando antenas caseras. Rob Flickenger, un administrador de sistemas en O'Reilly & Associates, editorial de libros informáticos de California, estudió en serio qué hacían las antenas caras y decidió qué podía conseguir lo mismo con una lata de Pringles, unos tubos de metal y algunas arandelas.

Suena ridículo, pero una lata de Pringles tenía el tamaño justo para alojar la antena y montar un conector externo para enchufar un cable a una tarjeta inalámbrica o punto de acceso. Utilizando medidas poco precisas y repuestos de hardware que costaban menos de 30$, Rob se comió las patatas fritas, ensambló la antena y vio un considerable aumento en la distancia que podía alcanzar su red.

La importancia de hacer la antena con una lata de Pringles tenía dos aspectos: la pura diversión y lo tonto que parecía; y la idea de que un individuo podía crear un equipamiento potente de forma barata para enlazar redes, compartir ancho de banda y reunir comunidades.

Docenas de comunidades de grupos de red se han formado en los EE.UU. y el resto del mundo para ampliar Internet y las redes locales más allá de algunas casas u oficinas, creando una nube de acceso en vecindarios, a menudo en zonas en que los servicios DSL y de cable de módem no son muy fiables.

En el proceso, estos grupos han aprendido un montón sobre cómo encontrar redes, conocer gente y construir antenas. El objetivo de estos grupos, generalmente, ya que se han formado con gente muy independiente, es extender el mensaje de las redes inalámbricas como herramienta y reunir gente para compartir recursos en beneficio de la comunidad.

Pero hay un problema: muchas de las conexiones de red compartidas que utilizan las comunidades nacen de cuentas de consumidor de alta velocidad

que prohíben específicamente compartir el ancho de banda. Algunos ISP ahora anuncian públicamente que prestan soporte a esta forma de compartir recursos, pero otros envían cartas legales a los usuarios que comparten el servicio. Está por ver en qué terminará todo, pero hablaremos más del conflicto en el capítulo 10.

Cuanta más gente participa en estos grupos comunitarios, más probable es que las redes se hagan lo bastante grandes y lo bastante redundantes para proporcionar acceso a gente de todos los vecindarios en muchas ciudades del mundo.

Nota *Como usuario, merece la pena que pregunte e investigue en las áreas públicas en las que pasa mucho tiempo, pues cada vez es más probable que haya algún tipo de red inalámbrica por la zona. Y si es del tipo activista que gusta de hacer de las comunidades en lugar mejor en el que vivir, un poco de investigación le ayudará a reunir una red comunitaria inalámbrica en su ciudad.*

Qué viene ahora

Esperamos que ya se haya hecho una idea de por qué las redes inalámbricas están tan bien, por no mencionar su utilidad y el ahorro de dinero. Profundicemos ahora en los detalles; ésta es una perspectiva de los próximos capítulos.

Capítulo 2, "Temas básicos del trabajo en red", es un curso intensivo sobre los temas básicos de redes. Aunque las redes inalámbricas son bastante sencillas, tan pronto como desee hacer algo poco usual, encontrará que es más fácil si entiende cómo fluyen los datos a través de una red. No se preocupe, no es nada demasiado técnico, y si alguna vez ha observado el paso de los trenes, entenderá bien el funcionamiento de las redes.

Capítulo 3, "Cómo funciona lo inalámbrico", estudia los detalles de cómo funcionan en realidad las redes inalámbricas, desde lo más básico de la radio al hardware necesario para conectar distintos tipos de ordenadores a una red inalámbrica. Preste atención y conocerá incluso el importante papel que la actriz Hedy Lamarr jugó en la evolución de las redes inalámbricas.

Capítulo 4, "Conectar el ordenador", se sumerge en instrucciones paso a paso sobre cómo configurar el ordenador para conectar redes inalámbricas, compartir una conexión de red y compartir archivos. Si tiene un ordenador Mac y un PC y quiere que compartan una conexión de Internet por módem de cable a través de un punto de acceso inalámbrico, puede pasar al capítulo 4 para encontrar lo que necesita.

Capítulo 5, "Construir la red inalámbrica", pasa al siguiente escalón, ofreciendo consejos realistas sobre cómo planificar y construir una red inalámbrica, complementado con una guía sobre cómo comprar una puerta de enlace que conecte una red pequeña con el resto del mundo.

Capítulo 6, "Seguridad inalámbrica", echa una mirada realista al a veces sórdido mundo de la seguridad. ¿Preocupado por si los *crackers* pueden robar sus contraseñas o curiosear en sus archivos? El capítulo 6 le proporciona el conocimiento necesario para evaluar su nivel de paranoia y las herramientas necesarias para que incluso el lector más paranoico se sienta seguros.

Capítulo 7, "De viaje", se concentra en cómo utilizar el acceso inalámbrico a Internet cuando estamos lejos de la oficina y de casa. Mostraremos qué hardware y software necesita, cómo configurar el portátil para conectar con redes inalámbricas para poder enviar y recibir correo electrónico y cómo encontrar redes inalámbricas en cualquier lugar en que esté. Incluso le mostraremos un símbolo secreto pintado con tiza en los paseos y edificios que identifica redes inalámbricas en las proximidades.

Capítulo 8, "A distancia", se centra en cómo podemos coger una conexión inalámbrica de Internet a kilómetros de distancia añadiendo sólo una barata antena o, si busca lo más barato, una lata de Pringles. Para aquellos que no disponen de un ISP inalámbrico (abreviado a menudo WISP), incluso veremos qué es necesario manipular en ambos lados de la conexión. Coja sus prismáticos y empiece a explorar el horizonte en busca de antenas inalámbricas.

Capítulo 9, "Las cosas pueden chocar en la red", admite, a diferencia de los fabricantes de equipamiento informático, que algo puede ir mal. Junto con una guía de resolución de problemas general, estudiaremos los problemas comunes y ofreceremos consejos y soluciones.

Capítulo 10, "El futuro de lo inalámbrico", escruta la bola de cristal para examinar el porvenir, tanto en términos de nuevas tecnologías que prometen redes más rápidas, más resistentes y más seguras como en términos de cambios sociales y desafíos que encararemos cuando las redes inalámbricas sean todavía más comunes.

2. Temas básicos del trabajo en red

Aunque las redes inalámbricas son fáciles de ensamblar y mantener, siguen siendo redes y un cierto nivel de comodidad con el trabajo en redes convencionales puede ayudarle a entender cómo funcionan las redes inalámbricas. Y más importante, la mayoría de la gente raramente conecta sólo dispositivos inalámbricos a una red, sino que también conecta impresoras Ethernet y máquinas más antiguas que utilizan cables, de modo que un conocimiento adicional de las redes convencionales le vendrá bien. En lo que tiene que ver con el conocimiento de redes, suponemos que el lector entra dentro de una de estas tres categorías:

- Aunque sabe que los ordenadores pueden estar conectados entre sí, no conoce mucho sobre Ethernet 10BaseT, nunca ha pensado en qué diferencia a un concentrador de una puerta de enlace y se siente totalmente perdido si tiene que decidir si utilizar o no un cable cruzado para conectar dos dispositivos de red. No se avergüence, todos hemos tenido que empezar en algún momento y le resultará útil leer todo este capítulo atentamente. Además, el capítulo le servirá como guía si encuentra puntos difíciles mientras configura una red.
- Ha trabajado con redes antes, pero quizá sólo conectando un par de ordenadores entre sí con un concentrador para poder transferir archivos de

uno a otro y compartir una conexión de Internet de alta velocidad. Si tiene necesidad, probablemente puede conseguir que funcionen la mayoría de los dispositivos de red por medio de prueba y error, pero no está seguro de cómo funciona todo. Le recomendamos que lea este capítulo saltándose las secciones con información que ya esté seguro de conocer. Vuelva atrás si encuentra conceptos que le resultan poco familiares más adelante en el libro: algunos minutos de lectura pueden ahorrarle horas de inútil experimentación.

- Es un administrador de red con montones de certificados respaldándole y es la persona a la que hay que pedir ayuda. No necesita dedicar tiempo a este capítulo, citando a Obi-Wan Kenobi, éstos no son los androides que busca.

Para aquellos que se encuentren en las dos primeras categorías, empezaremos por una analogía del mundo real para partir todos desde el mismo punto.

¿Qué es una red?

¿Qué es una red? En términos sencillos, las redes transportan datos desde un ordenador a otro. Para intentar entender el concepto de red, puede ser útil pensar en ellas comparándolas con sistemas de transporte de la vida diaria, como una autopista o una línea ferroviaria.

Por ejemplo, piense en una línea de ferrocarril. Está formada por estaciones y depósitos de mercancías unidos por una vía de tren. En las vías, los trenes de mercancías transportan contenedores de carga; cada contenedor está etiquetado con una descripción del destino final de la carga.

Ahora llevemos nuestra red de ferrocarril al mundo de las redes informáticas. Nuestros ordenadores son las estaciones del ferrocarril a lo largo de las vías, mientras que las propias vías son los cables que van de un ordenador a otro. La carga que lleva un tren de mercancías son los datos transportados por la red (archivos informáticos, páginas Web, mensajes de correo electrónico y demás) y viajan en paquetes.

En el mundo de las redes, los paquetes juegan un papel clave en el transporte de los datos. Un paquete contiene un pequeño trozo de un fragmento de datos más grande que ha sido dividido. Cada paquete tiene una cabecera que indica de dónde viene y a dónde va, llevando a cabo la misma tarea que las etiquetas con la ruta de cada contenedor de carga. Igual que la mayoría de los ferrocarriles utilizan ahora el mismo ancho de vía por razones de compatibilidad, ajus-

tarse a los estándares en las redes informáticas es esencial. Análogamente, no se pueden utilizar cables viejos para conectar ordenadores y si se mezclan tipos de cable, nos encontramos en la misma situación que los antiguos ferrocarriles con distintos anchos de vía: los operarios tenían que transferir la carga de un tren a otro utilizando un aparato especial, una grúa, retardando el tiempo de entrega de la mercancía.

Aunque podemos elegir entre varios tipos de cable, lo mejor es atenerse a un solo tipo de cable.

El mismo principio se aplica cuando conectamos una red convencional a una red inalámbrica. Hacer la conexión es como transferir los contenedores de un tren de mercancías a un avión. Los contenedores de carga siguen indicando a dónde se dirigen, pero hemos intercambiado el rígidamente constreñido mundo de las vías de tren por el abierto mundo de las rutas aéreas y los aeropuertos.

No importa cómo viaja el contenedor, una vez que llega a su destino, los operarios abren el contenedor y sacan su contenido. Aquí la analogía falla un poco, pues los contenedores de carga del mundo real son grandes y llevan un montón de material, mientras que los paquetes de red son porciones de cosas más grandes, como pueden ser mensajes de correo electrónico, páginas Web o archivos de hoja de cálculo. Cuando los paquetes de red llegan a su destino y son desempaquetados, su contenido debe combinarse con el de otros paquetes para volver a ensamblar el archivo, página Web o mensaje de correo electrónico original.

Podríamos continuar con esta analogía hasta llegar a lo ridículo, comparando las directivas implicadas cuando dos trenes recorren en direcciones opuestas la misma vía con cómo gestionan las redes Ethernet las colisiones entre paquetes. Pero no vamos a ir tan lejos; en lugar de ello, para aquellos lectores que todavía no tengan claro el funcionamiento de las redes, vamos a ver para qué sirven.

Usos de las redes

El que esté leyendo este libro significa que ya debe tener alguna idea de cómo puede usar una red, probablemente para compartir una conexión de Internet o copiar archivos entre ordenadores. De cualquier forma, puede haber usos que no había tenido en cuenta previamente, de modo que vamos a comentar los usos principales para los que nosotros hemos empleado las redes a lo largo de los años.

Compartir Internet

En la era de Internet, una política de una conexión por ordenador parece ridícula, pero la mayoría de los proveedores de servicios de cable y DSL ofrecen prácticamente las mismas limitaciones que las redes de acceso telefónico: cada conexión viene con una sola dirección de Internet, que a menudo no es fija, y las direcciones extra no están disponibles o son caras.

Los estudios de mercado muestran que la mayoría de las casas con ordenador tienen al menos dos máquinas, y algunas tres o cuatro. Todos estos usuarios quieren entrar en Internet al mismo tiempo, que significa que deben compartir esa única dirección.

Afortunadamente, compartir una conexión de Internet requiere un hardware barato o un software instalado sólo en la máquina conectada con Internet. Y, si está configurando una red inalámbrica, casi es inevitable comprar un punto de acceso inalámbrico que también deba compartir la conexión de Internet. Utilizar una red inalámbrica para compartir la conexión de Internet con un portátil es especialmente atractivo, pues así podemos navegar por la Web, leer el correo electrónico o utilizar la mensajería instantánea desde cualquier parte dentro del alcance del punto de acceso.

Dicho claramente, la Internet se considera hoy día equipamiento estándar. Si tiene varios ordenadores, deben compartir la conexión de Internet.

Nota *Algunos proveedores de servicios ofrecen opciones razonables para dar a cada máquina de una red una dirección de Internet pública única, pero hay algunas razones de seguridad para utilizar direcciones privadas a través de Traducción de direcciones de red (NAT). Comentaremos NAT más adelante en este capítulo y en el capítulo 5. También veremos las razones subyacentes del uso de NAT en el capítulo 6.*

Compartir e intercambiar archivos

Compartir archivos solía ser la aplicación definitiva de las redes y los que trabajan en oficinas siguen utilizándola mucho como medio de colaboración e intercambio de archivos. Las oficinas suelen tener servidores de archivos, ordenadores cuya única responsabilidad es proporcionar un lugar en el que almacenar archivos a los que puede acceder todo el mundo y hacer de intermediarios de las conexiones de red con esos archivos. Sin embargo, un

ordenador personal con Windows o el Mac OS puede actuar como servidor de archivos sin necesidad de software extra al tiempo que se ocupa de sus propias tareas como ordenador activo, de modo que se pueden compartir archivos fácilmente en pequeñas oficinas o incluso en la propia casa, donde un servidor de archivos dedicado en exclusiva sería excesivo.

Compartir archivos no implica necesariamente copiarlos de un ordenador a otro. Por ejemplo, cada uno de nosotros guardaba una colección de archivos MP3 de música (convertidos desde nuestras colecciones de CD) en un solo ordenador. Ahora nuestras familias pueden ejecutar un software de reproducción para escuchar la música a través de la red, sin tener que copiar los gigabytes de música en sus ordenadores individuales.

Hablando en términos prácticos, la mayor parte del trabajo para compartir archivos a través de una red se realiza en la configuración inicial y le ayudaremos en eso en el capítulo 4. Una vez configurada la red, descubrirá que es mucho más fácil compartir archivos a través de la red que copiarlos en disquetes (especialmente ahora que los ordenadores Mac ya no tienen unidades para disquetes) o CD "regrabables" (CD-RW). Compartir archivos entre sistemas Mac y PC es más complicado, pero también ofreceremos algunos trucos para hacerlo.

Compartir impresoras

Las impresoras son una parte de la vida, contradiciendo las expectativas de oficinas que no usaran papel. El papel es adecuado para muchos tipos de tareas, incluyendo la presentación gráfica de información y de fotografías, y la última generación de impresoras de inyección de tinta realiza un gran trabajo costando menos que un componente de un equipo estereofónico.

Nota

Para una visión fascinante de por qué funciona el papel tan bien, lea el artículo de Malcolm Gladwell titulado "The Social Life of Paper" en www.gladwell.com/2002/2002_03_25_a_paper.htm.

Pero incluso con el bajo coste y la gran utilidad de las impresoras actuales, rara vez tiene sentido que cada ordenador tenga su propia impresora dedicada. Compartir impresoras a través de la red, a menudo con distintas capacidades (si hay varias impresoras) es una estrategia mucho más sensata. Conectar una impresora a un ordenador o puerta de enlace casera puede permitir compartir incluso la impresora más barata.

Windows y el Mac OS ofrecen funciones para compartir impresoras recién desembalados; el único problema es que cada uno es bueno para compartir sólo entre ordenadores que ejecutan el mismo sistema operativo. De modo que si comparte una impresora a través de un sistema Windows, un ordenador Mac no podrá verla sin la ayuda de un software extra llamado Dave, de Thursby Systems (vea www.thursby.com/products/dave.html). Lo contrario también es cierto, una impresora compartida desde un sistema Mac no será visible para un ordenador Windows, aunque Dave también sirve de ayuda en este caso.

Truco *Las impresoras basadas en red suelen tener varios protocolos para imprimir incorporados, de modo que los ordenadores que ejecutan Mac OS o Windows pueden imprimir con ellas directamente.*

Copia de seguridad

La copia de seguridad más importante es la última que no se hizo. La mayoría de la gente cae en la cuenta de que debía haber hecho copias de seguridad de archivos importantes después de perderlos; pero seguro que no será su caso, ¿verdad?

Raramente se hacen copias de seguridad con la frecuencia que se debería, pues la mayoría de la gente la ve como una operación tediosa en la que hay que sentarse delante del ordenador a cambiar discos Zip o insertar CD-RW. Cada ordenador que se añade aumenta el problema, igual que los inmensos discos duros actuales, que parecen llenarse rápidamente con MP3, vídeo digital, software de juegos y grandes aplicaciones.

Las copias de seguridad basadas en red pueden contribuir a aliviar el problema. Con la instalación del software apropiado en cada ordenador y una unidad de cinta u otro dispositivo de almacenamiento (los discos duros de quita y pon son un buen medio de almacenamiento de copias de seguridad hoy día gracias a su bajo precio), podemos garantizar que todos los ordenadores de la red hacen copias de seguridad automáticamente. Nosotros utilizamos y recomendamos la aplicación de copia de seguridad Retrospect de Dantz Development (www.dantz.com) tanto para Macintosh como para Windows. Junto con una buena unidad de cinta o un juego de discos duros de quita y pon, dispondrá de una solución de copia de seguridad que no le defraudará.

No queremos decir que la copia de seguridad de red sea adecuada para todo el mundo ni que sea exactamente barata. En la mayoría de los sistemas particulares probablemente sea una solución excesiva. Pero en cualquier situación

en que se realicen trabajos importantes diariamente, es necesario protegerse ante la eventualidad de sufrir algún percance que provoque pérdida de datos.

Nota

Todo el mundo, y decimos todo el mundo, pierde datos en algún momento y las copias de seguridad son la única solución. Es mejor hacer varios grupos de copia de seguridad y mantener uno en un sitio seguro, como le dijimos a un amigo al que habían robado en casa, dejándole sin ordenadores y sin copias de seguridad.

Cableado de red

Como queda dicho, los cables de una red informática son como las vías de ferrocarril. Conectan los distintos ordenadores (las estaciones de ferrocarril) y transportan los datos (las mercancías). E igual que las vías de ferrocarril discurren paralelas, reuniéndose en las estaciones con cambio de vía, se pueden conectar cables de distintas formas al construir una red.

Topologías de red

Antes de que podamos ver los distintos tipos de cableado de red, tenemos que desviarnos brevemente para introducir el tema de *topologías de red*, un bonito término que indica cómo está dispuesta la red. Para los propósitos del libro, hay cuatro topologías de red principales: estrella, bus, anillo y malla.

Estrella

Con una topología de red en estrella, un dispositivo central (llamado concentrador) actúa como el centro de una rueda con radios. El concentrador está conectado con cada ordenador por medio de cables y los cables son como los radios de una rueda (vea la figura 2.1). Utilizando sus elementos electrónicos internos, el concentrador conecta todos los dispositivos entre sí.

Las topologías de estrella son, con mucho, las más comunes en la actualidad porque las utilizan las redes de cable estándar 10BaseT y 100BaseT (ampliaremos esto en un momento) y la mayoría de las redes inalámbricas. Lo bueno de las redes estrella es que si falla uno de los radios de la rueda, sólo se ve afectado el ordenador que corresponde a ese radio, mientras el resto de la

red sigue en funcionamiento. Como verá en un momento, eso no es cierto necesariamente en otras topologías de red.

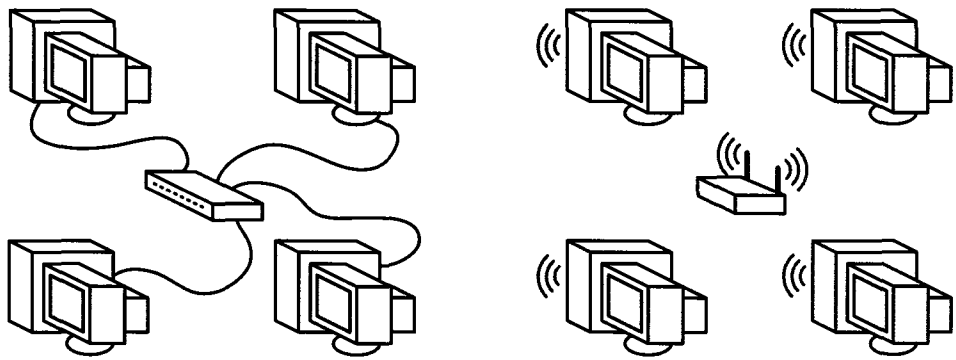

Figura 2.1. *Una topología de red en estrella.*

Nota *Los concentradores en redes estrella muy grandes a menudo están conectados entre sí en estrellas de un nivel superior (muchos concentradores conectados a un concentrador central de alta potencia) pero los concentradores también pueden estar conectados en una configuración bus, como describimos a continuación.*

Los ordenadores en red escuchan y después hablan

Todas las topologías están diseñadas para crear segmentos de red (partes de la red separadas física y lógicamente) en los que cada ordenador o dispositivo del mismo segmento puede "escuchar" a los otros dentro del periodo de tiempo mínimo necesario para transmitir una secuencia corta de datos completa, conocida como trama.

Aunque las señales de red viajan a la velocidad de la electricidad en los cables (cercana a la velocidad de la luz), sólo se pueden desplegar algunos cientos de metros de cable entre los dos dispositivos más distantes. Si el segmento fuera más largo, el ordenador más alejado podría no poder oír el inicio de la trama antes de que el ordenador emisor hubiera terminado. Eso es un problema porque todos los ordenadores de la red tienen que saber cuándo pueden empezar a transmitir sin interrumpir otra transmisión.

Veamos un ejemplo práctico: si el ordenador A y el ordenador B se encuentran en el mismo segmento Ethernet y ambos empiezan a transmitir datos al mismo tiempo, la única forma de que sepan que están interfiriéndose las transmisiones es escuchar al otro dispositivo (después de lo cual interrumpen el envío, antes de haber completado la trama de datos). Este tipo de interferencia se llama una colisión porque los datos de cada transceptor (transmisor-receptor) "colisionan". En la mayoría de los tipos de redes, incluyendo Wi-Fi y los distintos tipos de Ethernet, se han incorporado aparatos en los adaptadores de red para que esperen a que la línea esté vacía, empiecen a transmitir y se detengan si detectan una interrupción. Los dispositivos entonces dejan de hablar durante un corto periodo aleatorio y vuelven a intentar la transmisión; si tiene lugar de nuevo una colisión, cada dispositivo aumenta el periodo de silencio hasta que puede obtener una línea vacía. (Las redes Ethernet y Wi-Fi siguen estrategias ligeramente distintas debido a cómo se manipulan las señales inalámbricas, pero terminan funcionando prácticamente igual.) El procedimiento es un poco como en los viejos tiempos de las líneas de teléfono compartidas, en que todo un vecindario podía compartir una sola línea y había que esperar a que Betty, la de calle abajo, dejara de hablar antes de poder hacer una llamada.

Cada segmento de red tiene en esencia su propia línea compartida; dividiendo la red en más segmentos se aumenta el rendimiento o la cantidad de datos que se pueden transmitir de forma fiable en un momento dado a través de cada segmento. En los tipos de redes más comunes, 10BaseT y 100BaseT, un concentrador en la topología estrella puede ser pasivo, que es como un adaptador de enchufes eléctricos para varios tipos de enchufe, creando un segmento más grande compuesto de redes más pequeñas; o puede ser un conmutador, que aísla cada segmento de red y sólo permite el paso de los datos de un segmento a otro cuando es necesario. Encontrará más información sobre los concentradores un poco más adelante en este mismo capítulo.

Bus

Una topología de red bus utiliza un largo cable con cada ordenador conectado a ese cable (vea la figura 2.2). Las redes bus son poco comunes actualmente entre los ordenadores (aunque no entre concentradores de red), pero son

fáciles de configurar y se utilizaron más en el pasado. Las redes 10Base5, 10Base2, LocalTalk/PhoneNet, HomePNA y HomePlug (que veremos más adelante) utilizan todas topologías bus.

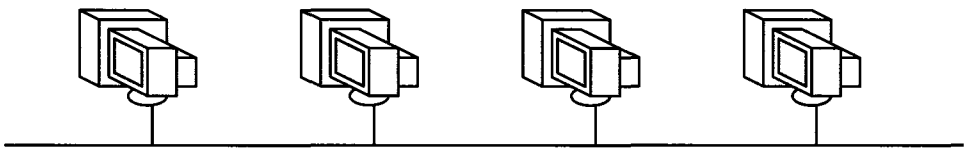

Figura 2.2. *Una topología de red bus.*

El problema de la topología bus, como puede imaginar, es que si algo corta el cable, es como si una excavadora descontrolada cortara el cable del teléfono mientras hablamos con alguien: la línea queda muerta. Y no hace falta decir que los administradores de red odian rastrear problemas de red que pueden estar en cualquier parte en el cable de red principal, de modo que las redes bus no son muy apreciadas.

Truco *Si se encuentra con una red en bus que parece intacta pero no funciona correctamente, compruebe que los dos extremos del cable de la red terminan correctamente. Si no hay un terminador apropiado actuando como tope en cada extremo del cable principal, las señales no viajarán a lo largo de la red bus correctamente.*

Anillo

Las topologías de red en anillo son similares a las redes bus, pero con los extremos del cable conectados formando un anillo (vea la siguiente figura). Las redes Token Ring (anillo de señales) ofrecen una solución al problema "¿quién está hablando?"; las máquinas envían una señal electrónica para determinar quién tiene permiso para emitir en cualquier momento dado. Las redes Token Ring se utilizan muy poco hoy día por la misma razón que las redes bus: un solo corte en el cable de red principal y se interrumpe toda la red.

Nota *Una de las caricaturas de Dilbert favoritas de Glenn muestra a Dilbert diciéndole a su jefe pelo-pincho que su conexión de red ha dejado de funcionar porque la señal se ha salido del anillo de señales y el jefe tiene que buscarla.*

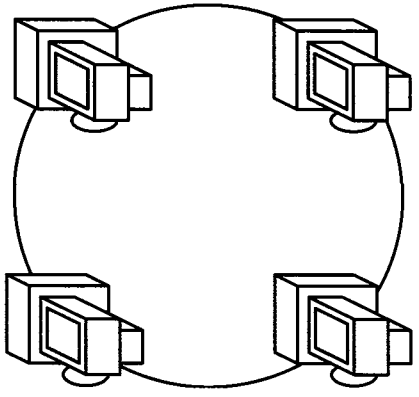

Figura 2.3. Una topología de red en anillo.

Malla

Las redes malla conectan de forma oportunista con cualquier otro dispositivo disponible que permita que el tráfico se acerque a su destino final (véase la figura 2.4). En un mundo cableado, la red en malla no tiene sentido porque se necesitarían cables independientes que fueran desde cada dispositivo al resto de dispositivos, la misma situación que resuelve la topología en estrella.

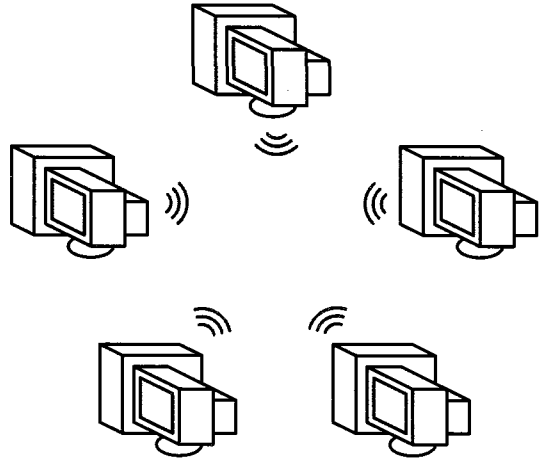

Figura 2.4. Una topología de red en malla.

Pero con una red inalámbrica basada en ondas de radio, en la que muchos transceptores tienen una ruta de señales a otros transceptores, las redes malla pueden reemplazar completamente las redes convencionales añadiendo las ven-

tajas de la redundancia: si una conexión está bloqueada, el tráfico simplemente sortea el bloqueo y se dirige a otras conexiones.

Aunque las redes en malla son populares, especialmente entre los entusiastas de las redes comunitarias, sólo unos pocos productos ofrecen capacidades de malla y únicamente están al alcance de empresas y proveedores de servicios. Quizá resulte al final que podremos encontrar acceso de alta velocidad a Internet proporcionado por un nodo de malla particular, pero aún no está claro si la tecnología va a resultar viable comercialmente.

Tipos de cableado Ethernet

Cuando se trata de redes, casi todos los ordenadores ajustados a redes utilizan el estándar de trabajo en red *Ethernet*, también conocido como IEEE 802.3. Las redes Ethernet pueden utilizar distintos cables físicos para establecer las conexiones entre máquinas y, de hecho, las redes inalámbricas también utilizan Ethernet, simplemente reemplazando los cables con ondas de radio.

Nota *El IEEE es clave para muchos de estos estándares de red, pero Ethernet fue inventado en realidad por Bob Metcalfe en los 70, cuando trabajaba en el laboratorio de investigación Xerox PARC. El IEEE estandarizó Ethernet posteriormente. La idea original de Metcalfe sobre cómo podía funcionar Ethernet está disponible en www.ethermanage.com/ethernet/ethernet.html.*

Nota *Quizá haya oído llamar a las redes inalámbricas "Ethernet inalámbrica". Eso es correcto, el estándar Ethernet especifica cómo se forman, envían y reciben los paquetes, el medio físico puede ser un cable o las ondas de radio.*

Por completitud, y por si se encuentra con una red en funcionamiento que utiliza un cable físico antiguo compatible con las redes Ethernet, vamos a examinar los tipos de cableado Ethernet en orden aproximadamente cronológico.

10Base5 o ThickNet

El tipo de cableado menos común que puede encontrarse es el cable coaxial grueso utilizado para Ethernet 10Base5. Se parece al cable utilizado para conectar los equipos de televisión por cable y recibe también el nombre de Ethernet

grueso o ThickNet. Su velocidad de transferencia de datos es de10 Mbps, y la longitud máxima de un segmento (de los cables que van de un ordenador a otro) es de 500 metros (de ahí el "5" en 10Base5). Ya no se pueden comprar fácilmente equipamiento ni cables para redes 10Base5, pero quizá se encuentre con alguna vieja instalación de red de este tipo. Las redes 10Base5 utilizan topología en bus.

10Base2 o ThinNet

Mientras 10Base5 ya casi es desconocida, es bastante más fácil encontrar cableado para el estándar Ethernet 10Base2, también llamada Ethernet fina o ThinNet. Cómo en el caso de 10Base5, 10Base2 tiene una velocidad de 10 Mbps y utiliza cables coaxiales; sin embargo, la longitud máxima de un segmento es 185 metros (de ahí el "2" en 10Base2, redondeando a 200 el 185). Los cables para 10Base2 son más delgados y, por tanto, resulta más fácil trabajar con ellos, y utilizan conectores BNC redondos como los de la TV por cable. También requieren una topología de red en bus.

Nota

BNC son las siglas de British Naval Connector, Bayonet Nut Connector o Bayonet Neill Concelman, dependiendo de con quién se esté hablando. Todo el mundo los llama simplemente BNC.

Adam utilizó una red 10Base2 en su casa anterior (en lugar de 10BaseT, que veremos a continuación) porque los despliegues de cable eran tan largos que habría necesitado comprar un concentrador Ethernet (comentado más adelante en este capítulo) para cada ubicación. Hoy, eso no habría sido mucha inversión, pero en aquel momento, los concentradores costaban alrededor de 100$ cada uno y comprar cuatro hubiera sido excesivo. La red 10Base2 funcionaba bien y, más adelante, cuando los ordenadores empezaron a incluir conexiones sólo para Ethernet 10BaseT, ya había disponibles baratos concentradores que conectaban cables 10Base2 y 10BaseT. (Glenn hizo lo mismo en 1995 en una oficina: era más barato taladrar las paredes de la oficina para crear un circuito que llevar cables hasta una ubicación central.)

10BaseT

Gracias al uso de cables de *par trenzado* comunes y una indulgente topología en estrella, 10BaseT domina el mundo de las redes. (La "T" de 10BaseT corresponde a par Trenzado.) Los cables de par trenzado son muy comunes porque se utilizan para conectar los cables de teléfono de un edificio con la

compañía telefónica. Los cables que utilizamos en casa para conectar un teléfono o un módem a la toma de la pared no son de par trenzado, sino que contienen pares paralelos de alambre.

La utilidad del par trenzado, en el que cada par de alambres va trenzado un cierto número de veces por metro, es que reduce la interferencia electromagnética entre las señales que recorren cada alambre. La mayoría de los cables de par trenzado contienen varios pares de alambres; aunque sólo se necesita un par para el uso telefónico, Ethernet 10BaseT requiere dos pares: uno para transmitir datos y el otro para recibirlos.

Truco *Si intenta reemplazar un cable de par trenzado por uno de par paralelo, la conexión no funcionará por las interferencias entre los dos alambres paralelos. Afortunadamente, si presta atención a los cables, es improbable que intente hacer tal cosa, pues los cables de par paralelo tienen enchufes estándar RJ-11 para conectores de teléfono RJ-11 (cuatro alambres). Por el contrario, los cables Ethernet 10BaseT tienen enchufes RJ-45 más grandes (ocho alambres).*

Las redes 10BaseT están limitadas a una longitud máxima de segmento de 100 metros, bastante menos que los antiguos estándares basados en cables coaxiales, pero más que suficiente para la mayoría de las situaciones. Recuerde que como las redes 10BaseT utilizan una topología en estrella, cada ordenador o dispositivo debe estar conectado a un concentrador central.

Hay muchas variaciones en los cables en par trenzado, pueden ser blindados o sin blindar: el cable blindado se utiliza en algunas situaciones de redes de empresa en que la camisa metálica alrededor de los pares trenzados actúa como toma de tierra. No es probable que vea ese tipo de cable y el par trenzado normal suele estar sin blindar, con las siglas UTP, *Unshielded Twisted Pair*.

Nota ***Nota:*** *Otro término que puede encontrar asociado al cable Ethernet es plenum-rated, que significa que el cable es resistente al fuego y la camisa produce poco humo. Eso es importante para cables que recorren conductos muy poblados entre salas, pues en caso de incendio, no producirán humos tóxicos que tengan vía libre desde una parte ya incendiada hasta otras que todavía estén a salvo.*

Los cables en par trenzado también se clasifican por categorías según la velocidad de transmisión. Aunque hay categorías de la 1 a la 6, las más comunes son la 3 y la 5 (Cat3 y Cat5). Compre siempre cable Cat5 (aunque Cat3

vale para 10BaseT, no resulta adecuado para los estándares nuevos y cada vez más rápidos, 100BaseT o 1000BaseT). Cat5 vale para esos estándares, aunque para 1000BaseT necesitará cuatro pares de cables en lugar de los dos pares estándar. También puede encontrar cables clasificados como Cat5e o Cat6; también son adecuados, pero son más caros y no producen ventajas a cambio.

Casi cualquier dispositivo de red que pueda comprar hoy día prestará soporte al menos a Ethernet 10BaseT, que se está convirtiendo en el mínimo común denominador delas redes.

100BaseT o Fast Ethernet

100BaseT, también conocida como Ethernet rápida o Fast Ethernet, funciona casi igual que 10BaseT y utiliza el mismo cable en par trenzado Cat5. Sin embargo, 100BaseT va a 100 Mbps, que es significativamente más rápido que la velocidad de 10 Mbps disponible con 10BaseT. Aunque Fast Ethernet no producirá ninguna diferencia en el acceso a Internet (si no trabaja en una gran empresa, tendrá suerte si consigue una conexión a Internet de 1 Mbps, y no digamos una conexión de 100 Mbps), sí podrá apreciar la mejora en el rendimiento cuando copie archivos de un ordenador a otro con Fast Ethernet en lugar de 10BaseT. Es bastante divertido, por ejemplo, arrastrar un archivo de 1 GB desde el Escritorio a otra máquina y ver como se copia en sólo unos minutos.

Cables cruzados y puertos uplink

Dado que los distintos cables Ethernet en par trenzado dedican unos pares a recibir y otros a enviar transmisiones, todo concentrador tiene agujas (o pins, pequeños cables rígidos) en sus conectores que coinciden con los pins equivalentes de los cables Ethernet. Pero cuando se conectan distintos tipos de dispositivos, como puede ser un concentrador con otro o un dispositivo especial que está diseñado para conectarse directamente con un ordenador, hay que intercambiar los cables de transmisión y recepción utilizando un cable cruzado (o de conexión directa porque conecta un ordenador a otro sin usar concentrador).

La única diferencia entre un cable cruzado y un cable Ethernet normal (o cable de conexión porque se utiliza para conectar un ordenador a un concentrador) es que en un cable normal los alambres tienen la misma posición en los dos extremos, mientras que en un cable cruzado los alambres de transmisión y recepción intercambian posiciones.

Concretando, en un cable de conexión, el pin 1 de un lado se conecta con el pin 1 del otro lado, el pin 2 con el pin 2, etc. En un cable cruzado, el pin 1 se conecta con el pin 3, el pin 2 con el pin 6, el pin 3 con el pin 1 y el pin 6 con el pin 2.
Es necesario utilizar cables cruzados en varias situaciones:

- *Conexiones de un ordenador con otro.*
- *Conexiones de un concentrador con otro.*
- *Conexiones de módems DSL u otros dispositivos especiales con un concentrador.*

Casi todos los concentradores vienen con al menos un puerto uplink, que es el equivalente de un cable cruzado. Conectar un cable de conexión con el puerto uplink produce el efecto de cruzar los alambres apropiados, igual que en un cable cruzado. Algunos dispositivos tienen un puerto separado y etiquetado; otros tienen un conmutador manual. Algunos dispositivos de red más nuevos, como el puente inalámbrico Linksys WET11, tienen un conmutador lateral para los modos de funcionamiento directo y cruzado.
Lea la documentación del concentrador, ya que algunos concentradores (especialmente algunos modelos antiguos de Linksys, Adam tiene uno de ellos) comparten la conexión entre el puerto uplink y el puerto convencional vecino. Eso significa que si se utiliza el puerto uplink, no se puede usar el puerto vecino para un ordenador u otro dispositivo de red. Si no puede encontrar la documentación, una indicación de esto es que, cuando el puerto uplink está conectado a otro concentrador, el LED del puerto vecino al puerto uplink está encendido.
La cosecha actual de ordenadores Mac y algunos conmutadores de red más caros tienen puertos Ethernet que detectan cuándo es necesario un cable cruzado y se reconfiguran ellos mismos para funcionar correctamente.
No es mala idea tener un cable cruzado en la caja de herramientas de red, pero si compra uno, asegúrese de etiquetarlo claramente. Intentar usar un cable cruzado en una situación que requiere un cable normal conduce a la frustración. Adam resolvió este problema tiempo atrás comprando un pequeño conector que, cuando se utiliza entre dos cables normales, convierte la combinación en un cable cruzado. Los cables cruzados a menudo son de color amarillo, por razones que desconocemos.

Las redes Fast Ethernet se han vuelto lo suficientemente comunes y baratas para que merezca la pena gastar algunos euros extra en equipamiento de red que le preste soporte, además de a 10BaseT. Si opta por la reciente especificación inalámbrica 802.11a, que opera a 54 Mbps, o desea conectar varios puntos de acceso 802.11b (cada uno a 11 Mbps) a una red, entonces usar 100 Mbps parece una idea todavía mejor.

Incluso aunque sus ordenadores actuales no presten soporte a Fast Ethernet, cada vez es más probable que en el próximo futuro cualquier ordenador que compre admita esa red. De hecho, hace varios años que Apple empezó a vender ordenadores Mac con puertos Ethernet que admiten tanto Fast Ethernet como 10BaseT (puede ver tales puertos con el nombre de "puertos 10/100 Mbps").

También hemos descubierto que los conmutadores o concentradores que conectan redes de par trenzado entre sí ahora admiten casi uniformemente tráfico configurado como 10/100 Mbps, que significa que es posible conectar un tipo de red con otro sin cambiar las posición de los conmutadores. También encontrará estos tipos de miniconcentradores en muchas puertas de enlace inalámbricas. Recalquemos que si desea utilizar dispositivos Fast Ethernet en una red, debe comprobar que el cable en par trenzado que compra es Cat5; el cable Cat3 no funcionará.

1000BaseT o Gigabit Ethernet

Finalmente, llegamos a 1000BaseT, llamada más comúnmente Gigabit Ethernet porque va a 1000 Mbps, o aproximadamente 1 Gbps. Aunque Gigabit Ethernet se está volviendo un tipo de red más común (todos los ordenadores profesionales de mesa de Apple, la línea Power Mac, prestan soporte a Gigabit Ethernet por defecto), no son bastantes los ordenadores y otros dispositivos de red que la admiten sin encarecer demasiado el precio para que merezca la pena. Además, los conmutadores Gigabit Ethernet son carísimos y es mejor utilizar cables Cat5e o Cat6 (Cat5 puede valer, pero reducirá el rendimiento de la red).

De cualquier forma, igual que con la mayoría de la tecnología de red, esperamos que en un año, poco más o menos, las redes Gigabit Ethernet sean una opción asequible y con gran disponibilidad, como sucede hoy con 100BaseT.

Otros tipos de red

Ethernet puede ser el gorila de 300 kilos en el mundo de las redes, pero sigue habiendo sitio para algunos chimpancés o, dependiendo de la actitud, macacos.

LocalTalk y PhoneNet

Aunque nunca terminó de despegar y salir del mundo Macintosh, durante muchos años en ese mundo hubo una tecnología de red de baja velocidad llamada LocalTalk. LocalTalk iba a sólo 230.4 Kbps y, cuando fue lanzada por primera vez, requería cables y conectores registrados de Apple. Pero la gente de Farallon Communications pronto descubrió que LocalTalk funcionaba bien a través de cables de teléfono normales. Los adaptadores PhoneNet de Farallon (y sus clones), usados con cables de teléfono estándar, pronto sustituyeron a los cables y conectores LocalTalk de Apple totalmente.

Nota *¿Dónde está ahora Farallon? En 1997, la compañía cambió de nombre y pasó a llamarse Netopia y, un año y medio después, dio origen a una división de hardware de nuevo con el nombre Farallon. Esta nueva Farallon fue comprada por Proxim en el 2000. El nombre Farallon ha desaparecido y su línea de productos ha quedado subsumida en los productos de Proxim, pero sigue centrada en los ordenadores Mac y Proxim es una de las pequeñas empresas dedicadas a las redes, junto con Asanté Technologies, que se esfuerzan por ofrecer equipamiento que explícitamente presta soporte a los sistemas Mac.*

Los conectores LocalTalk y PhoneNet se enchufaban en puertos en serie (concretamente en los puertos de impresora) de los viejos ordenadores Mac y formaban redes muy tolerantes. Aunque utilizaban topología bus, olvidar conectar un terminador en cualquiera de los extremos de la red no solía provocar problemas y los usuarios descubrieron rápidamente lo fácil que era adaptar el cableado telefónico existente para que funcionaran los conectores PhoneNet. Como PhoneNet sólo precisaba un par de alambres y la mayoría de los cables de teléfono contienen un par de alambres que no se utiliza, era sencillo añadir enchufes de red al cableado telefónico ya instalado.

Nota *Para dar una idea de lo flexibles que pueden ser las redes LocalTalk, un amigo nos habla de una red LocalTalk que utilizaba las tuberías de agua caliente y fría (!) en lugar de un par de alambres.*

Ninguno de los ordenadores Macintosh recientes tiene puertos en serie, de modo que las redes LocalTalk han ido desapareciendo lentamente sustituidas por las redes Ethernet convencionales e inalámbricas. Sin embargo, a diferencia de los tipos de cables Ethernet viejos, todavía puede ser común encontrar

redes LocalTalk en funcionamiento, incluso aunque sólo sea para proporcionar acceso a una de las primeras impresoras láser LaserWriter de Apple, que se añadían a las redes muy fácilmente con LocalTalk. Los ordenadores Mac modernos que no prestan soporte a LocalTalk todavía pueden enviar tareas a esas viejas impresoras y mucha gente es reticente, de forma comprensible, a dar por difuntas esas resistentes impresoras.

Afortunadamente, eso no es necesario, ya que un dispositivo llamado puente LocalTalk Ethernet puede conectar una red Ethernet inalámbrica o convencional con una red LocalTalk, incluso aunque el único dispositivo de esa red sea una impresora láser. Hablaremos más de los puentes un poco más adelante en este mismo capítulo; lo importante que hay que comprobar cuando se utiliza un puente LocalTalk Ethernet con un punto de acceso inalámbrico es si el punto de acceso permite el paso de AppleTalk (también hablaremos de AppleTalk en breve). Fundamentalmente, la cuestión es si el punto de acceso puede aceptar un paquete AppleTalk (que es un tipo específico de contenedor para datos) procedente de un ordenador de la red inalámbrica y enviarlo a la red LocalTalk sin dañar los datos de ningún modo. Algunos puntos de acceso pueden dejar intactos los paquetes AppleTalk, pero otros no.

HomePNA

Más moderno que LocalTalk es el estándar de red HomePNA, que fue desarrollado por un grupo corporativo llamado Home Phoneline Networking Alliance. Como LocalTalk, HomePNA utiliza cables de teléfono estándar en una red bus. Aunque HomePNA 1.0 sólo era capaz de llegar a 1 Mbps, HomePNA 2.0 ha aumentado esa velocidad hasta 10 Mbps. Naturalmente, como con todas las redes, esas velocidades son teóricas y nos han informado que la velocidad real de HomePNA 2.0 está alrededor de los 4 Mbps.

Lo más interesante de HomePNA es que utiliza los mismos cables que el teléfono, el módem o el fax, teóricamente sin interferencias. No hemos probado el equipamiento HomePNA y no podemos atestiguar por experiencia si funciona bien. Pero en teoría, sólo hay que conectar un adaptador de red HomePNA (disponible como tarjeta PCI, adaptador USB o adaptador Ethernet) a los ordenadores y desplegar un cable de teléfono desde el adaptador de red a los enchufes telefónicos. Se pueden comprar puentes HomePNA Ethernet que conectan las redes HomePNA estándar con redes Ethernet estándar, y el soporte a HomePNA está siendo incorporado también a otros dispositivos de red.

¿Por qué utilizar HomePNA? Podría ser útil para poner en red todos los ordenadores, pero teniendo en cuenta que está leyendo este libro, seguramente querrá evitar el uso de cables en lo posible. Para nosotros, por tanto, HomePNA

puede ser útil para conectar ordenadores de distintas habitaciones utilizando los cables de teléfono que ya haya instalados en la casa. Conectando un punto de acceso inalámbrico a un puente HomePNA Ethernet en cada habitación (o comprando un punto de acceso que preste soporte también a HomePNA), podríamos extender el alcance de una red inalámbrica hasta una parte de la casa u oficina que fuera inaccesible de otro modo.

Si tiene que desplegar nuevos cables, puede usar par trenzado Cat5 en lugar de cable telefónico, pues comprar adaptadores HomePNA para los ordenadores es mucho más caro que enchufar cables Ethernet en los puertos Ethernet del ordenador. Además, si tiene ordenadores modernos, probablemente admitan Fast Ethernet, que es mucho más rápida que HomePNA. Las redes HomePNA se enfrentan a varias dificultades que reducen su popularidad:

- En la mayoría de las casas hay relativamente pocas conexiones telefónicas por habitación, haciendo que sea improbable encontrar una toma en el lugar en que la necesitamos.
- Aunque el rendimiento de HomePNA ha aumentado con la versión 2.0, la velocidad real de 4 Mbps no es lo que se dice impresionante. La próxima versión, HomePNA 3.0, promete 100 Mbps como velocidad teórica, aunque el resultado real está por ver (lo comprobaremos este mismo año 2003).
- Otros aparatos que utilizan los mismos cables, como teléfonos, módems, máquinas de fax e incluso conexiones de Internet basadas en DSL (que a menudo utilizan frecuencias que se encuentran vacías en el mismo cable de la línea telefónica) pueden provocar interferencias con HomePNA, reduciendo el rendimiento e incluso impidiendo establecer conexiones.
- Ethernet es una opción mejor para usar en casa para casi cualquiera que desee utilizar el mismo ordenador en su casa y en el trabajo: en la mayoría de las oficinas se utiliza Ethernet.

Para más información acerca de HomePNA, visite el sitio Web de HomePNA en www.homepna.org.

HomePlug

Mucho más comunes que las tomas de teléfono en cualquier habitación son los enchufes de electricidad, y ahí es donde se ha fijado HomePlug Powerline Alliance con el estándar de red HomePlug. En lugar de conectar un adaptador de red a una toma de teléfono o de red, simplemente se conecta a una toma eléctrica.

Nota

Sí, han sido muy hábiles al averiguar cómo transferir los datos a través de las líneas de corriente estándar dentro de la propia casa. Los investigadores incluso han determinado cómo proporcionar acceso a Internet de alta velocidad a través de los cables de luz, aunque todavía no hemos oído que eso se haya implementado ampliamente en ninguna parte del mundo.

HomePlug va a 14 Mbps, aunque su rendimiento real, según nos informan, está entre 5 y 6 Mbps. Como HomePNA, HomePlug utiliza una topología de red bus, de modo que no es necesario un concentrador central. De hecho, aparte de usar líneas eléctricas en lugar de cables de teléfono, la red HomePlug es muy parecida a la red HomePNA (una vez leída la sección anterior, reemplace mentalmente "HomePNA" con "HomePlug" y ya está). HomePlug incluso coopera con otras tecnologías que transmiten datos a través de línea de corriente, como los dispositivos de automatización del hogar X10. Sin embargo, el equipamiento HomePlug cuesta actualmente un poco más que el equipamiento HomePNA.

Nota

Desgraciadamente, HomePlug sólo funciona en el sistema de corriente de 110 voltios, haciendo que no se pueda utilizar en los muchos países del mundo que no utilizan el voltaje 110.

Si vive en un apartamento y decide configurar una red HomePlug, reflexione sobre la seguridad de la red, pues los apartamentos comparten a menudo las líneas de corriente. Todo el hardware HomePlug puede cifrar los datos para que los vecinos no puedan conectar con nuestra impresora, ver carpetas compartidas o curiosear en las comunicaciones de red. Si le preocupa la seguridad, compruebe que activa el cifrado; es probable que esté desactivado por defecto.

¿Cómo decidir entre HomePlug y HomePNA para ampliar una red convencional o inalámbrica? La cuestión es fácil dependiendo de si dispone del voltaje de 110 voltios o si hay o no tomas de teléfono en los lugares apropiados. Si puede optar por las dos posibilidades, HomePlug es ligeramente más rápida, pero el equipo es más caro. También tenga en cuenta la edad y las condiciones de conservación del cableado. Si los enchufes son viejos y carecen de toma de tierra, pero la línea telefónica es más nueva, decídase por HomePNA. Cuanto más vieja y gastada esté la instalación eléctrica, más probable será que el rendimiento se vea reducido o los aparatos se desconecten de la red sin razón aparente. Para más información acerca de HomePlug, visite el sitio Web de HomePlug en www.homeplug.org.

Dispositivos de red

El siguiente paso en el aprendizaje de las redes es conocer los distintos tipos de dispositivos con los que se construye una red. Eso es fácil, pero hay que tener dos cosas en cuenta:

1. Aunque los dispositivos señalados en esta sección empezaron como aparatos separados, ha resultado que tiene sentido combinar varias funciones en el mismo dispositivo. Por ejemplo, hoy día es fácil comprar un aparato que combine un concentrador con conmutadores para cuatro puertos, punto de acceso inalámbrico, software de cortafuegos y puente Ethernet entre red convencional y red inalámbrica, todo junto.
2. Los fabricantes tienden a confundir la terminología, haciendo que a veces sea difícil identificar exactamente qué funciones tiene incorporadas un dispositivo dado.

De cualquier forma, siguiendo nuestras próximas descripciones y leyendo atentamente las especificaciones del producto que esté investigando, podrá averiguar qué funciones ofrece cualquier dispositivo.

Adaptadores de red (NIC)

La pieza de una red más sencilla de entender es el adaptador de red, llamado también frecuentemente tarjeta de interfaz de red (NIC en sus siglas en inglés). Dicho con sencillez, el adaptador de red es la pieza que conecta el ordenador con la red, nada puede suceder sin su presencia. Para continuar con la analogía del ferrocarril, un adaptador de red es como el andén de la estación; la estación puede estar en su sitio, pero no será útil si no hay un andén que permita pasar a la gente de la estación al tren y viceversa.

Como puede esperar, los adaptadores de red son específicos de cada tipo de red, de modo que si compra un adaptador 10BaseT, sólo puede conectar el ordenador a una red 10BaseT. Como el sistema de circuitos necesario para prestar soporte a los distintos tipos de Ethernet es prácticamente el mismo, los fabricantes a veces combinan el soporte a distintos tipos de red en un solo adaptador. Antiguamente, cuando las redes 10Base2 eran tan comunes como las redes 10BaseT, por ejemplo, era común que un adaptador de red tuviera un puerto RJ-45 para 10BaseT y una toma BNC para 10Base2. Cualquiera de los dos podía ser activado en cualquier momento (pero no los dos a la vez), sim-

plemente conectando el cable apropiado. Hoy día, muchos adaptadores de red combinan 10BaseT y 100BaseT, o incluso añaden 1000BaseT al conjunto. Estas tarjetas frecuentemente están etiquetadas como "10/100 Mbps" o incluso "10/100/1000 Mbps".

Tipos de adaptadores de red

Los adaptadores de red vienen con distintas formas y tamaños, y un siempre creciente número de ordenadores, incluyendo todos los ordenadores Macintosh fabricados en los últimos años, los han integrado. Si su ordenador tiene un puerto Ethernet, entonces tiene integrado el adaptador de red. Otros tipos de adaptadores de red son:

- Tarjetas PCI conectadas en ranuras PCI dentro de muchos ordenadores de mesa modernos que son probablemente el tipo más común de adaptador de red. Hay tarjetas PCI que proporcionan acceso a redes convencionales e inalámbricas. Para ordenadores más antiguos, anteriores a la aparición de PCI como estándar de ranura de expansión, todavía podrá encontrar tarjetas de adaptador de red ISA (para PC) o NuBus (para Macintosh) para redes convencionales, pero no para redes inalámbricas.
- PC Cards para ranuras PC Card en ordenadores portátiles. Los ordenadores de mesa casi nunca tienen ranuras para PC Cards. Muchos adaptadores de red PC Card de Ethernet convencional vienen con un pequeño cable que se conecta con el dispositivo PC Card del tamaño de una tarjeta de crédito para proporcionar un conector Ethernet normal. Los adaptadores de red inalámbrica PC Card típicamente sobresalen por el lateral del portátil para acomodar sus antenas.

Truco

Los veteranos todavía llaman a las PC Cards "tarjetas PCMCIA", el nombre original dado por la industria (corresponde a las siglas en inglés de "Asociación internacional de tarjetas de memoria de ordenador personal"). Si escucha a alguien soltar tantas letras, significa que ese alguien se está quedando anticuado.

- Los adaptadores de red USB se conectan en los puertos USB disponibles en la mayoría de los ordenadores modernos. Igual que el resto, los adaptadores de red USB tienen versiones para redes convencionales e inalámbricas.

- No faltan tampoco las soluciones personalizadas e incluso, en los ordenadores modernos, quizá encuentre tarjetas registradas como los adaptadores de red inalámbrica AirPort de Apple. Algunos ordenadores Mac más antiguos incluso tenían tarjetas de adaptador de red registradas CommSlot. La red Ethernet puede precisar que acudamos directamente a la compañía que desarrolló la tarjeta, aunque no es el caso con los periféricos Macintosh; Apple ya no las fabrica (si alguna vez lo hizo).

Nota *Antes que Apple empezara a construir puertos Ethernet 10BaseT en cada ordenador Mac, utilizaba un conector Ethernet genérico llamado un AAUI (Interfaz de unidad accesoria Apple). La idea era que se podía comprar un transceptor AAUI para el tipo de red Ethernet con el que se quería conectar: 10Base5, 10Base2 ó 10BaseT.*

- Los adaptadores de red de puerto paralelos se conectan a los puertos paralelos de los PC. Como los puertos paralelos son muy lentos (por no mencionar que cada vez son menos comunes en la actualidad), un adaptador Ethernet de puerto paralelo es el último recurso para añadir un viejo PC a una red Ethernet convencional.
- Los adaptadores Ethernet SCSI son una estrategia basada en Macintosh similar a los adaptadores de red de puerto paralelo en los PC. Los adaptadores Ethernet SCSI se conectan en los puertos SCSI estándar de todos los ordenadores Mac anteriores al iMac, aunque en realidad sólo se utilizaría un adaptador Ethernet SCSI en los ordenadores Mac de los primeros 90, ya que los otros ordenadores Macintosh ofrecen otras posibilidades. Ya no se venden adaptadores Ethernet SCSI y, si consigue comprar uno, compruebe que consigue software con él, pues la mayoría de las empresas que los fabricaban han desaparecido.

Encontrar adaptadores de red antiguos puede ser difícil, pero si todo lo demás falla, pruebe en el sitio de subastas eBay en www.ebay.com, es un buen recurso para encontrar viejo hardware. Afortunadamente, ninguno de estos aparatos resultará excesivamente caro.

Direcciones MAC

Es probable que su ordenador tenga un número de serie que seguramente sólo esté impreso en la parte externa de la carcasa; el ordenador no sabe qué es

un número de serie. Sin embargo, todo adaptador de red, Ethernet o inalámbrica, tiene un número de serie unívoco llamado una dirección MAC. MAC corresponde a las iniciales en inglés de Control de acceso a medios, no tiene nada que ver con los ordenadores Macintosh de Apple.

La red Ethernet funciona enviando paquetes a direcciones MAC específicas de la red. Si las direcciones MAC no fueran unívocas, sería posible que dos ordenadores con la misma dirección estuvieran conectados a la misma red. Y si sucediera esto, sería como intentar dirigir un tren a dos estaciones que tienen nombres idénticos. Si se tratara de una comedia de situación televisiva, las risas estarían aseguradas; pero en el mundo real nos enfadamos mucho cuando las cosas no se entregan correctamente. Y lo mismo sucede en el mundo informático.

Nota

Las direcciones MAC están asociadas con los adaptadores de red, no con los ordenadores; si un ordenador tiene integrados un adaptador de red Ethernet y un adaptador de red inalámbrica, los dos tendrán sus propias direcciones MAC unívocas.

Las direcciones IP necesarias para que un ordenador establezca comunicación con Internet se asocian con las direcciones MAC utilizando un proceso llamado Protocolo de resolución de direcciones (ARP). Las redes IP se extienden por muchas redes Ethernet y la asociación de IP con MAC permite que el tráfico salga del ordenador, llegue al enrutador, transite por Internet, llegue a un segundo enrutador para pasar a una red local y alcance una máquina determinada en el otro extremo. Gracias a ARP, los enrutadores saben qué direcciones IP están conectadas con cuáles direcciones MAC. Puede haber muchas direcciones IP asociadas a una sola dirección MAC.

En su mayor parte, no es necesario saber nada acerca de las direcciones MAC. Hay tres excepciones a esa regla y, aunque no vamos a entrar en ellas con mucho detalle aquí, volveremos a verlas en otras partes del libro, de modo que no se preocupe si parte de esta información no le resulta del todo clara.

- Podemos decir a ciertas puertas de enlace que asignen la misma dirección IP a una dirección MAC concreta en todo momento. De esta forma, podemos configurar el portátil para que obtenga una dirección IP a través de DHCP (Protocolo de configuración dinámica de host, que veremos con más detalle más adelante en este capítulo) sin que afecte dónde nos encontremos; tanto en casa como en la oficina el ordenador portátil tendrá siempre la misma dirección IP en esas redes. Sin embargo, durante los viajes no podremos obtener la misma dirección IP, pero no será

necesario cambiar la configuración de red para recibir una dirección IP asignada dinámicamente por el servidor DHCP de la red remota.

- Es posible configurar la seguridad en una red inalámbrica para que sólo los ordenadores con direcciones MAC específicas tengan permiso para conectar. Esta estrategia es bastante segura, pero...
- En la mayoría de los adaptadores de red puede modificarse la dirección MAC fácilmente o con algo de esfuerzo. Cuando un adaptador sale de la cadena de montaje, debe recibir una dirección única, que generalmente también se estampa en una etiqueta pegada al adaptador. La dirección se guarda además en memoria persistente variable en el adaptador de red. Hay dos razones por las que podemos querer cambiar una dirección MAC. Primera, algunos ISP de cable y ciertas universidades restringen las conexiones de red a direcciones MAC registradas. Las compañías de cable a menudo sólo permiten registrar una máquina. Si deseamos mover los ordenadores o compartir una conexión a través de una puerta de enlace inalámbrica, hay que asignar al nuevo adaptador de red (el adaptador que establece la conexión) la dirección MAC del adaptador de red registrado. La otra razón no es tan inocente: un *cracker* de redes inalámbricas puede clonar la dirección MAC de un ordenador que dispone de permiso para acceder a una red inalámbrica con motivos inconfesables. Triste pero cierto.

Concentradores y conmutadores

Volvamos un momento a nuestro debate sobre las topologías de red. ¿Recuerda que en la topología estrella siempre hay un concentrador central, del que parten todas las conexiones como los radios de una rueda? Bien, ése es el caso de los concentradores Ethernet: actúan como punto central con el que conectan todos los ordenadores.

Nota *De hecho, los puntos de acceso inalámbricos son en esencia concentradores para redes inalámbricas. Naturalmente, utilizan ondas de radio en lugar de cables Ethernet, pero por lo demás son prácticamente iguales. Comentaremos más los puntos de acceso inalámbricos en el capítulo 3.*

Los concentradores tienen dos o más puertos en los que se pueden conectar ordenadores (aunque un concentrador con sólo dos puertos no parece muy útil,

pues únicamente permiten conectar dos ordenadores, los concentradores de este tipo suelen ser muy pequeños y están pensados para crear rápidamente pequeñas redes cuando estamos de viaje).

Truco

Para decidir lo grande que debe ser el concentrador a comprar, busque uno con más puertos de los que piensa que puede necesitar. Los puertos extra siempre resultan útiles.

Igual que los adaptadores de red, los concentradores deben prestar soporte al tipo de Ethernet que utiliza la red, de modo que si hemos instalado Fast Ethernet (100BaseT) o Gigabit Ethernet (1000BaseT), debemos comprobar que el concentrador la admite. Los concentradores modernos pueden identificar automáticamente la velocidad de la red y configurar sus puertos de forma apropiada; no hay problema al mezclar aparatos 10BaseT y Fast Ethernet en un solo concentrador 10/100 con identificación automática.

Nota

Aunque ahora no son tan comunes, solía ser fácil encontrar concentradores con puertos 10BaseT RJ-45 y también un puerto BNC para redes 10Base2. Eso facilitaba la combinación de tipos de redes; por ejemplo, podíamos usar un cable coaxial 10Base2 para desplegar un cable largo y poner un concentrador en uno de los extremos para los aparatos que sólo pudieran conectar con redes 10BaseT.

Tipos de concentradores

Hay tres tipos de concentradores: pasivos, inteligentes y de conmutación.

- Un concentrador pasivo no hace más que actuar como conducto para los datos que van de un ordenador en uno de los radios de la rueda a otro que se encuentra en otro radio. Hay que conocer tres hechos importantes acerca de los concentradores pasivos, pues son los que constituyen la diferencia con los otros dos tipos de concentrador. Primero, los concentradores pasivos comparten todo el ancho de banda de la red internamente. Supongamos que hay ocho ordenadores conectados a un concentrador pasivo 10BaseT de 8 puertos. Si copiamos archivos de un ordenador a otro utilizando 5 Mbps de ancho de banda, los seis ordenadores restantes deben compartir para sus asuntos los 5 Mbps de ancho de banda que quedan libres. Eso es porque cuando un paquete llega des-

de un ordenador en uno de los radios, el concentrador pasivo lo copia en todos los radios, aunque sólo vaya destinado a un ordenador determinado. En un momento compararemos eso con el comportamiento de un concentrador de conmutación. Segundo, con un concentrador pasivo, la única información que tenemos de lo que está pasando es un LED que indica cuándo está conectado un ordenador a un puerto (el LED es una pequeña luz) y cuándo hay tráfico que proviene o se dirige a ese ordenador (el LED está intermitente). También compararemos eso con el comportamiento de un concentrador inteligente. Tercero, un concentrador pasivo hace que una red Ethernet parezca ser un segmento, limitando las distancias máximas y aumentando las colisiones.

- Un concentrador de conmutación, también llamado un conmutador, lee la dirección de destino de cada paquete y lo envía al puerto correcto (en lugar de enviarlo simultáneamente a todos los puertos, excepto en el caso de ciertos paquetes de difusión especiales utilizados por DHCP y algunos otros protocolos). Esta diferencia con los concentradores pasivos proporciona una importante ventaja: dado que cada puerto es una conexión independiente entre los aparatos conectados, en lugar de compartida, cada conexión recibe todo el ancho de banda disponible en ese tipo de red. Por ejemplo, supongamos que en nuestra red de ocho ordenadores del ejemplo del concentrador pasivo ahora usamos un concentrador de conmutación. Cuando empezamos a copiar archivos de un ordenador a otro, el concentrador de conmutación hace que esos dos ordenadores (y el resto de los ordenadores de la red) piensen que están conectados directamente. Si otros dos ordenadores establecen una comunicación mientras se están copiando los archivos, el concentrador de conmutación hace lo mismo para ellos, proporcionándoles una conexión directa virtual. Un concentrador de conmutación proporcionan un mejor rendimiento que el concentrador pasivo: la red va más rápido si normalmente hay pares de ordenadores comunicándose entre sí. Los concentradores de conmutación también son útiles para conectar concentradores pasivos u otros concentradores de conmutación en configuraciones de red más grandes. Para redes pequeñas, no habrá mucha diferencia, si hay alguna, entre usar conmutadores pasivos o de conmutación pero, afortunadamente, hoy día casi todos los concentradores son de conmutación gracias a que se ha reducido el coste de los circuitos necesarios.
- Un concentrador inteligente añade funciones que permiten a los administradores de red controlar el tráfico que atraviesa el concentrador y confi-

gurar cada puerto independientemente. Generalmente, se utilizan estas funciones a través de un navegador Web conectado a un servidor Web integrado en el concentrador. Es inusual que se necesite un concentrador inteligente en una red pequeña.

Nota

Si quiere conectar concentradores entre sí, debe usar un cable cruzado entre puertos normales o un cable de conexión entre un puerto normal de uno de los concentradores y el puerto uplink del otro concentrador. Encontrará más detalles en el cuadro "Cables cruzados y puertos uplink" visto anteriormente en este capítulo.

¿Qué tipo de concentrador debe comprar si tiene varias opciones? Recomendamos los concentradores de conmutación, pues son baratos y proporcionan el mejor rendimiento. Sólo las redes más grandes pueden aprovechar los concentradores inteligentes.

Puentes

La siguiente pieza importante en el hardware de red es el puente. A pesar de su nombre, imaginar un puente real no sirve de ayuda para entender los puentes de red. Piense mejor en lo que sucede cuando se quiere transferir un contenedor de mercancías (un paquete) desde un vagón a otro en una vía cercana pero distinta. El propio contenedor de mercancías no puede ocuparse del cambio por sí solo, sino que se necesita una maquinaria, como puede ser una cinta transportadora automática, para trasladar el contenedor de un vagón a otro.

En términos de red, esa cinta transportadora es el puente. Los puentes conectan tipos de red similares que utilizan medios diferentes o están separados físicamente de alguna forma. Para decirlo más técnicamente, un puente traslada los datos desde un tipo de medio físico a otro sin hacer demasiados cambios en los datos. Consideramos a los puentes dispositivos muy ingeniosos, pues son baratos y resuelven muchos problemas de red peliagudos. Se necesita un puente para conectar una red Ethernet convencional con una red inalámbrica, conectar una red LocalTalk con una red Ethernet convencional, conectar una red HomePNA con una red inalámbrica, etc.

Aunque los puentes a menudo están integrados en otros dispositivos, como un punto de acceso inalámbrico que también hace de puente entre redes convencionales e inalámbricas, también es posible encontrarlos como aparatos independientes. Son especialmente útiles cuando tenemos una red vieja, como

una red LocalTalk, que queremos conectar a una red Ethernet más moderna sin comprar nuevos adaptadores de red.

Los puentes no se interesan por el destino de los datos, simplemente hacen pasar el tráfico desde una red a otra. Esto hace que los puentes sean más rápidos, pues no observan el paso de los datos y generalmente no se ven afectados por qué protocolos de red hay implicados en la transacción. Cuando necesitamos traducir un tipo de protocolo a otro, como sucede al pasar de una Red de área local (LAN) a una Red de área extensa (WAN), por ejemplo de la red casera a Internet, necesitamos un enrutador, que es lo que describimos a continuación.

Enrutadores

En nuestra metáfora de los transportes, los puentes mueven los mismos tipos de contenedores entre tipos similares de sistema de transporte, como contenedores de mercancías desde un tren a otro que se encuentra en otra vía. Los enrutadores, por su parte, no sólo mueven los contenedores, también los abren y vuelven a empaquetar el contenido en contenedores más pequeños: piense en un envío que llega por tren a un punto de venta de muebles al por mayor, en el que hay que separar los juegos de comedor para enviarlos por camión a través de la red de autopistas.

Un ejemplo más orientado a Internet sería pensar en Amazon.com: la compañía solicita miles de libros a un solo editor, que llegan por tren o por camión. Los libros se descargan, clasifican y colocan en nuevos paquetes para cada destinatario que a su vez se cargan en camiones de empresas de transporte de paquetería, como UPS o Federal Express.

Los enrutadores convierten los protocolos basados en direcciones que describen cómo debe la información ir de un lado a otro. Cada paquete es inspeccionado y vuelto a empaquetar con la información de destino apropiada para la red a la que debe pasar. En la práctica, este papel a menudo se reduce a un enrutador que coge paquetes Ethernet con datos destinados a Internet o paquetes procedentes de Internet con datos destinados a máquinas conectadas a una red convencional o inalámbrica, y a convertir las direcciones IP en direcciones MAC. Los enrutadores también pueden hablar con otros enrutadores, por descontado, y el enrutamiento del tráfico a través de Internet puede ir Ethernet, enrutador, Ethernet, enrutador, Ethernet, mientras los datos encuentran su camino hasta un nivel lo suficiente alto para "ver" su camino hacia su destino.

Como quizá suponga, observar y actuar sobre cada paquete precisa potencia de procesamiento y RAM, haciendo que los enrutadores sean aparatos

significativamente más caros que los simples puentes. Aún así, los avances en tecnología han permitido que los fabricantes de equipamiento de red incorporen capacidades de enrutador en dispositivos baratos, como las puertas de enlace Linksys, que en realidad disponen de todas las capacidades de enrutamiento. Naturalmente, es probable que no cubran las necesidades de una red grande, pero en las redes pequeñas en las que se instalan normalmente, se comportan bien.

Dicho esto, si está interesado en una red pequeña y su conexión a Internet es por cable, DSL o incluso un módem estándar, probablemente no necesitará capacidades de enrutamiento en absoluto. Si da la casualidad que el aparato que quiere comprar tiene esas capacidades, estupendo, pero no pague dinero extra por ellas. También puede obligar a un ordenador viejo a actuar como enrutador añadiendo software especial: un programa llamado IPNetRouter, de Sustainable Softworks (visite www.sustworks.com), se ha hecho popular porque puede convertir cualquier Macintosh viejo en un buen enrutador.

Puertas de enlace

Ya hemos dicho que los fabricantes de equipamiento de red tienden a confundir la terminología, y en ninguna parte resulta más evidente que en las puertas de enlace. Hablando técnicamente, una puerta de enlace es en esencia el siguiente escalón después del enrutador: estamos hablando de la viga mayor de la red. Sin embargo, el término se utiliza mucho hoy día para aludir a un aparato que combina la mayoría de las capacidades, si no todas, de los dispositivos mencionados aquí, más algunas otras, como las de módems estándar y cortafuegos para aumentar la seguridad de la red. Además, las puertas de enlace ofrecen con frecuencias funciones de software adicionales, como un servidor DHCP y una puerta de enlace NAT.

Nota *Un término mejor sería "puerta de enlace particular", pero nos atendremos al uso estándar actual y sólo usaremos "puerta de enlace" para referirnos a estos dispositivos multiusos.*

Resumiendo, no podemos suponer muchas cosas al oír el término "puerta de enlace", pero seguramente no nos equivocaremos mucho si suponemos que el dispositivo dispone de varias funciones útiles para conectar la red inalámbrica o convencional con Internet. Más allá de eso, hay que leer la hoja de especificaciones atentamente para determinar qué funciones lleva a cabo.

Protocolos de red

En este capítulo, hablamos en general acerca de la transferencia de datos, pero es necesario decir algo sobre qué sucede en realidad. No es necesario conocer esta información para configurar una red, pero puede resultar útil para conseguir que funcionen ciertas cosas.

Toda la comunicación entre ordenadores tiene lugar de acuerdo con un conjunto de reglas preestablecidas, llamado un protocolo y también informalmente (a veces incorrectamente) un estándar. Es igual que en la comunicación entre personas, donde las reglas preestablecidas constituyen un idioma. Un protocolo de red no es más que eso, el idioma que deben hablar los dos ordenadores para entenderse.

Nota *Los estándares se establecen mediante acuerdos en las organizaciones de estándares, ya estén esas organizaciones reguladoras dirigidas por técnicos o por representantes de la industria. Cualquiera puede desarrollar un protocolo, e incluso puede resultar que ese protocolo se utilice mucho, pero sin el sello de aprobación de un cuerpo de estándares, no es un estándar.*

Igual que han nacido muchos idiomas en el mundo, muchos protocolos de red han aparecido con el tiempo. Sin embargo, la búsqueda de una comunicación común ha provocado que muchos de esos protocolos desaparezcan; a diferencia de los idiomas humanos amenazados con la desaparición, pocos movimientos se han hecho para impedir que un protocolo de red poco utilizado desaparezca.

Aunque quizá simplifiquemos en exceso, todo protocolo de red generalmente tiene una función concreta que se combina con las funciones de otros protocolos de red para hacer que las comunicaciones a través de la red sean posibles. Aquí vamos a ver un grupo selecto de protocolos que es probable que encuentre mientras configura su red.

Establecer una conexión

PPP (Protocolo punto a punto) es el campeón reinante en la negociación de conexiones de acceso telefónico y de banda ancha; la versión Ethernet de banda ancha se llama PPPoE, por PPP a través (*over*) de Ethernet.

PPP es una forma simple para que dos dispositivos, después de establecer un enlace de red de algún tipo, negocien un inicio de sesión y después proporcionen detalles de red para la máquina que establece la conexión.

Cuando un cliente conecta a través de PPP o PPPoE, envía el nombre de usuario y la contraseña, junto con otros detalles; el extremo servidor de la conexión abre el acceso al puerto de red o de conexión telefónica una vez que se ha negociado la conexión.

Negociar una dirección

Una vez conectados a la red, los aparatos necesitan direcciones. Los dispositivos Ethernet tienen sus direcciones MAC de hardware por defecto, y AppleTalk (lo veremos en breve) permite a un ordenador asignar su propia dirección unívoca. Pero en el mundo TCP/IP (también lo veremos en breve), cada aparato necesita una dirección IP, que hay que introducir manualmente (en redes estáticas) o asignar dinámicamente. Es este último caso el que vamos a estudiar aquí.

DHCP (Protocolo de configuración dinámica de host), que debatiremos en muchos contextos a lo largo del libro, permite a un servidor asignar una dirección IP a cualquier máquina de la misma red que la desee.

Cuando un ordenador con un cliente DHCP, presente en la mayoría de los sistemas operativos, conecta por primera vez con una red, emite un mensaje que pide una dirección. Uno o más servidores DHCP pueden responder ofreciendo una dirección. El cliente confirma al servidor DHCP apropiado que ha aceptado la dirección ofrecida y, después de eso, se convierte en un miembro de la red, con una dirección, una puerta de enlace y, normalmente, información de servidor DNS.

NAT (Traducción de direcciones de red) colabora con DHCP para convertir las direcciones privadas asignadas por DHCP, que no admiten enrutamiento y no están al alcance desde fuera de la red de área local, en direcciones IP públicas de la puerta de enlace.

De modo que, por ejemplo, DHCP puede asignar la dirección IP 192.168.1.20 a un ordenador, pero nadie desde Internet puede alcanzar esa dirección IP privada sin NAT actuando como policía de tráfico. El servidor NAT intercepta las solicitudes dirigidas al exterior que parten de la red y las rescribe para que parezcan provenir desde la dirección Internet pública de la puerta de enlace que sí admite enrutamiento.

También rescribe la respuesta a estas solicitudes y las envía a la máquina que hizo la solicitud.

Nota *Si está interesado, hay tres tipos de NAT: el tipo que encontramos en las puertas de enlace particulares asigna direcciones privadas a puertos específicos en la dirección pública de la puerta de enlace (traducción de dirección de puerto). De los otros dos tipos, uno asigna una dirección dinámica a otra (una dirección privada a una dirección pública dedicada) y el otro sigue una estrategia global en la que un fondo local de direcciones privadas se asigna arbitrariamente a un fondo de direcciones públicas.*

Empaquetamiento y direcciones de datos

El siguiente grupo de protocolos empaquetan datos en fragmentos discretos con dirección que pueden pasar a través de la red. La información de dirección ayuda a las máquinas individuales de la red o a los enrutadores a conectar con otras redes para entregar los fragmentos de datos en sus destinos.

En todos los casos, hay una parte del protocolo que se ocupa del empaquetamiento (la parte TCP en TCP/IP) y otra que se ocupa de las direcciones (la parte IP en TCP/IP). Estas partes casi siempre están agrupadas en un solo nombre o concepto. AppleTalk incluye las dos partes. TCP/IP domina en la mayoría de las redes actuales, pero también hay que entender cómo NetBEUI de Microsoft y AppleTalk de Apple interactúan con las modernas redes inalámbricas, porque siguen siendo bastante comunes.

Ethernet

Recordará de lo comentado anteriormente en este capítulo que Ethernet es un protocolo de red de bajo nivel que tiene varios tipos. Ethernet envía datos en fragmentos llamados *tramas* y todos los protocolos que comentamos a continuación (TCP/IP, NetBEUI y AppleTalk) pueden ser encapsulados o envueltos en tramas Ethernet. Ethernet utiliza direcciones MAC para entregar los datos.

TCP/IP

TCP/IP es un conjunto de dos protocolos distintos que funcionan en colaboración: TCP (Protocolo de control de transporte) e IP (Protocolo Internet).

TCP reúne los paquetes y los separa; IP se ocupa de las direcciones. Juntos, forman la base de la mayor parte de las comunicaciones de Internet.

La principal ventaja de TCP/IP sobre otros protocolos es que está completamente estandarizado y goza de soporte en los sistemas operativos de ordenador. También tiene otras ventajas, como su excelente rendimiento y la escalabilidad para redes muy grandes. Como TCP/IP está en todas partes, casi todas las aplicaciones relacionadas con redes se comunican a través de TCP/IP.

Tanto los ordenadores Mac como los Windows pueden usar TCP/IP sin problemas. En sistemas con Windows ME y anterior, el panel de control Red proporciona las opciones necesarias; el muy mejorado panel de control Conexiones de red se ocupa de ello en Windows XP. En Mac OS 9, se usa el panel de control TCP/IP; en Mac OS X, el panel de preferencias Red contiene todos los controles necesarios. Veremos los pasos necesarios para configurar los distintos sistemas operativos para el uso de TCP/IP en el capítulo 4.

NetBEUI

NetBEUI (Interfaz de usuario extendida de NetBIOS) fue desarrollada por IBM para utilizarla con su producto LAN Manager y, posteriormente, adoptada por Microsoft para Windows.

Entre sus ventajas están el alto rendimiento y la facilidad con que se descubren recursos de red como servidores de archivos e impresoras. NetBEUI sigue estando disponible en Windows para establecer comunicación con otros ordenadores Windows; sin embargo, limitaciones técnicas impiden que NetBEUI pueda utilizarse en redes grandes y, quizá por ello, nunca se utilizó para conectar ordenadores de distintos tipos.

Se puede usar NetBEUI como protocolo subyacente para compartir archivos e impresoras en Windows, pero probablemente resulte más sencillo en este momento atenerse a TCP/IP, particularmente dado que algunas puertas de enlace pueden no hacer de puente para NetBEUI entre redes convencionales e inalámbricas.

AppleTalk

AppleTalk es una suite de protocolos de red desarrollada por Apple para ordenadores Macintosh funcionando en red e impresoras láser LaserWriter y, cuando apareció, fue una revolución. Aunque AppleTalk no es un protocolo de red especialmente rápido, ofrece buenas funciones a los usuarios, como el descubrimiento automático de aparatos de red, para que los usuarios no precisen

conocer las direcciones de los ordenadores o impresoras con los que quieren conectar.

Nota *Un amigo nuestro en Apple, Stuart Cheshire, ayudó a dirigir el grupo de trabajo que desarrolló un protocolo estándar llamado ZEROCONF (por zero configuration), un intento de trasladar la facilidad de uso de AppleTalk a TCP/IP. Apple llama a la tecnología Rendezvous y la está promocionando con fuerza entre los fabricantes de hardware; sorprendentemente, Microsoft ya ha incorporado parte de ella en Windows XP. Como es un estándar en proceso de ser finalizado por el Grupo de trabajo de ingeniería de Internet (Internet Engineering Task Force o IETF), un cuerpo de estándares de Internet, ZEROCONF tiene muchas posibilidades de tener éxito. Para más información, visite www.zeroconf .org.*

Varios productos de software, incluyendo Servicios para Macintosh en Windows NT/2000 de la propia Microsoft, prestan soporte a AppleTalk en Windows y otras plataformas, pero AppleTalk nunca despegó para conectar ordenadores que no fueran Mac. Incluso Apple se ha alejado de AppleTalk, basando sus servicios de red en TCP/IP. Pero dado que los viejos ordenadores Mac y las viejas LaserWriters de Apple (que se comunican a través de AppleTalk) tienden a no desaparecer, es probable que AppleTalk siga teniendo validez durante un tiempo.

Si compró su hardware Macintosh en los últimos años, no tiene que preocuparse por AppleTalk en absoluto. Sin embargo, para conservar una vieja LaserWriter en su red, tiene que comprobar que AppleTalk está activado (compruebe el panel de control AppleTalk en Mac OS 9 y el panel de preferencias Red en Mac OS X). Si compra un punto de acceso, compruebe que puede actuar de puente para AppleTalk entre redes convencionales e inalámbricas; por ejemplo la Estación Base AirPort de Apple puede, mientras que los puntos de acceso de Linksys no.

Nota *Adam solucionó esta limitación de su punto de acceso Linksys conectando su LaserWriter a un viejo Performa 6400 que ejecutaba el servidor de impresoras AppleShare IP (ésta no es una solución para los de corazón débil). Ahora puede imprimir en el servidor de impresora AppleShare IP utilizando TCP/IP (hay que usar la utilidad de impresora de escritorio en Mac OS 9 o crear una impresora utilizando Impresión IP en la utilidad Centro de impresión de Mac OS X); el Performa pasa*

entonces la tarea de impresión a la LaserWriter a través de AppleTalk. Es sorprendente que funcione, pero la ventaja añadida es que las tareas de impresión pueden esperar en el servidor hasta que Adam enciende la impresora, aunque sea días después.

Aplicación de redes

Ascendiendo un nivel en el esquema, necesitamos programas que hablen a través de las redes intercambiando información. En otro caso, ¿por qué molestarse para tener una red? Es probable que ya esté familiarizado con muchos de los protocolos en esta categoría en el mundo TCP/IP o, al menos, con las aplicaciones que los implementan.

DNS

Todo ordenador de Internet debe tener una dirección IP unívoca que lo identifique. Pero las direcciones IP, como 216.168.61.154, no resultan fáciles de recordar o escribir para los humanos, de modo que se desarrolló el sistema de nombres de dominio (DNS) para convertir los nombres legibles para los humanos, como www.tidbits.com, en sus direcciones IP asociadas. Si visita www.tidbits.com con su navegador Web, éste pregunta a un servidor DNS qué dirección IP lleva a www.tidbits.com.

El servidor DNS comprueba si ya conoce la dirección IP de www.tidbits.com; si no es el caso, consulta a otros servidores DNS hasta que encuentra la dirección IP apropiada. Entonces, el servidor DNS devuelve la dirección IP, 216.168.61.154, al navegador Web, que procede a hacer la conexión con el servidor www.tidbits.com.

DNS puede ser un problema en cualquier red que utilice DHCP y NAT para convertir las direcciones internas privadas en una sola dirección IP externa. Muchos proveedores de servicios de Internet ofrecen direcciones IP dinámicas que pueden cambiar de un día a otro; esta estrategia impide que los servidores DNS de Internet conozcan nuestra dirección IP, evitando así que otras personas puedan conectar directamente con nuestro ordenador. Afortunadamente, hay un atajo que permite a la gente conectar con nuestro ordenador incluso aunque tengamos una dirección IP dinámica. Un servicio llamado DNS dinámico nos permite asignar un nombre de host que no cambia a la dirección IP actual que tengamos, sea cual sea. Hablaremos más de DNS dinámico en el capítulo 5.

Puertos en la tormenta

En este capítulo, hemos hablado de las distintas formas de asignar direcciones (direcciones MAC Ethernet y direcciones IP). Pero ¿cómo distingue un ordenador los tipos de datos que entran? ¿Qué diferencia a un mensaje de correo electrónico de una página Web y de un mensaje instantáneo? En una palabra: los puertos, y en este caso no estamos hablando de las conexiones físicas del ordenador.

Volviendo a nuestra analogía ferroviaria, si imaginamos el ordenador como estación de tren, el puerto es el andén de carga en la estación que acepta un solo tipo de mercancías. Los alimentos perecederos van a un andén de carga, la maquinaria pesada a otro, etc. Análogamente, cada servicio de Internet identifica el ordenador de destino, y el número de puerto identifica el tipo de datos que se está enviando a ese ordenador.

Muchos números de puertos han sido asignados desde hace tiempo (y se conocen como puertos "bien conocidos"), de modo que, por ejemplo, SMTP utiliza el puerto 25, DNS utiliza el puerto 53, la Web utiliza el 80, etc. Sin embargo, nada impide que se ejecute un servidor en un puerto que no se usa para otras cosas y a veces veremos servidores Web que se ejecutan en el puerto 8080. Y algunos protocolos, como FTP, deben iniciarse en un puerto para cambiar a otro puerto no utilizado una vez establecida la conexión.

Hay que conocer tres factores principales acerca de los puertos:

- *Si un sitio Web que queremos visitar está ejecutándose en un número de puerto inusual, hay que incorporarlo al URL que enviemos a otras persona o usemos en páginas Web, como en http://www.example.com:8080/index.html. El número de puerto viene después del nombre de dominio precedido por el signo de dos puntos.*
- *Los cortafuegos suelen funcionar permitiendo que el tráfico pase a sólo algunos puertos concretos. Si intentamos utilizar una aplicación que requiere un puerto cerrado por el cortafuegos, esa aplicación no funcionará.*
- *Ejecutar servidores detrás de una puerta de enlace NAT puede ser problemático, pues las puertas de enlace NAT no saben a dónde dirigir las solicitudes entrantes. Una técnica llamada asignación de puertas ayuda a solucionar el problema. En la puerta*

de enlace NAT, decimos simplemente que todo el tráfico del puerto 80, por ejemplo, debe ser dirigido a un ordenador interno que está ejecutando un servidor Web. Sin esta asignación de puertos, la máquina que actúa como puerta de enlace NAT supondría, incorrectamente, que ella era el propio destino.

FTP

FTP (Protocolo de transferencia de archivos) es un modo cada vez más chirriante de obtener o cargar archivos en un servidor remoto. FTP se utiliza más comúnmente en conjunción con servidores Web, en los que cargamos los archivos HTML que constituyen un sitio Web a través de FTP.

FTP es uno de los primeros protocolos de Internet y tiene un comportamiento que puede provocar problemas si se utiliza desde detrás de una puerta de enlace NAT y un cortafuegos. Cuando iniciamos una sesión FTP normal, el servidor FTP responde a un puerto arbitrario para iniciar la transacción. A menos que el cortafuegos y la puerta de enlace NAT estén configurados para permitir el acceso entrante a cualquier puerto antiguo, la conexión será bloqueada. Afortunadamente, muchos clientes FTP y la mayoría de los servidores prestan soporte a una opción llamada FTP pasivo. FTP pasivo inicia una conexión desde el puerto bien conocido 21, que está reservado para FTP, y el servidor responde a través del mismo puerto.

SMTP, POP e IMAP

Estos tres protocolos se utilizan para enviar y recibir correo electrónico. El correo que enviamos utiliza SMTP (Protocolo simple de transferencia de correo), mientras que recibimos el correo electrónico entrante a través de POP (Protocolo de oficina de correo) o IMAP (Protocolo de acceso de mensajes de Internet). En su mayor parte, no hay nada inusual en cómo interactúan estos protocolos con las redes convencionales e inalámbricas.

HTTP

El protocolo de aplicaciones más común que se utiliza en Internet actualmente es http (Protocolo de transferencia de hipertexto). Empezó como el lenguaje básico de la Web, aunque ahora se utiliza para muchas otras funciones, incluyendo el servicio de archivos WebDAV (Creación y control de versiones distribuidas en Web).

Contraseñas en la corriente

FTP envía sus contraseñas como texto simple, algo preocupante ya que un fisgón de la red que consiga robar la contraseña observando el tráfico FTP puede utilizarla para iniciar una sesión en una cuenta de terminal en la misma máquina o cargar nuevos archivos en el sitio Web.

Por defecto, POP e IMAP también transmiten sus contraseñas sin cifrarlas, que significa que alguien podría leer nuestro correo electrónico. Eso puede no sonar muy amenazador, pero dado que muchos servicios de Internet mantienen la seguridad enviando un mensaje de correo de confirmación y pidiendo que hagamos clic en un enlace de ese mensaje, permitir que sea posible que un fisgón lea nuestro correo eléctrónico puede originar muchos otros problemas.

Vea el capítulo 6 para encontrar consejos para evaluar el riesgo real y varias soluciones a estos problemas.

De los cables a lo inalámbrico

Si ha leído todo el capítulo, se habrá hecho una idea de lo básico de las redes y ese conocimiento le servirá en el futuro, pues podrá aplicarlo no sólo a las redes convencionales, sino también a las inalámbricas. Abundando en lo mismo, las redes inalámbricas amplían estos asuntos básicos de las redes con nuevos conceptos y protocolos que veremos a continuación.

3. Cómo funciona lo inalámbrico

El telégrafo inalámbrico no es difícil de entender. El telégrafo normal es como un gato muy largo. Tiras de su cola en New York y maúlla en Los Ángeles. El inalámbrico es igual, pero sin gato.

- Atribuido a Albert Einstein.

Ya fuera o no Einstein el que dijo esto, es acertado: la transmisión inalámbrica no es intuitiva, tenemos que usar analogías para comprender cómo va la información de un sitio a otro sin elementos físicos visibles que marquen un camino. Afortunadamente para nosotros, lo inalámbrico funciona: no hay más que pensar en los teléfonos inalámbricos, los móviles, la radio AM y FM, los *walkie-talkies* y las antenas de televisión por satélite. Lo inalámbrico está absolutamente presente en nuestra vida actual e, intuitivo o no, sus raíces están en la física básica.

Las redes inalámbricas utilizan los mismos principios que rigen los teléfonos inalámbricos y todos los demás aparatos sin cables. Un transceptor (combinación de transmisor y receptor) envía señales emitiendo ondas de radiación electromagnética desde una antena; la misma antena recibe señales al vibrar los electrones por efecto de las ondas que pasan con las frecuencias apropiadas.

En este capítulo, explicaremos cómo funciona la transmisión inalámbrica y cómo intercambian datos las redes inalámbricas. Veremos los tipos de redes inalámbricas más utilizados, dedicando más atención al estándar 802.11b, también conocido por los usuarios de Mac como AirPort.

Señales que atraviesan las paredes

Lo mágico de las redes inalámbricas no es sólo que funcionen sin cables, sino también funcionan cuando ni siquiera podamos ver el punto de acceso al que estamos conectando. Aunque ahora tomamos con normalidad la conexión a través de una vía obstruida, no siempre fue así.

Las primeras redes inalámbricas utilizaban frecuencias de radiación electromagnética más bajas, justo por debajo del espectro visible, concretamente la radiación infrarroja. Las redes infrarrojas tenían (y siguen teniendo) una fuerte limitación: se necesitaba una línea libre de visión entre un transceptor infrarrojo y otro. En oficinas grandes con muchos cubículos, era difícil colocar los transceptores lo suficiente altos para que las señales pasaran sobre los paneles de separación e igualmente difícil garantizar que la gente que paseaba de un sitio a otro no bloqueara la señal de la red.

Aunque la radiación infrarroja sigue utilizándose hoy en las agendas electrónicas basadas en Palm OS, aparatos PocketPC y algunos teléfonos móviles, su uso está reservado para conexiones *ad hoc* cortas especiales. Por ejemplo, se puede configurar una conexión ad hoc para transferir algunos archivos entre dos ordenadores portátiles. Las conexiones ad hoc requieren una gran proximidad e, igual que las antiguas redes inalámbricas, una línea de visión libre entre los dos transceptores.

Espectro sin licencia

Las bandas de frecuencia de 900 megahercios (MHz), 2,4 GHz y ciertas partes de 5 GHz están reservadas en los EE.UU. y en muchos otros países para uso sin licencia. Hay dos tipos de licencias: las que son propiedad de empresas que operan con equipamiento en varias frecuencias (como las compañías de teléfonos móviles) y las que utilizan esos equipamientos (como los aparatos de radioaficionados). Estas bandas no requieren licencia de ningún tipo. Sin embargo, el

equipamiento que utiliza estas bandas debe estar en los EE.UU. certificado por la FCC (Federal Communications Commission) y los cuerpos reguladores nacionales.
Dado que no es necesaria una licencia, los aparatos sin licencia utilizan muy poca potencia, limitando su alcance. También significa que los aparatos deben ser muy resistentes a las interferencias, porque no hay garantía de que un usuario tenga acceso exclusivo a cualquiera de las frecuencias sin licencia. Desgraciadamente, las interferencias siguen presentes si se utiliza un teléfono inalámbrico de 2,4 GHz o un horno microondas (que puede producir radiación de 2,4 GHz al hacer vibrar moléculas de agua) cerca de un punto de acceso.
La banda de 2,4 GHz tiene algunos usos con licencia que se solapan con el rango sin licencia, incluyendo las radios de aficionados en la parte baja y ciertas señales remotas de estaciones de televisión y transmisiones comerciales de microondas. Estos usuarios con licencia tienen prioridad, pero, hasta ahora, el uso de baja potencia de las redes inalámbricas no ha provocado ninguna disputa por el territorio.

Las redes inalámbricas superan el problema de la línea de visión saltando a una frecuencia más alta en el espectro electromagnético. Las redes inalámbricas modernas suelen funcionar a 2,4 gigahercios (GHz) o incluso mayor frecuencia, muy, muy por debajo del espectro de la luz visible (vea la figura 3.1). A esa frecuencia, la longitud de onda de las transmisiones es tan pequeña que puede atravesar objetos aparentemente sólidos.

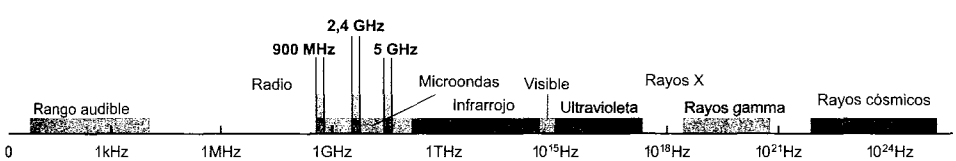

Figura 3.1. *El espectro electromagnético.*

Nota

No queremos entrar demasiado en la física involucrada, pero los objetos sólidos no son realmente sólidos: hay mucho espacio vacío entre los átomos, incluso dentro de ellos, que constituyen todo lo que consideramos sólido. Es decir, aunque la radiación de frecuencias relativamente bajas como la luz visible no puede atravesar los objetos sólidos, las ondas de frecuencias más altas sí puede penetrar en estos pequeños espacios entre los átomos.

Aunque las redes inalámbricas modernas ofrecen el alcance más alto cuando hay una línea de visión, también funcionan perfectamente a distancias cortas en espacios interiores (vea la figura 3.2). Algunos obstáculos de interior pueden reducir la calidad de la señal y hacer necesarios ajustar la disposición de la red. Por ejemplo, los muros de ladrillo pueden alojar mucha agua y el agua absorbe energía de las frecuencias a las que funcionan las redes de 2,4 GHz. Algunas casas y oficinas tienen metal en su interior, como las mallas de alambres que sujetan los techos de escayola o las tuberías, y el metal puede interferir también con las señales de la red.

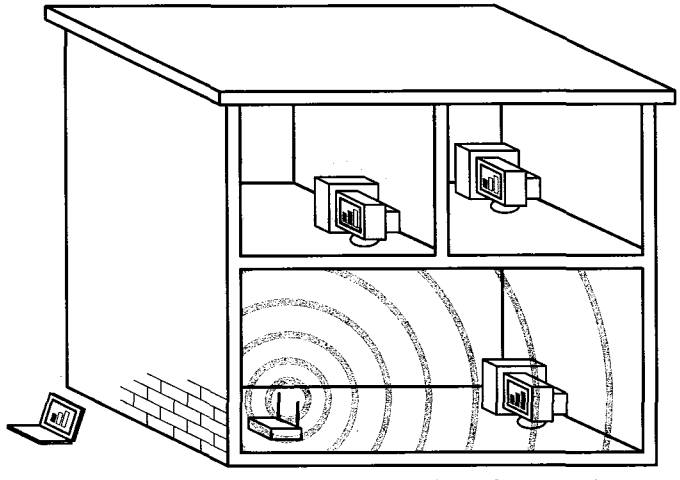

Figura 3.2. *Cómo viajan las ondas de radio por el espacio.*

Añadir datos a las ondas de radio

Utilizar una parte del espectro que puede atravesar los objetos sólidos fue un paso importante, pero hay otro aspecto de las redes inalámbricas de la misma importancia: cómo se transmiten en realidad los datos a través de las ondas de radio y cómo los clasifica el receptor. En la práctica, esta información sólo tiene valor como tal: no tenemos elección sobre qué estándar utilizan las piezas del equipamiento de red inalámbrica.

La transferencia de datos por medios inalámbricos puede emplear uno de los distintos estándares que comentaremos más adelante en este capítulo. Pero algo que todos los estándares inalámbricos tienen en común es su capacidad de ordenar señales de datos que se solapan. En áreas de mucha población, como una calle urbana llena de cafeterías o una oficina llena de gente, varias o inclu-

so varias docenas de aparatos pueden estar enviando señales al mismo tiempo utilizando un grupo de frecuencias. Los dispositivos inalámbricos utilizan una de dos estrategias distintas para hacer frente a este solapamiento de las señales: espectro extendido con salto de frecuencias (a menudo abreviado en sus siglas inglesas FHSS o simplemente FH) o espectro extendido de secuencia directa (abreviado como DSSS o DS). Con espectro extendido con salto de frecuencias, las frecuencias de las ondas sobre las que se transmiten los datos cambian muy rápidamente. En un estándar, las frecuencias cambian 1.600 veces por segundo. En otros, la tasa de cambios es más lenta. Pero todos los estándares de salto de frecuencias tienen muchos patrones de salto para que redes o grupos distintos que utilicen el mismo estándar en el mismo lugar tengan poca probabilidad de utilizar las mismas frecuencias al mismo tiempo.

Por el contrario, espectro extendido de secuencia directa divide una franja de ancho de banda en canales separados y nunca transmite durante mucho tiempo en una frecuencia del canal. Utilizando canales distintos en la misma zona, muchas redes distintas pueden solaparse sin que las señales de unas y otras se interfieran. Ambas formas de transmisión de espectro extendido son resistentes a las interferencias, pues no hay una sola frecuencia en uso constante, y el salto de frecuencias también puede ser resistente a los fisgones, pues los patrones de salto pueden evitar todos los analizadores de espectro excepto los de gama industrial y militar.

Nota

FHSS fue inventado y patentado por la actriz Hedy Lamarr (en colaboración con el compositor George Antheil) en 1942 y guardado en secreto (sin utilizarlo) por el gobierno de los EE.UU. durante la 2ª Guerra Mundial; Lamarr y Antheil nunca recibieron un centavo por la patente. La contribución de Lamarr fue "redescubierta" cuando el espectro extendido se convirtió en la base de las telecomunicaciones inalámbricas modernas. Cuando la Electronic Frontier Foundation le otorgó un Pioneer Award en 1997, se comenta que la actriz señaló desde su hogar en Florida: "Ya era hora". Murió en enero del 2000, justo antes del gran momento de Wi-Fi.

Hardware inalámbrico

En el nivel básico, se necesitan dos piezas de hardware para cualquier red inalámbrica: un punto de acceso central y un adaptador de red (vea la figura 3.3). Los puntos de acceso suelen ser dispositivos independientes. Por el con-

trario, las tarjetas de red se suelen instalar dentro de un ordenador con todos los métodos estándar que se pueden esperar, bahías PC Card, ranuras PCI y ranuras adaptadas, y algunos menos usuales, como tarjetas CompactFlash y Secure Digital. Para ordenadores que no admiten estas opciones internas, hay disponibles adaptadores externos que se conectan a puertos USB o Ethernet. Por último, aunque tanto los puntos de acceso como las tarjetas de red tienen antenas integradas, hay antenas externas que pueden ampliar el alcance de ciertas redes.

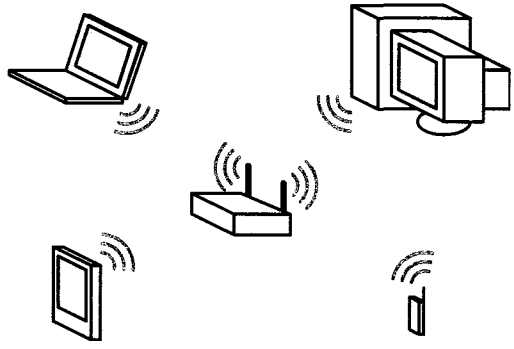

Figura 3.3. *Una red inalámbrica típica con distintos aparatos.*

Nota *Los puntos de acceso no tienen por qué ser piezas de hardware independientes, aunque a menudo lo son. Hay software tanto para Macintosh como para Windows que puede convertir un ordenador Mac o un PC con una tarjeta de red inalámbrica en un punto de acceso de software, sin impedir que también actúe como servidor normal o se ocupe de sus tareas de escritorio. La principal ventaja de un punto de acceso de software es que no es necesario comprar un aparato independiente; el principal inconveniente es que no hay un aparato independiente que pueda estar encendido todo el tiempo, que es improbable que se bloquee o que haya que reiniciar. Hablaremos de la configuración de puntos de acceso de software en el capítulo 5.*

Veamos las piezas de hardware individuales necesarias para las redes inalámbricas.

Puntos de acceso

Un punto de acceso es el cerebro de una red inalámbrica (vea la figura 3.4). Puede efectuar varias tareas distintas, algunas de las cuales son optativas,

dependiendo de lo que queramos que haga el punto de acceso. Desgraciadamente, es más que probable encontrar términos distintos como denominación de los puntos de acceso, incluyendo Puerta de enlace inalámbrica o Estación Base. Además, el término se abrevia como AP en la literatura técnica. Aquí nos atendremos a "punto de acceso" al hablar de dispositivos que tengan las características enumeradas a continuación.

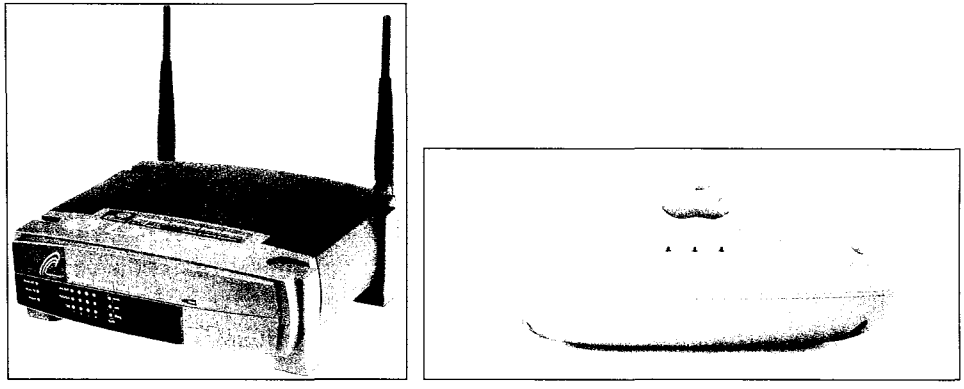

Figura 3.4. *Punto de acceso inalámbrico Linksys EtherFast con enrutador de cable o DSL y conmutador de 4 puertos (izquierda) y Estación Base AirPort de Apple.*

Lo más importante, el punto de acceso contiene uno o más transceptores inalámbricos que envían y reciben datos de ordenadores con equipamiento inalámbrico y otros dispositivos. La conexión entre un punto de acceso y un ordenador con una tarjeta de red inalámbrica se llama una *asociación cliente*.

Otra tarea común para un punto de acceso es actuar como puente de red que conecta los ordenadores de una red inalámbrica con los de una red convencional. Hemos visto el funcionamiento de los puentes en el capítulo 2, pero, en esencia, sólo hace falta conectar un cable Ethernet de una red convencional con el punto de acceso para enlazar dos redes de área local (LAN).

Dado que compartir una conexión de Internet entre varios ordenadores es el uso principal de la mayoría de las redes inalámbricas pequeñas, no es inesperado que un punto de acceso ofrezca un puerto Ethernet o un módem interno estándar para facilitar la conexión de la red inalámbrica a una conexión de Internet por cable o de acceso telefónico. Un módem de cable o una conexión de Internet DSL se conectan al puerto Ethernet; en una conexión de Internet de acceso telefónico, se conecta una línea de teléfono al módem.

De cualquier forma, cuando está conectado a Internet, el punto de acceso actúa también como puerta de enlace, conectando una LAN con una red de

área extensa (WAN), como es Internet. Los puntos de acceso puerta de enlace a menudo tienen varios puertos Ethernet para este propósito, otro para la WAN para hacer la conexión con Internet y hasta cuatro puertos Ethernet adicionales para ordenadores o impresoras conectados con cable de la LAN.

Cuando actúa como puerta de enlace, un punto de acceso a menudo ofrece otros servicios de red como asignación automática de una dirección Internet, creación de direcciones privadas para ordenadores locales inalcanzables desde el exterior, filtrado del tráfico como cortafuegos y control de qué clientes pueden estar asociados.

Las puertas de enlace pueden a menudo limitar el tráfico independientemente en el puerto WAN frente a los puertos LAN, proporcionando a los usuarios de la red local más privilegios que a los usuarios que acceden a la red desde Internet.

Los puntos de acceso también gestionan la seguridad. Pueden restringir el acceso basándose en un identificador integrado en el cliente inalámbrico o pasar información a otro hardware y software de la red para autenticar a un usuario en organizaciones más grandes. Los puntos de acceso también habilitan una forma simple de cifrado, útil sólo para usuarios particulares, que mezcla los datos entre el cliente y el punto de acceso.

Algunos puntos de acceso contienen funciones avanzadas, como el enrutamiento (utilizado en instalaciones de red que dividen las redes en fragmentos más pequeños), el clonado de direcciones Ethernet (para modificar el identificador de red unívoco del punto de acceso, algo útil cuando compartimos una conexión de módem por cable) y soporte a cifrado avanzado para Redes privadas virtuales (VPN) y otros sistemas. Que necesite o no alguna de estas funciones avanzadas dependerá completamente de su caso particular.

Nota *Para una red inalámbrica simple que vincule sólo unos pocos ordenadores, no será estrictamente necesario usar un punto de acceso. Una red creada por dos tarjetas de red inalámbrica que hablan entre sí (normalmente durante periodos cortos) se conoce como red ad hoc porque no precisa la coordinación de un punto de acceso fijo. En el capítulo 4 veremos detalles sobre la configuración de una red ad hoc.*

Adaptadores de red inalámbrica

La segunda pieza de hardware necesaria en cualquier red inalámbrica es una tarjeta de red inalámbrica. Igual que en los puntos de acceso, podemos

encontrar distintos nombres que designan estos dispositivos. Por ejemplo, Apple llama a su tarjeta de red inalámbrica "tarjeta AirPort" y otros fabricantes utilizan otros nombres. Como estas tarjetas se instalan en ordenadores que son clientes del punto de acceso, a menudo encontramos el término "cliente" añadido al nombre del software que controla el adaptador.

Nota

El cliente es una de las partes de una pareja, el servidor es la otra. Un servidor se configura para gestionar las solicitudes de muchas máquinas o usuarios distintos; los clientes hablan con el servidor para cada tarea. En las redes inalámbricas, el punto de acceso es en la práctica un servidor, aunque casi nunca se le da ese nombre.

Los adaptadores de red inalámbrica pueden tener distintas formas y tamaños y, aunque la siguiente lista puede parecer intimidante, puede usar la tabla 3.1 para escoger el tipo más apropiado.

Tabla 3.1. *Escoger la tarjeta de red inalámbrica más apropiada.*

	PC Card	PCI	USB	Ethernet	Compact Flash	Secure Digital	Tarjeta AirPort
PC de mesa		●P	●1	●2			
PC portátil	●P		●1	●2			
Power Macs anteriores a AirPort		●P	●1	●2			
iMacs sólo con USB			●P	●			
iMacs FireWire			●	●			●P
PowerBook G3	●P		●1	●			
iBooks Apple			●	●			●P
PowerBooks Titanium o sólo FireWire	●		●	●			●P
Ordenadores de bolsillo PocketPC	●3				●3		
Ordenadores de bolsillo Palm						●4	

P Adaptador preferido.
1 Para ordenadores con USB integrado o añadido.
2 Para ordenadores con Ethernet integrada o añadida.
3 Puede requerir adaptador dependiendo del modelo de PocketPC.
4 Ciertos Palm de bolsillo recientes tienen una ranura SDIO.

Tarjetas inalámbricas internas

La mejor opción, si está disponible para un ordenador cliente, es a menudo una tarjeta de red inalámbrica interna. Son más baratas y menos prominentes que los adaptadores externos. El único inconveniente de las tarjetas de red internas es que pueden ser más difíciles de instalar y, a menos que esté diseñada correctamente, la carcasa del ordenador puede bloquear algo la señal de la red, reduciendo su alcance.

- **PC Cards:** La familiar ranura PC Card se encuentra generalmente sólo en los portátiles. Como los portátiles son ideales para utilizarlos en redes inalámbricas, hay disponibles muchas tarjetas de red inalámbrica y sólo a veces en la forma de PC Card. La mayoría de las PC Cards inalámbricas tienen antenas integradas o que sobresalen y, aunque suelen ser pequeñas, a menudo se extienden fuera del cuerpo del portátil.

Nota *Las PC Cards recibían antes el nombre de tarjetas PCMCIA. PCMCIA son las iniciales inglesas de Asociación internacional de tarjeta de memoria de ordenador personal, a pesar de que a veces se ha dicho jocosamente que correspondían a "La gente no puede memorizar los acrónimos de la industria informática" (People Can't Memorize Computer Industry Acronyms).*

- **Tarjeta PCI:** La mayoría de los ordenadores de mesa actuales tienen ranuras PCI para tarjetas de expansión y hay algunas tarjetas de red inalámbrica basadas en PCI. Algunas tarjetas PCI tienen antenas externas; otras tienen adaptadores para conectar antenas de mayor potencia. Algunos otros fabricantes, como Proxim, utilizan la tarjeta PCI como soporte de una PC Card; esta combinación a menudo provoca extraños problemas con los controladores cuando un software intenta ocuparse de la tarjeta PCI que aloja la PC Card y otro software intenta controlar la propia PC Card.
- **Tarjetas mini PCI:** Ciertos modelos de portátil, como el Dell TrueMobile 1150, utilizan una tarjeta interna de expansión todavía más pequeña llamada tarjeta mini PCI. La mayoría de las ranuras mini PCI también tienen una conexión de antena interna.
- **Ranuras adaptadas:** Los modelos recientes de portátiles Compaq tienen una ranura especial multipuerto (*MultiPort*) que admite adaptadores de red inalámbrica. Desde 1999, Apple ha incorporado en cada modelo

del Macintosh conectores internos que aceptan una PC Card modificada, que Apple llama una tarjeta AirPort. Y al menos una firma, la división Xircom de Intel, fabrica un adaptador inalámbrico de presión para la ranura de expansión Springboard de la parte trasera de ciertos aparatos basados en Palm OS de Handspring.

Nota

Una tarjeta que encaja en un conector AirPort o MultiPort se conecta a una antena incorporada en la carcasa del propio ordenador portátil o de mesa. Dado que estas antenas pueden normalmente ser más grandes y estar diseñadas para mejorar su integración, ofrecen un alcance de la recepción significativamente mejor. Sin embargo, el Titanium PowerBook G4 de Apple tiene una carcasa tan blindada electromagnéticamente que reduce a la mitad el alcance de red inalámbrica en ese ordenador. Para sortear esta limitación, algunos usuarios utilizan una PC Card o un adaptador USB que lleva la antena al exterior de la carcasa. Las versiones más recientes del Titanium han mejorado el alcance de red inalámbrica de una tarjeta AirPort interna, pero sigue siendo poco.

- **Tarjeta CompactFlash:** Muchos ordenadores de bolsillo y aparatos digitales, como agendas electrónicas PocketPC, cámaras y reproductores de MP3, utilizan tarjetas CompactFlash para almacenamiento. Varios fabricantes van a lanzar pronto una variedad de adaptadores inalámbricos CompactFlash, aunque no todo el equipamiento con ranuras CompactFlash tiene incorporado software adecuado para gestionar el trabajo en red. Es más probable que sean aparatos futuros los que empiecen a aprovechar las tarjetas de red inalámbrica basadas en CompactFlash.
- **Tarjeta Secure Digital IO:** Varios ordenadores de bolsillo, incluyendo agendas electrónicas de Palm, aceptan pequeñas tarjetas Secure Digital IO (SDIO).

Adaptadores inalámbricos externos

Algunos ordenadores, como los iMac y Power Mac anteriores al lanzamiento del hardware AirPort de Apple, deben usar un adaptador inalámbrico externo porque simplemente no tienen dónde colocar una tarjeta inalámbrica interna. Los adaptadores inalámbricos externos pueden ser también útiles para algunas máquinas modernas si, por ejemplo, todas las ranuras PC Card de un ordenador están ocupadas o el ordenador requiere varias tarjetas inalámbricas.

Aunque encontrar un adaptador externo resultaba complicado en el pasado, hoy día es relativamente fácil encontrar uno que funcione en un ordenador dado. Igual que con algunas tarjetas PCI, los adaptadores inalámbricos externos a veces funcionan con una PC Card del mismo fabricante.

Nota *Es posible instalar un adaptador PCI inalámbrico en algunos Power Mac viejos, pero el software que le presta soporte puede no existir ya.*

- **Adaptadores USB:** El puerto USB, que a menudo se utiliza para conectar teclados, ratones e impresoras, también puede admitir adaptadores inalámbricos externos. No hay que preocuparse por una posible reducción del rendimiento, pues el estándar USB 1.1 va a 12 Mbps, ligeramente más rápido que el rendimiento máximo de 11 Mbps de las redes 802.11b.
- **Adaptadores Ethernet:** Algún equipamiento electrónico moderno del hogar, como la grabadora de vídeo digital ReplayTV y la Xbox de Microsoft, y algunos ordenadores algo antiguos tienen sólo un puerto Ethernet o no pueden aceptar controladores de software que gestionen las redes inalámbricas. En esos casos, se utilizará un adaptador inalámbrico que se conecte directamente al puerto Ethernet del aparato. Algunos adaptadores Ethernet pueden conectar con una red de aparatos Ethernet con cables y transferir todo el tráfico a/y desde una red inalámbrica a través del punto de acceso; uno de tales adaptadores puede ocuparse de hasta 30 ordenadores y otras piezas de equipamiento y conectarlos a un punto de acceso.

Antenas

Todos los puntos de acceso y tarjetas inalámbricas tienen antenas que están conectadas con ellos o integradas. Sin embargo, dado el tamaño de estos dispositivos, especialmente las diminutas tarjetas inalámbricas, hay un límite al alcance que proporcionan estas antenas integradas en los aparatos. Para un mayor alcance, se necesita una antena externa.

En los términos más simples, una antena aumenta la potencia de un transceptor. Un transceptor combina un transmisor y un receptor, de modo que, enfocando mejor la energía electromagnética que entra o sale, la antena aumenta tanto la fuerza de la señal transmitida como la sensibilidad de la recepción. La potencia de una antena se expresa en decibelios, o dB, y cada

antena tiene un rango de potencias en decibelios, generalmente conocido como ganancia. Los decibelios aumentan en escala logarítmica: un pequeño aumento de los decibelios provoca un gran aumento de la sensibilidad.

Nota

No es necesariamente cierto que cuanto más larga o grande la antena, mejor la señal. La forma, composición y varios otros factores se combinan para determinar la ganancia. Las antenas de mayor ganancia, por ejemplo, también enfocan su energía en estrechos haces adecuados sólo para intercambios punto a punto. Vea el capítulo 8 para más detalles sobre las antenas.

Usos de las antenas

Añadiendo una antena externa a un dispositivo de red inalámbrica, podemos ampliar el alcance del dispositivos desde cientos de metros a miles de metros o incluso decenas de kilómetros. Hay dos razones principales para querer ampliar el alcance de la red.

Primera, y más probable, si tenemos problemas para recibir la señal de la red inalámbrica en ciertas zonas de la casa u oficina, una pequeña antena omnidireccional podría aumentar lo suficiente la potencia para atravesar el obstáculo. (Si eso no funciona, añadir un segundo punto de acceso puede solucionar el problema con un poco más de trabajo y un pequeño coste adicional.)

Segunda, si queremos establecer una conexión inalámbrica punto a punto de largo alcance, es indispensable una antena que seguramente será bastante grande. Las conexiones punto a punto generalmente utilizan antenas parabólicas que emplean señales relativamente estrechas; cuanto mayor deba ser el alcance, más enfocada deberá estar la señal. En el capítulo 9 hablaremos de cómo utilizar globos, dispositivos GPS y otras herramientas para crear enlaces punto a punto a larga distancia.

Conectar una antena

Algunos dispositivos de red inalámbrica, como los de la línea Proxim Orinoco, incluyen conexiones de antena estándar. En estos casos, cada aparato ofrece una toma estándar en la que podemos conectar un adaptador de cable que a su vez se conecta a un cable de antena coaxial. La línea de equipamiento Linksys también ofrece un conector estándar, que algunos fabricantes de terceras partes ofrecen como opción de equipamiento fabricado a la medida.

Añadir una antena a veces requiere un esfuerzo especial. Si abrimos una Estación Base AirPort de Apple y taladramos un agujero en su carcasa de plástico, podemos añadir una antena externa, pero no es una solución para los de corazón débil, además ya existen modelos con conectores para antenas exteriores. Si todavía no ha comprado hardware de red inalámbrica y piensa que quizá quiera usar una antena externa, compruebe que añade esa característica a su lista cuando compare distintos dispositivos.

Antenas legales

Todas las redes inalámbricas sin licencia están sujetas a estrictas limitaciones de potencia creadas para prevenir la interferencia innecesaria entre dispositivos y evitar producir interferencias a los usuarios que sí tienen licencia en la misma banda.
En rigor, las antenas y transceptores están aprobados por la FCC y los cuerpos de regulación sólo como sistemas completos: cada antena y cada sistema se prueban y aprueban juntos para garantizar que no emiten más potencia de la que permiten las reglas y están ajustados a otras limitaciones. Algunas zonas del mundo son más estrictas que otras sobre la imposición de estas regulaciones.
Sin embargo, muchas piezas de equipamiento inalámbrico tienen tomas o conectores que permiten añadir antenas de otros fabricantes o incluso antenas caseras, como las desarrolladas por grupos comunitarios de redes inalámbricas. Estas antenas son, desgraciadamente, ilegales en la mayoría de los casos, aunque no habrá problemas a no ser que emita con tanta potencia o de tal forma que lo noten otras personas. Aquí hay una fina línea que no se debe cruzar y, aunque las reglas son claras, es difícil para las personas saber cómo actuar dentro de ellas sin ser expertos en antenas o especialistas legales de la FCC.
¿Nuestro consejo? La mayoría de los dispositivos que puede comprar y las antenas que los acompañan están dentro de las reglas de potencia de salida y no violarán el espíritu de la ley. Naturalmente, no es que recomendemos violar la letra de la ley, pero si sigue el sentido común no tendrá problemas.

Fidelidad inalámbrica

Hablando ahora de estándares de red inalámbrica, sólo hay un estándar que es probable que encuentre (o que quiera usar en la mayoría de los casos): el

IEEE 802.11b, conocido más familiarmente con su nombre de marca, Wi-Fi. Wi-Fi (Fidelidad Inalámbrica, *Wireless Fidelity*) desde finales de 2002, engloba el estándar 802.11b y otro estándar más rápido llamado 802.11a. Los usuarios de Macintosh conocen el 802.11b por el nombre que Apple ha dado a su tecnología: AirPort.

El estándar 802.11b se ha convertido en la tecnología de red inalámbrica dominante porque, en el espacio de unos años, se han vendido decenas de millones de tarjetas y puntos de acceso 802.11b y se han escrito miles de artículos sobre él. No intentamos separar ganadores y perdedores, pero sabemos que el 802.11b es el único estándar inalámbrico que se utiliza ampliamente, es fácil de configurar y no tiene costes de espectro o contador (a diferencia del servicio celular o algunas formas corporativas de trabajo avanzado en red inalámbrica).

Nota

El estándar 802.11b tiene competidores y estándares complementarios (y extensiones, y veremos más sobre ellos un poco más adelante en este capítulo), pero el 802.11b es la única red inalámbrica que encontrará en oficinas, espacios públicos y hogares. La mayoría de los otros estándares se encuentran actualmente en sólo uno de esos lugares e, incluso así, no se acerca a la penetración y amplia disponibilidad del 802.11b.

Ya se llamen Wi-Fi, 802.11b o AirPort, los aparatos que incorporan la tecnología colaboran entre sí, de modo que cualquier equipamiento que compre con alguno de esos nombres funcionará casi siempre con otro equipamiento identificado de forma similar. El hardware etiquetado Wi-Fi con un sello siempre colabora con otro equipamiento Wi-Fi en las bandas indicadas. Y sí, para los usuarios de Macintosh, AirPort de Apple tiene el sello Wi-Fi.

Funcionamiento de 802.11b

802.11b utiliza espectro extendido de secuencia directa para transmitir y recibir datos a 11 megabits por segundo (Mbps). Pero no deje que ese número le engañe. Esos 11 Mbps incluyen la carga de red del inicio y final de los paquetes, para sincronizar las transmisiones, y otros complejos detalles. La velocidad real es teóricamente de 7 Mbps, cercana a la velocidad real de Ethernet 10BaseT (cuya velocidad nominal es 10 Mbps), pero la mayoría de los usuarios obtienen entre 4 y 5 Mbps como máximo debido a las limitaciones del hardware barato y la congestión de señales en la mayoría de las redes.

802.11b admite cinco velocidades, empezando por la más rápida que va disminuyendo si las interferencias o la debilidad de la señal impiden que los datos lleguen a su destino. Las cinco velocidades son 11 Mbps, 5,5 Mbps, 2 Mbps, 1 Mbps y 512 Kbps (kilobits por segundo).

El IEEE

El IEEE (Instituto de Ingenieros en Electricidad y Electrónica) es una asociación profesional técnica sin ánimo de lucro con 377.000 miembros que desarrollan por consenso estándares técnicos para la electrónica en diversos campos. Mucho de los fabricantes de equipamiento 802.11b están implicados en subcomités del IEEE.
El comité IEEE 802 se ocupa de las redes; el grupo de trabajo 802.11 se ocupa de las redes de área local inalámbricas (WLAN); y los distintos grupos de tareas (a, b, e, g, h, e i, entre otros que comentamos) se ocupan de tipos concretos de WLAN o de problemas específicos, como los datos multimedia fluidos, la comunicación entre puntos de acceso y la seguridad.

Nota *Las tres velocidades más bajas son en realidad parte del protocolo 802.11 original, anterior al 802.11b. Algunos de los aparatos más antiguos todavía funcionan con equipos nuevos gracias a esta compatibilidad con lo anterior.*

Nota *Texas Instruments ofrece una tecnología que admite totalmente las velocidades existentes de 802.11b, pero añade una velocidad de 22 Mbps que llega hasta un rendimiento un 10 o un 20 por ciento mayor que los 11 Mbps. El estándar de Texas Instruments seguramente será un añadido opcional para el familiar del 802.11b, conocido como 802.11g, que debería aparecer a principios de 2003. Vea el capítulo 10 para más detalles sobre los próximos estándares.*

Certificado Wi-Fi

Wi-Fi es una marca registrada de Wi-Fi Alliance (conocida anteriormente como Wireless Ethernet Compatibility Alliance), una asociación corporativa que se ocupa de garantizar la compatibilidad entre disposi-

tivos de distintos fabricantes que utilizan el estándar IEEE 802.11b y, posteriormente, el recién implementado estándar 802.11a (www.wifialliance.com). La Wi-Fi Alliance requiere cuotas de pertenencia considerables a los miembros que envían su equipamiento (junto con cuotas adicionales) al laboratorio de certificación de la asociación para que sea probado.

El proceso de certificación comprueba que miles de características individuales funcionan correctamente utilizando una suite estándar de pruebas. Sólo si el dispositivo pasa esas pruebas puede el fabricante usar legalmente el sello y nombre Wi-Fi (vea la figura 3.5). Aunque otros grupos comerciales han tenido un éxito mediano impulsando estándares, la estrategia de la Wi-Fi Alliance origina un signo de compatibilidad totalmente fiable.

En el momento de escribir este libro, la marca Wi-Fi fue actualizada para determinar si una pieza de equipamiento podía trabajar con una de las bandas de 2,4 GHz y 5 GHz o con las dos, que actualmente incluye sólo los estándares 802.11b (2,4 GHz) y 802.11a (5 GHz). Posteriormente en este capítulo hablaremos del último estándar. Equipamiento Wi-Fi más viejo sólo tiene la propia marca; en el equipamiento más reciente, hay que comprobar en qué banda funciona; algunos aparatos funcionan en las dos.

La Wi-Fi Alliance ha accedido a añadir estándares adicionales al proceso de certificación Wi-Fi para garantizar que las nuevas y más sofisticadas opciones de las redes inalámbricas funcionan tan bien juntas como las básicas.

Figura 3.5. *El logotipo Wi-Fi.*

Algunas tarjetas y puntos de acceso inalámbricos permiten elegir la velocidad que queremos usar, pero en la mayoría de los casos no tiene sentido elegir a mano una velocidad, pues el hardware debe negociar la velocidad más alta posible en todo momento. Generalmente no es posible saber cuál es la velocidad de una conexión, aunque es bastante probable que una red inalámbrica con

toda la señal vaya a 11 Mbps, mientras que una conexión inalámbrica de corto alcance es probable que vaya a 1 ó 2 Mbps.

Truco *Los verdaderos manitas de lo inalámbrico pueden obtener un rendimiento ligeramente mejor deshabilitando las velocidades más bajas e imponiendo a todos los dispositivos que transmitan a las velocidades más altas o sólo a la más alta, 11 Mbps: 802.11b se come parte de su ancho de banda con cada fragmento de datos que envía para mantener la compatibilidad con sistemas más lentos o más lejanos.*

Como 802.11b utiliza secuencia directa, cada punto de acceso 802.11b puede ser establecido en uno de varios canales para evitar conflictos con otros dispositivos inalámbricos de las cercanías. 802.11b utiliza la banda sin licencia 2,4 GHz, que en los EE.UU. va de 2,4000 GHz a 2,4835 GHz. Aunque técnicamente hay 14 canales posiblemente solapados en la especificación de 802.11b, sólo 11 se pueden usar legalmente en los EE.UU.

Los canales están separados entre sí por algunos megaherzios para permitir la flexibilidad al elegir canales en caso de interferencia. Por ejemplo, la interferencia podría proceder de partes de la banda compartida con los radioaficionados, señales de televisión de transmisión remota y transmisiones de seguridad pública limitadas. O la interferencia puede suceder en un área que contiene varios puntos de acceso 802.11b; piense en una biblioteca universitaria en la que muchos estudiantes quieren navegador por Internet utilizando sus portátiles, todos en un pequeño espacio físico.

Los canales 1, 6 y 11 pueden utilizarse simultáneamente uno encima de otro sin que solapen las frecuencias (vea la figura 3.6).

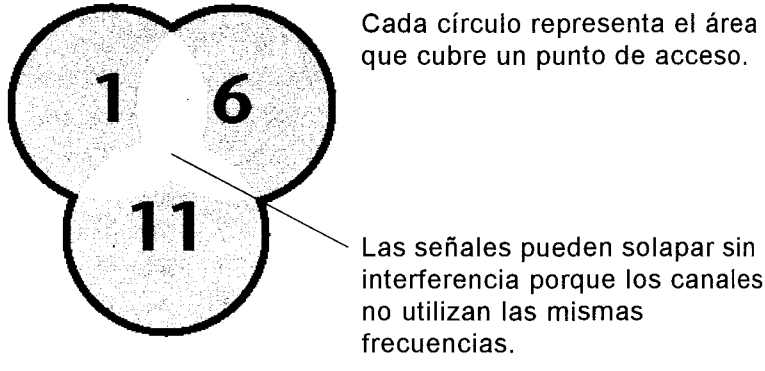

Figura 3.6. *Los canales 1, 6 y 11 se solapan sin interferencias.*

Conectar con 802.11b

Los clientes 802.11b se asocian con los puntos de acceso 802.11b a través delos siguientes pasos:

1. Un usuario activa un ordenador o dispositivo cliente con 802.11b habilitado encendiéndolo o conectando una tarjeta o seleccionando una opción de software para habilitar 802.11b.
2. El cliente busca redes locales explorando todos los canales locales legales en la banda de 2,4 GHz.
3. El cliente ofrece una visualización, generalmente un menú emergente o algo similar, con los nombres de las redes que emiten su identidad (redes abiertas).
4. El usuario selecciona una de estas redes, elige una de una configuración preestablecida o escribe el nombre de una red si está cerrada o no está emitiendo su nombre.

Nota

Cuando se configura una conexión por primera vez, el usuario tiene la opción de introducir una clave WEP (Privacidad equivalente de cable), que es una clave de cifrado utilizada en Wi-Fi para mezclar los datos entre un cliente y un punto de acceso. Algunas redes no utilizan claves WEP, incluyendo la mayoría de las redes de espacio público gratuito o con cuota. Cierto software permite introducir una clave WEP cada vez en lugar de guardarla en un perfil. Para más información sobre WEP, vea el capítulo 6.

5. El cliente intenta asociarse con el punto de acceso de la red seleccionada.
6. Si tiene éxito, el punto de acceso y el cliente tienen ahora una conexión de red activa a través de la que se pueden enviar TCP/IP, AppleTalk y distintos protocolos de red Windows y Unix.

Nota

Wi-Fi puede parecer muy similar a Ethernet con cable, y lo es: Wi-Fi comparte la mayoría de su funcionamiento interno con Ethernet de cable y sólo difiere en la parte de la especificación dedicada a la física del movimiento de bits de un lado a otro utilizando señales de radio en lugar de electrones en un cable físico.

7. Si el cliente está configurado para aceptar una dirección IP automáticamente y el punto de acceso o red está configurado para asignar una dirección IP a través de un servidor DHCP, empieza el baile y el cliente tiene ahora una dirección Internet, a menudo una dirección de red privada que no se puede alcanzar desde el mundo exterior. (Vea la sección "Protocolos de red" en el capítulo anterior.)

Modo ad hoc

802.11b también ofrece un modo ad hoc, en el que dos o más ordenadores intercambian datos directamente sin un punto de acceso central, algo muy parecido a los viejos tiempos en que se utilizaba un cable Ethernet cruzado o se enchufaba un cable de módem nulo entre dos puertos en serie de dos ordenadores.

En el modo ad hoc, uno de los ordenadores crea una red y después la ven los dos ordenadores (vea el paso 3 en la sección anterior). Como alternativa, cada usuario puede escribir la misma información de una red y se unen de facto. La diferencia entre el modo ad hoc y un punto de acceso de software o hardware es que las conexiones ad hoc no tienen un punto central de autoridad.

Las conexiones ad hoc son completamente privadas entre las máquinas en cuestión. (Podemos configurar un ordenador como puerta de enlace con Internet y compartir su conexión; comentaremos cómo gestionar esto en el capítulo 5.)

Dado que las conexiones ad hoc sólo existen entre dos o más ordenadores, son útiles principalmente para transferir archivos; si necesitamos dar un archivo a un colega y no tenemos otra forma de hacerlo, activar la opción de compartir archivos y establecer una red ad hoc bastará para llevar a cabo la tarea. La próxima vez que tenga un momento libre, le recomendamos que averigüe cómo configurar una red ad hoc y transferir archivos, pues recorrer los pasos lejos de casa o la oficina, posiblemente con alguien que no se conoce, puede ser un poco más complicado.

El modo ad hoc es uno de los pocos aspectos de Wi-Fi que no forma parte del proceso de certificación de dispositivos fabricados antes de 2002. El equipamiento antiguo o que no dispone de actualizaciones de software interno (llamado *firmware*), no usará necesariamente el modo ad hoc de la misma forma.

La Wi-Fi Alliance añadió un estándar ad hoc a su certificación Wi-Fi a finales de 2001, de modo que todo el equipamiento nuevo debe funcionar bien junto. Dicho esto, el equipamiento del mismo fabricante, como todas las tarjetas AirPort de Apple, generalmente admite el modo ad hoc sin problemas.

Otros estándares inalámbricos

El 802.11b es el estándar de redes inalámbricas más común en todo el mundo, pero hay otras tres especificaciones que merecen un poco de atención, aunque no las vamos a tratar con tanta atención en el resto del libro. Estas tres especificaciones son una versión similar al 802.11b de mayor velocidad, llamada 802.11a; un reemplazo del sistema de cable de corto alcance que no consume mucha batería llamado Bluetooth; y HomeRF, un modo orientado al pequeño consumidor de unir teléfonos inalámbricos, dispositivos multimedia, controles de televisión por cable e Internet.

802.11a

El equipamiento de red adherido al estándar IEEE 802.11a empezó a aparecer a mediados del 2002 y con razón se preguntará por qué apareció antes el estándar 802.11b que el 802.11a. El IEEE aprobó en realidad el 802.11a antes que el 802.11b, pero la tecnología necesaria para implementar el 802.11a y la parte del espectro en la que tenía que operar no estaban disponibles todavía.

Nota

La Wi-Fi Alliance planeaba originalmente certificar los dispositivos 802.11a bajo el nombre "Wi-Fi5", pero decidió finalmente modificar la marca Wi-Fi para incluir el estándar 802.11a. Si un dispositivo Wi-Fi presta soporte al estándar 802.11a, el texto debajo del sello Wi-Fi señala que se usa la banda de 5 GHz.

802.11a difiere principalmente en cuatro aspectos de su hermano, el estándar 802.11b. 802.11a:

- Utiliza tres partes de la banda de 5 GHz extendiéndose por unos cientos de megahercios no contiguos.
- Tiene 12 canales que no solapan que permiten que más puntos de acceso cubran la misma área física sin provocar interferencias entre sí.
- Va a una velocidad de 54 Mbps o alrededor de 25 Mbps de rendimiento real.
- Funciona en distancias más cortas en muchos casos, pero tiene mejores protocolos para clasificar la reflexión de señales en interior.

Las principales ventajas del estándar 802.11a surgen de estas cuatro diferencias: la banda de 5 GHz no está siendo utilizada por muchos otros aparatos inalámbricos y los 12 canales no solapados permiten que un número de usuarios considerablemente mayor aproveche todo el ancho de banda en el mismo espacio físico. La combinación de mayor rendimiento y menor solapamiento de canales significa que el 802.11a podría reemplazar o ampliar las redes Ethernet convencionales para servidores u oficinas en las que el estándar 802.11b puede no ser lo bastante rápido o no ofrecer el mismo ancho de banda simultáneamente.

Los cuatro canales superiores del 802.11a están reservados específicamente para conexiones punto a punto de alta potencia en exteriores (naturalmente, con antenas externas). Con las velocidades que ofrece el estándar 802.11a, la transmisión punto a punto es una forma atractiva de evitar los costes telefónicos de las líneas digitales T3 de 45 Mbps. Las líneas T3 pueden costar varios miles de euros al mes en conexiones de corta distancia en la misma ciudad, y además requieren caro equipamiento en los dos extremos de la línea.

El coste del equipamiento 802.11a empezó a bajar mucho antes de lo previsto y, aunque los analistas y la gente como nosotros pensamos inicialmente que el 802.11a no encontraría un sitio en las casas particulares rápidamente, los precios bajos pueden hacer que merezca la pena tenerlo en cuenta en pequeñas oficinas y en casa. Muchos aparatos 802.11a cuestan sólo entre 50 y 100€ más que el equipamiento 802.11b. Por supuesto, dada la velocidad de la mayoría de las conexiones de Internet caseras (casi nunca superiores a 1,5 Mbps), se necesita un uso especializado, como la distribución de vídeo no comprimido, para aprovechar el rendimiento real de 25 Mbps del estándar 802.11a. Pero incluso las oficinas más pequeñas pueden obtener ventajas, especialmente si los miembros del personal transfieren rutinariamente imágenes Photoshop y otros archivos grandes.

Como ventaja añadida, varios fabricantes de equipamiento para el consumidor particular y corporativo han empezado a lanzar y anunciar puntos de acceso que combinan el 802.11a y el 802.11b y pueden gestionar el tráfico utilizando simultáneamente los dos estándares. Hay algunos problemas de diseño en esta estrategia, pues el mayor alcance del 802.11b significa que se necesitará una antena más potente para el modo 802.11a o quizá otro punto de acceso 802.11a, pero el hardware que combina los estándares proporciona un gran método para facilitar la transición de una tecnología a otra.

Nota *Todas las redes públicas utilizan actualmente sólo el estándar 802.11b, pero es probable que cuando la combinación de puntos de acceso se*

haga más popular y el 802.11a se abra camino en las organizaciones, los proveedores de espacios públicos añadan el servicio de mayor velocidad. Naturalmente, la mayoría de las redes públicas proporcionan acceso a Internet a menos de 1,5 Mbps y la diferencia seguramente no será mucha.

Configurar clientes y puntos de acceso 802.11a es prácticamente igual que configurar aparatos 802.11b.

Bluetooth

Cuando note que ha olvidado coger el cable USB necesario para descargar las imágenes de la cámara digital, intente utilizar la conexión infrarroja para sincronizar el Palm o quiera compartir archivos sin una red a la vista, Bluetooth empezará a tener sentido.

Bluetooth es un estándar de red ad hoc de corto alcance que utiliza la misma banda de 2,4 GHz que el estándar 802.11b. Diseñado para ir a una velocidad de 1 Mbps o con un rendimiento en red de alrededor de 700 Kbps, Bluetooth omite toda la carga tipo Ethernet del 802.11b para permitir conexiones rápidas entre ordenadores y otros aparatos, a menudo durante periodos cortos o transacciones de un solo elemento.

Tecnología Bluetooth

Bluetooth utiliza salto de frecuencias en lugar de secuencia directa: los dispositivos Bluetooth cambian de frecuencia 1.600 veces por segundo. Esta combinación hace a Bluetooth un estándar muy resistente a las interferencias y obstrucciones, y permite que muchos transceptores Bluetooth funcionen en el mismo espacio sin pisarse unos a otros. El alcance de Bluetooth es sólo de unos 100 metros, que parece corto, pero hay que tener en cuenta que siempre estuvo pensado para funcionar a baja potencia para alargar la vida de las baterías de los ordenadores de bolsillo, los móviles y otros tipos de aparatos que pueden terminar con chips Bluetooth incrustados.

El descubrimiento es la clave de la facilidad de uso de Bluetooth: en lugar de saber nada sobre la pieza de equipamiento Bluetooth con la que queremos intercambiar información, como su dirección de red o número de adaptador, podemos simplemente hacer que el dispositivo se pueda descubrir para que el equipo desde el que conectamos pueda verlo, intercambiar una frase de paso para autenticación y después hacer pasar los datos de un lado a otro.

Bluetooth y el estándar 802.11b tienen algunos problemas de coexistencia: los fabricantes de los dos tipos de equipamiento advierten de que no se pueden poner transceptores a menos de un metro de distancia entre sí para evitar interferencias que reducirían el ancho de banda de los dos transceptores. Versiones futuras del 802.11b y de Bluetooth, gracias a los esfuerzo de otro comité IEEE conocido como 802.15.2, trabajarán codo a codo con menos conflictos. La especificación 802.15.2 requiere que los dispositivos minimicen su uso de frecuencias ocupadas.

Otro pequeño desarrollo que afectó al futuro desarrollo de Bluetooth fue la adopción en 2002 de un estándar establecido por el grupo Red de área personal (PAN) o grupo de trabajo 802.15 del IEEE.

El estándar 802.15.1-2002 (¡qué cantidad de números!) es un gran subgrupo de Bluetooth que pueden utilizar empresas que no están dentro del grupo industrial de Bluetooth y que será compatible con prácticamente todos los aparatos Bluetooth.

Usos de Bluetooth

Diseñado originalmente como un "reemplazo del cable" por un consorcio industrial llamado Bluetooth Special Interest Group (www.bluetooth.com), la utilidad real de Bluetooth parece recaer en su papel como traductor universal. Los estándares Bluetooth permiten a los fabricantes de aparatos de hardware totalmente distintos habilitar conexiones simples que requieren una mínima configuración y no precisan controladores especiales.

El soporte que Apple prestó inicialmente a Bluetooth permite hacer llamadas de módem a través de un móvil ajustado a Bluetooth que funciona en una red de datos GSM o GPRS, sincronizar una agenda electrónica basada en Palm OS y transferir archivos entre aparatos conectados, ya sean ordenadores u otros equipos. El software disponible para Windows también permite imprimir en impresoras ajustadas a Bluetooth.

Ya se puede encontrar soporte a Bluetooth en Mac OS X 10.2 Jaguar de Apple; Microsoft planea añadir soporte a Bluetooth en Windows XP en una actualización que debe estar a punto de salir al mercado, si no ha salido ya. En cuanto al hardware, hay varios aparatos que también admiten Bluetooth, incluyendo adaptadores USB y PC Cards fabricados por Belkin, 3Com, D-Link y otras compañías; móviles como el Sony Ericsson T68i; y tarjetas de presión para agendas electrónicas Palm y PocketPC (vea la figura 3.7). Incluso podemos comprar un adaptador de puerto paralelo de 3Com que convierte una impresora en un dispositivo Bluetooth, útil para imprimir desde un ordenador o aparato de bolsillo dentro de la misma habitación.

Figura 3.7. Varios aparatos Bluetooth de Belkin.

Una de las promesas de Bluetooth es que puede convertir un teléfono móvil en un accesorio puro que no es necesario tocar directamente. Podríamos hacer conexiones de datos desde el portátil con el teléfono móvil en un bolsillo del estuche del ordenador, marcar un número en el teléfono móvil desde el portátil o hablar a través de unos auriculares Bluetooth que transmiten la señal de voz al teléfono móvil.

Bluetooth tiene su verdadero papel entre las robustas redes tipo Ethernet y la mezcla de cables y estándares incompatibles que hacen que sea tan frustrante mover bits de información entre aparatos pequeños.

Conectar con Bluetooth

Para intercambiar datos entre dispositivos Bluetooth, primero hay que convertirlos en *pares*. Para convertir en un par dos o más dispositivos hay que intercambiar una corta frase de paso. Imagine, por ejemplo, un portátil con Windows XP y una tarjeta Bluetooth y un Power Mac Apple con un adaptador USB D-Link.

Primero hay que hacer que el ordenador pueda ser descubierto en el PC o la máquina Mac. El ordenador que puede ser descubierto empieza a emitir señales "estoy aquí" utilizando Bluetooth. La otra máquina puede ahora ver a ese ordenador, automáticamente (si el software Bluetooth permite la exploración constante en busca de dispositivos nuevos) o manualmente (seleccionando una opción tipo Buscar nuevos dispositivos).

Cuando la máquina que busca dispositivos Bluetooth identifica al ordenador que puede ser descubierto, puede solicitar una conexión enviando una frase de paso. Escribimos una corta frase o una contraseña y después se nos pide

en la máquina que puede ser descubierta que introduzcamos la misma información.

Si introducimos la misma frase de paso, las dos máquinas se convierten en un par y pueden intercambiar información utilizando programas como Bluetooth File Exchange, que se incluye en Jaguar o en software de impresora integrado en Windows, que trata a una impresora Bluetooth como cualquier otra impresora local.

HomeRF

El único verdadero competidor de Wi-Fi es un estándar llamado HomeRF, que fue desarrollado por un grupo industrial llamado HomeRF Working Group (www.homerf.org). Como Bluetooth, HomeRF utiliza salto de frecuencias en la banda de 2,4 GHz. La especificación 2.0 actual hace transmisiones a una velocidad de 10 Mbps; una versión anterior iba a menos de 2 Mbps. Para cuando la versión más rápida de HomeRF recibió la aprobación de la FCC, el estándar 802.11b había avanzado mucho.

El objetivo del diseño de HomeRF es permitir que los aparatos electrónicos de pequeño consumidor, teléfonos inalámbricos y ordenadores se comuniquen entre sí simultáneamente y con fiabilidad a través de la misma red. Los teléfonos inalámbricos que utilizan HomeRF tienen garantía de entrar cada pocos milisegundos para garantizar la claridad y continuidad de las conversaciones telefónicas, impidiendo las interrupciones que pueden ser la plaga de las redes que carecen de garantías para la continuidad de la transmisión. Igualmente, los multimedia fluidos, como la reproducción de películas de un aparato en otro, tienen prioridad frente a los datos puros, de modo que no hay saltos en películas o música.

A mediados de 2002, los principales fabricantes de equipamiento HomeRF, Proxim, Motorola y Siemens, por fin empezaron a lanzar aparatos atractivos para el consumidor, incluyendo una puerta de enlace central que puede conectarse a un módem de cable o DSL, ofreciendo conexión compartida con Internet que incluye cortafuegos, opciones estándar para compartir archivos y otros servicios de red, y soporte a distintos teléfonos inalámbricos.

Motorola y otros fabricantes han prometido también incluir HomeRF en equipos de cable para televisión y algunas compañías telefónicas aparentemente se han comprometido (aunque todavía no ha habido declaraciones en este sentido) a ofrecer servicios de telefonía digital que combinarían datos, televisión y voz en una sola oferta que se conectaría a un concentrador HomeRF en las casas.

Hay equipamiento HomeRF en cientos de miles de hogares, principalmente en Europa, donde un temprano estándar de teléfono inalámbrico establecido por Siemens, DECT, está bien establecido y es totalmente compatible con HomeRF para evitar interferencias.

HomeRF tiene un futuro menos claro en los EE.UU., incluso aunque los fabricantes de equipamiento HomeRF consigan asociarse con empresas de telefonía o cable. Aunque los consumidores pueden comprar equipamiento HomeRF en grandes tiendas de informática, es improbable que elijan tal opción si saben algo de las redes inalámbricas, pues no hay compatibilidad entre HomeRF y el estándar 802.11b más ampliamente establecido. HomeRF puede funcionar bien para redes inalámbricas particulares, pero la tarjeta HomeRF del portátil será inútil tan pronto como salgamos de casa. Hablando en plata, el objetivo de las redes inalámbricas es poder comunicarse con otros y si todo el mundo utiliza el estándar 802.11b, HomeRF deja de ser una opción. Además, es improbable que pueda abrirse camino en las redes corporativas y públicas en las que tanto predomina el 802.11b, no sólo por ser muy diferente, sino también porque carece de funciones que necesitan las empresas para integrar el equipamiento HomeRF en sus sofisticadas redes.

Manos a la obra

En el próximo capítulo, nos apartamos de toda esta información teórica para presentar material que podrá usar en la práctica: instrucciones paso a paso para muchas tareas comunes que hay que llevar a cabo al configurar una red inalámbrica.

4. Conectar el ordenador

En los capítulos anteriores del libro hemos visto los temas básicos de las redes y cómo funcionan las redes inalámbricas; ahora ha llegado el momento de poner manos a la obra y presentar las instrucciones necesarias para conectar un ordenador a una red inalámbrica. Esa tarea implica instalar un adaptador de red inalámbrica, configurar los ajustes de red del sistema operativo y configurar el software cliente de red inalámbrica para conectar con un punto de acceso. En este capítulo suponemos que desea conectar un PC basado en Windows o un ordenador Macintosh a través de un adaptador de red inalámbrica que utiliza uno de los estándares de la familia 802.11, concretamente 802.11a, 802.11b, 802.11g o incluso alguna combinación de ellos.

Casi no hay diferencia en los distintos tipos de 802.11 en cuanto a configuración, de modo que los vamos a ver a la vez, señalando las diferencias si es necesario. Por supuesto, lo más probable en este momento es que utilice un adaptador de red inalámbrica 802.11b, pues la inmensa mayoría de puntos de acceso utilizan actualmente el estándar 802.11b.

Nota

Es posible que el estándar 802.11g no esté entre las opciones que pueda escoger cuando lea este libro, pero esperamos que su configuración sea prácticamente idéntica a la del estándar 802.11b.

Conectar con una red inalámbrica

Para los propósitos de esta sección, vamos a suponer que ya dispone de un punto de acceso en funcionamiento o quiere conectar con el punto de acceso existente de alguna otra persona. Si no es el caso, lea la sección "Configurar una puerta de enlace" en el capítulo 5 y después vuelva a este capítulo.

Nota *Si todavía no ha comprado un punto de acceso, lea "Comprar una puerta de enlace inalámbrica" también en el capítulo 5 para encontrar detalles sobre qué debe buscar.*

Con un punto de acceso en su puesto, la tarea a realizar es establecer una conexión inalámbrica entre el ordenador y el punto de acceso, y usar el punto de acceso como piedra angular del resto de la red y, casi siempre, del acceso a Internet.

En la mayoría de los casos, una conexión inalámbrica gestiona TCP/IP, el lenguaje de Internet, pero opcionalmente puede prestar soporte a otros protocolos como AppleTalk (para ordenadores Macintosh) o NetBEUI (para sistemas con Windows).

Cómo se lleve a cabo la tarea depende, por descontado, de qué sistema operativo y versión se esté utilizando. Además, en las versiones de Windows anteriores a Windows XP, es probable que sea necesario utilizar el software cliente de red inalámbrica proporcionado por el fabricante de la tarjeta de red. Veremos dos de los programas cliente de red inalámbrica más comunes, pero tenga por seguro que la mayoría de los clientes inalámbricos son muy parecidos.

Conectar utilizando Windows

Antes, todos los fabricantes de equipamiento Wi-Fi tenían que crear su propio software, o dar la licencia a otra compañía de software, para que pudiéramos crear una conexión inalámbrica entre Windows y un punto de acceso. Afortunadamente, desde Windows XP, Microsoft se ha encargado de la tarea y ha creado un software cliente de red inalámbrica extraordinariamente simple y fácil de usar. (¡De verdad! ¡Lo ha hecho!).

Truco

Los usuarios de Windows pueden pensar que se necesita algo de magia para conectar con una Estación Base AirPort de Apple, pero no es así: es igual que con cualquier otro punto de acceso, excepto una cosa. Si la Estación Base AirPort está utilizando cifrado WEP, hay que sacar la clave WEP hexadecimal de la Estación Base. Vea el cuadro "Conectar con una Estación Base AirPort sin una tarjeta AirPort" en el capítulo 5.

Truco

En Windows XP, para seguir estas instrucciones, cambie a la vista clásica en Panel de control. En caso contrario, tendrá que navegar por iconos agrupados pensados para usuarios menos sofisticados.

La primera tarea es instalar y configurar el adaptador de red; la siguiente, configurar los ajustes de red. Por último, hay que configurar el software cliente de red inalámbrica que o viene con el adaptador de red o está incluido en Windows XP.

Ajustes de conexión inalámbrica comunes

Todo programa cliente de red inalámbrica requiere que se rellene o seleccione al menos uno (a veces todos) de los siguientes ajustes para establecer la asociación con un punto de acceso. No se preocupe demasiado por esta información ahora mismo, pero quizá desee volver a ella más adelante en este capítulo.

- ***Modo de red, infraestructura o ad hoc:*** *Infraestructura es la opción que hay que elegir para conectar con una red; sólo se utiliza ad hoc para conexiones entre equipos. Este ajuste está a menudo preestablecido en infraestructura. A veces se necesita un programa independiente para crear conexiones ad hoc.*
- ***Nombre de red, llamado técnicamente ESSID (para redes grandes) o SSID (para un solo punto de acceso):*** *En muchos clientes, podemos dejar vacío el nombre de red o introducir "any" para conectar con cualquier red disponible.*
- ***Clave WEP o frase de paso, si está habilitado el cifrado:*** *Una clave WEP tiene 10 ó 26 caracteres hexadecimales (los números hexadecimales están formados por los números del 0 al 9 y las letras de la A a la F). Algunas redes utilizan una frase de paso*

WEP, en la que se introduce una palabra o frase corta; ésta a su vez genera la clave. Muchos clientes permiten introducir hasta cuatro claves WEP si el administrador de red las ha definido. De forma confusa, si sólo se ha definido una clave WEP, ¡algunos de estos clientes requerirán que se introduzca la misma clave WEP en las cuatro entradas!

- ***Tamaño de clave WEP:*** *Esta opción está establecida en 40, 56 ó 64 bits (en realidad son exactamente iguales, a pesar de los distintos nombres, y se suelen llamar 40), o 104 ó 128 bits (también son iguales y se suelen llamar 128). La longitud de la clave se establece en el punto de acceso y todos los clientes deben usar claves de la misma longitud. Una clave de 40 bits tiene 10 caracteres hexadecimales; una clave de 128 bits tiene 26 caracteres, que la hacen más difícil de escribir pero también más segura.*
- ***LEAP:*** *Es un sistema de cifrado que funciona con WEP y puntos de acceso más avanzados, pero requiere un nombre de usuario y una contraseña para el inicio de sesión. Se utiliza principalmente en organizaciones grandes como las universidades; busca instrucciones de configuración específicas del sitio en la ayuda del ordenador o en un sitio Web de soporte.*
- ***Velocidad de transmisión:*** *En clientes que permiten cambiar este ajuste, podemos establecer nuestro sistema en una velocidad específica, como 11 Mbps, si estamos seguros de disponer de suficiente fuerza en la señal en todas partes. Los puntos de acceso también pueden tener asignadas velocidades altas. Eliminando las velocidades más bajas mejoramos el rendimiento general, pero es más probable que perdamos una conexión completamente si nos alejamos demasiado del punto de acceso.*
- ***Canal:*** *Los canales se seleccionan automáticamente en el software cliente, pues los puntos de acceso sólo pueden emitir en un canal por turno. Seleccionamos un canal sólo cuando creamos una red ad hoc.*

Instalar hardware y configurar los ajustes de red

No importa qué versión de Windows utilice, primero debe instalar el adaptador de red inalámbrica y configurar correctamente los ajustes de red.

Nota

Si su adaptador de red Wi-Fi ya está instalado y en funcionamiento, vaya al paso 4 siguiente que corresponda a su versión de Windows.

1. Instale los controladores de la tarjeta de red utilizando su CD-ROM o disquete o el instalador descargado del sitio Web del fabricante.
2. Apague el ordenador y conecte el adaptador de red al ordenador. Vuelva a encenderlo.

Nota

Apagar el ordenador no es indispensable si se trata de un adaptador de red inalámbrica PC Card o USB, pero sí para tarjetas PCI y otras tarjetas internas, y siempre es buena idea empezar de cero.

3. Si todo va bien, Windows identifica el nuevo adaptador de red inalámbrica, carga el controlador instalado y crea una entrada en el panel de control Red (95/98/ME/NT) o Conexiones de red (XP/2000) que corresponde al hardware (vea la figura 4.1).

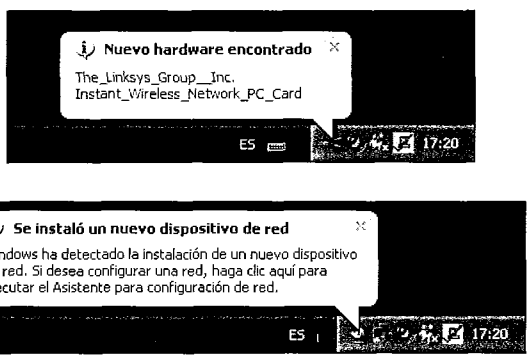

Figura 4.1. *Windows reconoce el nuevo hardware y lo configura.*

Nota

Si Windows no detecta y configura automáticamente su nuevo adaptador de red inalámbrica, acuda al capítulo 9 para encontrar tácticas que le permitan resolver el problema.

Aquí es donde divergen los pasos, dividiéndose en instrucciones para las versiones antiguas de Windows (95, 98, ME y NT) y para las versiones más recientes (2000 y XP).

Windows 95/98/ME/NT

4. Abra el panel de control Red y en la ficha Configuración compruebe que tiene asignado TCP/IP al nuevo dispositivo (vea la figura 4.2). Por ejemplo, si su tarjeta se identifica en Windows como "Adaptador de red inalámbrica Linksys WPC11", debe ver una entrada que diga "TCP/IP-> Adaptador de red inalámbrica Linksys WPC11".

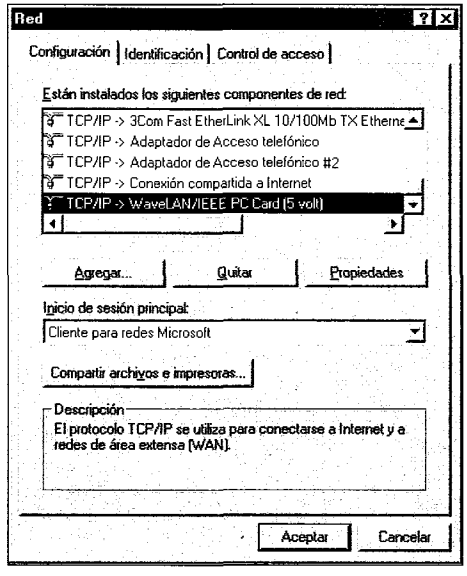

Figura 4.2. *Ficha Configuración del panel de control Red.*

5. Si necesita protocolos de red adicionales (no suele ser el caso para la mayoría de la gente), haga clic en **Agregar**, seleccione Protocolo, escoja en la lista de la izquierda Microsoft u otra compañía y seleccione NetBEUI o cualquier otro protocolo que desee o necesite.

   Si está utilizando asignación dinámica de direcciones con un servidor DHCP, que es lo que recomendamos por ser lo más sencillo, puede dejar los ajustes predeterminados como están e ir al paso 8, donde convergen de nuevo las instrucciones para todas las versiones de Windows.

6. Seleccione TCP/IP->*dispositivo* (donde aparece el nombre de su adaptador en lugar de *dispositivo*) en la lista y haga clic en **Propiedades** (vea la figura 4.3).

7. En cada una de las fichas Configuración DNS, Puerta de enlace y Dirección IP, haga clic en los botones de opción para habilitar DNS y

especificar una dirección IP; después puede introducir la dirección IP, la máscara de subred, la dirección de puerta de enlace y las direcciones de servidor DNS.

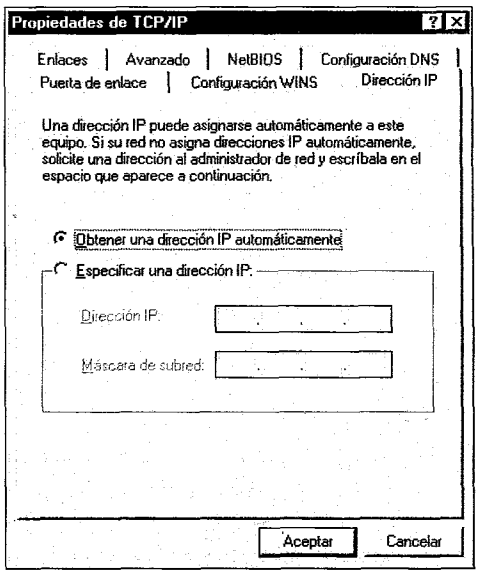

Figura 4.3. *Propiedades de TCP/IP.*

Truco *¿Dónde obtiene estos valores? vea más adelante la sección "Configurar a mano los ajustes de red" en este mismo capítulo.*

Windows XP/2000

4. Abra el directorio Panel de control (accesible desde el menú Inicio en Windows XP y desde el menú Configuración en el menú Inicio en Windows 2000) y después abra Conexiones de red en Windows XP (vea la figura 4.4) o Conexiones de red y de acceso telefónico en Windows 2000.

5. Haga clic derecho en el icono Conexión de red inalámbrica y seleccione Propiedades en el menú emergente para abrir el cuadro de diálogo Propiedades (vea la figura 4.5). Si no hay un elemento llamado Conexión de red inalámbrica en la lista, entonces el adaptador no está instalado correctamente y debe recorrer de nuevo los pasos para instalar el adaptador de red o leer los consejos para resolución de problemas del capítulo 9.

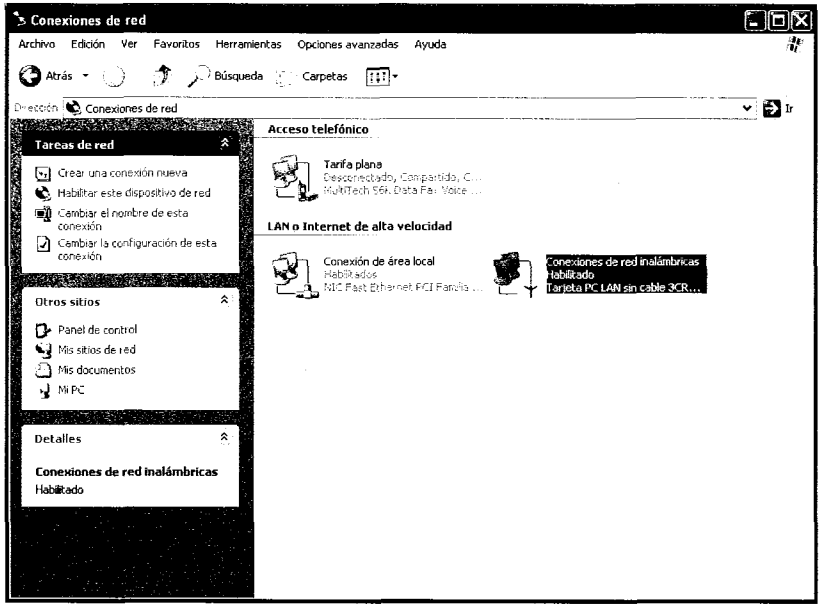

Figura 4.4. *La ventana Conexiones de red de Windows XP.*

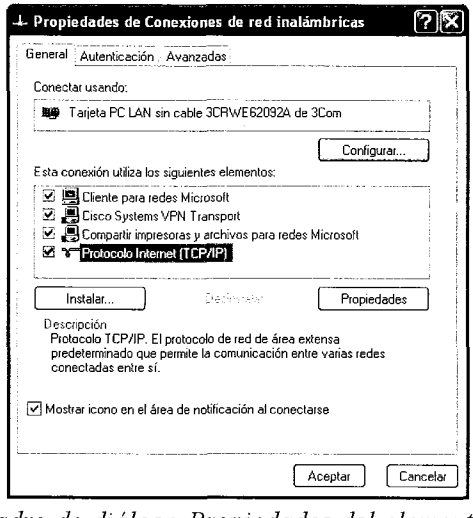

Figura 4.5. *El cuadro de diálogo Propiedades del elemento Conexión de red inalámbrica en Windows XP.*

Nota *Cada conexión inalámbrica está numerada independientemente y si quita y añade muchos adaptadores de red inalámbrica, puede terminar*

encontrándose con conexiones etiquetadas como Conexión de red inalámbrica 12, como le pasó a Glenn hace poco.

6. Seleccione Protocolo Internet (TCP/IP) en la lista. Si no hay una marca en la casilla de verificación próxima al nombre, active la casilla. Haga clic en el botón **Propiedades** para abrir el cuadro de diálogo Propiedades de Protocolo Internet TCP/IP (vea la figura 4.6). (Si TCP/IP u otros protocolos que necesite no aparecen en la lista, haga clic en **Instalar** y selecciónelos en la lista Protocolo o en la lista Cliente.)

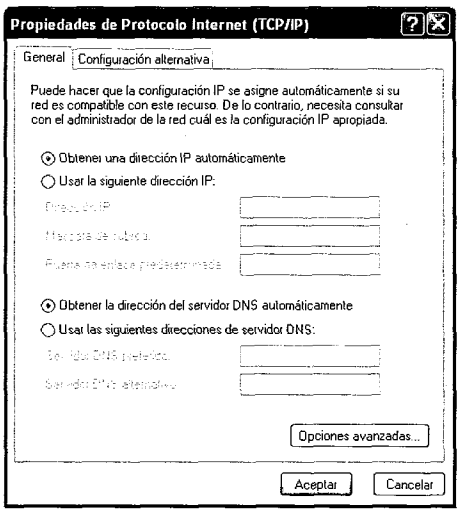

Figura 4.6. *Cuadro de diálogo Propiedades de Protocolo Internet TCP/IP de Windows XP.*

7. Si está utilizando asignación dinámica de direcciones con un servidor DHCP, deje los ajustes predeterminados y vaya al paso 8. En caso contrario, haga clic en los botones de opción Usar la siguiente dirección IP y Usar las siguientes direcciones de servidor DNS e introduzca los valores apropiados de su dirección IP y sus servidores DNS (vea el siguiente cuadro para averiguar cómo obtener estos números.)

Configurar a mano los ajustes de red

La estrategia más fácil y común para configurar los ajustes de red del ordenador es usar DHCP, que recibe el nombre de Protocolo de confi-

guración dinámica de host por una razón. Cuando utilizamos DHCP, el ordenador escoge todos sus ajustes de red dinámicamente en un servidor DHCP (normalmente la puerta de enlace inalámbrica) y no hay que configurar nada. Sin embargo, en algunos casos es posible que tengamos que introducir esos ajustes a mano. Si está trabajando en una red existente, pregunte al administrador de sistema o a la persona que configuró la red qué tiene que introducir. Si está conectando directamente con un proveedor de servicios de Internet, acuda a su documentación o a su servicio de ayuda.
La parte difícil aparece cuando conectamos con nuestro propio punto de acceso y hemos decidido no utilizar DHCP porque nadie puede decirnos cuáles son los números de red que hay que introducir. Eso no suele ser tan malo como parece, porque si queremos utilizar la configuración manual es porque sabemos qué hay que introducir. Para tal situación, he aquí un resumen.

- ***Dirección IP:*** *Ésta es la dirección IP del ordenador. Debe estar en el mismo rango de red privada que el punto de acceso, normalmente 192.168.1.x o 10.1.1.x, donde x es cualquier número excepto 0 y 255 (que están reservados para propósitos especiales). Los números tienen que ser únicos en la red privada local.*
- ***Máscara de subred:*** *Este ajuste indica el tamaño de la red y, si estamos utilizando una dirección IP dentro de uno de los dos rangos anteriores, hay que introducir 255.255.255.0 para la máscara de subred.*
- ***Dirección de puerta de enlace o enrutador:*** *Ésta es la dirección IP interna del punto de acceso y es probable que sea una dirección IP dentro del rango privado, como 192.168.1.1. (Nosotros siempre hacemos que nuestras puertas de enlace tengan una de las primeras direcciones en el rango IP, saltamos 9 direcciones y después empezamos a asignar direcciones IP a los ordenadores. De esa forma, la puerta de enlace suele terminar siendo 192.168.1.1, por ejemplo, y los ordenadores empiezan por 192.168.1.10.) Microsoft utiliza el término puerta de enlace; Apple llama a lo mismo router o enrutador.*
- ***Direcciones de servidor DNS:*** *Para estos números, introduzca las direcciones (usualmente serán por lo menos dos) recibidas del ISP.*

Todas las versiones de Windows

8. Haga clic en **Aceptar** dos veces: una para cerrar el cuadro de diálogo Propiedades de Protocolo Internet (TCP/IP) y otra para cerrar el panel de control Red o el cuadro de diálogo Propiedades de conexión de red inalámbrica.
9. Reinicie su ordenador cuando Windows le pida que lo haga, si se lo pide.

Configurar el software cliente Windows XP

Ahora que los ajustes de hardware y red están configurados apropiadamente, es el momento de configurar el software cliente de red inalámbrica que gestiona los ajustes específicos de la red. Este software cliente inalámbrico está integrado en Windows XP; si está utilizando una versión anterior de Windows, debe usar el software cliente que viene con el adaptador de red inalámbrica.

Nota

Si no utiliza Windows XP, o si decide no usar su cliente integrado por alguna razón, adelante unas pocas páginas para ver instrucciones de configuración del software cliente Linksys y Orinoco, más algunos consejos sobre qué es necesario en otros softwares cliente. En general, recomendamos utilizar el software cliente de Windows XP, es más fácil, está mejor integrado en Windows y probablemente absorberá a todos los demás cuando Windows XP se extienda todavía más. Algunos adaptadores de red Wi-Fi todavía no pueden aprovechar el software cliente de Windows XP porque los controladores de hardware todavía no han sido actualizados para gestionar la interacción.

Veamos cómo se habilita y configura el software cliente de red inalámbrica de Windows XP.

Nota

Quizá quiera acceder a varias redes inalámbricas, una en casa, otra en el trabajo y una tercera mientras asiste a un congreso, o tener acceso a varias redes en un solo lugar. Por ello, este software cliente de Windows XP permite configurar los detalles de varias redes y apilarlos en el orden en que queremos conectar si hay disponibles varias redes. La parte superior del cliente muestra las redes disponibles, mientras que la parte de abajo muestra las redes que hemos configurado.

1. Para habilitar el software cliente inalámbrico integrado en Windows XP, abra Mis sitios de red en el escritorio.
2. Haga clic en Ver conexiones de red.
3. Haga clic derecho en el elemento Conexión de red inalámbrica en la sección LAN o Internet de alta velocidad. En el menú emergente, si ve la opción Utilizar Windows para configurar mi red inalámbrica y no tiene una marca, selecciónela. (Si la opción no aparece, siga adelante.)
4. De nuevo, haga clic derecho en Conexión de red inalámbrica y seleccione Ver redes inalámbricas disponibles en el menú emergente.
5. Haga clic en el botón **Opciones avanzadas** (vea la figura 4.7).

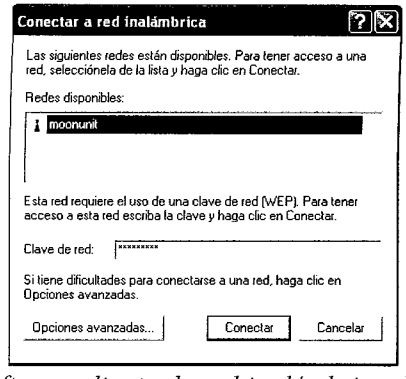

Figura 4.7. *Software cliente de red inalámbrica de Windows XP.*

6. Haga clic en el botón **Agregar** debajo de Redes preferidas para abrir el cuadro de diálogo de configuración de una nueva red Wi-Fi (vea la figura 4.8).
7. Introduzca el nombre o SSID de la red.
8. Si está utilizando WEP, active el cifrado de datos e introduzca la clave. Para el formato de clave, seleccione caracteres ASCII, si está utilizando una frase de paso, o hexadecimal si usa la forma abstracta. Elija la longitud de la clave en el menú emergente.

Nota *El menú dice 13 caracteres para claves de 104 ó 128 bits cuando debería decir 13 bytes hexadecimales o 26 dígitos hexadecimales.*

9. Haga clic en **Conectar**.

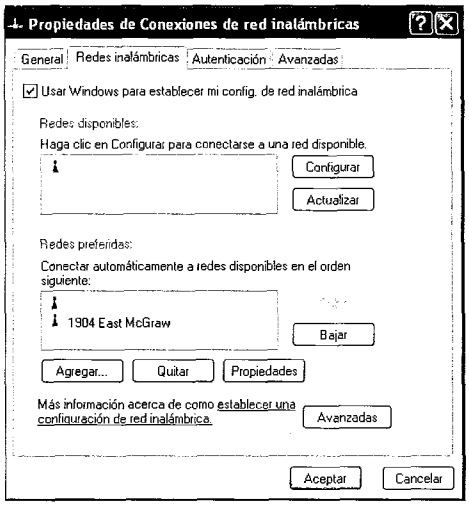

Figura 4.8. *Propiedades de conexión de red inalámbrica.*

¡Ya está! Repita los pasos tantas veces como sea necesario para otras redes con las que quiera conectar. Puede cambiar la red con la que está establecida la conexión en el cuadro de diálogo Propiedades de conexiones de red inalámbrica (vuelva a ver la figura 4.8). En la lista Redes disponibles aparecen las redes de las que hemos introducido detalles (si están cerradas) o de las que el adaptador puede recibir una señal. Redes preferidas contiene una lista con todas las conexiones de red que hemos configurado, como ya hemos dicho. Hay otra diferencia útil entre las listas Redes disponibles y Redes preferidas. Aunque parezca que seleccionar una red en Redes disponibles y hacer clic en **Configurar** proporciona acceso a ajustes de seguridad, no es posible hacer cambios desde esa ventana. Sólo podemos modificar los ajustes de seguridad y otros detalles de una red seleccionándola en Redes preferidas y haciendo clic en el botón **Propiedades** para abrir el cuadro de diálogo Propiedades de esa red.

Configurar el software cliente Linksys

Linksys fabrica gran parte del equipamiento de red que utilizan los pequeños consumidores, según los estudios de mercado y los números de ventas, pero no escribe el software para ese equipamiento. En lugar de ello, otorga licencias del software cliente de red inalámbrica que gestiona las conexiones bajo Windows. La versión que utiliza es prácticamente idéntica al software que ofrecen varias grandes compañías de hardware que utilizan los mismos chips y placas de circuitos, como D-Link Systems y otras.

Una vez instalado, el icono del software cliente Linksys debe aparecer en la bandeja del sistema y representa un pequeño ordenador con una antena en la parte de arriba (vea la siguiente figura). Antes de configurar una conexión, la pantalla del icono es roja; después, verde o amarilla, dependiendo de la calidad del enlace. Siga estos pasos para configurar el software cliente Linksys.

Figura 4.9. *Icono en la bandeja del sistema del software cliente Linksys.*

Nota *Si el icono no aparece en la bandeja del sistema, abra el directorio Panel de control y busque el panel iPrism. (Prism es el nombre de serie del grupo de chips del adaptador inalámbrico.)*

1. Abra el panel de control iPrism o haga clic en el icono de la bandeja del sistema.
2. Haga clic en la ficha Configuration (vea la figura 4.10).

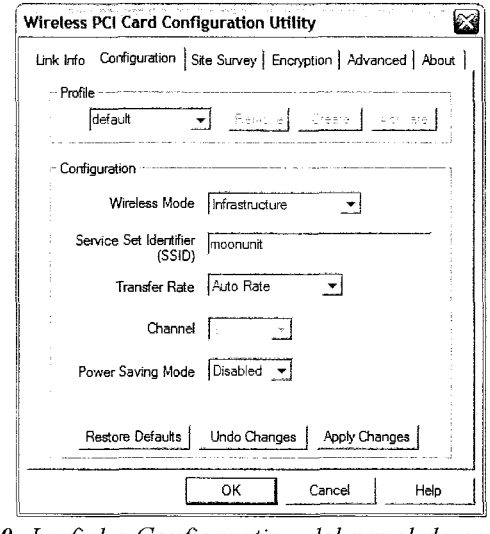

Figura 4.10. *La ficha Configuration del panel de control iPrism.*

3. Si el adaptador de red encuentra redes inalámbricas en las proximidades, aparecen en el menú emergente. Seleccione una para conectar con ella o, si es una red cerrada, introduzca el nombre de la red en el campo SSID.

4. Si la red utiliza cifrado WEP, haga clic en la ficha Encryption (vea la figura 4.11). Introduzca la frase de paso, si se la han proporcionado, o la clave o claves WEP hexadecimales.

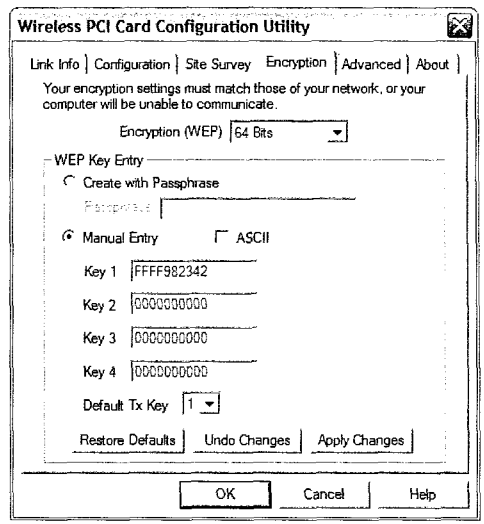

Figura 4.11. *La ficha Encryption del panel de control iPrism.*

Ya debe haberse establecido la conexión. La ficha Link Info muestra la fuerza de la señal para transmisión y recepción, y también detalles acerca del punto de acceso y la red con la que se ha establecido la conexión (figura 4.12). La ficha About proporciona detalles de versión del propio software de configuración, el controlador y el firmware del adaptador.

Configuración del software cliente Orinoco

La línea Orinoco (www.orinocowireless.com) de adaptadores de red inalámbricos también es muy popular y los adaptadores de red Orinoco también vienen con un sencillo cliente de red inalámbrica.

Nota

No deje que el nombre Orinoco le confunda: antes se llamaba WaveLAN y fue desarrollado por Lucent Technologies, cedido a una empresa llamada Agere Systems y más recientemente vendido a Proxim. El hardware y el software han sido actualizados muchas veces, pero tiene la misma apariencia y funcionan más o menos igual que hace tres años.

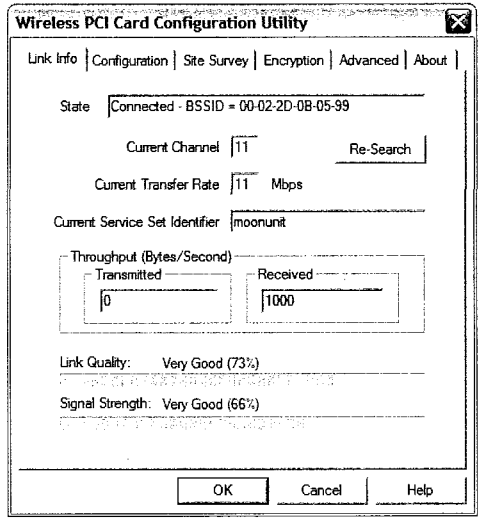

Figura 4.12. *La ficha Link Info del panel de control iPrism.*

Nota *Los adaptadores de red inalámbrica Orinoco pueden ser de las versiones silver y gold: los adaptadores silver están limitados a claves de cifrado WEP de 40 bits, mientras que las versiones gold admiten claves de 40 bits y de 128 bits para disponer de un cifrado ostensiblemente más fuerte.*

El software cliente Orinoco aparece en la bandeja del sistema como una pequeña gráfica con barras de distintas alturas (vea la figura 4.13). El número de barras rellenadas y el color de esas barras indica la fuerza de la señal (mejor cuantas más barras rellenadas, y el color va de rojo a amarillo y a verde según mejora la fuerza de la señal).

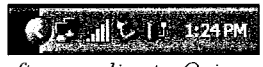

Figura 4.13. *El icono del software cliente Orinoco en la bandeja del sistema.*

Para configurar el software Orinoco para conectar el ordenador a una red inalámbrica, siga estos pasos.

1. Haga clic en el icono de las barras en la bandeja del sistema para abrir el software cliente Orinoco.

Nota *Haga clic derecho en el icono para acceder directamente al cuadro de diálogo Add/Edit Configuration Profile.*

2. Seleccione Add/Edit Configuration Profile en el menú Actions.
3. En el cuadro de diálogo, dé nombre a la configuración en el lado izquierdo y deje seleccionado Access Point en el derecho (vea la figura 4.14).

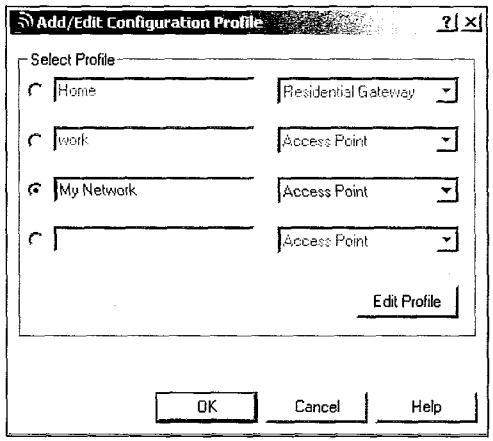

Figura 4.14. *El cuadro de diálogo Add/Edit Configuration Profile del software cliente Orinoco.*

4. Haga clic en el botón **Edit Profile** para abrir el cuadro de diálogo Edit Configuration (vea la figura 4.15).

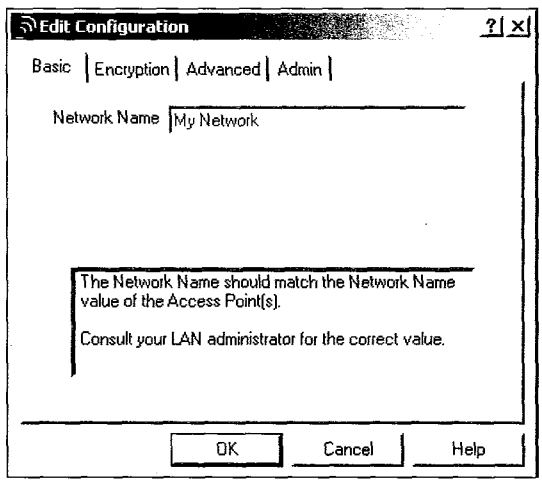

Figura 4.15. *El cuadro de diálogo Edit Configuration del software cliente Orinoco.*

5. En el cuadro de diálogo Edit Configuration, introduzca o seleccione el nombre de la red o el SSID en la ficha Basic; si hay redes en las proximidades, seleccione una red en el menú emergente.
6. Si está habilitado el cifrado WEP, introduzca su clave WEP en la ficha Encryption.
7. Haga clic en **OK** para cerrar el cuadro de diálogo Edit Configuration y de nuevo clic en **OK** para cerrar el cliente Orinoco.

El cliente Orinoco tiene un ingenioso monitor que muestra la señal a lo largo del tiempo que puede servir de ayuda para comprobar el acceso mientras se pasea con un portátil. En el menú Advanced, seleccione Link Test y haga clic en la pestaña Test History (vea la figura 4.16).

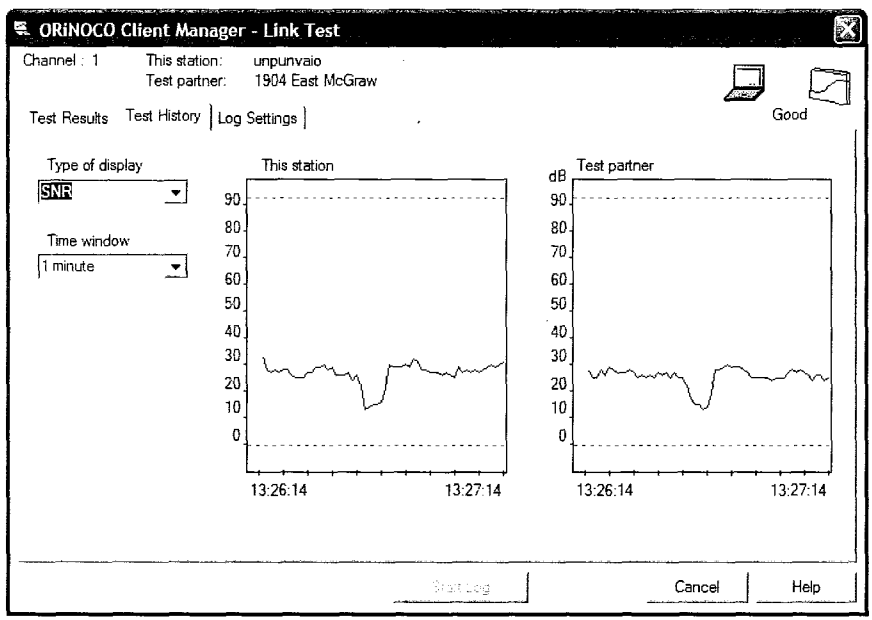

Figura 4.16. *Control de la señal a lo largo del tiempo en el software cliente Orinoco.*

Configurar otro software cliente inalámbrico

¿Qué sucede si no utiliza el software cliente inalámbrico Windows XP, Linksys u Orinoco? No tiene por qué preocuparse, pues como habrá visto si ha leído las instrucciones de estos softwares cliente, no hay mucho que configurar. Sólo necesita tener a mano el cuadro "Ajustes de conexión inalámbrica

comunes" (fijándose especialmente en nombre de red y clave WEP) al configurar el software.

Igual que los clientes inalámbricos que hemos comentado, otros clientes suelen tener herramientas de control que muestran la fuerza de la señal. Algunos ofrecen gestores de configuración para guardar ajustes diferentes para redes distintas y todos ofrecen algún modo de mostrar la revisión actual del firmware y el software de controlador, que le ayudará a saber si es necesaria una actualización para resolver un problema.

Conectar utilizando el Mac OS

Dado que Apple ha prestado soporte al estándar 802.11b durante tanto tiempo con su tecnología AirPort, conectar con un punto de acceso siempre ha sido un proceso bastante directo, ya sea con una Estación Base AirPort o con un dispositivo de otro fabricante.

Afortunadamente, la mayoría de las tarjetas AirPort vienen instaladas de fábrica cuando compramos un ordenador Macintosh; si necesita instalar una tarjeta posteriormente, siga las instrucciones que incluye la propia tarjeta y tenga cuidado al trabajar dentro de la máquina.

No importa qué sistemas operativos de Apple se utilicen, los antiguos Mac OS 8.6 ó 9, o el actual Mac OS X: tiene que configurar los ajustes de red y los ajustes de red inalámbrica.

Configurar los ajustes de red en Mac OS 8.6 ó 9.x

El primer paso para conectar con un punto de acceso es configurar los ajustes de red en los paneles de control TCP/IP y AppleTalk.

1. En el menú jerárquico Paneles de Control dentro del menú de la manzana, seleccione TCP/IP para abrir el panel de control TCP/IP.
2. En el menú Archivo, seleccione Configuraciones para abrir el cuadro de diálogo Configuraciones y ver las distintas configuraciones que puede tener (vea la siguiente figura 4.17).
3. Si hay una configuración llamada AirPort, selecciónela y haga clic en **Activar**. Si no es así, seleccione cualquier otra configuración, haga clic en **Duplicar** y llame a la configuración "AirPort" (o utilice cualquier otro nombre, pues no es importante). Después seleccione su nueva configuración AirPort y haga clic en **Activar**.

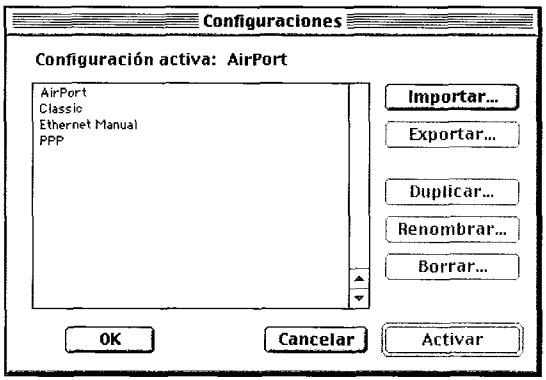

Figura 4.17. Creación de una nueva configuración AirPort.

Introducir claves WEP en un ordenador Macintosh

El software AirPort de Apple espera que utilicemos una Estación Base AirPort como punto de acceso. Cuando pide que introduzcamos la contraseña para la Estación Base AirPort, escribimos una contraseña en lugar de una verdadera calve WEP. Pero si estamos utilizando un Macintosh equipado con AirPort, tenemos que escribir 10 ó 26 caracteres hexadecimales.

Introducir la clave WEP hexadecimal funciona bien en las últimas versiones del software AirPort en Mac OS 9 y Mac OS X, cuando introducimos la clave WEP como respuesta a que se nos haya pedido. Mac OS 9 acepta una clave hexadecimal sin problemas.

Sin embargo, la petición de Jaguar de Mac OS X 10.2 ofrece opciones para lo que estamos introduciendo en un menú emergente (vea la figura 4.18). Seleccionar Contraseña *nos permite introducir una contraseña estilo AirPort. Las otras cuatro opciones corresponden a la longitud de la clave (40 ó 128 bits) y la codificación (ASCII o hexadecimal). Seleccione la opción ASCII apropiada sólo cuando su acceso WEP sea a través de una frase de paso. (Estas frases de paso WEP son convertidas en verdaderas claves WEP, pero no de la misma forma en que Apple convierte las contraseñas AirPort en claves WEP.)*

Con versiones anteriores del software AirPort y en el campo contraseña del panel Red *de las* Preferencias del Sistema *en Mac OS X, simplemente introducir la clave WEP no será suficiente. ¿El truco? Introduzca el signo de dólar ($) antes de la clave WEP hexadecimal y todo irá bien. El signo de dólar le dice al software AirPort que envíe la clave*

hexadecimal exacta al punto de acceso en lugar de interpretarla como una contraseña que se envía a la Estación Base AirPort.

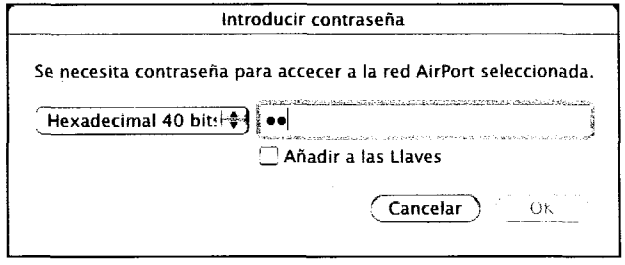

Figura 4.18. *Selección de opciones para contraseñas en Mac OS X 10.2 o superior.*

Para introducir una frase de paso estilo WEP en versiones anteriores del software AirPort o en el panel Red de las Preferencias del Sistema de Mac OS X, escríbala entre dobles comillas.
Hemos descubiertos que estas frases de paso WEP no siempre son compatibles entre sí y recomendamos utilizar verdaderas claves WEP hexadecimales en lugar de frases de paso siempre que sea posible al configurar puntos de acceso que no sean Estaciones Base AirPort.

4. De vuelta a la ventana principal del panel de control TCP/IP, seleccione AirPort en el menú emergente Conexión vía (véase la figura 4.19).

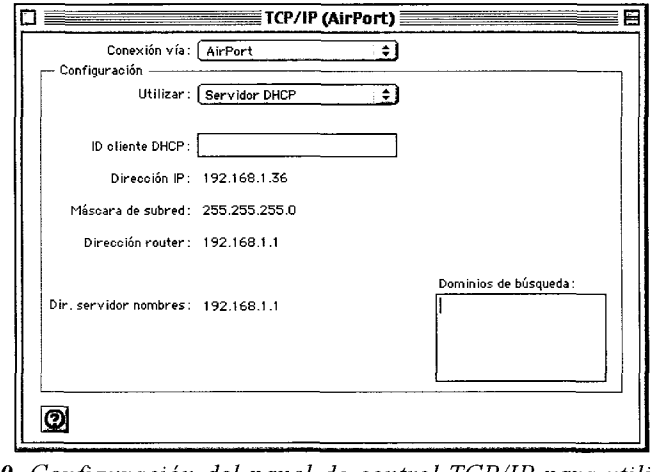

Figura 4.19. *Configuración del panel de control TCP/IP para utilizar AirPort.*

5. Suponiendo que va a conectar con una Estación Base AirPort u otro punto de acceso que tenga activado DHCP, seleccione Servidor DHCP en el menú emergente Utilizar. Si quiere utilizar una dirección IP estática, seleccione Manualmente en el menú emergente Utilizar e introduzca la dirección IP apropiada, la submáscara de red, la dirección de router y las direcciones de servidor DNS (Apple etiqueta este campo como "Dir. servidor nombres"). Si no está seguro de qué debe introducir aquí, vuelva al cuadro "Configurar a mano los ajustes de red" anterior en este mismo capítulo.
6. Cierre el panel de control TCP/IP y guarde los ajustes cuando le sea solicitado.
7. En el menú jerárquico Paneles de Control del menú de la manzana, seleccione AppleTalk para abrir el panel de control AppleTalk.
8. Siga de nuevo los pasos 2 y 3 para seleccionar o crear una nueva configuración AirPort.
9. En el menú emergente Conexión vía, seleccione AirPort (vea la figura 4.20).

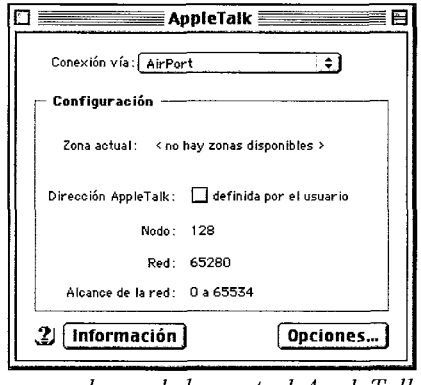

Figura 4.20. *Configurar el panel de control AppleTalk para utilizarlo con AirPort.*

10. Cierre el panel de control AppleTalk y guarde los ajustes cuando le sea solicitado.

Configurar AirPort en Mac OS 8.6 ó 9.x

Ahora que ya ha configurado los ajustes de red, es el momento de pasar a los ajustes específicos de AirPort. En estas versiones anteriores del Mac OS,

configuramos AirPort con la aplicación AirPort que se encuentra en la carpeta AirPort, normalmente instalada por defecto en la carpeta Aplicaciones o Apple Extras. También puede acceder a ella desde el módulo AirPort en la banda de control, si utiliza esa característica.

1. Abra la aplicación AirPort.
2. Haga clic en el triángulo de expansión Ajustes para ampliar la ventana y ver controles adicionales.
3. Seleccione la red deseada en el menú emergente Seleccionar red (vea la figura 4.21). O, si está en una red cerrada que no muestra su nombre, active la casilla de verificación Permitir la selección de redes cerradas, seleccione Otra en el menú emergente Seleccionar red e introduzca el nombre exacto de la red.

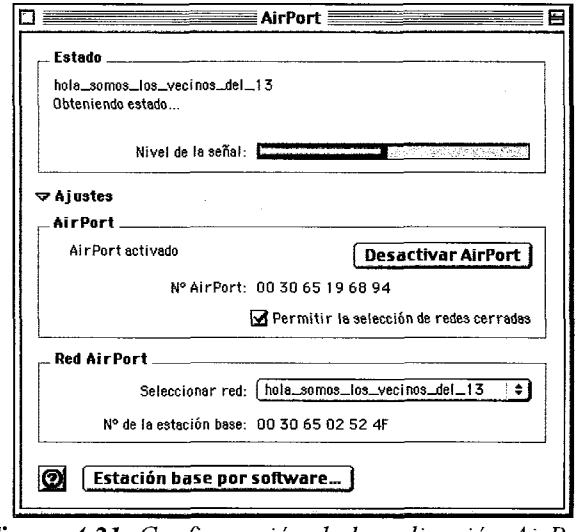

Figura 4.21. *Configuración de la aplicación AirPort.*

4. Si se le pide una contraseña para entrar en la red, escriba la contraseña de red de la Estación Base AirPort; si no está utilizando una Estación Base AirPort, lea el cuadro " Introducir claves WEP en un ordenador Macintosh" que hemos mostrado un poco antes para encontrar instrucciones sobre qué introducir.

¡Eso es todo! Si no hay ningún problema, debe estar conectado a la Estación Base AirPort o el punto de acceso, y si está compartiendo una conexión de Internet, podrá acceder a la Web con el navegador.

Configurar AirPort en Mac OS X

En Mac OS X, Apple integró los ajustes de red y de AirPort en el panel Red de Preferencias del Sistema, de modo que toda la configuración se desarrolla en un solo lugar. Siga estos pasos.

1. Seleccione Preferencias del Sistema en el menú de la manzana o haga clic en su icono en el Dock; una vez abiertas las Preferencias del Sistema, haga clic en el icono Red para abrir el panel de preferencias Red.
2. Seleccione AirPort en el menú emergente Configurar.

   Si AirPort no aparece en el menú, seleccione Configuraciones del puerto de red, seleccione la casilla de verificación Activo próxima a AirPort, y seleccione AirPort en el menú emergente Configurar.

   Cambia la visualización para mostrar la pantalla de configuración de AirPort.
3. Haga clic en la ficha TCP/IP y, en el menú Configurar, seleccione Usar DHCP si su dirección la asigna dinámicamente un servidor DHCP. Si quiere introducir una dirección IP estática, seleccione Manualmente e introduzca su dirección IP, máscara de subred, router y servidores DNS (vea la figura 4.22). Si no está seguro de qué debe introducir aquí, vuelva al cuadro "Configurar a mano los ajustes de red" anterior en este mismo capítulo.
4. Haga clic en la ficha AppleTalk y active la casilla de verificación Activar AppleTalk para permitir el paso de AppleTalk a través de la red inalámbrica junto con TCP/IP (vea la figura 4.23).

Truco *Con AirPort y otro método de red activo, como Ethernet, Mac OS X advierte que AppleTalk sólo puede funcionar en una de las redes. Sin embargo, a menudo hemos visto que AppleTalk fallaba completamente, incluso cuando sólo estaba activo en una de las redes.*

5. Haga clic en la ficha AirPort.

   Se presentan tres opciones: Acceder a la red con la mejor señal, Acceder a la última red utilizada disponible (y puede activar Recordar la contraseña de red) y Acceder a una determinada red (vea la figura 4.24). Con esta última opción, podemos elegir una red en el menú emergente próximo a Nombre de red.

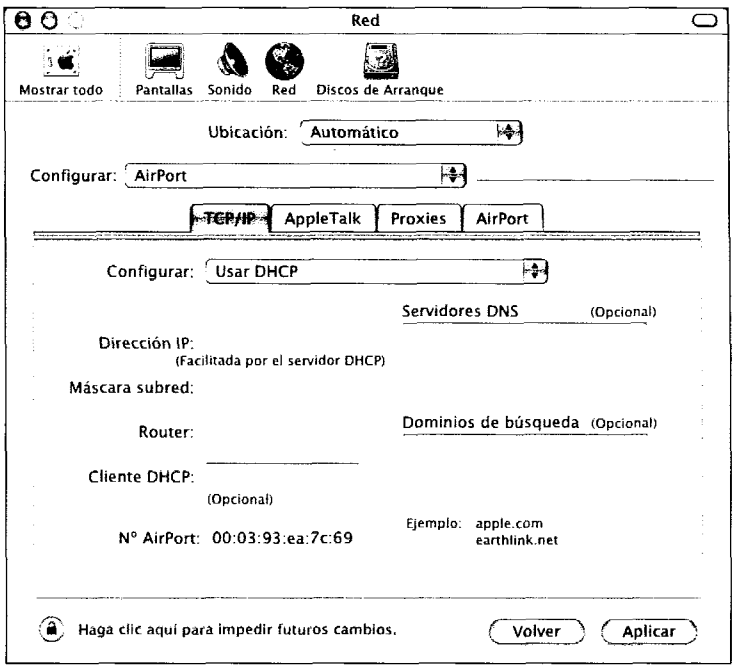

Figura 4.22. *Configuración de TCP/IP para utilizarlo con AirPort.*

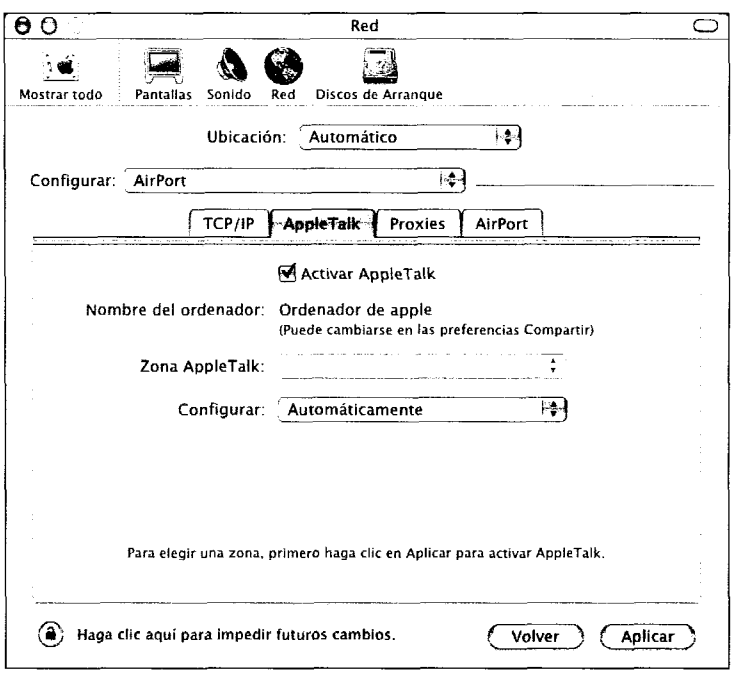

Figura 4.23. *Configuración de AppleTalk para utilizarlo con AirPort.*

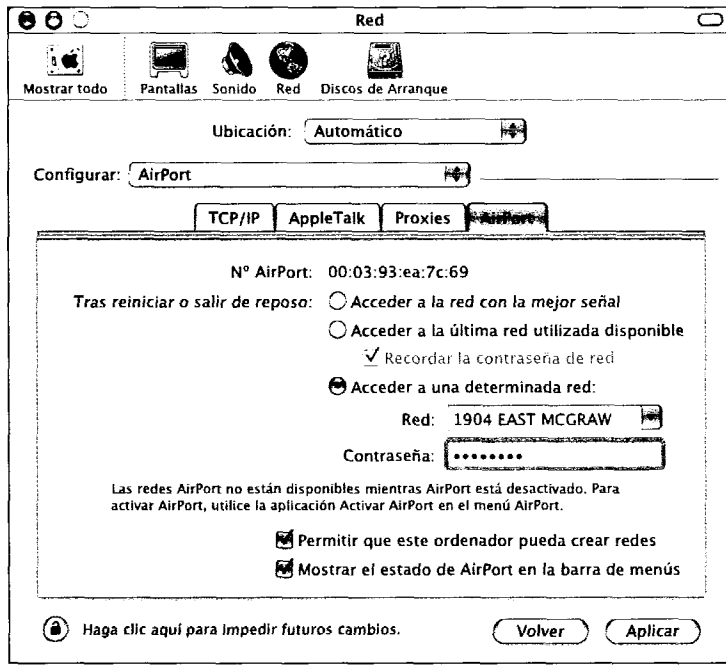

Figura 4.24. *Configuración de las opciones de selección de red AirPort en Mac OS X 10.2.*

6. Si piensa usar una red abierta que no tiene una contraseña la mayor parte del tiempo, seleccione Acceder a la red con la mejor señal. Si la red que más utiliza tiene contraseña o si quiere garantizar que siempre se une a la red que utilizó la última vez, seleccione Acceder a la última red utilizada disponible y active la casilla de verificación Recordar la contraseña de red. Por último, si tiene que unirse a una red cerrada, seleccione Acceder a una determinada red e introduzca su nombre en el campo Red. Si la red tiene habilitado el cifrado WEP, introduzca una contraseña en el campo Contraseña que aparece.
   Estas opciones aparecieron por primera vez en Mac OS X 10.2. En versiones anteriores, sólo se podía elegir o introducir un nombre de red y escribir una contraseña.
7. Haga clic en el botón **Aplicar** para activar los cambios.

Truco *Si viaja con frecuencia y descubre que necesita cambiar sus ajustes a menudo, puede crear varias ubicaciones utilizando el elemento Ubicación nueva en el menú Ubicación en la parte superior del panel de*

preferencias Red. Cada localización puede tener su propia configuración AirPort y es fácil cambiar entre ellas usando el menú Ubicación.

Configurar otro software cliente

La única ocasión en que puede necesitar usar un software cliente de red que no sea el software AirPort de Apple es si configura un adaptador de red inalámbrica de terceras partes en un viejo Macintosh que carece de ranura AirPort. Por ejemplo, los primeros PowerBooks, Power Macs e iMacs pueden conectarse inalámbricamente a través de PC Cards, tarjetas PCI o adaptadores USB Proxim.

Truco

Las PC Cards WaveLAN y Orinoco funcionan con el software AirPort de Apple porque las tarjetas AirPort son en realidad tarjetas Orinoco adaptadas.

Truco

La mayoría de las PC Cards de fabricantes centrados en Windows no vienen con software para Macintosh, pero puede comprar por unos 25 euros el controlador AeroCard Universal Driver de Macsense Connectivity. Visite www.xsense.com/product/broadband/aerouni.html para encontrar más detalles.

Afortunadamente, aunque el software cliente de red inalámbrica de terceras partes puede tener una apariencia ligeramente distinta al software AirPort de Apple, siempre requiere los mismos ajustes que hemos comentado anteriormente en el capítulo en el cuadro "Ajustes de conexión inalámbrica comunes", igual que sucede en el software cliente de terceras partes para Windows. Por ejemplo, conectar utilizando el software cliente Orinoco es prácticamente igual en Windows y en Mac OS.

Crear una red inalámbrica ad hoc

Los dispositivos Wi-Fi prestan soporte a dos modos de funcionamiento en red: el modo infraestructura en el que los clientes se conectan a puntos de acceso que actúan como centros de enrutamiento y un modo más informal lla-

mado ad hoc, que significa, en este contexto, "para el propósito particular actual". Las redes ad hoc (o entre equipos) se crean entre dos o más máquinas que actúan entonces como si estuvieran en una pequeña red.

Nota *Las redes ad hoc pueden ser enrutadas hacia otra red, como Internet, a través de una conexión de llamada telefónica o una red Ethernet. Comentaremos esto en "Crear un punto de acceso de software" en el capítulo 5.*

Ninguna máquina mantiene la red, pero continúa en efecto mientras haya una máquina en el modo ad hoc. De cualquier modo, una red de una sola máquina es como una isla desierta.

Truco *Las redes ad hoc pueden no funcionar correctamente entre adaptadores de red inalámbricos de distintas compañías comprados antes de 2002. Vea el capítulo 3 para más información sobre este tema.*

Cómo habilitemos el modo ad hoc en el ordenador varía dependiendo del sistema operativo y el software. Típicamente, habilitamos un ajuste en el software cliente que activa la red entre equipos o el modo ad hoc (fabricantes diferentes utilizan nombres distintos). También hay que elegir un canal a través del que se conectarán los dos ordenadores, pero una vez establecido un canal, otros ordenadores lo encontrarán automáticamente. Casi siempre se puede habilitar el cifrado WEP a través de una conexión ad hoc.

Nota *Afortunadamente, no es necesario configurar los ajustes de red cuando lo único que queremos hacer es conectar un par de ordenadores entre sí en el modo ad hoc. Eso es porque tanto Windows XP como Mac OS desde la versión 8.6 prestan soporte a un método estándar para seleccionar direcciones IP que no provoca conflictos.*

Crear una red ad hoc en Windows XP

El proceso de crear una red ad hoc en Windows XP requiere varios pasos, pero no son difíciles de llevar a cabo.

1. En Panel de control, seleccione Conexiones de red y después abra el cuadro de diálogo Conexión de red inalámbrica.

2. Haga clic en **Propiedades**.
3. Haga clic en la ficha Redes inalámbricas.
4. Haga clic en **Avanzadas** en la parte de abajo del cuadro de diálogo.
5. Seleccione Sólo redes de equipo a equipo (ad hoc) y desactive la casilla de verificación Conectar automáticamente a redes no preferidas (vea la figura 4.25).

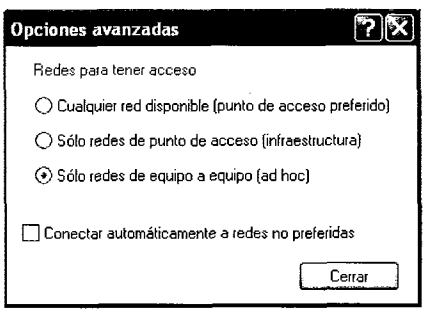

Figura 4.25. *Crear una red ad hoc en Windows XP.*

6. Haga clic en **Cerrar**.
7. Haga clic en el botón **Agregar** bajo Redes preferidas.
8. Introduzca un nombre de red para la red ad hoc (vea la figura 4.26).

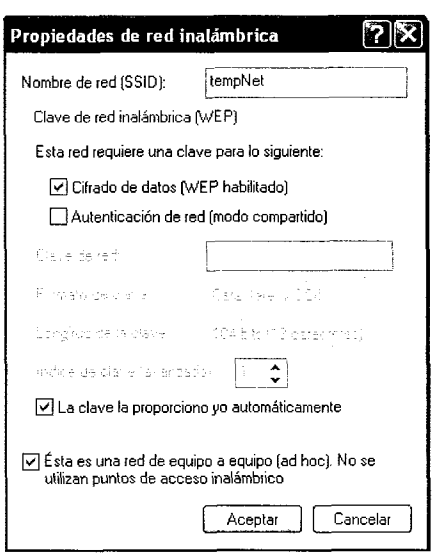

Figura 4.26. *Configurar una red entre equipos en Windows XP.*

Windows identifica las conexiones como ad hoc en la parte de debajo de la ventana utilizando un extraño método: una casilla de verificación activada pero en gris y deshabilitada.

9. Establezca las opciones WEP que desee.
10. Haga clic en **Aceptar**.

En la lista Redes preferidas, ahora aparece la red con un icono PC Card a su lado para indicar que es una red ad hoc. Una X roja en el icono indica que todavía no hay otros ordenadores conectados. Otros clientes Windows XP muestran esta red en su lista de Redes disponibles con el mismo icono.

Crear una red ad hoc con un Macintosh

Bajo Mac OS 8.6, 9 y X, crear una red ad hoc es una operación sencilla:

- En Mac OS 8.6 ó 9, abra la aplicación AirPort, haga clic en el triángulo de expansión Ajustes para ver más ajustes y seleccione Crear red de ordenador a ordenador en el menú emergente Seleccionar red en la sección Red AirPort (vea la figura 4.27). En el cuadro de diálogo De ordenador a ordenador, dé nombre a su red. Si quiere asignar una contraseña o cambiar el canal por defecto, haga clic en **Más opciones** e introduzca la información deseada. Haga clic en **OK** cuando haya terminado. (La siguiente figura muestra un botón **Menos opciones** porque hemos abierto las opciones extra.)

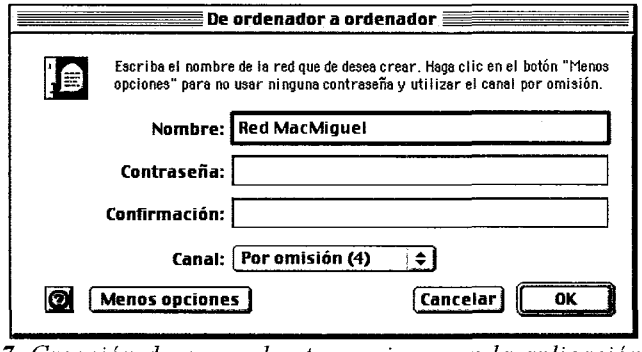

Figura 4.27. Creación de una red entre equipos con la aplicación AirPort en Mac OS 9.

- En Mac OS X, seleccione Crear red en el menú AirPort en la barra de menú o en el menú Red en la aplicación Internet Connect. De ambas

formas, en el cuadro de diálogo De ordenador a ordenador que aparece, introduzca el nombre de su red y escoja un canal. Si quiere proteger con contraseña su red ad hoc, active la casilla de verificación Activar encriptación (usando WEP) e introduzca su contraseña (vea la figura 4.28).

Una vez que ha creado una red ad hoc, otras personas pueden conectar con ella igual que harían con cualquier red inalámbrica, ya utilicen ordenadores Macintosh o PC con Windows.

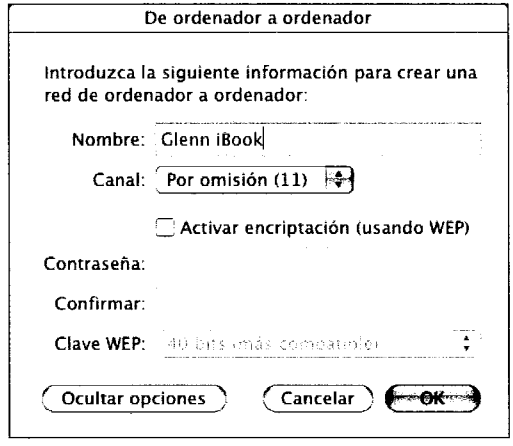

Figura 4.28. *Creación de una red entre equipos en Mac OS X.*

Compartir archivos

El propósito principal de la mayoría de la gente al configurar una red inalámbrica es compartir su conexión de Internet. Sólo en segundo lugar está el deseo de compartir archivos localmente o a través de Internet utilizando servidores de archivos locales en el mismo extremo de la red o remotamente. Se puede configurar la opción de compartir archivos en Windows y en Macintosh con relativa facilidad, e incluso podemos compartir archivos entre los dos sistemas operativos (con algunas excepciones).

Compartir archivos en Windows XP

Compartir archivos varía en las distintas versiones de Windows, aunque lo básico es igual. Nos vamos a centrar en XP, ya que es la versión más simple y nueva.

1. En el Panel de control, abra Conexiones de red, abra Conexión de red inalámbrica y haga clic en el botón **Propiedades** para abrir el cuadro de diálogo Propiedades.
2. Compruebe que están seleccionadas las casillas Cliente para redes Microsoft y Compartir impresoras y archivos para redes Microsoft y haga clic en **Aceptar** (vea la figura 4.29).

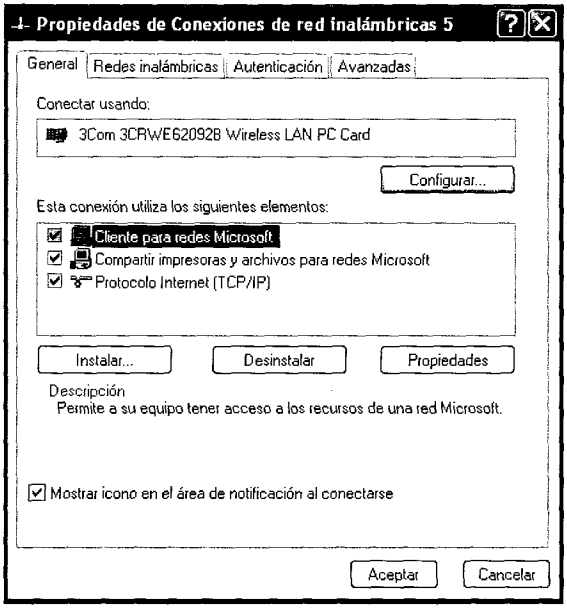

Figura 4.29. *Habilitar compartir archivos en Windows XP.*

3. Localice la carpeta que quiere compartir, haga clic derecho sobre ella y seleccione Compartir y seguridad.
4. En el cuadro de diálogo Propiedades, active la casilla Compartir esta carpeta, introduzca un nombre para la carpeta compartida (vea la figura 4.30) y haga clic en **Aceptar**.

Acceder a archivos compartidos en Windows XP

Una vez compartida una carpeta en Windows XP, podemos acceder a esa carpeta desde otros PC que utilicen el sistema Windows.

1. En otro ordenador, en el menú Inicio, escoja Mis sitios de red.
2. Haga clic en Ver equipos del grupo de trabajo. Por omisión, Windows muestra sólo las máquinas que están en nuestro mismo grupo de trabajo. Para llegar a ordenadores de otros grupos de trabajo, utilice la barra de direcciones en la parte superior de la ventana para ascender un nivel.

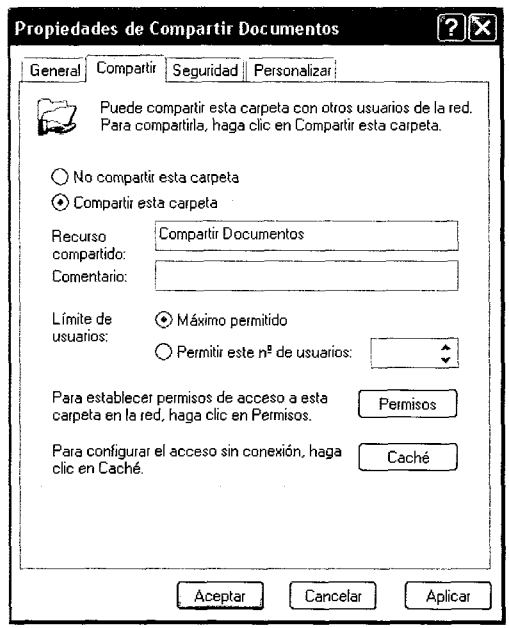

Figura 4.30. *Compartir una carpeta en Windows XP.*

3. Haga doble clic en el nombre del ordenador con el que quiere conectar.
4. Normalmente, Windows pide que introduzca el nombre y contraseña para acceder a ese ordenador; no es buena idea tener carpetas sin proteger, pero hay gente que todavía lo hace.

La carpeta compartida ya está montada y muestra listas de volúmenes disponibles en Mi PC y otras vistas. Podemos abrirlos y navegar por ellos como en cualquier otro volumen.

También podemos asignar una letra a una unidad de red con el comando Conectar a unidad de red del menú Herramientas para establecer que un volumen remoto se monte automáticamente con la misma letra de unidad cada vez que reiniciamos.

Compartir archivos en Macintosh

El proceso de compartir archivos es muy diferente dependiendo de si se utiliza Mac OS 9 o Mac OS X.

Configurar compartir archivos en Mac OS 9

En Mac OS 9, si va a ser la única persona que utilice los archivos comunes entre ordenadores, podrá saltarse algunos de los pasos de configuración. En caso contrario, debe recorrerlos todos.

1. En el menú jerárquico Paneles de Control del menú de la manzana, seleccione Archivos compartidos para abrir el panel de control Archivos compartidos.
2. En la ficha Iniciar/detener, compruebe que están introducidos el nombre de propietario y el nombre de ordenador. Si hay posibilidad de que alguien más puede acceder al ordenador Macintosh, introduzca una contraseña de propietario (vea la figura 4.31). Introduzca siempre una contraseña si habilita compartir archivos TCP/IP en el siguiente paso.

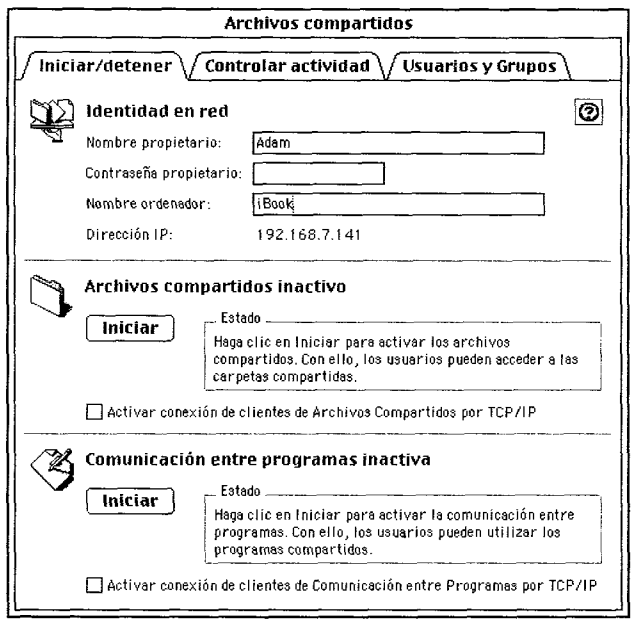

Figura 4.31. *Configuración del panel de control Compartir archivos en Mac OS 9.*

3. Haga clic en el botón **Iniciar** en la sección Archivos compartidos del panel de control y, si quiere que Compartir archivos esté disponible a través de TCP/IP además de AppleTalk, active la casilla de verificación Activar Conexión de clientes de Comunicación entre Programas por TCP/IP. Si va a ser la única persona que conecte con su ordenador desde otras máquinas, ya ha terminado, pues sólo necesita un nombre de propietario y una contraseña para conectar.

Nota

Habilitar la opción de compartir archivos a través de TCP/IP es necesario si queremos compartir archivos a través de Internet.

4. Haga clic en la ficha Usuarios y grupos. Puede crear usuarios y grupos si desea un control más preciso de quién puede acceder a cuáles carpetas, pero para esta situación, haga doble clic en el usuario predeterminado Invitado, seleccione Compartir en el menú Mostrar y active la casilla de verificación Permitir conexión a este ordenador (vea la figura 4.32).

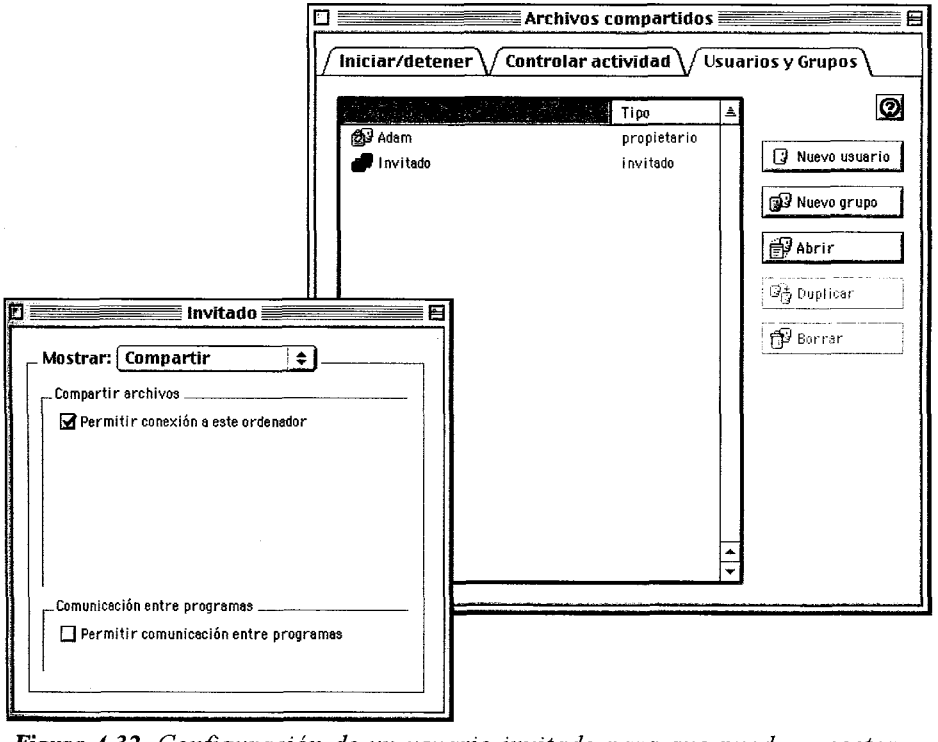

Figura 4.32. *Configuración de un usuario invitado para que pueda conectar.*

5. Seleccione un disco o carpeta a compartir, haga Control-clic sobre ella y en el menú jerárquico Obtener información, seleccione Compartir para abrir la vista Compartir de la ventana Obtener información (vea la figura 4.33).

Figura 4.33. *Compartir un disco en Mac OS 9.*

6. Active la casilla de verificación Compartir este ítem y su contenido y, en el menú emergente próximo a la línea Todos, elija los privilegios que quiere otorgar a otras personas que conecten con el ordenador.

Nota *Los privilegios Leer y escribir permiten a los usuarios ver, copiar, añadir y modificar archivos. Los privilegios Sólo leer permite ver y copiar archivos. Sólo escribir (buzón) permite que la gente ponga archivos en la carpeta sin que pueda ver nada más de lo que contiene. Y, por supuesto, Ninguno impide que se puedan ver o tocar archivos.*

7. Cierra la ventana Obtener información.

Configurar compartir archivos en Mac OS X

El proceso de compartir archivos en Mac OS X es un poco más fácil que en Mac OS 9.

1. Abra Preferencias del Sistema y haga clic en el icono Compartir para abrir el panel de preferencias Compartir.
2. En la ficha Compartir, seleccione la casilla de verificación Activo próxima a Compartir archivo. Si también quiere compartir archivos con usuarios de Windows o a través de FTP, active las casillas de verificación próximas a esos servicios (vea la figura 4.34).

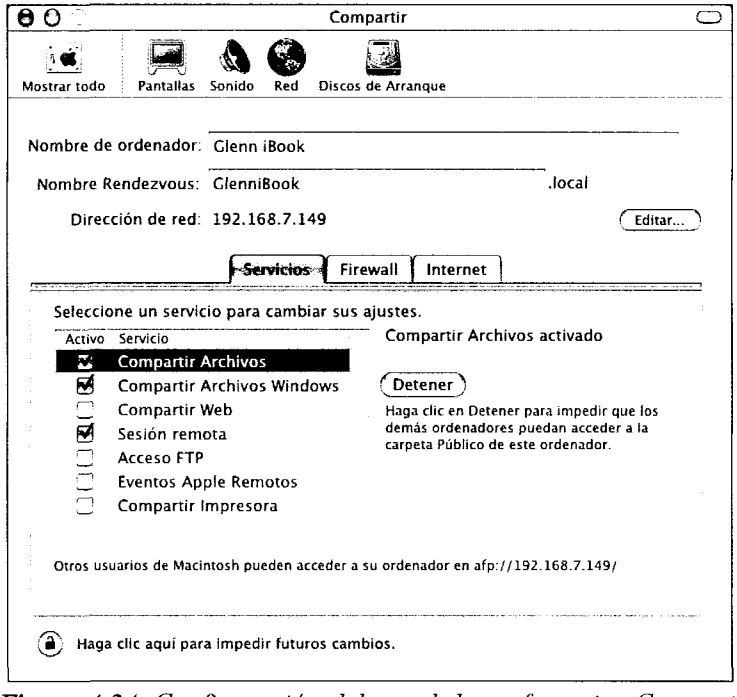

Figura 4.34. *Configuración del panel de preferencias Comparti en Mac OS X.*

3. Para compartir archivos, póngalos en la carpeta pública dentro de su carpeta de inicio; ya puede acceder cualquier persona a ellos.

Nota

Una vez que está activada la opción de compartir archivos, cualquiera que tenga una cuenta en la máquina Mac OS X puede acceder a ella utilizando un nombre de usuario y una contraseña, pero sólo pueden ver los archivos que están a su disposición cuando inician una sesión normal dentro de la propia máquina. Si la cuenta es de administrador, casi todo es visible.

Acceder a archivos compartidos en Mac OS 9

Una vez que un Macintosh tiene archivos compartidos, podemos acceder a ellos desde otros ordenadores Macintosh. Para acceder a ellos en Mac OS 9, siga estos pasos.

Nota *Si quiere acceder a archivos compartidos de un PC desde un Macintosh que utiliza el Mac OS 9, necesitará un programa llamado Dave de Thursby Systems. Visite www.thursby.com/products/dave.html para más información.*

1. En el menú de la manzana, seleccione Selector.
2. En el Selector, haga clic en el icono AppleShare.

   Si alguno de los Macintosh utiliza AppleTalk para compartir archivos, aparecen en la lista bajo Seleccione un servidor (vea la figura 4.35).

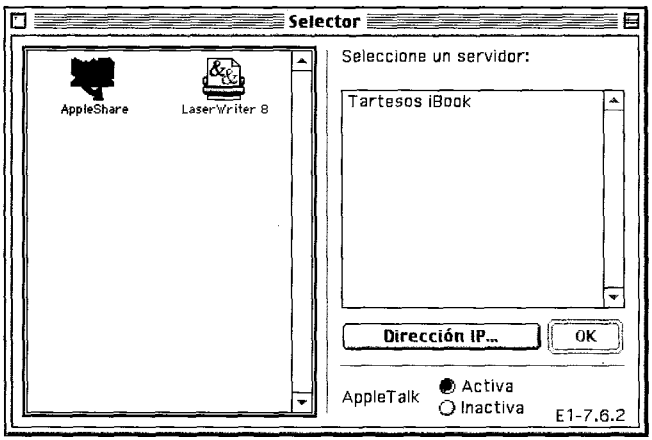

Figura 4.35. *Navegación por ordenadores Macintosh compartidos en el Selector.*

3. Haga doble clic en un ordenador de la lista o haga clic en el botón **Dirección IP...** e introduzca la dirección IP del servidor con el que quiere conectar y haga clic en el botón **Conectar** (vea la figura 4.36).
4. En el cuadro de diálogo, introduzca el nombre de usuario y la contraseña para la máquina que comparte los archivos a los que quiere acceder y haga clic en **Conectar** (vea la figura 4.37).

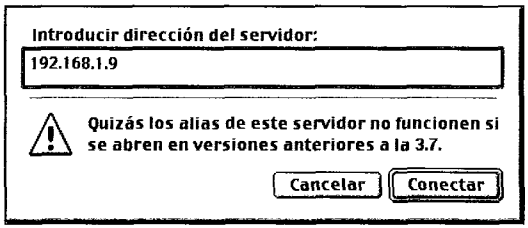

Figura 4.36. Introducir la dirección IP de un ordenador Macintosh compartido.

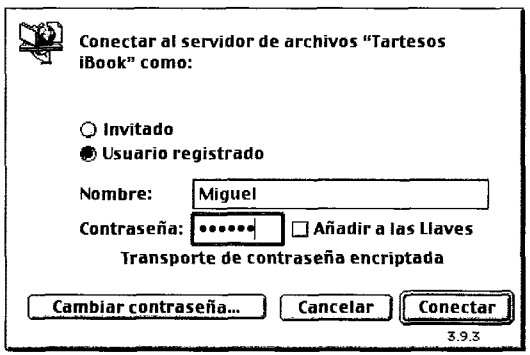

Figura 4.37. Introducir el nombre de usuario y la contraseña.

Active la casilla de verificación Añadir a las llaves si no quiere tener que escribir su contraseña cada vez que acceda a esta máquina Macintosh.

Nota

Aparece un cuadro de diálogo con una lista de volúmenes a los que puede acceder (vea la figura 4.38).

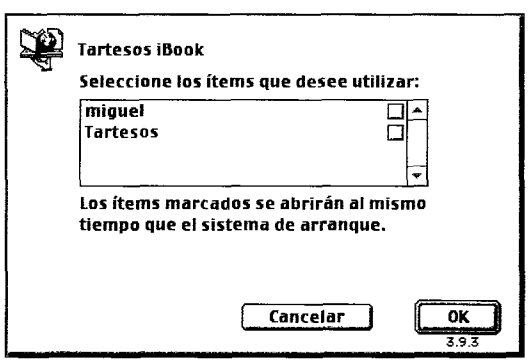

Figura 4.38. Selección de un volumen al que acceder.

5. Seleccione el volumen al que quiere acceder y haga clic en **OK**. El ordenador Macintosh con el que estamos conectando aparece en el escritorio como cualquier otro icono de disco, ¡ya hemos terminado!

Acceder a archivos compartidos en Mac OS X

Para acceder a archivos compartidos en Mac OS X, siga estos pasos:

1. En el menú Ir del Finder, seleccione Conectar al servidor para abrir el cuadro de diálogo Conectar al servidor (vea la figura 4.39).

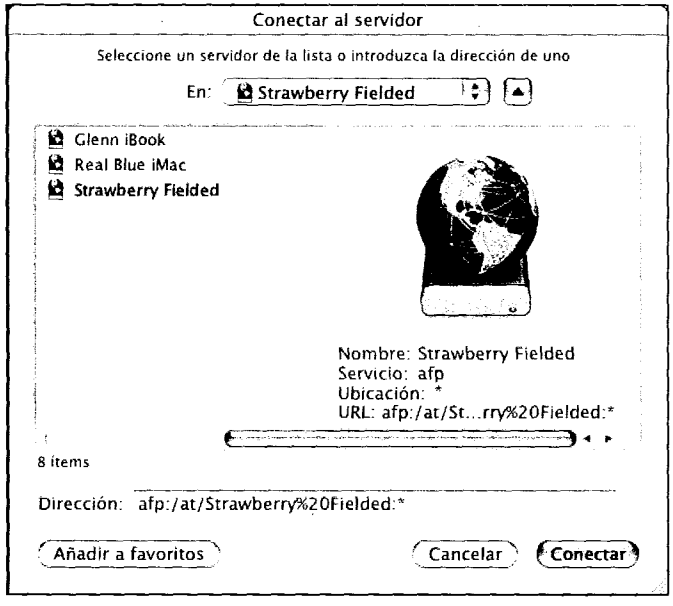

Figura 4.39. *Acceso a ordenadores Macintosh compartidos en el cuadro de diálogo Conectar al servidor en Mac OS X.*

2. Si el ordenador Macintosh al que quiere acceder aparece en la lista de servidores, haga doble clic sobre él para montarlo. En caso contrario, probablemente el Macintosh sólo comparte archivos utilizando TCP/IP; escriba su dirección IP en el campo Dirección en la parte de abajo del cuadro de diálogo y haga clic en **Conectar**.

Truco *No es necesario escribir afp:// al principio de la dirección si conecta con otro Macintosh que comparte archivos a través del Protocolo de archivo AppleTalk (AFP); sin embargo, para conectar con servidores*

Windows, FTP y WebDAV, hay que poner el prefijo smb://, ftp:// o http://, respectivamente, en la dirección IP o el nombre de dominio.

Se abre un cuadro de diálogo de conexión preguntando el nombre y contraseña (vea la figura 4.40).

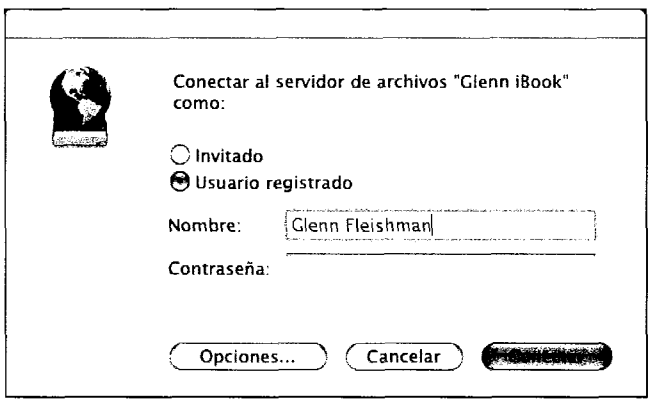

Figura 4.40. *Introducción del nombre de usuario y la contraseña.*

3. Introduzca su nombre y contraseña y haga clic en **Conectar**.

Truco

*Haga clic en **Opciones** y active la casilla de verificación Añadir contraseña a las llaves si no quiere tener que escribir la contraseña cada vez que acceda a esta máquina Macintosh.*

Aparece un cuadro de diálogo con una lista de los volúmenes accesibles (vea la figura 4.41). Si está conectando a una máquina Mac OS X con una cuenta de administrador, verá al menos dos volúmenes: uno el disco duro y otro el directorio de inicio.

4. Seleccione el volumen al que quiere acceder y haga clic en **OK**. El ordenador Macintosh al que está conectando aparece en el escritorio como cualquier otro icono de disco, ¡ya está!

De ordenadores a redes

En este capítulo nos hemos centrado en las tareas que hay que llevar a cabo con el ordenador para conectarlo a una red inalámbrica o a otro ordenador en

el modo ad hoc, y para compartir sus archivos. Pero conectar el ordenador a una red existente es sólo la mitad de la diversión, si quiere aprender a configurar toda una red inalámbrica, desde la planificación de la disposición hasta la compra del equipamiento para establecer la comunicación, empiece a leer el siguiente capítulo.

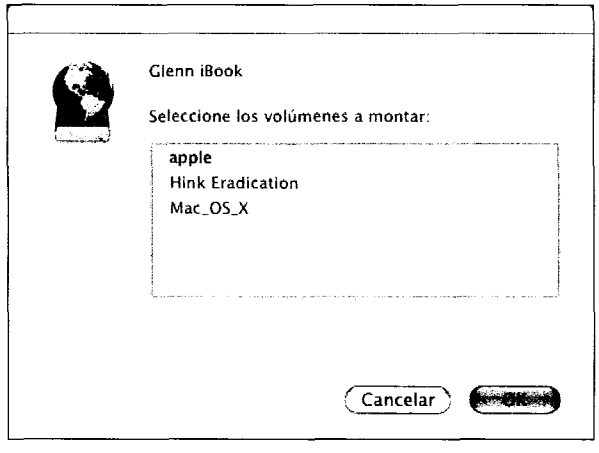

Figura 4.41. *Selección del volumen al que acceder.*

5. Construir la red inalámbrica

Un buen conocimiento teórico de la tecnología es algo maravilloso, pero no sirve de ayuda si somos incapaces de conseguir que nuestro aparato de vídeo deje de tener parpadeando la hora "12:00".

Igualmente, entender cómo funcionan las redes y cómo viajan las señales inalámbricas de un lado a otro puede servir de ayuda para planificar una red, pero todo será inútil si no conseguimos que las piezas de la red se comuniquen entre sí. Ése es el objetivo de este capítulo, proporcionar consejos prácticos que podrá utilizar al construir una red inalámbrica, con el objetivo de ayudarle a hacer todas las conexiones, ya impliquen hardware o software, cables u ondas de radio.

En este capítulo, recorremos los pasos necesarios para preparar una red. Mostramos como diseñar la red identificando todos los ordenadores y otros aparatos que quiera conectar. Después, le ofrecemos consejos para comprar una puerta de enlace inalámbrica, la pieza más importante de la red inalámbrica.

Por último, proporcionamos instrucciones para la configuración de puertas de enlace populares y llevar a cabo tareas como configurar un punto de acceso de software y crear puentes entre redes. Evidentemente, no pretendemos sustituir la documentación que acompaña al equipamiento de red que haya comprado, pero nuestra experiencia nos dice que la documentación describe partes

específicas de cada aparato, más que ayudar a conectar todos los puntos que forman la red final.

Planificar la red inalámbrica

Es tentador cuando pensamos en preparar una red comprar todas las piezas que pensamos que vamos a necesitar y conectarlas directamente. ¡Resístase a esa tentación!

La primera tarea que hay que llevar a cabo al pensar en crear una red o en hacer grandes cambios en una red existente, es dibujar un diagrama de la red, que es una imagen de cómo esperamos que encajen todas las piezas de la red. Dedicar un poco de esfuerzo a crear el diagrama aclara qué tenemos que comprar exactamente, revela errores que podríamos estar a punto de cometer, garantiza que no olvidemos alguna pieza esencial y facilita en general todo el proceso.

No piense que los diagramas de red sólo son necesarios para los poco avezados. Tenemos amigos que se ganan la vida instalando redes y siempre crean primero un diagrama de la red. La diferencia principal es que sus diagramas de red son fantásticos, mientras que los nuestros (por lo menos los de Adam) parecen hechos por un niño de preescolar (los diagramas que mostramos en este capítulo son cortesía del ilustrador profesional Jeff Tolbert). Afortunadamente, nadie va a criticar la estética de los diagramas de red, simplemente son una herramienta de referencia.

Un comentario final antes de profundizar en la creación de un diagrama de red: si tiene un programa de dibujo en su ordenador, es mejor que lo utilice, no tanto para que el diagrama quede más bonito como para tenerlo en un archivo en el disco duro y resulte fácil encontrarlo. Si hace un dibujo a mano sobre papel, archive el dibujo para que no sea fácil que se pierda. Tener a mano el diagrama de red posteriormente, facilitará que pueda hacer cambios en la red y, más importante, ayudará a resolver problemas si algo va mal.

Dibujar un diagrama de red

Imagine la siguiente situación, que, aunque es inventada, no es ni mucho menos exagerada. Amanda y Bob Quiggle trabajan en casa, ella como contable autónoma y él como programador.

El programa contable de Amanda se ejecuta en un PC de mesa, mientras que Bob escribe y prueba los códigos en un Power Mac G4, un PC de mesa y

un iBook de Apple. Tienen tres hijos, Sam, Chloe y Nick, cada uno con su propio ordenador. Sam está en su primer año en la universidad, vive en casa y tiene un PC portátil que utiliza constantemente, mientras que Chloe y Nick están todavía en el instituto y utilizan un Macintosh Quadra y un Power Mac que antes utilizaba su padre y que les ha dado para que hagan sus trabajos escolares y jueguen.

Los Quiggle acaban de mudarse a una nueva casa y quieren poner en red todos sus ordenadores para compartir una conexión de Internet por cable de módem y sus dos impresoras, una impresora USB color conectada al PC de mesa de Bob y una LaserWriter basada en LocalTalk más antigua. Quieren que sus portátiles se conecten a una red inalámbrica y el iBook de Bob y el PC portátil de Sam tienen adaptadores de red inalámbrica. Los ordenadores de mesa de la familia tendrán que estar conectados entre sí a través de Ethernet, aunque los Macintosh de Chloe y Nick no van a estar cerca del Power Mac y el PC de mesa de Bob, de modo que será necesario un concentrador adicional.

El principal problema es el PC de Amanda, que por estar en la oficina que se ha hecho en el sótano, inaccesible por otros métodos, conectará con el resto de la red a través de puentes HomePlug. En un principio Amanda pensó en instalar un adaptador de red HomePlug en su PC, pero quería dejar abierta la posibilidad de conectar ordenadores adicionales sin verse forzada a comprar más hardware HomePlug.

Nota

Las habitaciones inaccesibles son algo común en las casas. Glenn ayudó a un amigo a configurar una red en su casa de tres plantas y encontró una barrera impenetrable en la cocina de la planta baja. La fuerza de la señal llegaba bien hasta ese punto, aunque el punto de acceso estaba en la planta superior (donde se encontraba el módem de cable). Dando un paso más allá del umbral de la cocina, la señal desaparecía.

¿Le parecen demasiadas cosas a recordar? Estupendo, eso es exactamente lo que sucede con las redes en la vida real. Afortunadamente, un diagrama de red facilita que veamos rápidamente cómo deben conectarse las cosas.

Seguramente su red será distinta de la de los Quiggle, pero su diagrama de red le dará una idea del asunto. Y no piense que hace falta dibujar nada que no sean cuadros etiquetados, eso es lo que vamos a dibujar en las instrucciones.

Si va a dibujar la red sobre una hoja de papel, recomendamos que lea primero todas estas instrucciones antes de empezar, para que tenga una idea de dónde dejar espacio en blanco antes de empezar. Primero mostramos el diagrama terminado para que vea el resultado (vea la figura 5.1).

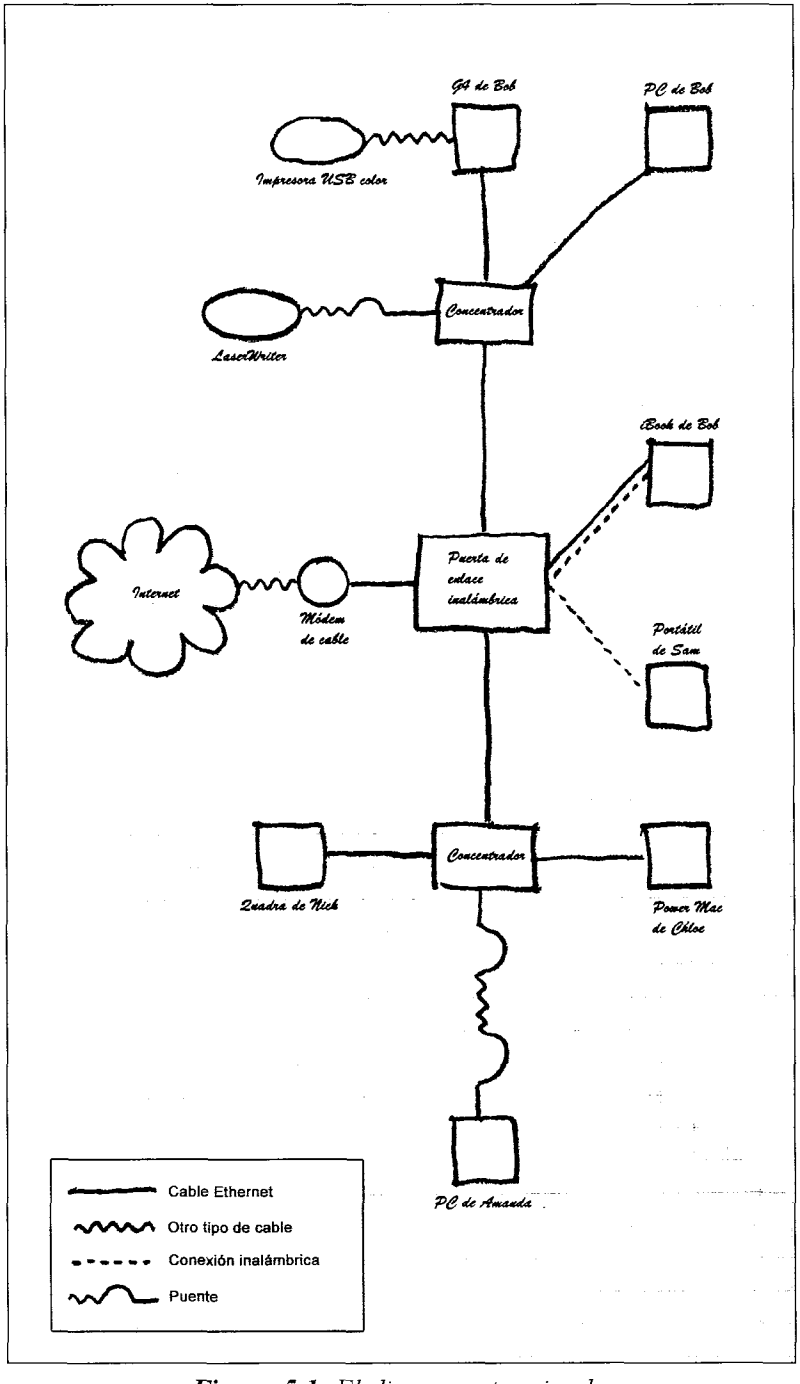

Figura 5.1. *El diagrama terminado.*

Nota

No pretendemos superponer este diagrama de la red sobre un plano de la casa: ese nivel de detalle es innecesario y puede resultar confuso, pues la posición física de los ordenadores puede no tener relación con dónde encajan en la red.

1. Por cada concentrador o punto de acceso inalámbrico (que, como se señaló en el capítulo 2, en esencia es un concentrador), dibuje un pequeño cuadro rectangular (vea la figura 5.2). Deje mucho espacio alrededor de cada rectángulo. La red de los Quiggle necesitará cuatro dispositivos concentradores (dos concentradores con cables y un punto de acceso inalámbrico con un concentrador integrado), pero como su puerta de acceso inalámbrica combina un punto de acceso y un concentrador normal, sólo hace falta dibujar tres aparatos.

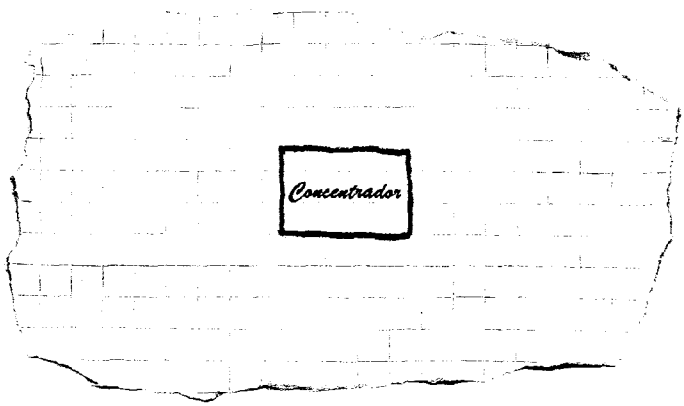

Figura 5.2. *Empiece por dibujar los concentradores de red.*

2. Cerca de cada uno de los rectángulos de concentrador, dibuje cuadrados que representen cada ordenador y, bajo cada cuadrado, escriba el nombre del ordenador para saber a qué ordenador corresponde cada cuadrado (vea la figura 5.3). Si tiene un dispositivo, como puede ser un punto de acceso inalámbrico, que combina un concentrador con cable y un concentrador inalámbrico, dibuje los ordenadores que se conectarán con cables a un lado del punto de acceso y los que se conectarán inalámbricamente al otro lado. Dibújelos en lados distintos para organizarlos por separado en el diagrama.
3. Si tiene una impresora que quiere compartir a través de la red, dibuje un óvalo (vea la figura 5.4). Donde coloque la impresora depende del tipo

de ésta. Si es una impresora USB conectada a un ordenador que la comparte a través de la red, dibuje la impresora cerca del cuadrado de ordenador y conéctela con una línea ondulada para indicar que están conectados por un método distinto de Ethernet. Si es un dispositivo de red de pleno derecho que se conectará a un concentrador, dibújela cerca del concentrador en cuestión. Si la impresora es tipo LocalTalk y requiere un puente para conectarse con la red, dibújela separada del concentrador al que se conectará y dibuje un arco para representar el puente. Los Quiggle tienen una impresora USB y una vieja LaserWriter basada en LocalTalk, de modo que las dibujamos conectando la LaserWriter a su puente con una línea ondulada.

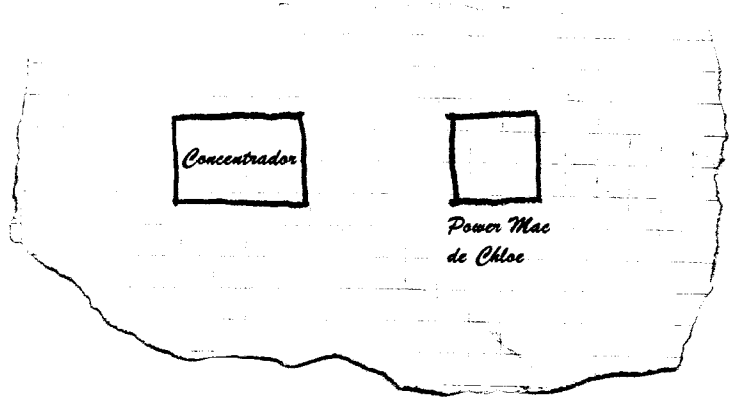

Figura 5.3. *Añada los ordenadores de la red.*

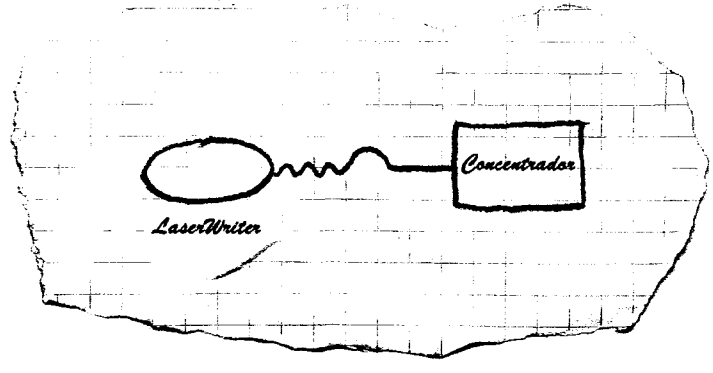

Figura 5.4. *A continuación dibujamos las impresoras y sus cables de conexión.*

4. En el lateral de la página, cerca del dispositivo que piensa usar como puerta de enlace, dibuje una forma de nube para representar Internet. Después dibuje un pequeño círculo para representar el módem de cable, el módem DSL o lo que sea necesario para conectar su red a Internet. Ponga una etiqueta apropiada, como hemos hecho con el módem de cable de los Quiggle (vea la figura 5.5).

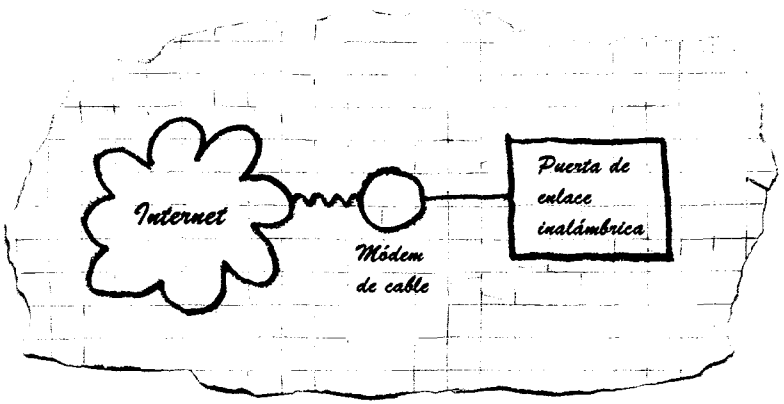

Figura 5.5. *Amplíe el diagrama añadiendo Internet y el dispositivo que utilizará para conectar con ella.*

Truco

Algunos módems de cable o DSL pueden conectarse directamente a un concentrador Ethernet, pero otros deben conectarse directamente a un dispositivo de puerta de enlace o un ordenador, como mostramos aquí.

5. Si, como Amanda, necesita conectar un ordenador al resto de la red utilizando puentes HomePlug o HomePNA, dibuje dos pequeños arcos (uno para cada puente) y una línea ondulada entre los puentes para mostrar la conexión (vea la figura 5.6).
6. Por último, conecte todos los ordenadores con cables con sus concentradores con líneas sólidas y conecte todos los ordenadores inalámbricos con sus puntos de acceso con líneas punteadas (vuelva a ver la figura 5.1 con el diagrama completo).

Nota

Es muy posible que un ordenador tenga dos adaptadores de red, uno para Ethernet de cable y otro para Ethernet inalámbrica, y cambie de uno a otro dependiendo de la situación. Si es éste el caso, dibuje el

ordenador entre los concentradores apropiados y conéctelo con una línea sólida y otra punteada. El iBook de Bob está dentro de esta categoría en la red que utilizamos como ejemplo.

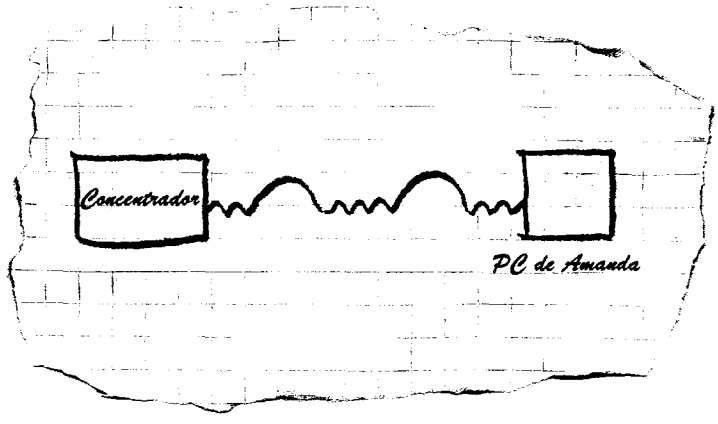

Figura 5.6. *Muestre los puentes necesarios.*

¡Ya está! Lo mejor de un diagrama de red es que podemos utilizarlo para determinar los dos siguientes pasos para crear la red: preparar la lista de la compra y configurar la red.

Localizar puntos de acceso

Hemos dicho anteriormente que no tiene sentido superponer un diagrama de red sobre un plano de la casa u oficina porque eso complica innecesariamente el diagrama. Eso es cierto, pero en algún momento hay que trasladar el diagrama a la casa u oficina. Este proceso requiere algunos recursos, pero pedir prestado equipamiento a un amigo puede ayudarnos a tomar decisiones sobre qué comprar.

En redes en los que todos los aparatos están a la vista de un punto de acceso, quizá no sea necesario reflexionar sobre la estructura de la red: basta con conectarlo todo y ya funciona. Pero en situaciones ligeramente más complicadas en las que, por ejemplo, la red tiene que atravesar paredes y suelos o desplegarse más de un centenar de metros, la planificación es crítica. Empecemos por la ubicación de la red.

- *Si la ubicación es la casa, sea realista al pensar dónde va a trabajar. ¿De verdad piensa trabajar tumbado en una hamaca en el*

jardín? ¿Sólo va a utilizar PC de mesa? Si es usuario de televisión por cable, ¿está seguro de querer añadir un adaptador de red inalámbrica para no desplegar un cable a través de varias paredes para conectar con la red Ethernet?

- *Si la ubicación es un edificio de oficinas, piense en las paredes interiores y la densidad de usuarios. ¿Qué distancia debe alcanzar la red con o sin paredes? ¿Es posible añadir un punto de acceso a la red con las conexiones de cable existentes o será necesario sacar un nuevo cable o configurar puentes?*
- *Piense también en sitios múltiples. ¿Es posible que quiera conectar su red con otras, quizá en oficinas o edificios distintos, o en la casa de un vecino?*

La mayoría de los sitios pequeños necesitan sólo un punto de acceso, pero si hay mucha distancia o paredes (especialmente paredes de ladrillo, pues los ladrillos pueden contener agua y el agua absorbe las señales 802.11b), hay que tener en cuenta la necesidad de utilizar varios puntos de acceso a lo largo de la red.
Aquí es donde puede servir de ayuda el equipamiento prestado: conecte un punto de acceso en una ubicación probable y pasee por el lugar con un portátil que tenga conexión inalámbrica observando el indicador de fuerza de la señal del software cliente de red inalámbrica. Con NetStrumbler o MacStrumbler, también puede ver una indicación de la fuerza de la señal mientras pasea (en el capítulo 6 comentaremos más detalles de estas herramientas). Todavía mejor, el software cliente Orinoco para Windows puede producir una gráfica con la fuerza de la señal a lo largo del tiempo, que podemos asociar con puntos de la casa u oficina. Si la ubicación inicial del punto de acceso no proporciona la cobertura deseada, cambie de ubicación y repita el proceso hasta que encuentre la posición ideal en la que colocar el punto de acceso.

Comprar y configurar

Para crear la lista de la compra, primero mire su diagrama de red y determine qué dispositivos de red necesita comprar. Por ejemplo, los Quiggle van a necesitar una puerta de enlace inalámbrico, un puente LocalTalk Ethernet para su LaserWriter, un par de concentradores Ethernet y un par de puentes

HomePlug Ethernet. Después mire cada ordenador y determine si necesita comprar para él un adaptador de red y, si va a conectar a través de Ethernet con cable, si necesita un cable. Quizá ya tenga parte del hardware y los cables, pero compruebe que son lo bastante largos para llegar a los puntos deseados. Es más rápido, más fácil y más barato comprar todo lo necesario al mismo tiempo que ir comprando una pieza de la red tras otra mientras averigua qué necesita a continuación.

Truco *Acepte nuestro consejo sobre la utilidad de planificar antes de comprar y configurar el equipamiento; queriendo compartir dos conexiones de Internet entre todos sus ordenadores, Adam configuró una red especialmente complicada cuando se mudó a su nueva casa. Como el diagrama de la red era tan complejo y pensaba estar quitando y poniendo distintos dispositivos, decidió seguir el proceso evolutivo. Todo acabó funcionando, pero tardó meses en terminar la red.*

Una vez que tenga todas las piezas, llega el momento de conectar los cables y configurar los ordenadores y dispositivos. Vuelva a repasar cada elemento del diagrama y conéctelos de acuerdo con el dibujo. Después coja cada elemento individualmente y configúrelo. Lo más importante es configurar la puerta de enlace para conectar con Internet, algo que se hace mejor usando un solo ordenador. (Más adelante en este capítulo encontrará instrucciones y consejos sobre la configuración de la puerta de enlace.)

Una vez que funcione la puerta de enlace, configure cada ordenador para que acceda a Internet a través de la puerta de enlace. Para ello, vuelva al capítulo 4. Configurar los archivos compartidos es lo que viene a continuación, y después garantizar que todos los demás ordenadores pueden conectar con las máquinas que comparten archivos. Si tiene impresoras que quiere compartir, compruebe que están configuradas para compartir y configure todos los ordenadores para que puedan imprimir en las impresoras compartidas. Si tiene problemas, vea el capítulo 9 para encontrar consejos para resolverlos.

Truco *Por nuestra experiencia, conectar con Internet es fácil, mientras que conseguir que funcionen las impresoras compartidas requiere más prueba y error con instalación de controladores y otras tareas desagradables. Afortunadamente, incluso aunque cueste algo de tiempo compartir las impresoras correctamente, siempre es posible imprimir desde el ordenador conectado directamente con la impresora en cuestión.*

Comprar una puerta de enlace inalámbrica

Un punto de acceso Wi-Fi técnicamente gestiona sólo las tareas relacionadas con permitir a los clientes asociarse con él y enviar datos de un lado a otro entre dispositivos inalámbricos. Todo lo demás son extras, pero extras que contribuyen a decidir qué pieza de equipamiento necesitamos.

La mayoría de los puntos de acceso orientados a oficinas contienen acuerdos de seguridad y autenticación, de modo que los sistemas que ya están en su lugar pueden permitir a los usuarios acceder al resto de la red. La red de oficina tiene un cortafuegos, asignación dinámica de direcciones y otro software para gestionar y proteger toda la red.

Los usuarios individuales y las pequeñas oficinas quizá necesiten también las mismas funciones utilizadas en organizaciones grandes, pero es mucho menos probable que haya sistemas que ya los proporcionen. También es posible que no dispongan del dinero y la experiencia necesarios para añadirlas. Aquí entra la puerta de enlace particular, una sola pieza de equipamiento que puede asignar direcciones, proteger máquinas locales, evitar el acceso de personas externas y hacer de puente para el tráfico entre conexiones con cable, inalámbricas y de banda ancha. Concretamente, estamos hablando de las puertas de enlace inalámbricas, que también tienen integrado un punto de acceso inalámbrico. Hemos descubierto que, a menos que se desee configurar una red corporativa, muchas de estas puertas de enlace inalámbricas tienen las funciones necesarias para hasta 50 usuarios, a pesar de la etiqueta "particular". Examinemos las características y opciones comunes que hay en las puertas de enlace inalámbricas y qué tenemos que tener en cuenta antes de comprar una. Para verificar la existencia de estas funciones, compruebe las especificaciones técnicas de la puerta de enlace o el manual, ambos disponibles generalmente en el sitio Web del fabricante. Como alternativa, póngase en contacto con el fabricante o distribuidor para preguntar directamente por estas funciones.

Nota

No recomendamos modelos específicos cuando hablamos de estas funciones porque el campo cambia tan rápidamente que cualquier recomendación podría estar anticuada cuando lea el libro.

Nota

Todos los protocolos y servicios de red mencionados aquí, como DHCP, NAT, PPoE y AppleTalk, se comentan con más detalle en el capítulo 2.

Nota *Los puntos de acceso baratos, como el Linksys WAP11, no tienen funciones de puerta de enlace y no deben confundirse con las puertas de enlace inalámbricas completas diseñadas para conectar la red inalámbrica con Internet.*

Interfaces de configuración

La mayoría de las puertas de enlace ofrecen una interfaz basada en Web para configurar los ajustes, reiniciar el dispositivo e instalar actualizaciones del firmware (el software integrado de la puerta de enlace). Algunas puertas de enlace requieren software registrado de Macintosh o Windows para gestionarlas, limitando innecesariamente su cuota de mercado pero facilitando su configuración en esas plataformas.

Un par de puertas de enlace utilizan programas sólo Windows que dan caza a la dirección IP consignada predeterminada de una puerta de enlace para conectar con ella, después de lo cual podemos configurarla completamente a través de una interfaz basada en Web. Algunas puertas de enlace basadas en Web utilizan herramientas Windows para la actualización del firmware o tienen limitaciones que impiden innecesariamente que herramientas basadas en Web efectúen las actualizaciones bajo Linux o Mac OS.

Puntos a considerar al comprar: Los usuarios de Macintosh deben comprobar que los puntos de acceso que están pensando comprar pueden configurarse completamente desde un ordenador Macintosh.

Servicios de red

Las puertas de enlace ofrecen una selección de servicios de red que permiten compartir una conexión y añadir máquinas sin necesidad de más configuración después la inicial.

Servidor DHCP

Prácticamente todas las puertas de enlace incluyen un servidor DHCP que ofrece direcciones IP a las máquinas locales. Estos servidores DHCP casi siempre funcionan también en el modo puente, que les permite proporcionar el servicio DHCP a través de una red local con cables y a clientes inalámbricos.

Algunas puertas de enlace limitan cómo podemos configurar un servidor DHCP. Por ejemplo, la Linksys EtherFast, un modelo popular, puede configu-

rarse para proporcionar un cierto número de direcciones empezando por una dirección IP de la red local. Por ejemplo, si tenemos tres ordenadores en la red 192.168.1.0, podemos hacer que nuestro servidor DHCP proporcione cinco direcciones DHCP (que pueden ser necesarias, por ejemplo, si tenemos tres ordenadores en uso y después dos invitados con sus propios portátiles que están de visita quieren conectar con Internet) empezando por 192.168.1.10 y llegando hasta 192.168.1.14.

Desgraciadamente, ninguno de los servidores DHCP de las puertas de enlace que hemos visto ofrece una opción útil: enlazar una dirección IP determinada con una dirección MAC de un adaptador de red. Esta opción sería útil en varias situaciones. Un ejemplo común implica conectar con una ordenador concreto a través de compartir archivos. Con direcciones IP y MAC enlazadas, podemos saber, por ejemplo, que nuestro iBook es siempre 192.168.1.10 y el equipo Windows 2000 es 192.168.1.11 sin tener que comprobar qué dirección IP han recibido más recientemente del servidor DHCP. Hacer que el servidor DHCP asigne la misma dirección IP a un ordenador determinado es también una combinación útil con servicios de activación o reenvío de puertos (que comentaremos más adelante en el capítulo). Esperamos que esta opción aparezca en puertas de enlace más sofisticadas del futuro.

Truco

Podemos sortear el problema de cambio de las direcciones IP ajustando el tiempo en que DHCP otorga el usufructo de una dirección para que sea lo más largo posible en algunos casos y cero en otros. El periodo de usufructo es el tiempo que puede tardar un ordenador en obtener una nueva dirección IP del servidor DHCP o en renovar las direcciones existentes. Un tiempo de usufructo largo o infinito puede garantizar a menudo que una máquina conserve la misma dirección IP.

Puntos a considerar al comprar: La puerta de enlace inalámbrica debe incluir un servidor DHCP si queremos que asigne direcciones dinámicamente a las máquinas de la red.

NAT

Casi todas las puertas de enlace prestan soporte a NAT (Traducción de direcciones de red), un servicio de red que posibilita que varios ordenadores compartan una sola dirección IP. NAT es especialmente útil porque la mayoría de los ISP de banda ancha ofrecen una sola dirección en la cuota mensual más baja. Con NAT, cuando la puerta de enlace recibe una dirección IP del ISP,

convierte en todas las solicitudes entrantes y salientes esa única dirección IP pública en las direcciones privadas internas de todos los ordenadores de la red local. Como sólo la dirección IP de la puerta de enlace es visible para el mundo exterior, NAT también proporciona un nivel extra de seguridad. NAT y DHCP colaboran entre sí, con NAT gestionando la traducción de direcciones y DHCP ofreciendo las direcciones privadas a los ordenadores.

Los servidores NAT pueden configurarse de varias maneras, pero la mayoría de las puertas de enlace carecen de sofisticación en este campo. Como mucho, podemos especificar sólo el número máximo de direcciones que un servidor DHCP puede ofrecer. (Esta opción debe incluirse además como un ajuste de servidor DHCP, no como un ajuste NAT.)

Puntos a considerar al comprar: Si hay que compartir una sola dirección IP, necesitamos un servidor NAT. Incluso aunque el ISP proporcione varias direcciones, podemos aprovechar la seguridad extra de una puerta de enlace con NAT.

Protocolos especiales

Sistemas operativos distintos tienen protocolos registrados diferentes para establecer la comunicación entre servidores de archivos e impresoras. Mientras que TCP/IP es un lenguaje universal, estos otros protocolos requieren cierta adaptación. Toda puerta de enlace admite TCP/IP, pero no todas ellas funcionan con protocolos registrados como NetBEUI de Microsoft. Todavía menos común es el soporte completo a AppleTalk de Apple. Por ejemplo, aunque la puerta de enlace Linksys EtherFast ofrece soporte no oficial a AppleTalk y este protocolo funciona bien entre ordenadores de red de cable u ordenadores de red inalámbrica, la puerta de enlace no hace de puente para AppleTalk entre ordenadores de red de cable *y* ordenadores de red inalámbrica. Al comprar una puerta de enlace, es muy importante qué protocolos gozan de soporte.

Puntos a considerar al comprar: Debemos comprobar qué protocolos vamos a usar (quizá sólo TCP/IP) y después confirmar que la puerta de enlace presta soporte a todos. AppleTalk, en concreto, goza de soporte sólo en algunas puertas de enlace, pero a menos que necesitemos conectar algunos ordenadores Mac antiguos o impresoras Apple, el soporte a AppleTalk puede no ser importante.

DNS dinámico

El servicio DNS normal asigna nombres de dominio a direcciones IP permanentes de ordenadores que actúan como servidores de Internet. Pero si el

ISP proporciona sólo una dirección IP dinámica y queremos ejecutar un servidor que pueda encontrar la gente en Internet, necesitamos DNS dinámico. DNS dinámico permite que los ordenadores que tienen direcciones IP cambiantes puedan ser encontrados a través de un nombre de dominio permanente. Cada vez que cambia la dirección IP del ordenador (cuando conecta con Internet, por ejemplo, o su tiempo de usufructo DHCP expira), un pequeño programa activa un servidor DNS para reestablecer que el nombre de dominio señale a la nueva dirección IP del ordenador. (También podemos activar este cambio manualmente a través de un sitio Web.) Para más información acerca de DNS dinámico, visite www.technopagan.org/dynamic/.

Algunos fabricantes de puertas de enlace han incorporado recientemente esta función directamente en su firmware, eliminando la necesidad de software adicional. Por ejemplo, la puerta de enlace MaxGate Ugate-3300 (www.maxgate. com.tw/tania/product_3300.htm) no sólo presta soporte a DNS dinámico internamente, también incluye una suscripción anual a un servicio DNS dinámico. Si acoplamos DNS dinámico con reenvío de puertos (que veremos en breve en este mismo capítulo), ¡podemos mantener un sitio Web permanente incluso con una dirección IP dinámica y traducción de dirección de red!

Puntos a considerar al comprar: Si queremos una dirección de host permanente (como www-adam.dyndns.org), resultará más fácil usar una puerta de enlace que preste soporte internamente a DNS dinámico que usar un software de DNS dinámico separado.

Seguridad y filtros

Podemos asegurar nuestra red para impedir que los malhechores roben contraseñas, fisguen el tráfico o incluso tomen el control de nuestros ordenadores. Para ver muchos más detalles concernientes a la seguridad, vea el capítulo 6.

Cortafuegos

La mayoría de las puertas de enlace ofrecen funciones de cortafuegos que permiten filtrar tipos especiales de tráfico que llegan desde el mundo exterior a la red. Algunas pueden filtrar el tráfico en las dos direcciones. La mayoría de estos cortafuegos son simples, permitiendo sólo o limitar el tráfico entrante no solicitado que no responde a una solicitud saliente o servicios de Internet específicos, como FTP.

Dado que muchas puertas de enlace incluyen también múltiples puertos Ethernet, podemos crear un cortafuegos no sólo entre la conexión de Internet

de banda ancha (conectada al puerto WAN) y los ordenadores y dispositivos inalámbricos, sino también entre la red inalámbrica y cualquier máquina conectada a los puertos LAN Ethernet de la puerta de enlace.

Algunos cortafuegos basados en puerta de enlace más sofisticados controlan los patrones de ataque y registran las violaciones del cortafuegos, ayudando a determinar la severidad de un ataque.

Puntos a considerar al comprar: Un cortafuegos en una puerta de enlace puede ayudar a proteger la red, sin dejar de permitir el acceso total de los usuarios legítimos.

Reenvío de puertos y activadores

Si utilizamos NAT o cortafuegos, puede resultar un poco más complicado que ordenadores en el exterior de la red local conecten con los ordenadores de la red aunque tengan permiso. Muchas puertas de enlace ofrecen una opción (llamada reenvío de puertos o asignación de puertos) para aliviar este problema. El reenvío de puertos funciona asociando el tráfico destinado a un puerto concreto a un ordenador de la red interna al que no se puede acceder de otro modo desde el exterior.

Por ejemplo, si queremos ejecutar un sitio Web público en una de las máquinas, podemos hacer que la puerta de enlace reenvíe el tráfico que llega al puerto 80 (el puerto reservado por omisión para los servidores Web) en la dirección IP estática asignada a la puerta de enlace al puerto 80 (o cualquier otro puerto) en una de las direcciones IP privadas en la red local.

Truco *Tenga en cuenta que las puertas de enlace sólo permiten una asignación un puerto-una máquina: esto es, no podemos ejecutar servidores Web en varias máquinas locales diferentes todos en el puerto 80. Hay formas de sortear esta limitación, pero requieren mucha experiencia y software potente apropiado.*

Nota *Si queremos reenviar todo el tráfico entrante a una máquina concreta, podemos usar una versión más amplia de reenvío de puertos, llamada DMZ (un uso muy inapropiado del término "zona desmilitarizada") o servidor virtual. Una función DMZ permite exponer una sola máquina al mundo exterior; está al alcance del exterior como si estuviera en Internet, aunque NAT está traduciendo todo el tráfico dirigido a esa máquina o procedente de ella.*

Los que juegan en red a menudo se encuentran con un problema relacionado, que es que algunos juegos de red requieren que el tráfico entrante vaya a un rango de puertos. La solución es una función llamada activadores. Cuando una máquina local intenta conectar en un puerto activador, la puerta de enlace nota la petición saliente y se reconfigura para permitir que el tráfico entrante vuelva a un rango de puertos en esa máquina local. Los activadores permiten así la interactividad en juegos de red. Si es aficionado a este tipo de juegos, busque en Google (www.google.com) instrucciones de configuración de puertas de enlace diferentes para distintos juegos.

Puntos a considerar al comprar: Si quiere exponer ciertos servicios en determinadas máquinas o desea utilizar juegos basados en Internet, necesita una puerta de enlace que preste soporte a reenvío de puertos y activadores.

Cifrado WEP

WEP (Privacidad equivalente de cable), que ayuda a impedir que gente no autorizada acceda a la red inalámbrica, es uno de los aspectos más complicados de la tecnología Wi-Fi que podemos encontrar. Todos los puntos de acceso y puertas de enlace inalámbricos que hemos visto prestan soporte a WEP, aunque algunos, como la Estación Base AirPort de Apple, lo enmascaran tras un aspecto más amigable. Para ayudar a controlar el acceso a la red, la puerta de enlace asigna una o más claves WEP que los usuarios deben introducir en el software cliente de red para asociarse con el punto de acceso e intercambiar datos. Algunas puertas de enlace todavía prestan soporte sólo a la versión de 40 bits más corta y menos segura de WEP, que a veces recibe el nombre 56 bits o 64 bits, pero es siempre lo mismo. Puertas de enlace más modernas ofrecen soporte a la versión completa de 128 bits de WEP, que es sólo ligeramente más segura. Muchas puertas de enlace requieren que pensemos una clave WEP e introduzcamos los 10 (claves de 40 bits) o 26 (claves de 128 bits) dígitos hexadecimales partiendo de cero. Varias ofrecen una función de frase de paso que genera una clave WEP a partir de algunas palabras que introducimos. Sin embargo, esta estrategia se considera menos segura porque las claves que crea el algoritmo de frase de paso son más predecibles.

Nota

Algunos adaptadores de red inalámbrica prestan soporte sólo a la clave WEP más corta de 40 bits. Aténgase a las claves WEP más cortas o compruebe que todos los adaptadores de red admiten la clave más larga antes de configurar la red para que utilice claves WEP de 128 bits.

La interfaz afecta al configurar claves WEP. Por ejemplo, hemos probado una puerta de enlace SMC Networks que oculta lo que se escribe al crear la clave WEP en su formulario de configuración basado en Web. Para empeorar las cosas, no requiere que escribamos dos veces la clave para confirmar la precisión. Una vez enviado el formulario de configuración, la puerta de enlace cambia la clave y si hay una errata oculta en lo que pretendíamos escribir no habrá forma de conectar con la unidad de forma inalámbrica. (Afortunadamente, la puerta de enlace también tiene puertos de cable, de modo que es posible conectar a través del cable Ethernet y corregir el error.)

Puntos a considerar al comprar: Como WEP es una herramienta de seguridad útil para usuarios domésticos y pequeñas empresas, compruebe si la puerta de enlace presta soporte a las claves WEP de 128 bits ligeramente más seguras.

VPN

Las VPN (Redes privadas virtuales) utilizan cifrado extremo a extremo para garantizar que el tráfico no será espiado o interceptado en forma legible entre la máquina de un usuario y el extremo final (un servidor VPN) dentro de una red de empresa. Hay dos protocolos muy utilizados para VPN, PPTP (Protocolo de túnel punto a punto) e IPsec (Seguridad IP). Si necesita usar VPN a través de la puerta de enlace, compruebe que ésta permite el paso del protocolo que utilice su empresa. El soporte varía mucho y cambia constantemente. Muchas puertas de enlace no ofrecían soporte al paso de IPsec hace sólo un año, pero ahora la mayoría lo admiten por su creciente uso.

Un problema relacionado es que si está utilizando NAT para convertir la dirección IP pública de la puerta de enlace en direcciones privadas de máquinas de la red local, puede haber problemas al usar una VPN. Compruebe en el escritorio de ayuda de su organización si las máquinas tienen las configuraciones sugeridas para sortear el problema.

Puntos a considerar al comprar: Si está utilizando una VPN para conectar con la red interna de su compañía, compruebe que la puerta de enlace que compra puede gestionar el protocolo necesario y pida recomendaciones al escritorio de ayuda de su organización.

Puertos de red

Las puertas de enlace vienen equipadas con distintos puertos para proporcionar métodos adicionales de comunicación por red.

La interfaz afecta al configurar claves WEP. Por ejemplo, hemos probado una puerta de enlace SMC Networks que oculta lo que se escribe al crear la clave WEP en su formulario de configuración basado en Web. Para empeorar las cosas, no requiere que escribamos dos veces la clave para confirmar la precisión. Una vez enviado el formulario de configuración, la puerta de enlace cambia la clave y si hay una errata oculta en lo que pretendíamos escribir no habrá forma de conectar con la unidad de forma inalámbrica. (Afortunadamente, la puerta de enlace también tiene puertos de cable, de modo que es posible conectar a través del cable Ethernet y corregir el error.)

Puntos a considerar al comprar: Como WEP es una herramienta de seguridad útil para usuarios domésticos y pequeñas empresas, compruebe si la puerta de enlace presta soporte a las claves WEP de 128 bits ligeramente más seguras.

VPN

Las VPN (Redes privadas virtuales) utilizan cifrado extremo a extremo para garantizar que el tráfico no será espiado o interceptado en forma legible entre la máquina de un usuario y el extremo final (un servidor VPN) dentro de una red de empresa. Hay dos protocolos muy utilizados para VPN, PPTP (Protocolo de túnel punto a punto) e IPsec (Seguridad IP). Si necesita usar VPN a través de la puerta de enlace, compruebe que ésta permite el paso del protocolo que utilice su empresa. El soporte varía mucho y cambia constantemente. Muchas puertas de enlace no ofrecían soporte al paso de IPsec hace sólo un año, pero ahora la mayoría lo admiten por su creciente uso.

Un problema relacionado es que si está utilizando NAT para convertir la dirección IP pública de la puerta de enlace en direcciones privadas de máquinas de la red local, puede haber problemas al usar una VPN. Compruebe en el escritorio de ayuda de su organización si las máquinas tienen las configuraciones sugeridas para sortear el problema.

Puntos a considerar al comprar: Si está utilizando una VPN para conectar con la red interna de su compañía, compruebe que la puerta de enlace que compra puede gestionar el protocolo necesario y pida recomendaciones al escritorio de ayuda de su organización.

Puertos de red

Las puertas de enlace vienen equipadas con distintos puertos para proporcionar métodos adicionales de comunicación por red.

Ethernet

Cada puerta de enlace lanzada recientemente tiene al menos dos puertos Ethernet: uno para la conexión WAN con el módem de banda ancha y otro para la conexión LAN, para conectarla a los ordenadores directamente o a un concentrador.

Los puertos Ethernet LAN pueden actuar como un concentrador o como un conmutador. Un concentrador es un fondo común de ancho de banda compartido, mientras que un conmutador separa el tráfico, permitiendo que cada puerto tenga todo el ancho de banda disponible. Esta distinción es útil si la red local tiene mucho tráfico, como será el caso si hay un servidor de archivos activo o incluso un programa de copia de seguridad de red que transfiere gigabytes de datos al llevar a cabo las copias.

La mayoría de las puertas de enlace ofrecen conexiones de sólo 10 Mbps en el puerto WAN, pues hay muy pocas posibilidades de obtener más ancho de banda para la red doméstica, y puertos de conmutación automática de 10/100 Mbps para la conexión LAN. (La conmutación automática permite que el puerto determine si el dispositivo conectado admite 10BaseT de 10 Mbps o Fast Ethernet de 100 Mbps). La mayoría de las puertas de enlace con varios puertos LAN también ofrecen al menos un puerto que puede actuar como conexión uplink, que es una forma de conectar con otro concentrador o conmutador sin utilizar un cable especial. Las puertas de enlace también ponen sus servicios de red (DHCP, NAT y cortafuegos) a disposición de los ordenadores conectados a los puertos LAN, igual que a los ordenadores conectados inalámbricamente. Algunas puertas de enlace ofrecen una opción que permite desactivar estas características en la LAN. Busque una casilla etiquetada "Puente DHCP", "Bridging DHCP" o algo similar.

Puntos a considerar al comprar: Incluso la red inalámbrica con menos cables probablemente incluirá uno o dos aparatos con cables, e incluso las puertas de enlace más baratas incluirán uno o más puertos Ethernet LAN. Si el rendimiento de la parte con cables es importante, compruebe que la puerta de enlace ofrece un conmutador en lugar de sólo un concentrador pasivo.

Módem

No todo el mundo tiene la fortuna de disponer acceso a Internet de banda ancha y, para aquellos que utilizan acceso telefónico para llegar al resto del mundo, una puerta de enlace con un módem incorporado es una bendición. Varios puntos de acceso tienen integrado un módem "56K" o un puerto serie RS-232C que puede conectarse a un módem externo o un módem ISDN (RDSI).

Truco *Dado que es posible compartir una conexión de llamada telefónica a través de un punto de acceso, Glenn pretende llevarse uno a la casa de sus suegros estas vacaciones para no tener que enchufar y desenchufar cables de teléfono frecuentemente y así poder trabajar en el piso bajo de la casa (más cálido).*

Nota *Como todos los módems modernos, los "56K" de las puertas de enlace inalámbricas pueden recibir datos a una velocidad sólo justo por encima de 50 Kbps, y esa velocidad es improbable en las condiciones del mundo real, donde las líneas de teléfono no son perfectas. Además, los módems "56K" envían datos a sólo 33,6 Kbps.*

Puntos a considerar al comprar: Si alguna vez necesita acceder a Internet a través de una conexión de llamada telefónica, busque una puerta de enlace con un módem o un puerto serie. Si tiene un puerto serie, compruebe con el fabricante qué módems valen para ese puerto.

Funciones de autenticación ISP

Muchos ISP de banda ancha efectúan algún tipo de inicio de sesión o prueba de autenticación para comprobar que se está utilizando un solo ordenador o sólo el ordenador que se ha registrado en el ISP. Es una limitación molesta e innecesaria y, en respuesta, muchos fabricantes de puertas de enlace han añadido funciones que permiten compartir una conexión simulando el aspecto de una conexión de un solo ordenador para el proveedor de banda ancha.

Cliente DHCP

Casi todas las puertas de enlace incluyen un cliente DHCP que puede solicitar una dirección IP al servidor DHCP del proveedor de banda ancha. Eso está bien, porque si no se admite que se coja una dirección IP a través de DHCP, las puertas de enlace no funcionarían con los ISP que entregan direcciones IP dinámicas. Una vez que la puerta de enlace tiene una dirección IP, puede utilizar NAT para proporcionar acceso Internet al resto de la red.

Algunos ISP utilizan el identificador de cliente DHCP, un campo registrado añadido a DHCP por Microsoft hace años que ahora goza de soporte por parte de todos para mantener la igualdad. El identificador de cliente es un bit de

texto extra enviado como parte de una solicitud de dirección por un cliente DHCP. Los ISP que utilizan el campo identificador de cliente a menudo requieren que se introduzca un texto específico, que ayuda a confirmar la identidad del usuario.

Puntos a considerar al comprar: Si el ISP le asigna una sola dirección dinámica, debe tener un cliente DHCP en su puerta de enlace y si su ISP requiere que utilice un identificador de cliente, compruebe que la puerta de enlace lo admite.

PPPoE

Algunos ISP de banda ancha utilizan una tecnología llamada PPPoE (PPP sobre Ethernet) como medida de seguridad y para controlar la duración de la sesión. En esencia, PPPoE trata a una conexión Ethernet siempre activa como si viajara a través de un módem. Con cuentas Internet que utilizan PPPoE, la puerta de enlace debe iniciar una sesión con nombre de usuario y contraseña antes de que el servidor DHCP del ISP proporcione una dirección IP y empiece a enviar el tráfico.

A los ISP les gusta PPPoE porque les permite controlar qué clientes están conectados en un momento dado y el tiempo que un cliente dado ha estado conectado. PPPoE también se integra con los servidores de autenticación que muchos ISP ya utilizan para sus clientes de llamada telefónica.

Puntos a considerar al comprar: No todas las puertas de enlace prestan soporte a PPPoE; determine, por tanto, si lo necesita para conectar con su ISP antes de comprar una puerta de enlace.

Clonación de direcciones MAC

Algunos proveedores de banda ancha utilizan direcciones MAC (la dirección Control de acceso a medios Ethernet única asignada de fábrica a todo adaptador de red) para limitar el acceso a una sola máquina. Algunos módems de cable, por ejemplo, escogen la primera dirección MAC que ven cuando se activan y funcionan sólo con esa dirección a menos que los apaguemos y volvamos a encender. Más problemáticos son los ISP que registran de verdad la dirección MAC de un solo ordenador y rechazan la conexión de cualquier otra dirección MAC a menos que pidamos al ISP que modifique la dirección MAC que tiene permiso para conectar. La solución a este problema es clonar o duplicar la dirección MAC de la máquina aceptada en la puerta de enlace; después de eso, los equipos del ISP piensan que la puerta de enlace es el ordenador que tiene permiso para conectar.

Puntos a considerar al comprar: No es probable que necesite esta característica, pero si su ISP funciona de esta manera, el soporte a la clonación de dirección MAC es inestimable.

Problemas de firmware y firmas

Tenga en cuenta un problema que Glenn se encontró al ayudar a un amigo a solucionar un problema de red. El ISP de su amigo le había dicho que necesitaba establecer una dirección IP para su puerta de enlace, una Linksys EtherFast, y usar PPPoE para conectar con su red. Después de una hora o más investigando los ajustes en la página de configuración principal del enrutador, Glenn estaba desconcertado. Podía conseguir que una sola máquina conectara directamente, pero no que lo hiciera la puerta de enlace.

Por fin, hizo lo que tenía que haber hecho primero: visitó el sitio Web de Linksys y descargó el firmware, o software interno, más actualizado para la puerta de enlace que estaban utilizando. Después de una corta instalación y de reiniciar el enrutador, Glenn tenía una pantalla de configuración principal nueva que separaba correctamente la selección de IP estática de PPPoE. No se pueden hacer las dos cosas y el ISP había llevado a confusión al amigo de Glenn. Había que utilizar sólo PPPoE que, a su vez, asignaba una dirección a la puerta de enlace. Las cosas que aprendemos siempre parecen obvias a posteriori, aunque en su día nos llevaran a darnos cabezazos contra la mesa.

Miscelánea

Hay otras cuatro variables que no encajan en ninguna categoría existente, pero que pueden jugar un papel en la puerta de enlace que escoja.

Distribución a impresora

Algunas puertas de enlace incluyen distribuidores a impresora, que permiten conectar una impresora directamente a un puerto de la puerta de enlace. Después enviamos las tareas de impresión al distribuidor de la puerta de enlace, que recibe las tareas rápidamente y las envía a la impresora. Tener oculto el distribuidor a impresora dentro de la puerta de enlace permite que no sea necesario tener la impresora conectada permanentemente a un ordenador que deba estar encendido siempre que alguien quiera imprimir.

Muchos de estos distribuidores a impresora funcionan sólo con impresión estilo Windows, desgraciadamente, que no goza de soporte en sistemas Mac sin un software extra como Dave de Thursby Software (www.thursby.com/products/dave.html). Algunos también gestionan impresión estilo LPR Unix, que es accesible tanto a sistemas Mac como a PC (y cualquier ordenador Unix o Linux).

Puntos a considerar al comprar: Si tiene una impresora que deba ser conectada a un ordenador a través del que se envían las tareas de impresión, puede pasar la tarea a una puerta de enlace.

Usuarios simultáneos

El número de máquinas que admite cada puerta de enlace varía y no hay que creer necesariamente las recomendaciones de los fabricantes. Hay una clara distinción entre el número máximo de direcciones IP que puede producir una unidad a través de DHCP (normalmente alrededor de 250) y el número de usuarios que puede admitir simultáneamente.

Muchas compañías proclaman que sus puertas de enlace pueden prestar soporte a todas las direcciones que el servidor DHCP puede repartir, no el número verdadero de usuarios que pueden utilizar simultáneamente la puerta de enlace. Si ve un número entre 35 y 50, es más probable que sea el número de usuarios real, mientras que un límite entre 100 y 250 no es realista en el equipamiento de consumidor. Los puntos de acceso orientados a empresas que se utilizan en organizaciones grandes pueden aceptar varios cientos de usuarios simultáneos, pero cuestan entre 500 y 1000€.

Puntos a considerar al comprar: Cuente el número de máquinas que necesitan conexión y, si está cerca del límite de usuarios, piense si merece la pena añadir puntos de acceso extra en lugar de sobrecargar un solo aparato de 150€.

America Online

Diez millones de personas conectan con America Online (AOL) cada semana, pero sólo hay una puerta de enlace que puede conectar con Internet a través de AOL y hacer que la conexión esté disponible inalámbricamente: la Estación Base AirPort de Apple. Se necesita el último software de AirPort con el modelo nieve actual de la Estación Base AirPort o el anterior modelo grafito. (La versión 2.0 del software AirPort actualiza la Estación Base AirPort para que admita AOL.) También es necesaria la versión 5.0 (Build 20.9) del software AOL para Macintosh. Tenga en cuenta que compartir su conexión AOL entre varios ordenadores requiere varias cuentas AOL.

Puntos a considerar al comprar: Si es usuario de Macintosh AOL, la decisión es fácil, dado que sólo le servirá la Estación Base AirPort. Desgraciadamente, los usuarios de Windows AOL no están de suerte, pues el software cliente Windows AOL no presta soporte a la Estación Base AirPort correctamente.

Coste

Los precios de las puertas de enlace varían bastante dependiendo de sus características. Algunas cuestan tan solo 100€, aunque la Estación Base de AirPort sigue costando unos 300€, tres años después de la presentación del producto. Tenga cuidado si quiere comprar las puertas de enlace más baratas, que generalmente no incluyen todas las funciones de puerta de enlace necesarias, como la asignación dinámica de direcciones y los puertos Ethernet. Afortunadamente, no hay que pagar mucho por tales funciones; por entre 130 y 150€ podrá encontrar todas las funciones que necesite y más.

Puntos a considerar al comprar: Las puertas de enlace baratas no son malas necesariamente, pero las muy baratas pueden carecer de funciones muy útiles.

Configurar una puerta de enlace

Anteriormente en este capítulo, en el cuadro "Localizar puntos de acceso", hemos comentado la tarea de colocar el punto de acceso para que la fuerza de la señal sea óptima. La siguiente tarea es configurar el punto de acceso para proporcionar acceso de red inalámbrico a los ordenadores y para conectar con la cuenta de Internet.

Configurar una puerta de enlace genérica

Para configurar cualquier punto de acceso, hay que introducir cierta información (vea la tabla 5.1). Afortunadamente, aunque esto puede parecer intimidante, la mayoría de las puertas de enlace vienen con una configuración predeterminada o pueden escoger algunos ajustes apropiadamente una vez que hemos hecho las conexiones necesarias. Otros ajustes los determinamos al planificar la red, acudiendo a la documentación del ISP o hablando con un amigo o colega que domine las redes.

Algunas puertas de enlace, como la Estación Base AirPort de Apple, ayudan con la configuración, y también nosotros; dentro de algunas páginas encontrará instrucciones para configurar la Estación Base AirPort, la popular Linksys EtherFast y puntos de acceso de software.

Nota

La mayoría de los elementos de la tabla se explican con más detalle en capítulos anteriores o en este mismo capítulo, en la sección "Comprar una puerta de enlace inalámbrica".

Tabla 5.1. *Ajustes de configuración comunes para puertas de enlace*

Ajuste	Qué otro nombre puede tener	Explicación	Ajustes y valores de ejemplo
SSID (Servicio identificador de seguridad)	Nombre de red, ESSID (SSID Extendido para redes con dos o más puntos de acceso)	Los clientes conectan con redes Wi-Fi por nombre. Para redes con varios puntos de acceso, todos deben tener el mismo nombre	Moonunit
Nombre de punto de acceso	Nombre de estación base, nombre de unidad	Cierto software de configuración utiliza este nombre para distinguir entre puntos de acceso accesibles	Bobmarley
Dirección IP	Dirección IP WAN	La dirección IP externa de la puerta de enlace. Con la mayoría de los ISP, la puerta de enlace coge esta dirección a través de DHCP, aunque también es posible introducirlo a mano	24.6.5.130
Puerta de enlace		La dirección IP del enrutador de Internet con el que conecta la puerta de enlace. De nuevo, DHCP normalmente los proporciona automáticamente	24.6.5.1

Ajuste	Qué otro nombre puede tener	Explicación	Ajustes y valores de ejemplo
Máscara de subred		La máscara de subred define el tamaño de la red local. DHCP la proporciona en la mayoría de los casos; en caso contrario, pregunte a su ISP	255.255.255.0
Servidores DNS	Servidores de nombres	Los servidores DNS son necesarios principalmente si la puerta de enlace actúa como servidor DHCP, de modo que las direcciones DNS puedan ser pasadas a los ordenadores cliente	24.6.15.100 24.6.15.22
Dirección IP local	Dirección IP LAN	La dirección de la puerta de enlace en la red interna	192.168.1.1
Canal		802.11b tiene 14 canales; sólo se permite utilizar algunos de ellos dependiendo del país; escoja entre los canales 1, 6 u 11 para puntos de acceso adyacentes en redes densas para evitar el solapamiento de las señales	6
Red cerrada	Red oculta	Oculta el nombre de la red a los navegadores casuales	
PPPoE	PPP sobre Ethernet	Se utiliza para iniciar una sesión en una cuenta Internet, frecuentemente con módems de cable	Nombre de usuario: tristane Contraseña: 98fink1e!
Cliente DHCP		Activa el cliente DHCP si la puerta de enlace necesita obtener su dirección IP de un servidor DHCP en lugar de usar una dirección estática	ID cliente DHCP:SWBELL001

Ajuste	Qué otro nombre puede tener	Explicación	Ajustes y valores de ejemplo
Servidor DHCP		Un servidor DHCP proporciona direcciones IP a ordenadores cliente de la red. Algunas puertas de enlace permiten escoger un rango de direcciones a utilizar y el periodo de tiempo que dura un usufructo DHCP	192.168.1.1-192.168.1.150 Tiempo de usufructo: 10 minutos
NAT	Traducción de direcciones de red, servidor de dirección privada	NAT está a menudo incluido en la opción de servidor DHCP, más que ser una opción independiente	
Cortafuegos	Filtrado	Restringe el tráfico procedente o dirigido a servicios concretos o direcciones IP	Vetar todo el tráfico procedente de la red 36.44.0.0
Reenvío de puertos	Asignación de puertos	Redirige las peticiones entrantes de un servicio específico a un puerto en una máquina concreta	El puerto 80 entrante en la puerta de enlace conecta con el puerto 8127 en la máquina 192.168.1.53
DMZ	Servidor virtual	Permite que una sola máquina aparezca como si fuera accesible directamente desde Internet en lugar de la puerta de enlace	
Activador		Habilita la compatibilidad con juegos que necesitan aceptar el tráfico entrante en determinados rangos de puertos	Cuando un ordenador local conecta con el exterior a través del puerto 3307, abre los puertos de entrada 4000-5000 a esa máquina

Ajuste	Qué otro nombre puede tener	Explicación	Ajustes y valores de ejemplo
SWEP	Cifrado, seguridad, contraseña de red	Permite que se utilicen hasta cuatro claves para cifrar todo el tráfico que pasa entre los adaptadores y el punto de acceso	F71A82FF0D
Diversidad de antena		Unidades con varias antenas que pueden tener asignadas una antena para recibir y otra para transmitir, o ambas para solapar estas funciones	
Velocidad de transmisión	Velocidad Tx, compatibilidad	Para compatibilidad total con 802.11b, las puertas de enlace deben utilizar velocidades menores; desactivando esto en redes pequeñas de corto alcance es posible mejorar el rendimiento general de la red	
Contraseña de administración		Todas las puertas de enlace que hemos visto permiten asegurar la configuración asignando una contraseña	ish234#kab
Direcciones MAC clónicas	Rescribir contraseña MAC	Permite cambiar la dirección Ethernet única del punto de acceso para que coincida, por ejemplo, con una dirección registrada de otra máquina a la que el ISP permite entrar en su red	08:23:1c:55:F4:0D
Firmware	Software actualizado	No es un ajuste, sino un control que suele permitir seleccionar un archivo de actualización firmware para descargarlo en la puerta de enlace, después de lo cual la puerta de enlace se reinicia	

Ajuste	Qué otro nombre puede tener	Explicación	Ajustes y valores de ejemplo
Ajustes de módem		Introducimos el número de teléfono del ISP y, a menudo, otro número alternativo, junto con información de nombre de usuario y contraseña	Número: 123-4567 Nombre de usuario: tristane Contraseña: 98fink1e!

Configuración de una Estación Base AirPort

La Estación Base AirPort de Apple es muy fácil de configurar por dos razones: sus ajustes están etiquetados claramente y sus propósitos están bien definidos; y además proporciona una pieza de software dedicado, la Utilidad de administración de AirPort, en lugar de una interfaz Web. (No es indispensable utilizar un Mac; vea el siguiente cuadro.) En Mac OS 9, puede encontrar la Utilidad de administración de AirPort en la carpeta Apple Extras dentro de la carpeta Aplicaciones. En Mac OS X, está anidada en la carpeta Utilidades de la carpeta Aplicaciones. Inicie el programa y empecemos con la configuración.

Truco

Apple actualiza frecuentemente su software AirPort. Compruebe que tiene instalada la última versión utilizando Software Update o visitando la zona de descarga de Apple.

Nota

A menudo, después de instalar una actualización de software AirPort, la siguiente vez que conectamos con la Estación Base AirPort, la Utilidad de administración de AirPort pide que actualicemos el firmware de la unidad. Antes de actualizar el firmware, es buena idea guardar la configuración de la unidad por si la actualización borra alguno de los valores.

La ficha AirPort

La ficha AirPort contiene la información básica acerca de la Estación Base AirPort, incluyendo detalles como el nombre de la unidad (usado para identifi-

carla en la Utilidad de administración de AirPort) y opciones como la persona de contacto y la ubicación (vea la figura 5.7). Podemos asignar una contraseña administrativa haciendo clic en **Cambiar contraseña**.

La sección Red AirPort permite asignar los ajustes básicos del punto de acceso. El Nombre es el SSID. Activar la casilla de verificación Crear una red cerrada impide que la Estación Base AirPort emita su nombre para que los usuarios casuales no puedan ver la red.

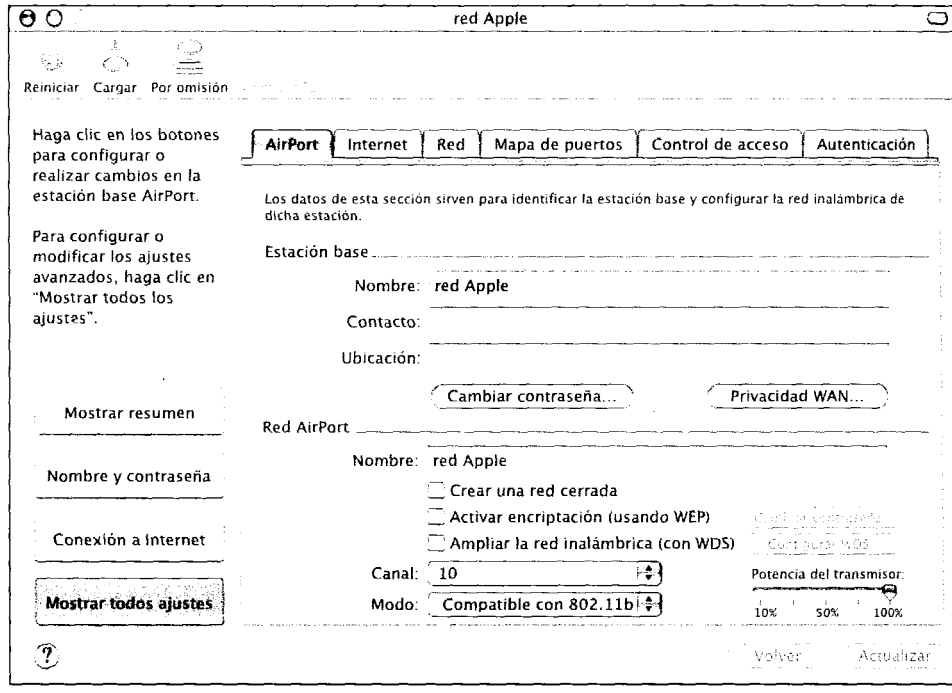

Figura 5.7. *Configuración de los ajustes básicos en la ficha AirPort de la Utilidad de administración de AirPort.*

Seleccione un canal en el menú emergente Canal. Habilite la casilla de verificación Activar encriptación (usando WEP) para activar el cifrado WEP; después introduzca aquí una palabra o frase.

Ficha Internet

En la ficha Internet, establecemos las opciones para conectar la Estación Base AirPort a un ISP (vea la figura 5.8). El menú Conectar vía permite elegir el método de red, como Ethernet, PPPoE, Módem o AOL. Si utiliza un módem de cable o DSL sin PPPoE, seleccione Ethernet.

Los valores que hay que introducir aquí son idénticos a los que utilizaríamos para conectar con el ISP desde un solo ordenador; acuda a la información proporcionada por el ISP para conocer detalles.

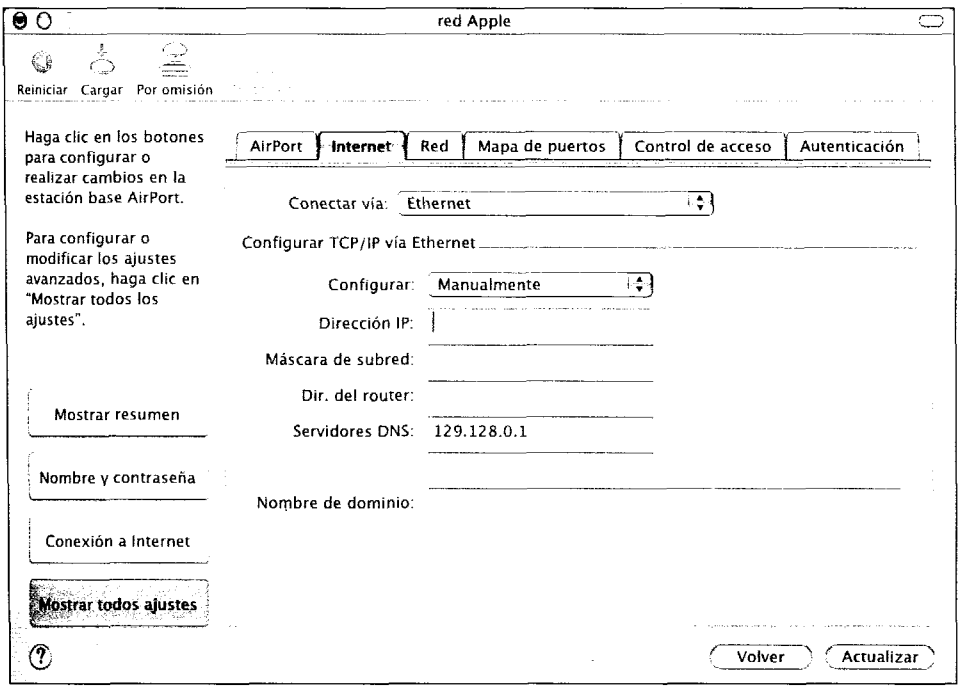

Figura 5.8. *Configuración de los ajustes de conexión a Internet en la ficha Internet de la Utilidad de administración de AirPort.*

Configuración sin una tarjeta AirPort o un Macintosh

Si no dispone de un ordenador Macintosh, o el que tiene no utiliza un Mac OS lo suficiente moderno para ejecutar la Utilidad de administración, puede usar una de estas dos herramientas para configurar una Estación Base AirPort:

- ***Un programa de configuración basado en Java que se ejecuta en varias plataformas:*** *Lo puede descargar de http://edge.mcs.drexel.edu//GICL/people/sevy/airport/.*
- ***La Utilidad de administración de AirPort Windows que no goza de soporte de Apple:*** *Puede descargarla de http://docs.info.apple.com/article.html?artnum=120093. Esta utilidad sólo la admite la versión nieve (snow) más nueva de la Estación Base AirPort.*

Naturalmente, siempre puede hacer igual que han hecho siempre los usuarios de Windows antes de que aparecieran estas utilidades: invitar a cenar a un amigo que tenga un iBook o un PowerBook. Una vez configurada la Estación Base AirPort, normalmente no se vuelve a usar nunca la AirPort Admin Utility.

Ficha Red

La ficha Red ofrece distintas opciones interrelacionadas que juntas proporcionan servicios de red como DHCP y NAT. La ayuda contextual en la parte de abajo de la ventana explica cada ajuste a medida que lo seleccionamos (vea la figura 5.9).

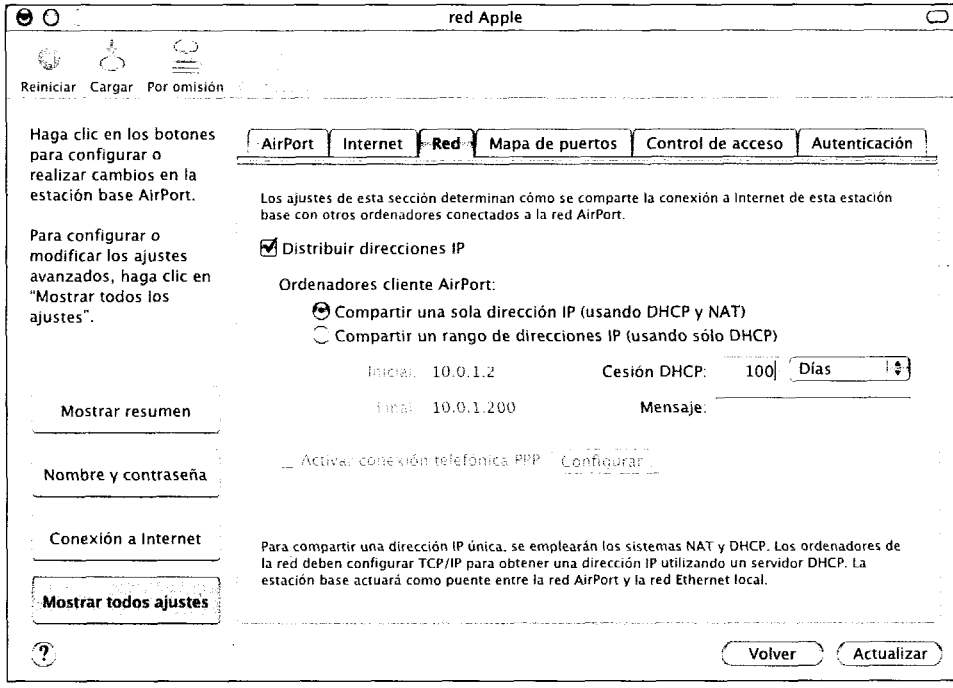

Figura 5.9. *Configuración de los ajustes de red en la ficha Red de la Utilidad de administración de AirPort.*

Seleccionando la casilla de verificación Distribuir direcciones IP activamos el servicio DHCP, que dice al servidor DHCP de la Estación Base AirPort que ofrezca direcciones IP a todos los ordenadores que conectan con ella. Hay

dos opciones para compartir las direcciones: usar NAT y DHCP o un rango de direcciones IP utilizando sólo DHCP. Hay que seleccionar NAT y DHCP si la conexión de Internet proporciona una sola dirección IP.

Nota *Un rango de direcciones debe contener direcciones legítimas de la red local.*

Fichas Mapa de puertos y Control de acceso

Las opciones en la ficha Mapa de puertos permiten asignar puertos externos a ordenadores de la red inalámbrica que queremos que sean accesibles desde Internet.

Hemos hablado de la asignación de puertos anteriormente en este capítulo en la sección "Comprar una puerta de enlace inalámbrica". La ficha Control de acceso ofrece opciones para controlar qué dispositivos de red inalámbrica pueden establecer una conexión con la Estación Base AirPort; para más información sobre cómo controlar el acceso utilizando dirección MAC, vea la sección "Impedir el acceso a la red" en el capítulo 6.

Conectar con una Estación Base AirPort sin una tarjeta AirPort

Los usuarios de sistemas PC y los usuarios de sistemas Mac con equipamiento antiguo pueden encontrarse con el problema de intentar conectar con una Estación Base AirPort de Apple sin tener acceso al software cliente AirPort de Apple. Eso no suele ser tan difícil como parece, pues conectar con una Estación Base AirPort es como conectar con cualquier otro punto de acceso. La única diferencia está en determinar la clave WEP utilizada para cifrar las comunicaciones.
Si está habilitado el cifrado WEP en la Estación Base AirPort, hay que usar la Utilidad de administración de AirPort de Apple para obtener la clave WEP no AirPort.

1. *Inicie la Utilidad de administración de AirPort.*
2. *Conecte con la Estación Base AirPort.*
3. *En la lista de iconos en la parte superior de la ventana, haga clic en* ***Contraseña*** *o seleccione Contraseña equivalente de red en el menú Estación Base.*

Si no dispone de un ordenador Mac que pueda ejecutar la Utilidad de administración de AirPort, intente utilizar una de las dos herramientas señaladas en el cuadro anterior.

Guardar los cambios

Después de hacer cualquier cambio, haga clic en el botón **Actualizar** en la parte de abajo de la ventana para guardar los cambios y reiniciar la Estación Base AirPort con los nuevos ajustes.

Configuración de una Linksys EtherFast

La puerta de enlace de extenso nombre Linksys EtherFast Wireless AP + Cable/DSL Router w/4-Port Switch (número de modelo BEFW11S4) es una de las que más se venden en la actualidad, siendo un buen ejemplo de punto de acceso que utiliza una interfaz basada en Web.

Las interfaces basadas en Web que utilizan otras puertas de enlace utilizan información muy similar.

Nota *Linksys fabrica varios modelos EtherFast, pero cuando hablamos de EtherFast en esta sección, nos referimos específicamente al modelo BEFW11S4. Las interfaces Web de los otros modelos son prácticamente iguales, dependiendo de las funciones que gozan de soporte en un modelo dado.*

Para conectar a través de la interfaz Web de EtherFast, el ordenador debe estar en la red privada 192.168.1.0; vea el próximo cuadro para configurar correctamente el ordenador. Recién sacada de su caja, la EtherFast tiene asignada la dirección IP 192.168.1.1 y su contraseña por omisión es sólo *admin* (no es necesario un nombre de usuario).

Una vez configurado el ordenador correctamente, abra un navegador Web y en su campo Dirección, escriba 192.168.1.1 y pulse **Intro** o **Retorno**. El navegador conecta con el servidor Web integrado en la EtherFast y presenta un cuadro de diálogo en el que introducir la contraseña. Escriba admin como contraseña y vuelva a pulsar **Intro** o **Retorno** para convencer a la EtherFast de que tiene permiso para configurar la puerta de enlace.

Nota

Aunque la EtherFast no permite a nadie externo a la red privada local manipular la puerta de enlace, incluso aunque tenga contraseña, sigue siendo necesario cambiar la contraseña por omisión en la ficha Password para impedir que alguien conecte a través de una conexión inalámbrica y cambie los ajustes. Si sucediera esto, el único recurso sería reestablecer en la EtherFast los ajustes de fábrica predeterminados y volver a configurarla.

El manual de la EtherFast es bastante bueno y contiene muchos detalles, pero vamos a comentar algunos puntos destacados de las fichas de la interfaz y a traducir la nomenclatura no estándar de Linksys a términos Wi-Fi más comunes.

Configurar el ordenador para efectuar los ajustes iniciales

Para configurar un punto de acceso con un servidor Web integrado que tiene su dirección IP predeterminada en una red privada (usualmente la red 192.168.1.0), hay que establecer las opciones de red del ordenador para que se encuentre en la misma red. Generalmente esta conexión inicial se efectúa a través de un cable Ethernet, no inalámbricamente, aunque el resto de la configuración posterior se puede llevar a cabo a través de la conexión inalámbrica.
Para configurar Windows XP:

1. *Abra el Panel de control, abra Conexiones de red y abra el dispositivo de Conexión de área local correspondiente al adaptador Ethernet.*
2. *Haga clic en la ficha General.*
3. *Seleccione Protocolo Internet (TCP/IP) y haga clic en* ***Propiedades****.*
4. *Para no modificar una conexión existente, seleccione la ficha Configuración alternativa.*
5. *Seleccione el botón de opción Configurada por el usuario.*
6. *Asigne 192.168.1.49 a Dirección IP, 255.255.255.0 a Máscara de subred y 192.168.1.1 a Puerta de enlace. Puede dejar en blanco el resto de los campos (vea la figura 5.10).*
7. *Haga clic en* ***Aceptar.***

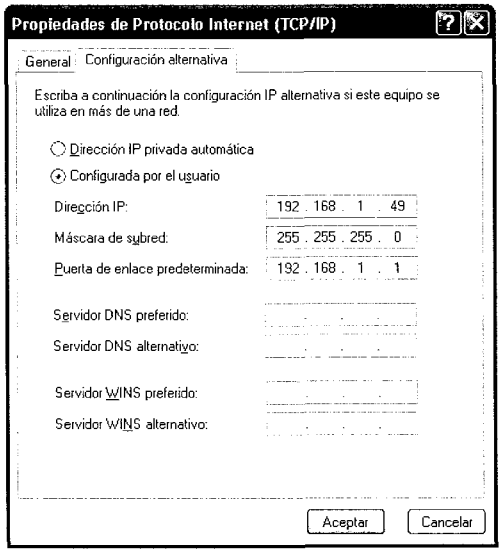

Figura 5.10. *Configuración de Windows XP para conectar con un punto de acceso por primera vez.*

Para configurar Mac OS X:

1. *Abra el panel de preferencias Red y seleccione las configuraciones de puerto de red en el primer menú emergente Configurar.*
2. *Haga clic en el botón* ***Nueva****, seleccione Built-In Ethernet e introduzca como nombre Configuración privada.*
3. *Compruebe que está seleccionado el cuadro próximo a Configuración privada y seleccione Configuración privada en el menú Configurar.*
4. *En la ficha TCP/IP, asigne 192.168.1.49 a Dirección IP, 255.255.255.0 a Máscara de subred y 192.168.1.1 a Router (vea la figura 5.11). Puede dejar en blanco el resto de los campos.*
5. *Haga clic en* ***Aplicar****.*

Después podrá deshabilitar o eliminar estas configuraciones de red si quiere.

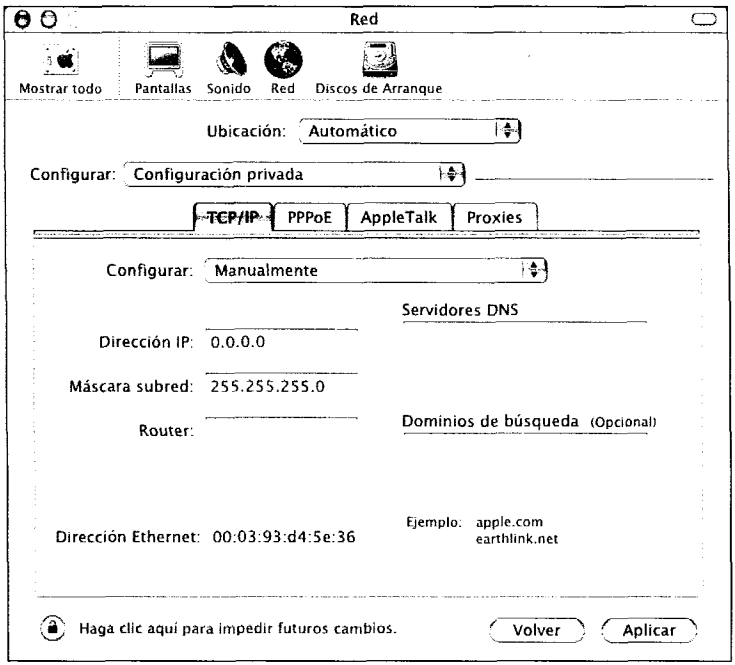

Figura 5.11. *Configuración de Mac OS X para conectar con un punto de acceso por primera vez*

Ficha Setup

La ficha Setup contiene todos los ajustes básicos necesarios para configurar el punto de acceso y la conexión a Internet de EtherFast (vea la figura 5.12).

Truco

Si su modelo de EtherFast es el mismo que estamos configurando aquí, pero su interfaz es algo distinta, visite el sitio Web de Linksys y compruebe si hay alguna nueva versión del firmware. Como puede ver, estamos utilizando la versión 1.42.7 del 23 de abril de 2002, pero versiones anteriores pueden tener una apariencia distinta.

Podemos habilitar o deshabilitar la red inalámbrica, establecer el SSID y seleccionar un canal. Si desactivamos Allow "Broadcast" SSID to Associate, creamos una red cerrada que los usuarios casuales no pueden ver en su lista de redes disponibles.

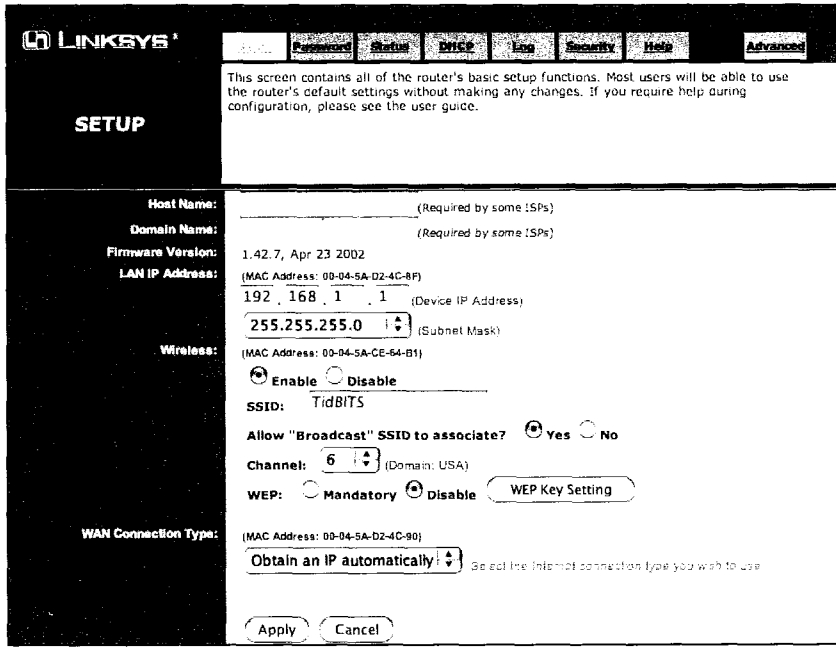

Figura 5.12. *Configuración de los ajustes básicos en la ficha Setup de EtherFast.*

Para conectividad Internet, seleccione el método de conexión, como Obtain an IP Automatically (cliente DHCP), Static IP (si su ISP le ha asignado una dirección IP estática) o PPPoE. Después puede asignar los valores apropiados para cada uno.

Ficha DHCP

Si desea que la EtherFast proporcione direcciones IP a los ordenadores a través de DHCP, haga clic en la ficha DHCP y seleccione el botón de opción Enable próximo a DHCP Server (vea la figura 5.13). Puede asignar la dirección IP de inicio y el número de direcciones que asigna el DHCP, pero recuerde que este número de direcciones no afecta a cuántos ordenadores cliente puede gestionar realmente la EtherFast al mismo tiempo.

Nota *Dado que la EtherFast enruta toda la red local hacia Internet se asignen o no direcciones mediante DHCP, también podemos asignar direcciones IP estáticas en la red local debajo de la dirección de inicio que hayamos definido. Por ejemplo, si iniciamos DHCP en la dirección 192.168.1.100, podríamos asignar las direcciones estáticas de la*

192.168.1.2 a la 192.168.1.99 a máquinas que utilizan reenvío de puertos u otras características que requieren una dirección fija. Adam siempre hace esto para poder conectar fácilmente con todos los ordenadores de su red local utilizando la dirección IP.

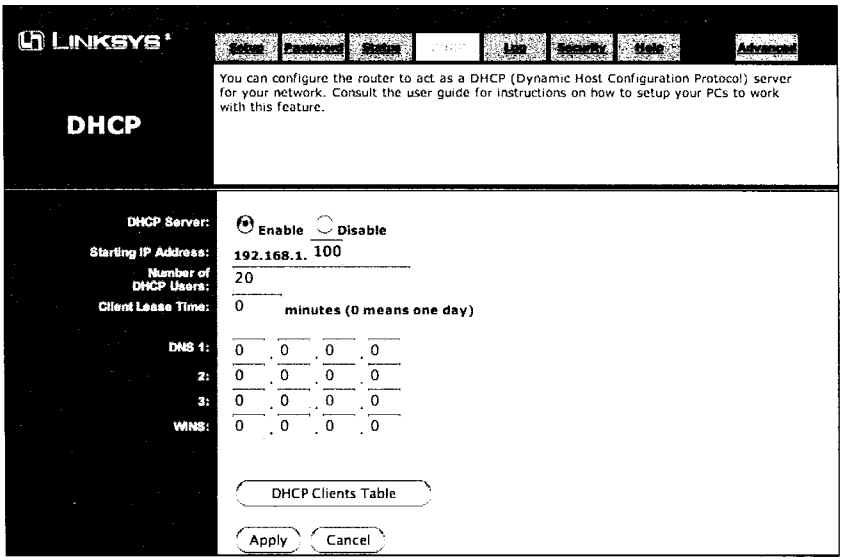

Figura 5.13. *Configuración de ajustes DHCP en la ficha DHCP de la EtherFast.*

El Client Lease Time define el periodo durante el que un adaptador de red concreto conserva la misma dirección IP. Los ordenadores cliente pueden renovar la misma dirección, de modo que dejar que expire el tiempo de usufructo no significa necesariamente que tenga que cambiar la dirección IP de un ordenador. Si queremos establecer servidores DNS concretos (y un servidor WINS para los sistemas Windows) para ordenadores que están escogiendo su configuración a través de DHCP, introduzca las direcciones IP apropiadas en esta pantalla.

Haciendo clic en el botón **DHCP Clients Table** se abre una ventana emergente que muestra cada cliente DHCP activo actualmente con su dirección IP, dirección MAC Ethernet y tipo de conexión.

Ficha Advanced

Aunque las fichas Setup y DHCP que acabamos de comentar contienen todas las opciones necesarias para empezar a usar la EtherFast, la interfaz

también proporciona una colección de pantalla de opciones más técnicas. Para verlas, haga clic en la ficha Advanced. Igual que en los ajustes básicos, es probable que sólo tenga interés por algunas de estas fichas.

La ficha Filters permite impedir que ordenadores de la red local accedan al mundo exterior de Internet, utilizando la dirección IP, el puerto o, haciendo clic en el botón **Edit MAC Filter Setting**, la dirección MAC (vea la figura 5.14).

Truco *Se pueden utilizar estos filtros para restringir ciertos puertos, impidiendo así que un adolescente adicto pase jugando en red demasiadas horas del día.*

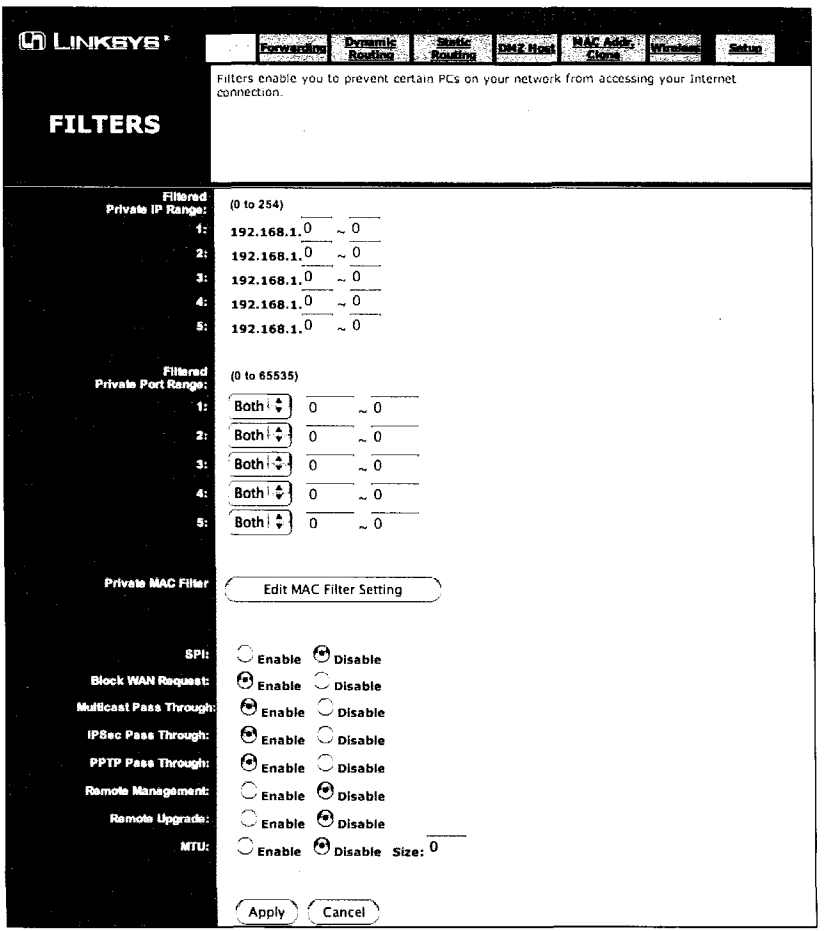

Figura 5.14. *Ficha Filters de la EtherFast.*

La ficha Forwarding (vea la figura 5.15) proporciona ajustes de reenvío de puertos que especifican cómo el tráfico entrante es redirigido hacia puertos concretos de máquinas locales (como suele hacerse para ejecutar un servidor Web en un ordenador interno, por ejemplo). El botón **Port Triggering** permite establecer activadores para jugar en red.

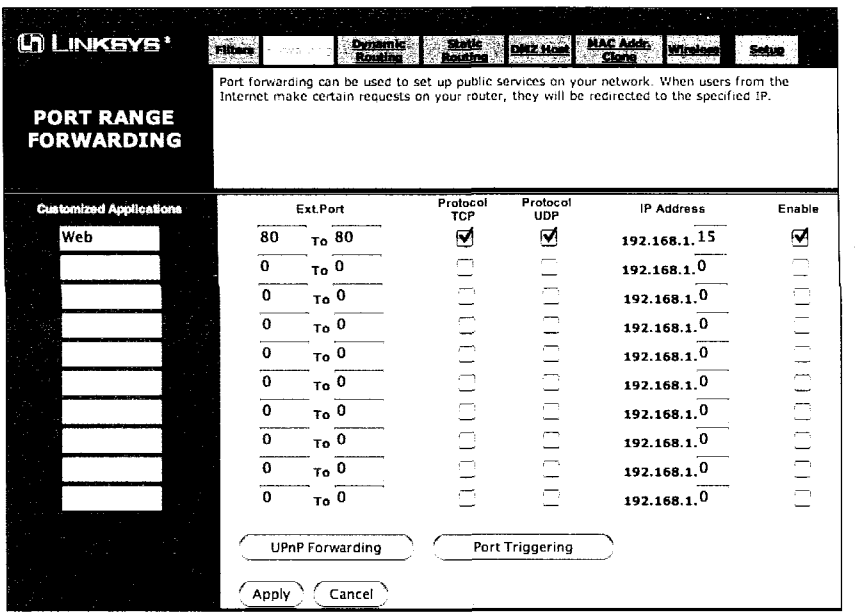

Figura 5.15. La ficha Forwarding de la EtherFast.

Crear un punto de acceso de software

Aunque hemos estado hablando sólo de hardware hasta ahora, no hay razón que impida que haya un punto de acceso de software en un ordenador normal. De hecho, hace años que Apple adoptó la idea de que con una tarjeta AirPort, debía ser posible convertir un ordenador en el equivalente de un punto de acceso sin abandonar por ello otras tareas.

A pesar del temprano soporte por parte del software de Estación Base de Apple en Mac OS 8.6 y después en Mac OS 9, el Mac OS X careció de esta característica durante un año y medio, hasta la aparición de Mac OS X 10.2 Jaguar en agosto de 2002.

Nota *Gracias a un acuerdo exclusivo con un fabricante de chips, sólo Apple puede descargar a la tarjeta AirPort el firmware extra especial que la convierte en un verdadero punto de acceso de software.*

Aunque Microsoft no haya creado una función de punto de acceso de software, podemos simularlo utilizando redes ad hoc. Es improbable que Microsoft añada esta función en el futuro, pues recientemente ha comenzado a vender puertas de enlace inalámbricas de hardware; otros fabricantes de equipamiento tampoco es probable que lo ofrezcan por la misma razón.

La principal ventaja de un punto de acceso de software es claramente el coste: los usuarios de ordenadores Mac, por ejemplo, pueden obtener prácticamente todas las funciones de una Estación Base AirPort, incluyendo DHCP, NAT e incluso cortafuegos, utilizando la función integrada de Mac OS X 10.2 para compartir Internet, todo sin tener que pagar los 300€ que cuesta una Estación Base AirPort.

Múltiples puntos de acceso

Si su red precisa múltiples puntos de acceso para llegar a más ubicaciones o usuarios, es necesario algo más de planificación y configuración:

- *Compruebe que tiene energía eléctrica en cada ubicación en la que piense añadir un punto de acceso. También puede usar Potencia a través de Ethernet (PoE), una manera de llevar corriente DC por un cable Ethernet modificado. No querrá hacer usted mismo estos cables, de modo que compre cables prefabricados en recursos en línea. PoE permite evitar tener que poner electricidad en tejados o lugares difíciles de alcanzar. (¡La energía solar también puede ser una opción para instalaciones en el exterior!)*
- *Conecte todos los puntos de acceso a una red Ethernet con cables. Todos los puntos de acceso deben estar en una red común para que todo su tráfico esté en la misma red que la conexión Internet. Como alternativa, puede usar uno o más puentes inalámbricos, descritos anteriormente en este capítulo, para encadenar puntos de acceso.*
- *Dé nombre a cada punto de acceso con el mismo nombre de red (SSID). El SSID es el identificador que utiliza el cliente para aso-*

ciarse con un punto de acceso; se dice de un grupo de puntos de acceso con el mismo SSID que tiene un ESSID o identidad de set de servicio. En redes con dos o más puntos de acceso, un cliente normalmente conecta con la unidad que tenga la señal más fuerte, siempre que todos los puntos de acceso compartan el mismo nombre.

- *Seleccione canales que no solapen para puntos de acceso adyacentes. Los canales 1, 6 y 11 tienen frecuencias que no solapan: podríamos apilar tres puntos de acceso con esos canales uno encima de otro y funcionarían bien. Qué canal de los tres escoja para cada punto de acceso es irrelevante, siempre que sean distintos (vea la figura 5.16). Dos anotaciones: primera, fuera de los EE.UU. los canales 1, 6 y 11 pueden no estar todos disponibles para el uso legal. Segunda, si trabaja con 802.11a, dispone de ocho canales que no solapan y puede hacer locuras.*
- *Habilite el servicio DHCP en sólo uno de los puntos de acceso. La mayoría de los servidores DHCP pueden (como opción) hacer de puente del servicio DHCP entre redes convencionales e inalámbricas y proporcionar acceso a clientes inalámbricos. No hay ninguna ventaja si se ejecutan servidores DHCP en varios puntos de acceso, y tener varios servidores DHCP puede provocar confusiones. Utilizando un solo servidor DHCP con NAT habilitada creamos una sola red local privada.*

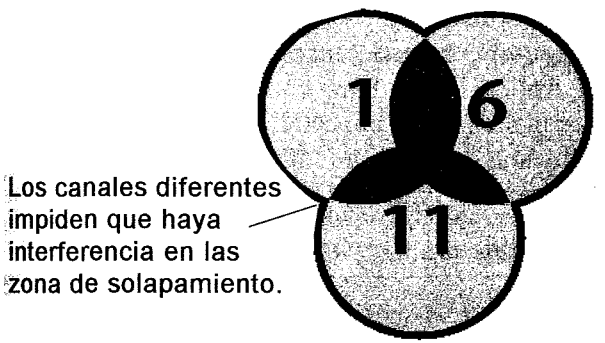

Figura 5.16. *Disposición de canales no solapados.*

Otras ventajas son la posibilidad de tener un control más preciso y una mejor interfaz que las a menudo confusas interfaces Web.

Sin embargo hay limitaciones al ejecutar un punto de acceso de software que dan ventajas al modelo de hardware:

- **Alcance:** Los adaptadores de red inalámbrica para ordenadores generalmente no tienen el alcance de las antenas más avanzadas o de mayor ganancia que hay en los puntos de acceso y puertas de enlace de hardware.
- **Disponibilidad:** Al hacer que un ordenador sea un punto de acceso de software se convierte en algo que hay que controlar y mantener. El equipamiento independiente tiende a ser más fuerte que los sistemas operativos de escritorio y, aunque incluso los puntos de acceso de hardware pueden tener confusiones, requieren menos mantenimiento que los ordenadores que ejecutan puntos de acceso de software.
- **Energía eléctrica:** Si es de la clase de personas que prefieren apagar la luz cuando salen de un cuarto, la corriente extra que utiliza un ordenador que tiene que estar encendido en todo momento quizá le irrite. Un punto de acceso de hardware quema alrededor de una docena de vatios, mientras que un ordenador necesita 150 vatios si su monitor está encendido. El ahorro seguramente sea mínimo, pero el principio de no desperdiciar energía innecesariamente es lo que importa.

Configurar una Estación base por software en Mac OS 8.6 y 9.x

La función Estación base por software en Mac OS 8.6 y 9.x se configura a través de la aplicación AirPort, que se suele encontrar en la carpeta Apple Extras dentro de la carpeta Aplicaciones. Para compartir una conexión de Internet entre los ordenadores inalámbricos conectados a la Estación base por software, también necesitamos una conexión de Internet en funcionamiento a través de Ethernet con un módem de cable o DSL o de llamada telefónica estándar.

Nota *Si desea compartir archivos entre dos ordenadores inalámbricos, puede crear una red ad hoc inalámbrica sin utilizar la Estación base por software. En el capítulo 4 encontrará más información sobre redes ad hoc y compartir archivos.*

1. Ejecute AirPort y haga clic en el botón **Estación base por software** en la parte inferior izquierda de la ventana principal.

2. En la ficha Iniciar/detener, introduzca el nombre de la red (SSID) en el campo Nombre de la red y seleccione el canal en el menú emergente Frecuencia del canal (vea la figura 5.17).

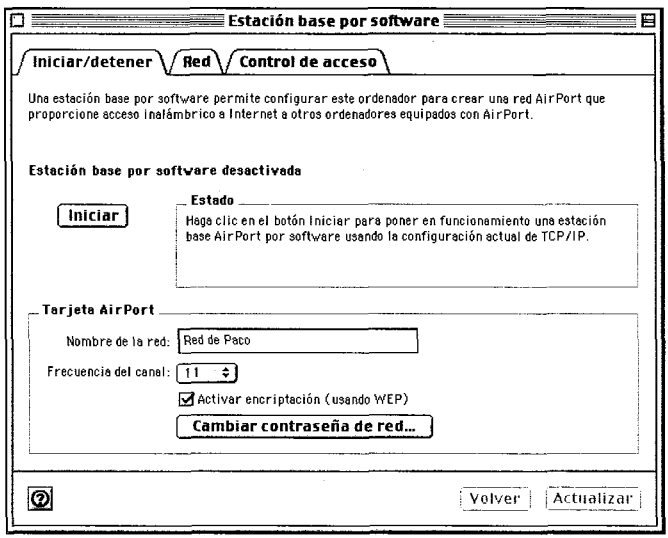

Figura 5.17. Configuración de la Estación Base por software en la ficha Iniciar/detener.

3. Si quiere habilitar el cifrado WEP, active la casilla de verificación Activar encriptación (usando WEP) y haga clic en el botón **Cambiar contraseña de red** para introducir la clave WEP.

4. Haga clic en **Iniciar** para empezar a compartir la conexión Internet.

La Estación Base por software de Apple siempre proporciona direcciones IP a los ordenadores cliente a través de DHCP; en la ficha Red, puede seleccionar también, si lo desea, proporcionar direcciones IP a los ordenadores conectados con cables a través de Ethernet. Por último, la ficha Control de acceso permite restringir el acceso a adaptadores de red específicos introduciendo sus direcciones MAC.

Truco

Si está utilizando un adaptador de red inalámbrica de terceras partes o desea más control del que proporciona la función Estación Base por software de Apple, visite IPNetRouter de Sustainable Softworks (www.sustworks.com/site/prod_ipr_overview.html). Puede hacer todo igual que Estación Base por software y mucho más, en parte porque

Sustainable Softworks escribió gran parte de la Estación base por software para Apple.

Configurar compartir Internet en Mac OS X 10.2

En Mac OS X 10.2 Jaguar, Apple cambió el nombre de Estación base por software por el de Compartir Internet y lo llevó desde la utilidad AirPort al panel de preferencias Compartir en Preferencias del Sistema.

Nota *Para compartir archivos entre dos ordenadores inalámbricos, sólo se necesita una red ad hoc, no una Estación base por software. Puede ver más información acerca de redes ad hoc y compartir archivos en el capítulo 4.*

Antes de empezar, compruebe que tiene configurada una conexión Ethernet o de módem interno en el panel de preferencias Red, pues no es posible crear un punto de acceso de software sin una de las dos activas. A diferencia de Estación base por software en Mac OS 9, la función Compartir Internet de Jaguar funciona si se recibe la conexión de Internet a través de Ethernet, módem interno o incluso AirPort. Para este ejemplo, suponemos que la conexión de Internet viene a través de Ethernet desde un módem de cable.

1. Abra Preferencias del sistema, haga clic en Compartir y clic en la ficha Internet (vea la figura 5.18).
2. Active la casilla de verificación Compartir la conexión a Internet con ordenadores que usen AirPort.
3. Si desea habilitar el servicio DHCP a través de las redes inalámbrica y convencional, active la casilla de verificación Compartir la conexión con otros ordenadores en Built-In Ethernet.
4. Haga clic en el botón **Opciones AirPort** para establecer el nombre de la red, el canal y la clave WEP.

Truco *Si activa WEP y tiene previsto que sistemas PC o Mac sin tarjetas AirPort vayan a acceder alguna vez a la red, recomendamos que esta-*

blezca la clave WEP utilizando un signo de dólar, seguido de la clave hexadecimal de 10 ó 16 dígitos. ¿Por qué? Si establece la clave utilizando una frase de paso normal, no hay manera de extraer la contraseña hexadecimal para utilizarla con adaptadores de red inalámbrica no AirPort.

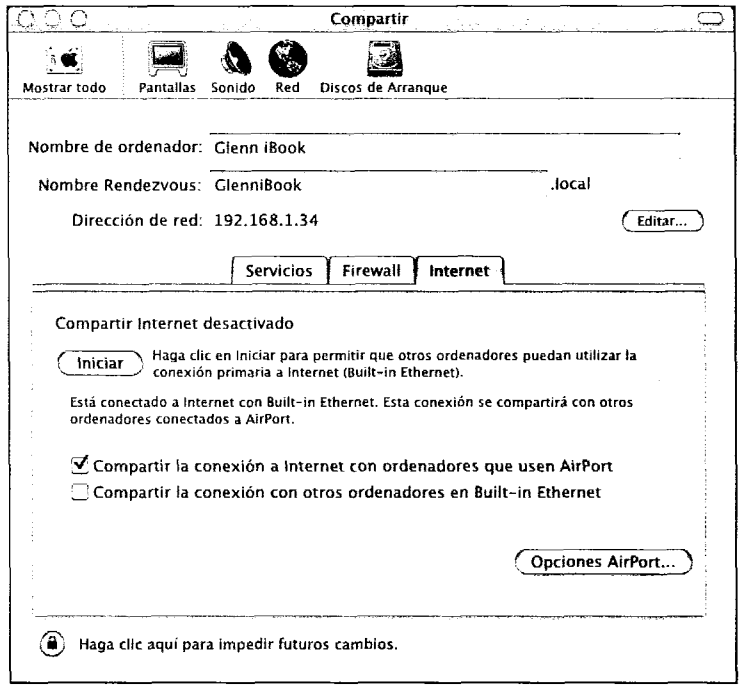

Figura 5.18. *Configuración de compartir Internet en la ficha Internet del panel de preferencias Compartir.*

Windows XP y software de enrutamiento

Aunque no es posible habilitar un verdadero punto de acceso de software bajo ninguna versión de Windows, podemos simular uno con redes ad hoc. Aunque las redes ad hoc no utilizan una sola máquina para enrutar el tráfico entre máquinas de una red, podemos hacer que uno de los ordenadores de una red ad hoc inalámbrica esté conectado con una conexión de Internet basada en Ethernet. Esa máquina conectada a Internet puede entonces actuar como puerta de enlace que permite que otras máquinas de la red ad hoc lleguen a Internet.

Esta estrategia no es tan resistente como un verdadero punto de acceso de software, pero puede funcionar bien en redes pequeñas con sólo algunas máquinas.

Bajo Windows XP, conseguimos hacer este juego de manos combinando redes ad hoc con la función de Windows XP para compartir una conexión de red con otros ordenadores. Como ventaja añadida, esta función activa el servicio DHCP.

Primero, siga las instrucciones de la sección "Crear una red ad hoc en Windows XP" del capítulo 4, para configurar una red ad hoc. A continuación, compruebe que tiene una conexión de Internet activa a través de otra interfaz, ya sea una conexión Ethernet o de llamada telefónica. Ahora siga estos pasos.

1. En Panel de control, seleccione Conexiones de red y después el elemento Conexión de red inalámbrica.
2. En la barra vertical Tareas de red del lado izquierdo, seleccione Cambiar la configuración de esta conexión (vea la figura 5.19).

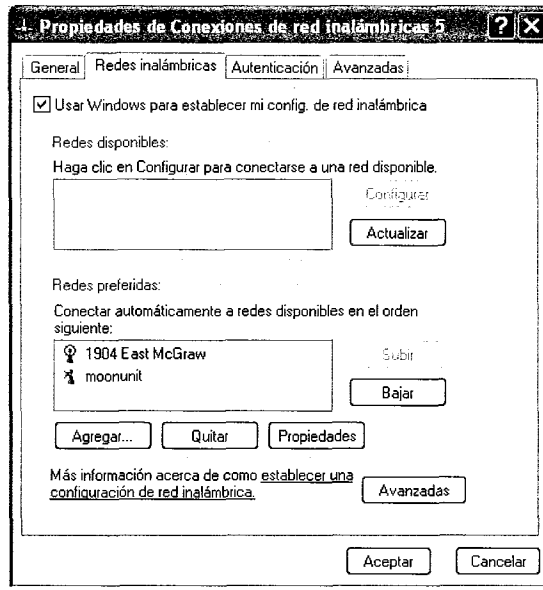

Figura 5.19. *El cuadro de diálogo Conexión de red inalámbrica de Windows XP.*

3. Seleccione la ficha Avanzadas.
4. Active la casilla de verificación Permitir a usuarios de otras redes conectarse a través de la conexión a Internet de este equipo (vea la figura 5.20).

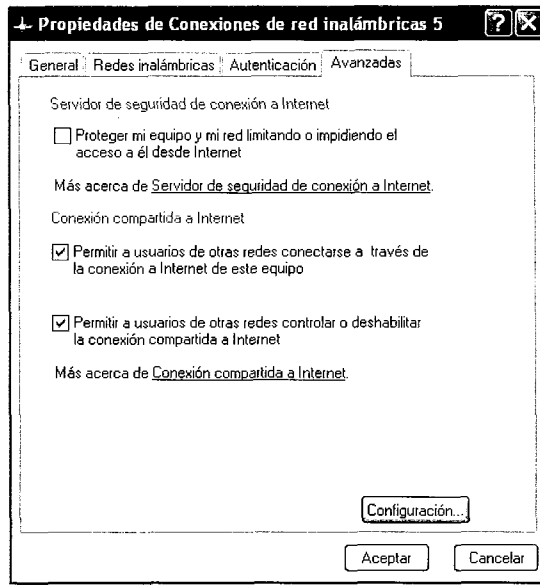

Figura 5.20. *Configuración de compartir Internet en Windows XP.*

5. En el menú emergente Conexión de red doméstica, seleccione su adaptador de red inalámbrica para compartir la conexión de cable o llamada telefónica con otros aparatos de la red inalámbrica.
6. Haga clic en **Aceptar**.

Truco

Para hacer configuraciones de compartir Internet más complejas en Windows XP, puede usar su opción de puente para que conecte varias redes a través de su ordenador. Utilice la ayuda integrada de Windows XP para más detalles sobre esta función.

Ahora ya hemos convertido el sistema Windows XP en algo parecido a un punto de acceso inalámbrico, complementado con conexión compartida a Internet y asignación de direcciones IP a otros ordenadores de la red ad hoc a través de DHCP.

Puentes en redes inalámbricas

Una vez picados por el insecto de las redes inalámbricas, es muy fácil añadir máquinas y ampliar la red hasta que de pronto nos topamos con una pared

de ladrillos, quizá literalmente. La siguiente ampliación se ve obstaculizada porque algunos ordenadores cliente no pueden llegar al único punto de acceso.

Es común en casas grandes y oficinas que no haya un lugar ideal desde el que un solo punto de acceso pueda servir a todos los ordenadores cliente. Como queda dicho en este capítulo, en el cuadro "Múltiples puntos de acceso", añadir un punto de acceso puede resolver el problema; pero los puntos de acceso suelen tener que estar conectados con cables Ethernet, formando en esencia la espina dorsal de la red inalámbrica.

Aunque es barato, el cable puede no ser la mejor opción si la distancia es grande o hay barreras físicas. En lugar de cable, hay varios dispositivos baratos que pueden hacer de puente de forma inalámbrica entre puntos de acceso aislados, sin necesitar una gran inversión de tiempo, taladrar agujeros ni gastar en la instalación.

El concepto que subyace a los puentes inalámbricos es que conectamos un solo punto de acceso a una conexión de Internet, que casi siempre implica el uso de un cable de Ethernet o teléfono. Después instalamos un segundo punto de acceso que amplia el alcance de la red hasta lugares inalcanzables para el primer punto de acceso. El segundo punto de acceso debe estar ubicado en una zona desde la que el adaptador inalámbrico todavía pueda llegar hasta el primer punto de acceso.

La magia llega al configurar los puntos de acceso (o el hardware adicional conectado a los puntos de acceso) para que el tráfico de los ordenadores cliente inalámbricos del segundo punto de acceso pase a través del segundo punto de acceso y utilice el puente para llegar al primer punto de acceso y de ahí a Internet.

Los puentes son una buena solución para algunas situaciones comunes, como ampliar una red de oficina a otras salas, pisos o edificios; conectar una red doméstica otra red más grande; o sortear un obstáculo que bloquea la señal inalámbrica entre dos zonas.

En efecto, un puente permite sortear la mayoría de las limitaciones físicas y convertir la red inalámbrica en algo más grande y más divertido.

Elegir hardware de puente

El equipamiento barato actual para crear puentes de redes inalámbricas funciona en uno de tres modos: un par o más de puentes que no funcionan como puntos de acceso en absoluto, pero hacen de puente para el tráfico de red entre las redes a las que están conectados con cables; un puente que puede conectar sólo a un punto de acceso fabricado por la misma empresa; y un

puente que puede conectar a cualquier punto de acceso, pero limita el número de máquinas para las que puede hacer de puente.

Nota

Linksys fabrica aparatos, el WAP11 y el WET11, que funcionan en los tres modos. Algunas otras compañías también venden piezas de equipamiento muy similares o idénticas con licencia de los mismos fabricantes (vea la figura 5.21).

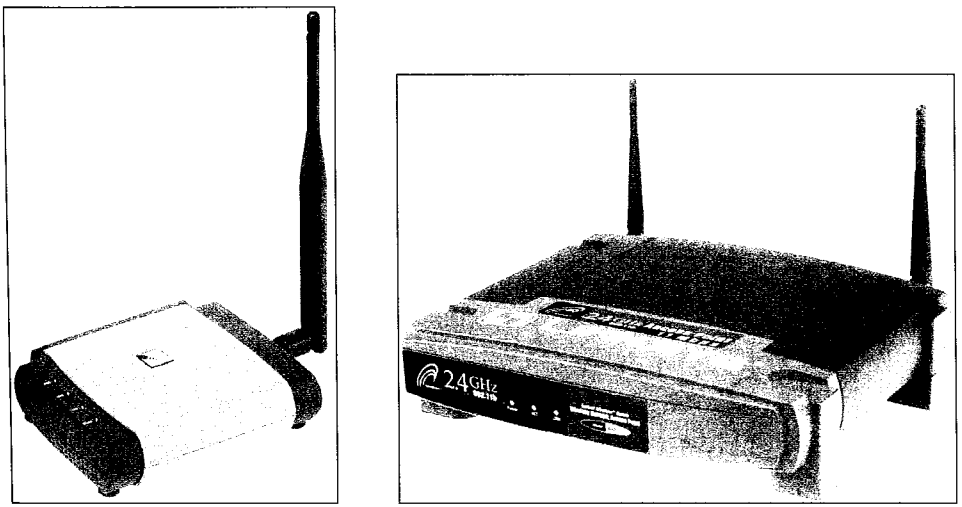

Figura 5.21. *WET11 y WAP11 de Linksys.*

Decidir cuál de estas tres alternativas tiene más sentido para una situación depende de la distancia que tiene que atravesar el puente y la naturaleza de la red.

Puentes en pares

Los puentes en pares son la opción más cara, ya que requiere al menos dos aparatos puente que no hacen otra cosa que hablar entre sí (vea la figura 5.22). El Linksys WAP 11, por ejemplo, tiene opciones punto a punto y punto a multipunto que permiten conectar dos o más redes.

Nota

En el modo multipunto, un puente recibe y retransmite el tráfico de muchos otros puentes, que están en el modo punto a punto. Este puente también retransmite el tráfico de aparatos conectados con él a través de su puerto de cable.

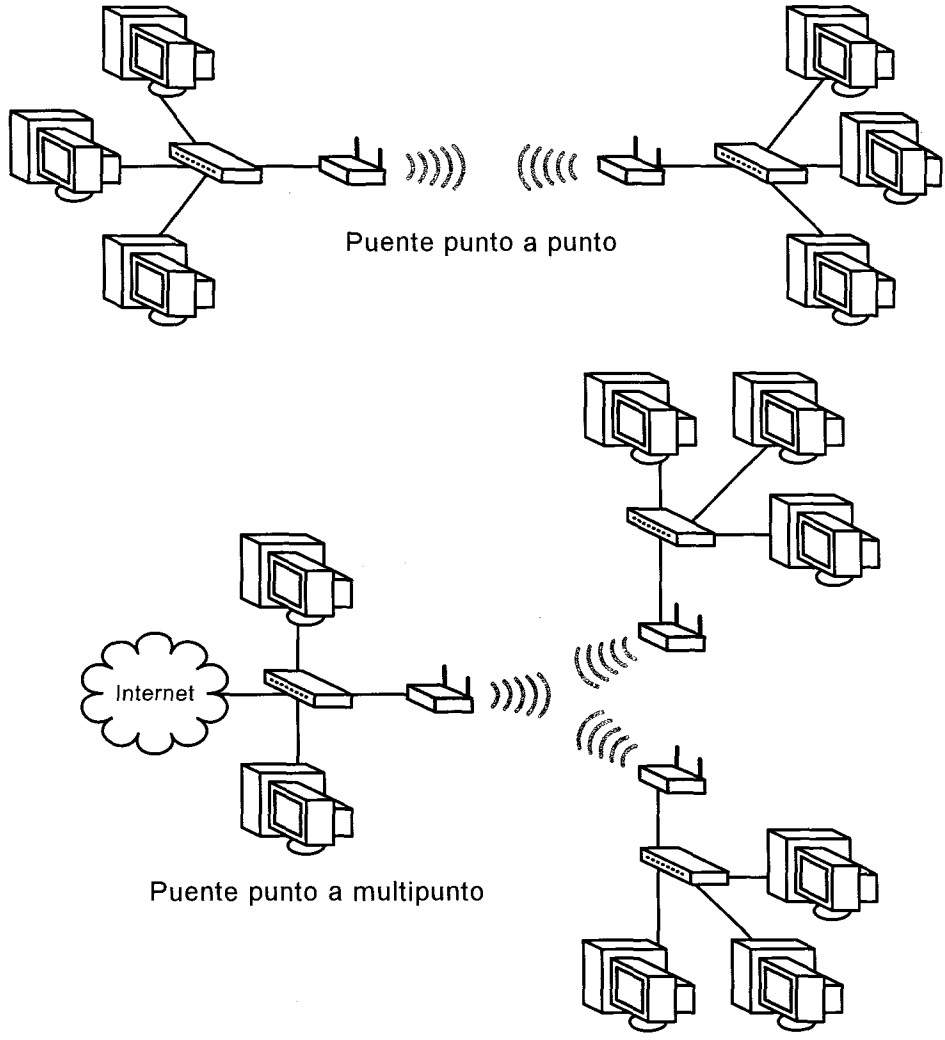

Figura 5.22. *Puente punto a punto y punto a multipunto.*

La ventaja del WAP11 es que podemos colocarlo lejos de la oficina para tener una mejor línea de visión. Muchas empresas e individuos que utilizan WAP11 despliegan un cable de Ethernet (que también lleva corriente a través de Ethernet) hasta el tejado y después utilizan un contenedor a prueba de agua para alojar el WAP11.

Con una antena adjunta, el WAP11 puede hacer de puente entre una red inalámbrica y otro WAP11 a kilómetros de distancia.

El WAP11 sólo cuesta unos 100€ en el momento de escribir esto, de modo que fácilmente se puede crear una red punto a punto por sólo 200€ y un par de cables de Ethernet.

Nota

El WAP11 y puentes similares son puentes de protocolo: esto es, pueden llevar cualquier tráfico que utilice uno de los varios protocolos a los que prestan soporte. El WAP11 gestiona TCP/IP, IPX y NetBEUI, pero tenga en cuenta que no se puede utilizar AppleTalk a través de la conexión.

Puente a un punto de acceso idéntico

Hay una opción más barata, pero similar por lo demás, a utilizar pares de puentes. En lugar de usar un par de puentes, configuramos un puente que conecta de forma inalámbrica con un punto de acceso central (vea la figura 5.23). El Linksys WAP11 es el héroe aquí también, pues ofrece un modo adaptador cliente en el que uno o más dispositivos conectados a través de Ethernet al WAP11 pueden utilizarlo como puente para llegar a otro WAP11 que funciona como punto de acceso.

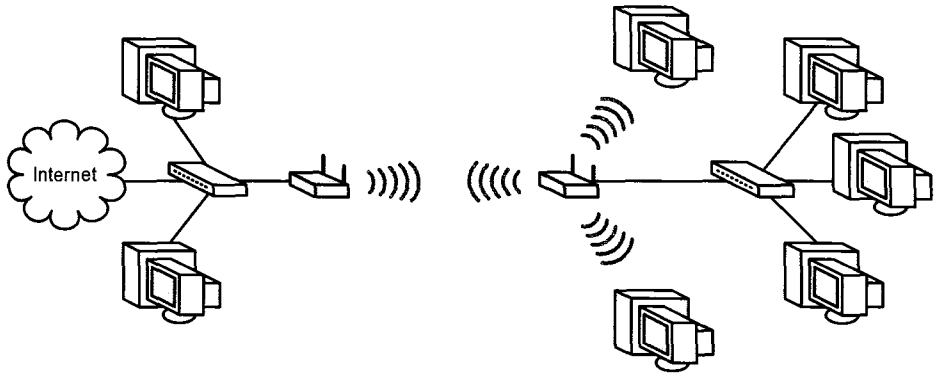

Figura 5.23. *Puente a un punto de acceso.*

Nota

Distintas piezas de equipamiento similares, incluyendo hardware D-Link, también pueden funcionar en este modo con equipamiento Linksys. Sin embargo, como los fabricantes no garantizan la compatibilidad, versiones futuras pueden no funcionar bien juntas. Recomendamos que se atenga al equipamiento de un solo fabricante si piensa utilizar puentes entre redes.

En el modo cliente-adaptador, el WAP11 hace de puente para los mismos protocolos comentados anteriormente (TCP/IP, IPX y NetBEUI). El inconveniente de esta solución es que el WAP11 es un punto de acceso algo raquítico, sin casi funciones de puerta de enlace, de modo que quizá necesite comprar una puerta de enlace para complementar al WAP11 que actúa como punto de acceso.

Puentes a cualquier punto de acceso

¿Qué sucede si no queremos comprar todas las piezas de equipamiento del mismo fabricante o, más probable, tenemos que añadir un puente inalámbrico a una red, pero ya disponemos de un punto de acceso? Eso nos trae una tercera alternativa, en la que utilizamos un puente, en este caso el Linksys WET11, que puede llevar cualquier tipo de tráfico a cualquier punto de acceso (vuelva a ver la figura 5.23).

Aunque esto puede parecer la solución ideal, hay algunos problemas menores en el WET11 y un aparato similar de 3Com, la 3Com Wireless Workgroup Gateway. El más notable es que los dos dispositivos hacen que todas las direcciones Ethernet únicas de los aparatos conectados a ellos parezcan ser una sola dirección MAC. Es un poco como el modo en que NAT convierte todas las direcciones IP privadas de los ordenadores de una red local para que el tráfico procedente de ellos parezca salir de una sola dirección IP pública de la puerta de enlace.

Aunque esta limitación puede sonar esotérica, este tipo concreto de traducción a dirección MAC puede provocar extraños problemas porque cierto software y hardware utiliza la dirección MAC para autenticar un ordenador u otras piezas del equipamiento de red. Todas las identidades de la red están unidas a las direcciones MAC, de modo que tener varias direcciones IP que parecen provenir todas de la misma dirección MAC puede llevar a confusión a los servidores de red haciendo que no estén disponibles.

Por otro lado, dado que este tipo de puente puede permitir el paso de cualquier tipo de protocolo que vaya sobre Ethernet y como funciona con cualquier tipo de punto de acceso, no sólo los modelos Linksys, una pequeña incomodidad y algunos ajustes pueden merecer la pena si permiten ahorrar cientos de euros y no necesitamos cambiar los equipos existentes.

Una ventaja de WET11 comparado con la 3Com Wireless Workgroup Gateway es que el WET11 dice poder gestionar alrededor de 30 aparatos simultáneamente, mientras que la puerta de enlace 3Com sólo admite 4 aparatos en el momento de escribir esto. (El hardware del WET11 técnicamente puede gestionar alrededor de 50 aparatos, pero el director de productos inalámbricos

de Linksys le dijo a Adam que no recomienda que más de 30 dispositivos lo utilicen como puente al mismo tiempo, para que el rendimiento se mantenga en un nivel razonablemente bueno.) Esperamos que aparezcan más puentes de este tipo con distintas opciones y diferentes herramientas de configuración después de que este libro vaya a las prensas.

Seguridad en puentes a larga distancia

La seguridad en el puente parece una tarea para Worf o Tuvok de Star Trek, pero en realidad es un asunto serio: con enlaces a larga distancia, ya sea entre edificios próximos o alejados varios kilómetros, los puentes exponen todo el tráfico de red ante cualquiera que esté dentro de la distancia de recepción. Todos los puentes que hemos visto prestan soporte al protocolo de cifrado WEP y suponemos que también admitirán cualquier solución con más capacidades que termine reemplazando a WEP. Pero mientras tanto, piense que incluso con el cifrado WEP activado, quizá no haya verdadera seguridad. Muchas compañías grandes se han vuelto hacia una interesante opción que complementa a las VPN. Las VPN fueron diseñadas principalmente para conexiones de un cliente con la red desde fuera del cortafuegos corporativo, como en el caso de una conexión de llamada telefónica durante un viaje, pero no para hacer de túnel para toda una red.

En lugar de una VPN, las empresas crean una LAN virtual (VLAN) en la que todo el tráfico que atraviesa la red local está cifrado durante el tránsito. Esta estrategia añade una sobrecarga al funcionamiento de la red, pero significa que sin el software, las contraseñas y el acceso apropiados los fisgones no pueden espiar el tráfico por cable o inalámbrico. Para ver una perspectiva general de las VLAN, visite el artículo de Cisco sobre el tema en www.cisco.com/warp/public/cc/pd/wr2k/cpbn/tech/vlan_wp.htm. La alternativa menos dirigida a empresas a una VLAN es usar SSH y SSL para cualquier conexión que requiera contraseñas que serían enviadas a las claras en caso contrario; comentaremos esas dos opciones y ofreceremos más información acerca de las VPN en el capítulo 6.

Configuración del Linksys WAP11

Configuramos el Linksys WAP11 ejecutando un software Windows adaptado que puede conectar con el dispositivo en la red Ethernet convencional local

o conectando con su interfaz basada en Web directamente con un navegador, igual que con la Linksys EtherFast comentada anteriormente en este capítulo. Otra razón para usar la interfaz basada en Web es que las opciones de seguridad avanzadas que ofrece no están disponibles en el software Windows.

Truco *La dirección IP predeterminada del WAP11 es 192.168.1.251 y podemos conectar con él utilizando cualquier navegador siempre que estemos en la misma red IP. La contraseña es admin y no se necesita nombre de usuario. Vea el cuadro "Configurar el ordenador para efectuar los ajustes iniciales" ya visto con anterioridad en este capítulo.*

Nota *La versión final del firmware original del WAP11, 1.4i, es más difícil de configurar que la versión 2.2 del hardware disponible al escribir esto porque utiliza una conexión USB directa o un extraño cliente de red SNMP. Desgraciadamente, sólo los WAP11 que llevan la etiqueta WAP11v2.2 pueden ejecutar el nuevo firmware 2.2, que utiliza configuración basada en Web.*

Sea cual sea el modo puente que vayamos a utilizar, la ficha Setup controla todas las opciones básicas, como la dirección IP y funciones de punto de acceso como WEP.

Truco *Al configurar el modo puente de dos o más WAP11, compruebe que asigna a cada uno direcciones fijas distintas para poder llegar a ellos para actualizar su configuración más adelante.*

La ficha Setup también contiene los cuatro modos de funcionamiento al lado de la etiqueta AP Mode: punto de acceso estándar, cliente de punto de acceso, puente inalámbrico (punto a punto) y puente inalámbrico punto a multipunto (vea la figura 5.24).

- **Punto de acceso estándar:** En este modo, el WAP11 funciona como un punto de acceso normal, sin funciones de puente.
- **Cliente de punto de acceso:** Asigne a AP Mode la opción Access Point Client e introduzca la dirección MAC del punto de acceso al que quiere conectar el WAP11. Este otro punto de acceso debe ser también un WAP 11, como se ha señalado en la sección "Puente a un punto de acceso idéntico" ya vista anteriormente.

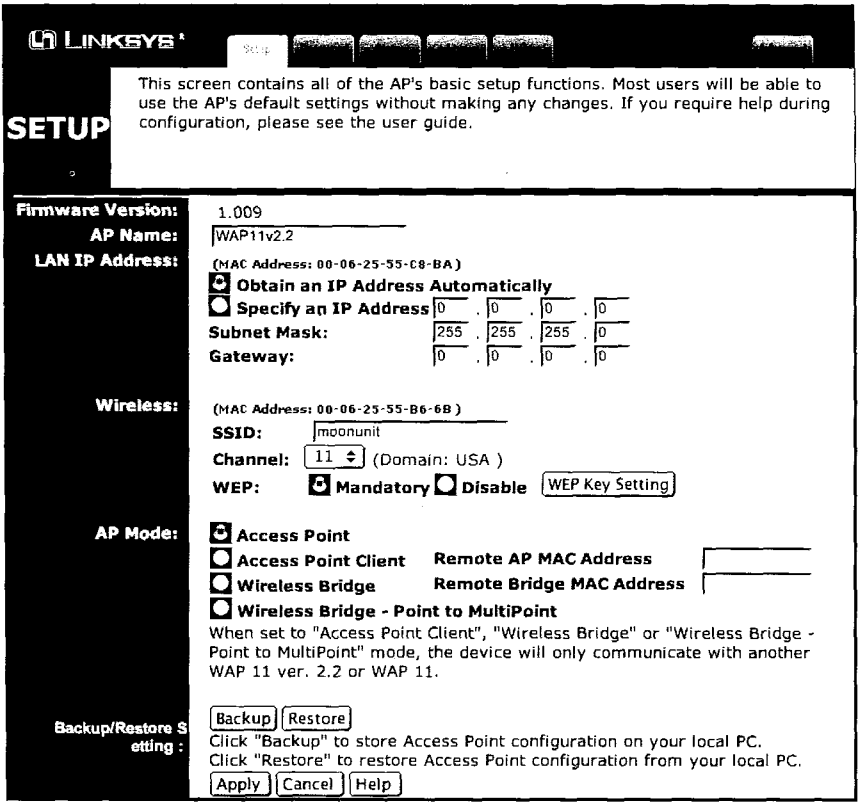

Figura 5.24. Configuración de un WAP11 para hacer de puente.

- **Puente inalámbrico (punto a punto):** Introduzca en cada WAP11 la dirección MAC del otro WAP11. Una vez configuradas y reiniciadas, las dos unidades establecen un enlace continuo entre sí, como comentamos en la sección anterior "Puentes en pares".
- **Punto a multipunto:** Configurado en este modo, un WAP11 sirve como puente central multipunto y todos los demás WAP11 se configuran en el modo Puente inalámbrico (punto a punto) utilizando la dirección MAC de este WAP11 central.

Configuración del Linksys WET11

La configuración del Linksys WET11 es muy parecida a la del WAP11 y se lleva a cabo ejecutando un software Windows adaptado o conectando con la interfaz basada en Web utilizando un navegador.

Nota *La dirección IP predeterminada del WET11 es 192.168.1.251 y podemos conectar con él utilizando cualquier navegador siempre que estemos en la misma red IP. La contraseña es admin y no se necesita nombre de usuario. Vea el cuadro anterior "Configurar el ordenador para efectuar los ajustes iniciales" en este mismo capítulo.*

La configuración del WET11 está dividida en varias fichas que proporcionan las distintas opciones necesarias para la configuración. Tres de ellas resultan útiles:

- **Ficha Info:** La ficha Info muestra detalles acerca del WET11 y de las redes inalámbricas locales. La mitad superior muestra la revisión del firmware, la red inalámbrica actual a la que está conectado y la calidad del enlace; la mitad inferior muestra todas las redes que el WET11 haya encontrado durante la exploración (vea la figura 5.25).

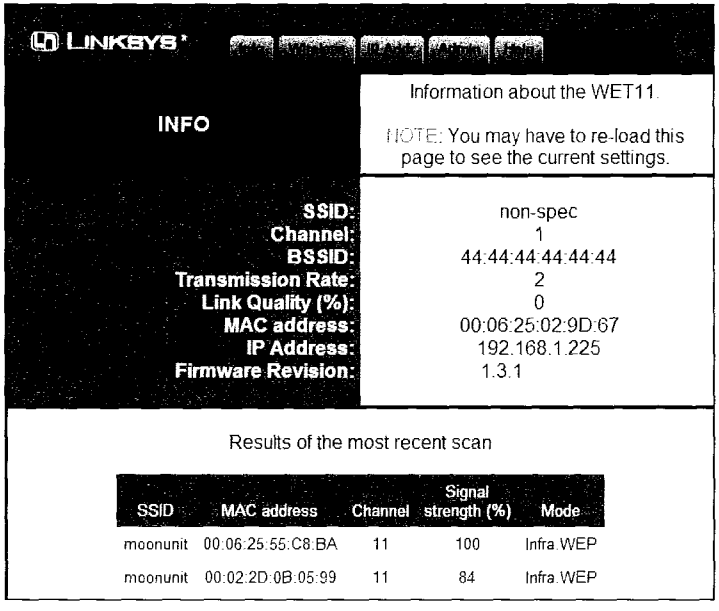

Figura 5.25. *Examen de los detalles de la conexión para el WET11.*

- **Ficha Wireless:** Esta ficha tiene la misma apariencia que un cuadro de diálogo de configuración de cliente genérico porque eso es lo que es: introduzca el nombre de red (ESSID/SSID), las claves WEP y otros detalles que necesite para conectar a un punto de acceso (vea la figura

5.26). La configuración efectuada aquí habilita el WET11 para que haga de puente entre el tráfico inalámbrico y el punto de acceso, como se comentó en la sección "Puentes a cualquier punto de acceso".

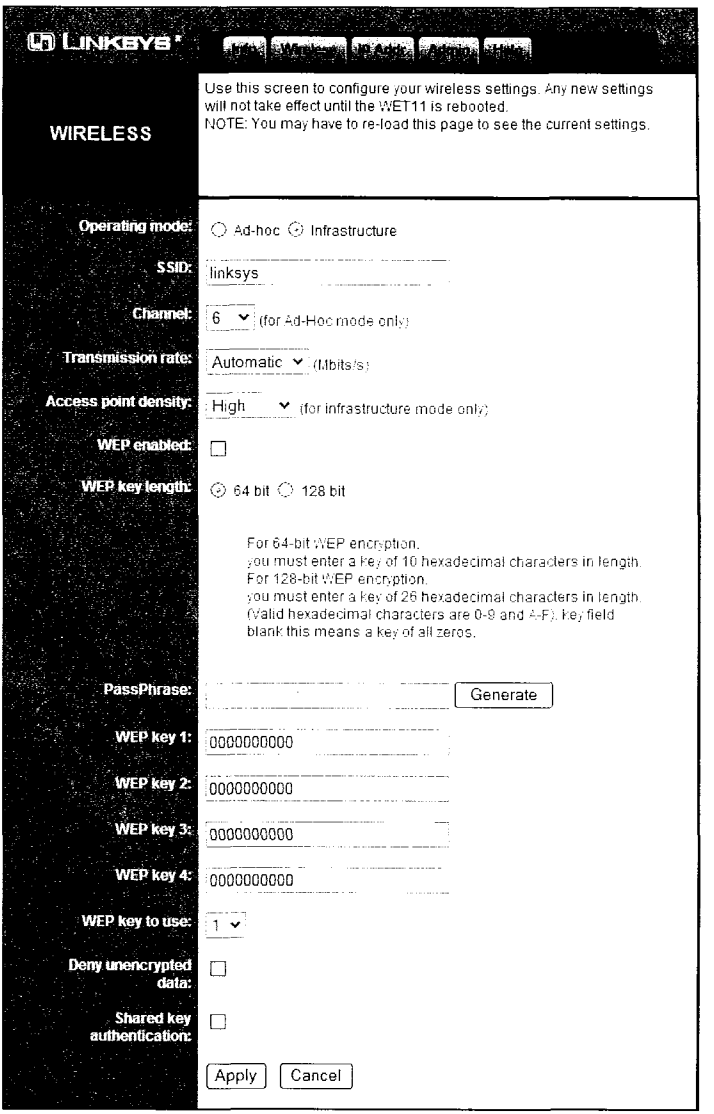

Figura 5.26. *Configuración de un WET11 para que haga de puente.*

- **Ficha IP Addr:** En esta ficha podemos cambiar la dirección IP del WET11, en caso de no querer usar la predeterminada.

Asegurar la red

Construir una red inalámbrica es útil y divertido (y como ha visto, no demasiado difícil), pero hay un problema, no en la propia red, sino en que alguien pueda espiar todo el tráfico de la red. Es cierto, las redes inalámbricas tienen algunos problemas de seguridad y, aunque mucha gente no necesita preocuparse demasiado por ellos, si hay datos sensibles recorriendo la red, hay que tomar precauciones de seguridad para impedir que un espía rastree el tráfico. A eso dirigimos nuestra atención en el próximo capítulo.

6. Seguridad inalámbrica

A todos nos gusta pensar que tenemos privacidad, incluso aunque a menudo no la tengamos. Hay gente que se marcha al interior de Alaska, a 50 kilómetros de la parada de autobuses más cercana, para garantizar que no hay posibilidad de toparse con otro ser humano. Otros mantienen límites psicológicos mientras viven en entornos densamente poblados: aunque Glenn puede ver a sus vecinos a través de la ventana de la cocina, gracias a un acuerdo tácito mutuo, ni él ni sus vecinos dan muestra de percibir tal presencia en esos casos.

Estas anécdotas ilustran también casos de las redes inalámbricas. Siempre que nuestras redes inalámbricas estén aisladas, no tenemos que preocuparnos de otras personas. En el momento en que alguien entra dentro del alcance de la red, la privacidad puede verse comprometida. Las transmisiones a través de redes inalámbricas, dado que atraviesan paredes, techos, suelos y otros obstáculos, se pueden interceptar fácilmente con equipamiento de pequeño consumidor igual que el que utilizamos para conectar los ordenadores y el punto de acceso.

Adam vive tan alejado del centro de la población en Ithaca, que él y su mujer Tonya no necesitan preocuparse porque alguien entre en su red: sería difícil para alguien compartir su conexión sin aparcar delante de la entrada de

la casa. Por el contrario, Glenn y su esposa Lynn residen en una zona bastante poblada de Seattle. Un día, poco después de que sus jóvenes vecinos alquilaran la casa de al lado, Glenn abrió su portátil y encontró la red inalámbrica que utilizaban.

A diferencia de las formas más avanzadas de funcionamiento en red o los servicios de teléfonos móviles, las redes Wi-Fi y similares no pretenden intrínsecamente limitar quién puede conectar. Por ejemplo, siempre que utilizamos Wi-Fi, cualquier persona cuyo ordenador puede recibir la señal tiene posibilidad de acceder a la red, utilizar la conexión de Internet, observar el paso del tráfico y conectar con los ordenadores de la red.

Nota *En este capítulo nos vamos a centrar en Wi-Fi, en parte porque los riesgos de seguridad de las redes HomeRF, Bluetooth y de datos celulares son menos claros y más desconocidos en este momento por su menor uso. Los riesgos probablemente son menores, pues HomeRF y Bluetooth utilizan salto de frecuencias y métodos de seguridad integrados mejor concebidos que las funciones de seguridad de Wi-Fi. Los dos protocolos también funcionan de forma más aislada: HomeRF en redes domésticas y Bluetooth en distancias muy cortas.*

La cuestión, por supuesto, es lo probable que sea que alguien desee entrar sin permiso en la red inalámbrica. Una empresa, pongamos por caso, se preocupará más si alguien estacionado en su aparcamiento puede acceder a sus datos confidenciales. Y las empresas tienen montones de datos que deben considerarse confidenciales, como facturas que van de empleados a bases de datos, mensajes de correo electrónico que contienen información que podría interesar a la competencia o incluso números de tarjetas de crédito de clientes. Los usuarios domésticos tienen menos preocupaciones, naturalmente, pero deben proteger las contraseñas que un atacante pueda usar para iniciar una sesión en una cuenta bancaria en línea o un sistema que pase facturas a la tarjeta de crédito, por ejemplo. En este capítulo, valoramos distintos aspectos de seguridad y cifrado: la seguridad es el arte de proteger la integridad de los sistemas; el cifrado protege el contenido de las transmisiones y los datos guardados. Le mostraremos por qué y cuándo debe pensar en utilizar medidas de seguridad y sistemas de cifrado, y cómo puede establecer esos sistemas en su red de forma sencilla y, a menudo, barata.

Nota *No hay una forma fácil de decir esto. La seguridad, ya hablemos de proteger el coche, la casa o la red doméstica, es difícil, principalmente*

porque siempre consiste en una batalla con otro ser humano. Cerrando la puerta con un cerrojo podemos desanimar a los ladrones poco avezados, pero ante los más expertos quizá no sirva ni siquiera una puerta blindada. Y si vivimos en una zona en la que los robos son frecuentes, habrá que pensar en cuántos cerrojos, sistemas de alarma y verjas en la ventana serán necesarios. Desgraciadamente, el tipo de personas que se dedica a robar en vecindarios es muy hábil y las medidas de seguridad a tomar frente a ellos son más complicadas que si se trata de ladrones ocasionales. De modo que, disculpándonos por adelantado, este capítulo no puede por menos que ser más técnico que la mayor parte del resto del libro.

Preocupaciones inalámbricas

A diferencia de los fanáticos de la privacidad, no queremos ofrecer razones para que se vuelva paranoico. Preferimos presentar un debate claro acerca de los riesgos y posibles resultados de utilizar una red inalámbrica.

Nota

Adam escribió un artículo para su boletín TidBits que habla sobre una teoría de la privacidad y de por qué la mayoría de la gente no le presta demasiada atención. Puede leerlo consultando los articulos en http://db.tidbits.com.

Veamos primero qué papel juega la ubicación en las consideraciones de la seguridad, después los tipos de datos que pueden viajar a través de la red y, por último, cómo valorar los factores de riesgos individuales para que pueda ver qué partes de este capítulo necesita leer.

Nota

Dejamos de lado aquí si se debe permitir a cualquiera conectar con nuestra red: aunque permitir intencionadamente que la gente conecte con la red aumenta el riesgo de seguridad, el hecho de que conozca la presencia de gente externa en la red significa que probablemente ya tiene en cuenta las consideraciones de seguridad que engendra su presencia. Vea el capítulo 10 para encontrar información acerca de redes compartidas y comunitarias.

Dónde vive, trabaja y deambula

Antes de que le hagamos preocuparse o despertemos sus temores sobre qué está enviando o recibiendo a través de la red inalámbrica, debe primero reflexionar acerca de dónde utiliza las redes inalámbricas, pues la ubicación afecta a la vulnerabilidad ante los ataques.

Es probable que utilice redes inalámbricas en una o más de estas situaciones:

- **Medio rural, sitio alejado:** En su casa, que está alejada de otras casas.
- **Largo alcance:** A través de un enlace punto a punto de largo alcance con un ISP inalámbrico.
- **Medio urbano densamente poblado:** En su casa en una zona urbana muy poblada o con al menos varias casas cercanas.
- **Vecindario de espacio público:** En un vecindario cerca de un aparcamiento público o donde la gente puede aparcar en la calle.
- **Cerca de redes existentes:** En un área con redes activas o comunitarias.
- **Edificio de oficinas:** En un edificio de oficinas con otras empresas o un aparcamiento cercano dentro de la línea de visión.
- **Uso mixto:** En un vecindario de uso mixto residencial y comercial.
- **Deambulando:** Mientras se encuentra de viaje, en aeropuertos, cafés, hoteles y otros lugares.

Desgraciadamente, a menos que su caso sea el del primer punto, la categoría de medio rural o sitio alejado, siempre hay un ligero riesgo de que los datos de una red abierta sean interceptados.

En el resto de los casos, recomendamos utilizar al menos los mínimos niveles de protección comentados en la sección "Impedir el acceso a la red". Para casos que impliquen el uso en empresas, alentamos a tener en cuenta las recomendaciones de la sección "Asegurar los datos en tránsito".

Preste especial atención a la categoría deambulando. Incluso si protege su red, si utiliza el ordenador durante los viajes fuera de las redes fiables, los datos pueden sufrir riesgos.

Al usar redes públicas, ya sean gratuitas o con cuotas de pago, no tenemos control sobre las precauciones de seguridad basadas en red y todo el que utilice la misma red puede ver los datos en tránsito.

Su tráfico de red

Todos los datos enviados o recibidos a través de una red convencional o inalámbrica se transmiten a las claras para cualquiera que pueda unirse o conectarse a la red. "A las claras" significa simplemente que los datos se envían en una forma que los humanos pueden interceptar y leer directamente o convertir fácilmente en un programa o una imagen que se puede usar.

Ésta es una lista de lo que puede estar enviando o recibiendo a las claras:

- La contraseña de su cuenta de correo electrónico.
- El texto de todos los mensajes de correo electrónico enviados y recibidos.
- El contenido de cualquier documento enviado o recibido como archivo adjunto.
- La ubicación y contenido de las páginas Web visitadas.
- El nombre de usuario y contraseña utilizados en cualquier sitio Web no seguro (sitios que no utilizan SSL).
- El nombre de usuario FTP y la contraseña.
- Cualquier archivo transmitido vía FTP.
- El texto de cualquier mensaje instantáneo enviado o recibido.
- El contenido de archivos de música o similares enviados o recibidos utilizando LimeWire, Kaza u otros programas para compartir archivos entre pares.
- Las direcciones IP y los números de puerto de cualquier conexión que se haya establecido.
- La sesión de control Timbuktu o las sesiones de transferencia de archivos.

Estos elementos no se envían a las claras:

- El contenido de las sesiones cifradas utilizando SSH, SSL o VPN (lo describimos todo más adelante en este capítulo).
- La contraseña de correo electrónico si el ISP utiliza SMTP AUTH (salida) o APOP (entrada).
- Las contraseñas Timbuktu.

- Contraseñas AppleShare (si el cliente y el servidor tienen los dos habilitados el cifrado).
- Las páginas Web seguras que utilizan SSL (sus URL comienzan por https://).
- El contenido de cualquier mensaje de correo electrónico o archivo cifrado con PGP (cifrado de clave pública) o una tecnología similar.

Nota *Incluso si cierra la red con los medios descritos más adelante en este capítulo, todavía puede terminar exponiendo datos ante piratas de red y otras personas que pueden forzar algunos de los métodos básicos que impiden el acceso. Hablaremos sobre cómo asegurar los datos que se envían en la sección "Asegurar los datos en tránsito".*

Cada elemento que se pueda transmitir a las claras cae en una de estas tres categorías: información de acceso a cuenta (nombres de usuario y contraseñas), información que podría utilizarse para seguir nuestros pasos en la Web y contenido relacionado con lo que decimos y hacemos.

Somos personas bastante transparentes (bueno, no en el sentido literal), y no hay mucho que podamos decir o hacer en línea que nos preocupe que alguien más vea. Que la persona equivocada lea el documento que no debe puede resultar embarazoso, pero eso es todo. Pero ¿y si el documento fuera colocado en una lista de correos o un sitio Web de amplia difusión? Incluso para nosotros eso podría ser un problema, y otras personas podrían tener datos que quizá llevaran a su despido, dañaran su empresa, los humillaran públicamente o provocaran demandas o divorcios. Probablemente ya tenga una idea de si corre riesgo o no con las cosas que hace o dice.

Igualmente, la información que controla los movimientos en la Web tampoco resulta preocupante para nosotros que, como periodistas, siempre podemos alegar que hemos visitado un sitio Web llevando a cabo un estudio de mercado. Pero no se necesita mucha imaginación para suponer que un político podría ver arruinada su carrera si ha visitado ciertos sitios dedicados al sexo. De nuevo, probablemente sepa si sus movimientos en la Web pueden dañarle de algún modo.

Por último, y más importante, está la información de acceso a cuentas, que, cuando alguien la roba, presenta dos tipos de riesgo. Primero, como la mayoría de la gente tiende a utilizar las mismas contraseñas en varios sitios, una contraseña de correo robada puede comprometer un sistema mucho más sensible, como la cuenta bancaria en línea. Segundo, los atacantes a menudo utili-

zan la contraseña de una cuenta para penetrar en otra cuenta, abriéndose camino dentro de un ordenador con el objetivo final de robar datos, provocar daños o utilizar el ordenador para que ejecute un programa automatizado que ataque a otros ordenadores. Respecto a esto, proteger la contraseña no es algo que hagamos sólo en nuestro propio beneficio, sino algo que beneficiará a cualquier otro que pueda verse afectado si el atacante toma el control del servidor que utilizamos.

Truco

Teniendo en cuenta que es casi imposible recordar todas las contraseñas distintas para cada posible servicio, recomendamos utilizar tres contraseñas diferentes. La primera debe ser simple y fácil de recordar, pero se utilizará sólo en sitios Web que no almacenan información personal (como la dirección, fecha de nacimiento o número de tarjeta de crédito). La segunda debe ser más difícil de escribir, incluyendo mayúsculas, minúsculas, números y signos de puntuación, y se utilizará en cuentas donde hay datos personales que no deben sufrir riesgos.

Por último, todo el mundo debe tener una contraseña verdade-ramente segura que sea larga, difícil de escribir y prácticamente imposible de adivinar. Se utilizará para cuentas que implican dinero, como la cuenta de un banco en línea. Utilizar una contraseña larga no impide que sea robada de una transacción inalámbrica no protegida, pero siendo realistas, hay que decir que la mayoría de las contraseñas se roban adivinándolas o porque alguien las ha escrito en un Post-it.

En general, dado que todo lo que enviamos o recibimos puede ser interceptado y leído (texto) o utilizado (archivos o programas), debemos aceptar la idea de que todo puede ser examinado o robado si nos encontramos en un lugar donde otras personas pueden conectar con la red que estamos utilizando.

Quién debe preocuparse y por qué

Combinemos las variables de los tipos de datos que recorren la red inalámbrica y la ubicación de esa red para evaluar los riesgos reales y determinar qué secciones de este capítulo son más importante para leer.

- Si es un usuario doméstico sin vecinos muy cercanos o espacios públicos próximos y no piensa que sus datos sean demasiado sensibles, no tiene mucho de qué preocuparse. Como mucho, lea la sección posterior

"Proteger sus sistemas" para ver si desea tomar medidas para impedir que alguien pueda atacar a sus ordenadores desde Internet. Por lo demás, puede saltarse el resto del capítulo.

- Si es un usuario doméstico en un entorno urbano, debe leer la sección "Impedir el acceso a la red" y la parte dedicada a la protección de contraseñas de correo electrónico de la sección "Asegurar los datos en tránsito". Si le preocupa la sensibilidad de los datos, lea también el resto de la sección "Asegurar los datos en tránsito". También merecerá la pena que lea la sección "Proteger sus sistemas", por si acaso.
- Si utiliza o mantiene una red inalámbrica en su oficina, debe leer todo el capítulo, reflexionando en serio acerca de los factores de riesgo que afronta su compañía. En particular, en la sección "Asegurar los datos en tránsito", piense lo lejos que quiere ir en la protección de los datos.
- Si utiliza regularmente redes inalámbricas durante sus viajes, lea la sección "Asegurar los datos en tránsito". Cuanto más sensibles sean sus datos, más seriamente debe reflexionar sobre las distintas estrategias que muestra la sección.

Impedir el acceso a la red

Con sólo algunos pasos puede desalentar a los navegantes casuales que quieran entrar en su red. Estos pasos son la primera línea de defensa, pero pueden ser suficientes para los usuarios domésticos.

Hay tres herramientas principales para desalentar el acceso a la red: cerrar la red, usar el cifrado WEP y limitar el acceso a adaptadores de red inalámbrica específicos.

Cerrar la red

Cuando desplegamos una red inalámbrica, empezamos por una elección fundamental: ¿la red va a ser abierta o cerrada? Esta elección queda a menudo oscurecida por el marketing y la complejidad. Desgraciadamente, cerrar la red suena mejor de lo que es realmente.

En el caso de una red abierta, el punto de acceso está constantemente emitiendo el nombre de la red. Eso facilita que un navegante casual vea la red y conecte con ella.

La mayoría de los puntos de acceso ofrecen una opción simple que permite ocultar el nombre de la red. Algunos llaman a esta opción "red cerrada", otros "deshabilitar la emisión de nombre". La terminología no importa, el nombre de una red cerrada no aparece en la lista de redes disponibles del software cliente (vea la figura 6.1).

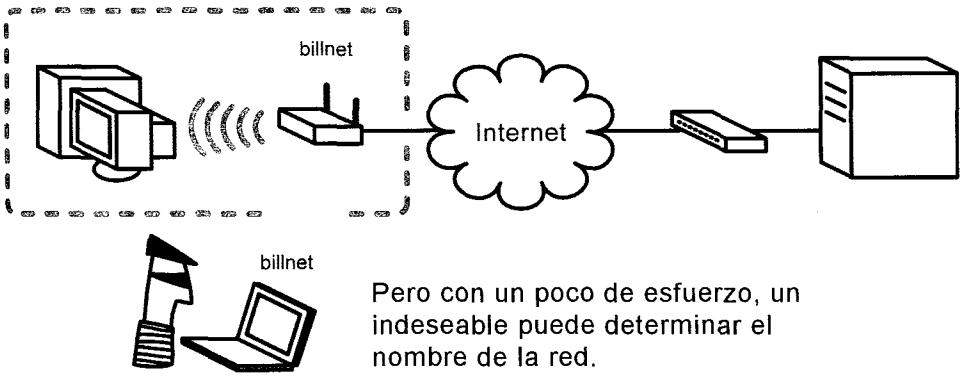

Figura 6.1. Cerrar la red impide que usuarios casuales vean el nombre de la red.

Pero no se deje engañar por un sentido de falsa complacencia. Aunque una red cerrada ofrece protección frente a los observadores casuales, todo el software de rastreo que comentaremos más adelante en la sección "Conocer al enemigo" puede obtener el nombre de la red sin esfuerzo.

Resumiendo, si no desea que la gente pueda conectar con su red, no hay inconveniente en que la convierta en una red cerrada, pero las únicas personas a las que impedirá la entrada serán las que en definitiva no plantean ningún riesgo de seguridad.

Dicho esto, cerrar la red es útil si no quiere compartir la conexión de Internet con todo el que pasa, pues a menos que alguien se haya molestado en instalar un programa de rastreo y en entender su funcionamiento, no podrá ver la red cerrada.

Cifrado WEP

Las personas que desarrollaron el estándar 802.11b pretendían que WEP (Privacidad equivalente de cable) hiciera precisamente lo que dice su nombre: ofrecer la privacidad equivalente a la que había en una red de cable estándar. Para comprometer una red de cable, un atacante generalmente tiene que entrar en una habitación e instalar un programa de rastreo que observe el tráfico que

viaja por el cable. WEP se diseñó para actuar como una puerta cerrada, para impedir que los intrusos penetraran en el propio tráfico de la red inalámbrica; la idea era que otras medidas complementaran esta línea de defensa inicial. WEP básicamente cifra todos los datos que fluyen por la red inalámbrica, impidiendo que los atacantes rastreen el tráfico de la red (vea la figura 6.2).

Desgraciadamente, incluso esta protección bastante mínima se vio mermada por varias decisiones de criptografía y porque algunas opciones se integraron pero nunca fueron habilitadas. Además, aunque el cifrado WEP sigue ofreciendo cierta protección, la mayoría de la gente no lo activa porque es una molestia utilizarlo.

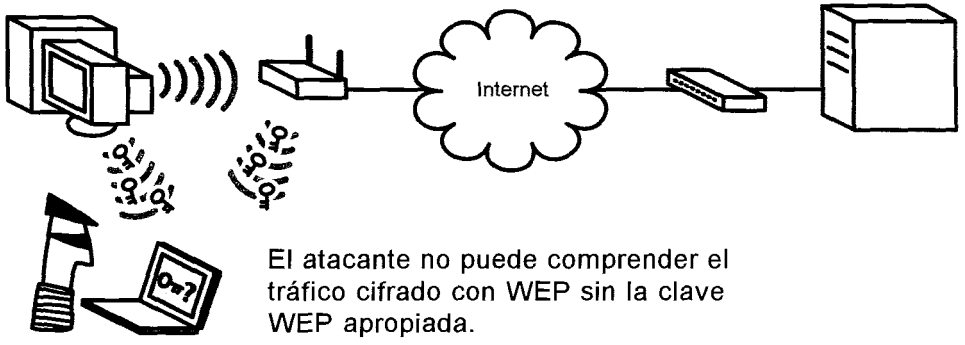

Figura 6.2. *Activando WEP impedimos que los atacantes espíen el tráfico de la red.*

Nota *La mayoría de los sistemas que requieren que el usuario escriba largas secuencias de caracteres aleatorios también utilizan algo llamado comprobación de suma (checksum), que es un cálculo efectuado sobre la cadena de texto. Cuando escribimos la cadena solicitada, el sistema comprueba dos veces la entrada calculando su checksum: si las dos checksums no coinciden, el sistema dice al usuario que hay un error. No tenemos idea de por qué el cifrado WEP no tiene esta parte del protocolo. Sólo podemos suponer que los diseñadores nunca pensaron que millones de usuarios escribirían claves WEP.*

El cifrado WEP funciona utilizando un "secreto compartido": una clave de cifrado (hasta cuatro por red) compartida por todos los usuarios de la red. El adaptador de red inalámbrica utiliza la clave de cifrado para codificar todo el tráfico antes de que salga del ordenador. Después, cuando llegan los datos, el punto de acceso utiliza la clave para decodificarlos en su forma original.

Los usuarios deben introducir a mano (tediosamente) la clave WEP en cada ordenador que vaya a formar parte de la red protegida por WEP. Aún peor, la clave se expresa a menudo en el sistema de numeración hexadecimal de base 16 en el que las letras de la A a la F representan los números del 10 al 15 con un solo dígito. La mayoría de los usuarios no tienen la menor idea de cómo enfrentarse a los números hexadecimales (algo razonable, ¡para eso están los ordenadores!). Si combina la confusión de los usuarios con lo aburrido que es inventar (en el punto de acceso) e introducir cadenas de números hexadecimales, puede imaginar por qué utilizar el cifrado WEP resulta molesto.

Nota

De Kudos a Microsoft sobre cómo configurar su Estación Base Inalámbrica: la forma predeterminada es guiar al usuario para que añada una clave WEP de 128 bits y guarde la copia de seguridad en un disquete.

Habilitamos WEP en un punto de acceso inventando una secuencia de 10 ó 26 dígitos hexadecimales (correspondientes a una clave 40/56/64 o a una clave de 104/128 bits). Afortunadamente, algunos puntos de acceso tienen una función en la que escribimos una frase de paso y es el punto de acceso el que la convierte en dígitos hexadecimales. Si los clientes y el punto de acceso pueden admitir la clave WEP más larga, utilícela; cuanto más larga mejor, aunque sólo un poco mejor.

Truco

Vea los capítulos 4 y 5 para encontrar trucos sobre cómo introducir claves WEP en el software cliente y los puntos de acceso. Fíjese especialmente en los trucos para utilizar el cifrado AirPort de Apple para trabajar en una red con ordenadores y dispositivos sin tarjetas AirPort.

Cómo se rompe WEP

Aparte de la dificultad de uso, ¿cómo se rompe WEP desde el punto de vista de la seguridad? Ésta es una rápida gira por los principales puntos débiles de WEP:

- **Secreto compartido:** Cada ordenador de una red inalámbrica protegida con WEP necesita un grupo de cuatro claves que los usuarios deben generalmente escribir y que a veces se leen como texto puro. La complejidad de la gestión de claves facilita a los atacantes conseguir una clave mediante trato social (preguntando la clave a alguien), descuido (la cla-

ve escrita en un trozo de papel perdido) o descontento (un empleado despedido). La mayoría de las claves no cambian después de haber sido introducidas por primera vez.

- **Problemas del vector de inicialización:** El vector de inicialización es un fragmento de 24 bits de una clave WEP de 64 ó 128 bits que se supone que ayuda a aumentar el número de claves diferentes posibles generadas a partir de los bits restantes variando las claves con el tiempo. Desgraciadamente, el uso del vector de inicialización es optativo, y muchos fabricantes no lo utilizan en absoluto, y no está bien implementado, de modo que aunque los fabricantes utilicen el vector de inicialización en las claves WEP, éstas no varían de forma compleja y aleatoria. Los ataques que utilizan el vector de inicialización incluyen vigilar la reutilización de claves, que sólo debería suceder después de periodos extremadamente largos (si acaso), pero en situaciones de tráfico denso ocurre después de sólo algunas horas.

Truco *¿Se ha preguntado por qué hablamos de claves WEP diciendo que son de 40/56/64 bits y 124/128 bits en lugar de decir que son simplemente de 64 bits y de 128 bits? Algunas compañías y en algunos debates se excluye o cuenta incorrectamente el vector de inicialización de 24 bits como parte de la longitud total de la clave.*

- **Defectos de RC4:** El algoritmo de cifrado RC4 tal como lo implementa WEP puede ser roto fácilmente interceptando pasivamente entre 1.000.000 y 6.000.000 de paquetes de datos. En una red con tráfico denso, esa cantidad de datos puede atravesar un punto de acceso en cuestión de minutos. Las redes que utilizan una simple frase de paso WEP en lugar de una clave hexadecimal pura se ven comprometidas más fácilmente; pero aunque romper el cifrado RC4 en redes que utilizan claves WEP hexadecimales lleva algo más de tiempo, no es bastante para proporcionar verdadera seguridad.

Quizá piense que estos problemas son poco claros, especialmente los dos últimos, pero un atacante no necesita un conocimiento especializado para aprovecharlos; las herramientas automatizadas se ocupan de todo el trabajo.

Truco *Para más información acerca de los problemas de cifrado inalámbrico, vea el informe del estado de la seguridad, regularmente actualizado, de Glenn en http://80211b.weblogger.com/weak.defense.html.*

A pesar de estos fallos de WEP, un usuario de una red con relativamente poco tráfico y con poco de qué preocuparse en cuanto a intercepción (contraseñas, pero no datos importantes) puede generalmente confiar en el cifrado WEP como medio para proteger la red. Una persona tiene que estar muy determinada y posiblemente espiar la red durante días o semanas, para reunir las piezas necesarias para romper una clave WEP.

El futuro de WEP

El comité 802.11i del IEEE ha estado trabajando durante años en un reemplazo para WEP con una solución compatible con ese cifrado que devolverá a WEP su papel como primera línea de defensa. Idealmente, esta solución también proporcionará una forma fiable para que las redes pequeñas aseguren su tráfico completamente.

La última propuesta está programada para ser ratificada a mediados de 2003, aunque el equipamiento que incluya la tecnología puede aparecer antes. El nuevo estándar se llama TKIP o Protocolo de integridad de clave temporal. Las actas de reuniones del comité indican que gozará de mucho soporte para garantizar que TKIP funcionará en equipos anteriores gracias a actualizaciones de firmware.

Nota

Originalmente, TKIP llevó el nombre de WEP2, pero debido a los defectos de WEP que hemos expuesto, el comité decidió optar por un nombre totalmente nuevo.

Es posible que soluciones todavía más sofisticadas se conviertan en parte de varios protocolos de red. La barrera que cierra el paso a las soluciones más sofisticadas es que los algoritmos requeridos implican chips dedicados para gestionar la computación criptográfica. El coste de los chips baja continuamente, de modo que probablemente veamos estas soluciones de seguridad más sofisticadas en un futuro no muy lejano.

Control de acceso por adaptador de red

Hay una forma de restringir el acceso a una red y es permitiendo la conexión a sólo adaptadores de red específicos (vea la figura 6.3). Como todos los adaptadores de red Ethernet, los adaptadores Wi-Fi están identificados por

su dirección MAC (Control de acceso a medios), un número de serie único asignado a cada adaptador de red.

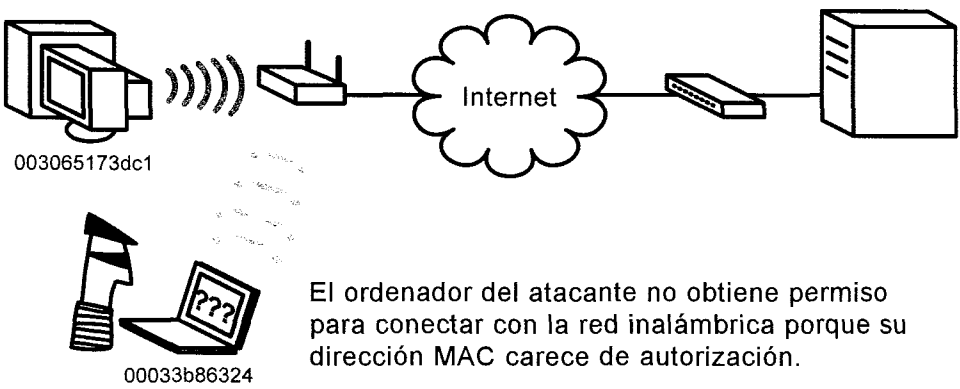

Figura 6.3. *Restringir el acceso mediante dirección MAC impide que los ordenadores no autorizados entren en la red inalámbrica.*

Sin embargo, como hemos señalado en el capítulo 2, las direcciones MAC no son inmutables y pueden ser falsificadas fácilmente. Muchas puertas de enlace y puntos de acceso permiten introducir direcciones MAC distintas para simplificar la conexión con ISP que sólo permiten conectar a un adaptador de red determinado.

De cualquier forma, esta flexibilidad, combinada con el hecho de que las direcciones MAC se envían a las claras incluso en redes que tienen habilitado el cifrado WEP, significa que un cracker puede ver fácilmente las direcciones MAC que se están utilizando y asignar una de esas direcciones a su equipo. Por tanto, igual que en las redes cerradas, restringir el acceso utilizando la dirección WEP sólo impedirá el paso a la gente honesta, pero no supondrá un impedimento a un intruso decidido.

EAP, PEAP, LEAP y 802.1x

Los problemas de WEP se centran en su uso de claves compartidas, que sólo pueden ser cambiadas manualmente. Hay una mejora significativa sobre WEP que soluciona este problema, pero actualmente requiere hardware de marca más caro, software cliente e incluso servidores de red de última línea.

EAP (Protocolo de autenticación extensible), PEAP (EAP Protegido) y LEAP (La versión de Cisco de EAP) funcionan todos independientemente o como parte de un armazón llamado 802.1x asegurando cla-

ves en una red de forma más flexible, rápida e individual que WEP. Estos nuevos tipos de autenticación permiten a cada cliente iniciar una conexión con un punto de acceso, negociar su propia clave individual con un servidor de autenticación basado en red (seguramente de varias maneras, dependiendo del tipo de EAP) y después rotar las claves rápidamente para impedir que una de las claves sea utilizada durante un tiempo lo bastante largo como para ser rota.
902.1x actúa como una forma general de introducir estos protocolos de autenticación en la red; Microsoft incluyó una versión de 802.1x en Windows XP. El nuevo WPA (Acceso protegido Wi-Fi) de la Wi-Fi Alliance pone 802.1x y EAP en todo el hardware certificado por Wi-Fi desde la primavera de 2003 y lo convertirá en un requerimiento a finales de 2003.
Como 802.1x puede funcionar a través de red local o Internet, esperamos que los ISP añadan estos tipos de protocolos de rotación negociada de clave para que los usuarios domésticos y las oficinas pequeñas puedan aprovechar la seguridad adicional sin construir sistemas de red completos.
Para más información sobre estos sistemas, lea el artículo acerca de la autenticación inalámbrica en www.cisco.com/warp/public/784/packet/exclusive/apr02.html.

Trabajos en desarrollo: WPA

Aunque el trabajo del 802.11i sigue en desarrollo en el momento de escribir este libro, la Wi-Fi Alliance decidió abordar inmediatamente el problema de la seguridad. En noviembre de 2002, distribuyó una actualización interina del cifrado Wi-Fi que se apoya en el trabajo del comité 802.11i hasta la fecha. El estándar, llamado WPA (Acceso protegido Wi-Fi) corrige algunos de los defectos de WEP y añade soporte para 802.1x y EAP.
WPA aumenta el tamaño del vector de inicialización a 48 bits, garantizando que la elección de ese número no es predecible. Este cambio amplía mucho la complejidad del sistema de cifrado, en varios órdenes de magnitud. La integridad de los paquetes ahora también está garantizada, que significa que un intruso no puede insertar en un sistema paquetes falsos que parecen proceder de un adaptador o punto de acceso.

Los usuarios domésticos ya no tienen que introducir complicadas claves WEP, sino que basta con una simple contraseña que genera un grupo de claves de cifrado que el cliente hace rotar. Las claves se modifican mediante un algoritmo que coge parte de una clave maestra y la combina con un vector de inicialización aleatorio, de modo que cada paquete tiene su propio cifrado.

Todavía no hemos visto estimaciones, pero es probable que romper una clave requiera, en lugar de millones de paquetes (horas o días), miles de millones o posiblemente billones de paquetes (semanas o cientos de años). Los expertos en criptografía empezarán a evaluar el nuevo estándar inmediatamente.

Para usuarios corporativos, la adición de soporte integrado a 802.1x y EAP reduce los costes y la complejidad añadiendo una fuerte seguridad inalámbrica. Como Microsoft y Apple son miembros de la Wi-Fi Alliance, es casi seguro que el soporte necesario en los sistemas operativos aparecerá al mismo tiempo que las actualizaciones de hardware.

Los cambios del WPA serán compatibles con gran parte del hardware anterior existente, haciendo que la conformidad con el estándar sea posible gracias a actualizaciones del firmware de adaptadores de red y puntos de acceso. La compatibilidad con lo anterior fue uno de los objetivos del comité 802.11i, pero quizá no sea posible actualizar todos los aparatos antiguos. WPA requiere que cada aparato de una red inalámbrica incluya soporte a WPA. Si un solo adaptador sigue precisando que se utilice WEP, toda la red retrocederá a cifrado WEP.

Dado que la Wi-Fi Alliance certifica la conformidad del hardware, el estándar WPA se convertirá en una parte imprescindible que los fabricantes deberán incorporar en su hardware para que esté certificado con la marca Wi-Fi. La Wi-Fi Alliance ha dicho que empezará a certificar la conformidad de las piezas de equipamiento con WPA en febrero de 2003 y que WPA será imprescindible para conseguir la aprobación de Wi-Fi a finales de 2003.

Para ver los últimos detalles de la disponibilidad y el soporte a WPA, vea el informe del estado de la seguridad, regularmente actualizado, de Glenn en http://80211b.weblogger.com/weak.defense.html.

Truco *Muchas redes ni siquiera utilizan la dirección MAC para autenticar usuarios, sino que utilizan la dirección IP asignada por DHCP, ¡que*

todavía es más fácil de adivinar! Lea este preocupante informe en la revista New Architect en 222.newarchitectmag.com/documents/s=2445/na0902h/.

Asegurar los datos en tránsito

Como hemos comentado en la sección anterior, sólo podemos disuadir de unirse a la red a los transeúntes casuales, especialmente si están pasando cantidades significativas de datos de un lado a otro. En lugar de hacer hincapié en mantener a la gente fuera de la red inalámbrica, hay que pensar en cifrar parte, la mayoría o todos los datos en tránsito entre el ordenador y su destino. Creando enlaces cifrados extremo a extremo mediante estándares fuertes, actualmente irrompibles, podemos mantener la seguridad de los datos frente a posibles maleantes. Incluso si alguien consigue unirse a la red y llegar a Internet, pirateando nuestra conexión, sigue sin poder ver los datos. Cifrar los datos en tránsito es mucho más difícil que configurar una red cerrada y protegida por WEP, pero también mucho más prudente.

Truco

Una ventaja añadida del cifrado de datos extremo a extremo es que los datos no sólo resultan completamente ilegibles en la red inalámbrica, sino también en todos los enlaces de la red entre el ordenador y la máquina destinataria. Ésa es la razón por la que las organizaciones grandes suelen requerir que sus empleados utilicen tecnología de cifrado.

Vamos a ver cuatro categorías y métodos populares para asegurar datos, que van desde la simple protección mediante contraseña al cifrado de red completo de todos los datos de cualquier tipo.

Cifrado de contraseña de correo electrónico

Como queda dicho, incluso aunque no resulte preocupante que la gente pueda leer nuestro correo electrónico, sí hay que tomar precauciones para proteger las contraseñas de cuentas (vea la figura 6.4).

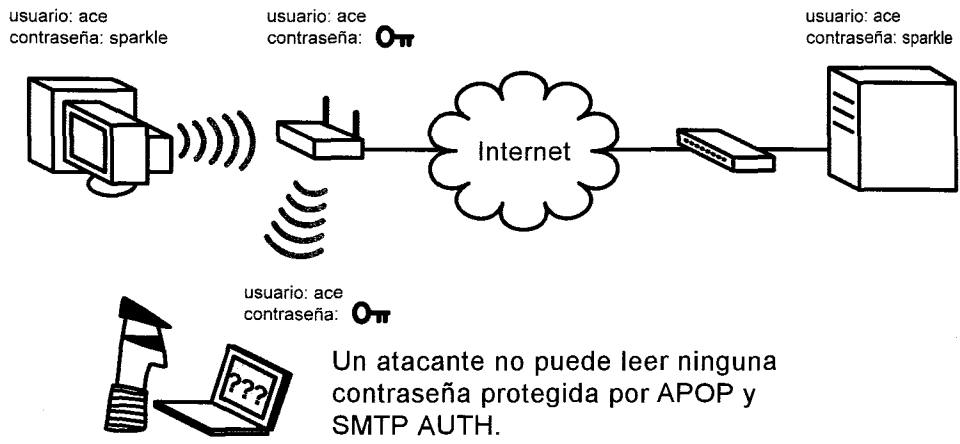

Figura 6.4. Cifrar las contraseñas de correo electrónico impide que puedan ser robadas.

Nota *No olvide que muchos sitios Web utilizan los nombres de usuario y contraseñas sólo para identificación y no aseguran las páginas cuando piden esas contraseñas. Como estas contraseñas se roban fácilmente, garantice que son distintas de las que utiliza en el correo electrónico o en sitios con información más sensible.*

Hay principalmente dos métodos de cifrar sólo la contraseña, y los dos deben gozar de soporte en el servidor de correo, aunque casi todos los servidores de correo modernos tienen estas opciones.

Es probable que el ISP o el administrador de red ya los hayan habilitado, requiriendo sólo que establezcamos una opción en el programa de correo electrónico.

APOP

APOP (POP Autenticado) protege la contraseña cuando obtenemos el correo entrante de un servidor POP (Protocolo de oficina de correos). En lugar de enviar la contraseña a las claras, APOP envía una señal única por sesión que el servidor utiliza para confirmar que el programa de correo electrónico conoce la contraseña correcta.

APOP no cifra los mensajes de correo electrónico ni hace nada aparte de proteger la contraseña.

SMTP AUTH

SMTP AUTH (la parte AUTH es en realidad un comando SMTP) identifica al usuario ante el servidor SMTP cuando queremos enviar mensajes salientes. Técnicamente, no hay razón para requerir autenticación al enviar correo, pero SMTP AUTH se ha convertido en un lugar común en esta época de correo basura, pues si un servidor SMTP requiere SMTP AUTH, impide que alguien envíe correo basura utilizando el servidor.

Otra ventaja de SMTP AUTH es que permite enviar correo desde cualquier lugar conectado a Internet (como una cafetería con red inalámbrica en otra ciudad), no sólo desde las ubicaciones de red específicas que haya definido el administrador de sistema.

SMTP AUTH generalmente utiliza el mismo nombre de usuario y contraseña que empleamos para comprobar el correo vía POP o IMAP.

Cifrar contenido

Aunque recomendamos proteger como mínimo las contraseñas, hay un punto medio entre cifrar las contraseñas y cifrar todos los datos: utilizar cifrado de contenido en archivos y mensajes de correo electrónico específicos. Esta estrategia permite proteger el contenido más sensible. El cifrado de contenido también hace que sea muy improbable que cualquier persona que no sea el destinatario pueda leer el archivo o el mensaje de correo electrónico. Eso es porque cuando ciframos el contenido a mano en nuestro extremo, generalmente eso requiere que el destinatario lo descifre con una acción manual en el otro extremo. El software más popular que cifra el contenido de mensajes y archivos enteros es PGP (Privacidad bastante buena). PGP utiliza criptografía de clave pública para asegurar un mensaje de modo que sólo el destinatario pueda leerlo (vea la figura 6.5).

Nota

A mediados de 2002, Network Associates vendió PGP a una nueva compañía, PGP Corporation, que se comprometió a desarrollar y ampliar el soporte del software (www.pgp.com).

Cómo funciona la criptografía de clave pública

En sistemas de criptografía de clave pública, cada usuario genera un par de claves, una pública y la otra privada. Utilizando combinaciones de las dos

claves, los usuarios pueden firmar archivos o mensajes para demostrar que son los remitentes y pueden cifrar archivos o mensajes para que sólo su destinatario pueda abrirlos. Las claves se combinan como las piezas de un puzzle: si alguien cifra algo con nuestra clave pública, sólo nuestra clave privada es capaz de descifrarlo. Y, si firmamos algo con nuestra clave privada, sólo nuestra clave pública puede verificar que lo hemos firmado.

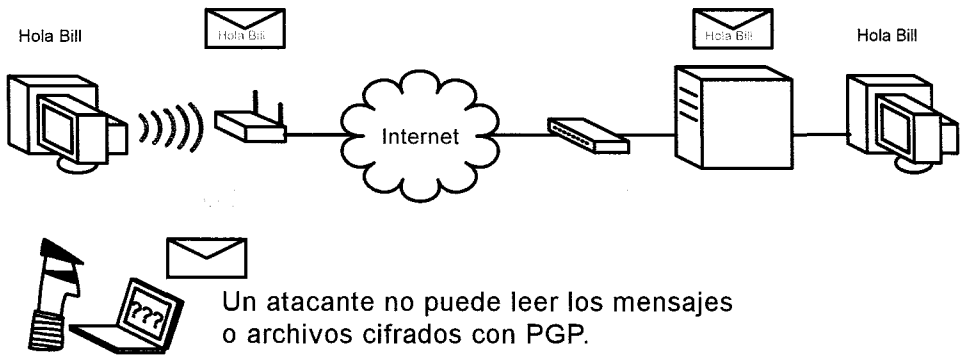

Figura 6.5. *Cifrar mensajes de correo electrónico y archivos específicos con PGP impide que un pirata informático lea esos mensajes o archivos.*

Como ejemplo, supongamos que Glenn y Adam establecen PGP para poder intercambiar borradores cifrados de este libro sin preocuparse por el espionaje industrial de otros editores que desean ver el libro antes de su publicación. (En realidad, no somos, ni mucho menos, tan paranoicos.)

El primer paso en la criptografía de clave pública es generar una clave pública y una clave privada. Junto con las claves, hay que generar una frase de paso que permita descifrar y abrir la clave privada propia para utilizarla. Adam y Glenn recorren estos pasos, de modo que cada uno tiene claves pública y privada, y después comparten sus claves públicas uno con otro. He aquí cómo funciona.

Adam quiere enviar a Glenn un mensaje de correo electrónico importantísimo sobre las fechas de entrega de los capítulos del libro. A Adam no le preocupa que alguien más vea el mensaje, pero quiere garantizar que Glenn sepa que es él quien lo ha enviado y que no lo ha falsificado algún bromista desde Internet. (La falsificación de correo electrónico es bastante sencilla, aunque hacerlo de modo que no se puedan seguir los pasos o notar que es una falsificación es más difícil.) Por tanto, Adam firma el mensaje utilizando su clave privada.

Cuando Glenn recibe el mensaje, puede leerlo sin problema, pero para verificar que de verdad procede de Adam, utiliza la clave pública de Adam para comprobar la firma. Cuando coinciden, Glenn sabe que el mensaje es legítimo

(vea la figura 6.6). Si alguien hubiera utilizado otra clave privada para firmar el mensaje, no habría coincidido con la clave pública de Adam y la verificación de firma habría fallado.

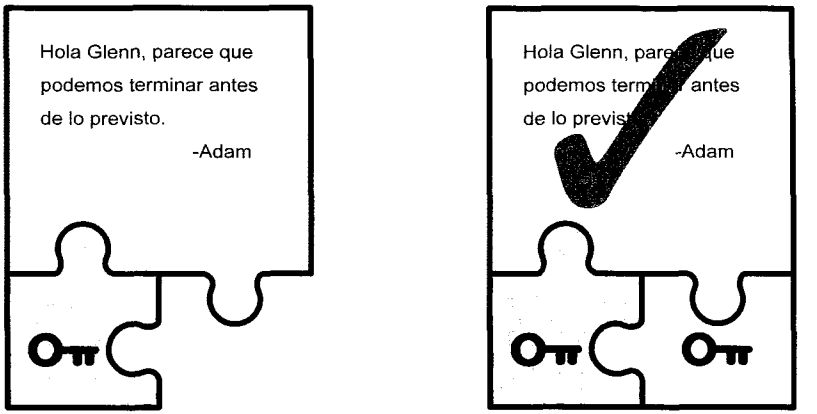

Figura 6.6. *Firma y verificación de un mensaje.*

A continuación, supongamos que Glenn quiere enviar a Adam un borrador del libro, pero como sospecha que uno de sus vecinos puede estar espiando el tráfico de su red inalámbrica, decide cifrar el archivo antes de enviarlo. Esta vez, Glenn utiliza la clave pública de Adam para cifrar el archivo y después lo envía. Cuando Adam recibe el archivo, utiliza su clave privada para descifrarlo (vea la figura 6.7). Si alguien interceptara el archivo e intentara descifrarlo, no podría porque sólo la clave privada de Adam puede descifrar los archivos cifrados con su clave pública.

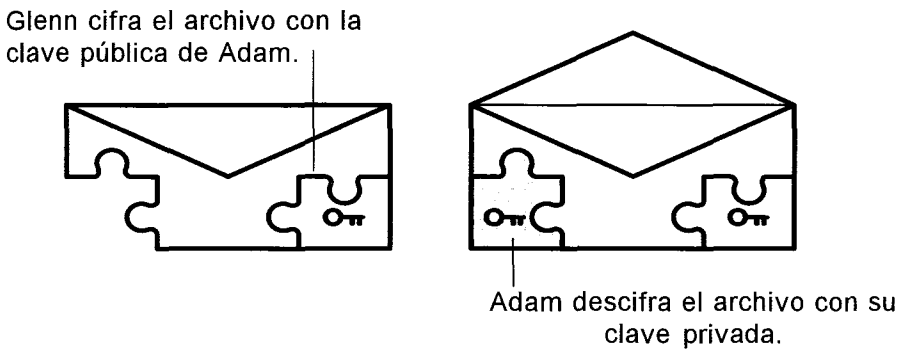

Figura 6.7. *Cifrar y descifrar un documento.*

En este ejemplo puede ver lo importante que es guardar segura la clave privada y no compartirla con nadie. Si alguien consiguiera nuestra clave privada, podría fingir que somos nosotros y descifrar la información cifrada que nos enviaran. De hecho, si la seguridad de la clave privada se viera comprometida, habría que revocar la clave pública asociada.

Que las claves públicas puedan compartirse sin poner en peligro el cifrado es lo que hace que la criptografía de clave pública sea un método único. Pero compartir la clave pública es también su talón de Aquiles: ¿cómo distribuimos nuestra clave pública y recibimos claves de otras personas para la primera transacción? Podemos simplemente enviarla por correo electrónico, incluirla en nuestra firma de correo electrónico, ponerla en nuestro sitio Web o colgarla en un directorio público, llamado un *servidor de claves* (como www.keyserver.net). Aunque todos estos métodos son válidos, ninguno de ellos es infalible, pues alguien puede suplantarnos y falsificar un correo simulando que procede de nosotros o colgar una clave en el servidor de claves diciendo que es la nuestra. Una vez que la clave falsa está en circulación, revocarla es peliagudo.

La solución es intercambiar las claves de modo que se garantice la identidad de la otra parte. Por ejemplo, Glenn y Adam podrían haber creado sus claves públicas durante una comida juntos: ver a la otra persona enfrente es una gran forma de verificar la identidad. Un poco menos seguro, pero más razonable, es utilizar un teléfono o un fax; en esos casos no hay que leer o escribir toda la clave pública (que es un método demasiado largo para la trascripción exacta). En lugar de ello, se transmite una secuencia más corta de letras y números que permite a la otra persona garantizar que la clave pública enviada procede de donde debe (la secuencia de letras y números recibe el nombre de *huella dactilar*).

Ciertas personas ponen sus huellas dactilares en su firma de correo electrónico, suponiendo que un destinatario puede enviarles un mensaje de correo electrónico para verificar la identidad.

Afortunadamente, aunque puede ser complicado verificar que una clave pública pertenece a una persona concreta, el peor resultado posible es que alguien distribuya una clave pública utilizando nuestro nombre, poniendo en cuestión los documentos firmados por nosotros. Pero cuando alguien nos envía un archivo o mensaje cifrado que utiliza esta clave pública falsa, no podemos descifrarlo con nuestra clave privada. Esto nos avisa de posibles problemas pero nuestra seguridad sigue intacta.

Una vez que tenemos una clave pública de alguien y hemos verificado quién es, podemos intercambiar mensajes con seguridad durante el tiempo de vida de la clave. Muchas claves públicas tienen fecha de caducidad para aumentar la seguridad.

Utilizar PGP

Es necesario un software especial para firmar o cifrar (y verificar o descifrar) archivos y mensaje utilizando PGP. Puede descargar versiones gratuitas (visite www.pgpi.org/products/pgp/versions/freeware/) o comprar una versión comercial de PGP Corporation (www.pgp.com). La versión comercial ofrece funciones extra y es más fácil de usar, y además incluye soporte técnico.

Muchos programas de correo electrónico prestan soporte a PGP a través de *plug-ins*. Por ejemplo, la versión 9 de PGP Corporate Desktop para Mac OS X incluye los plug-ins Microsoft Entourage y Apple Mail. Dentro del programa, podemos componer un mensaje, seleccionar una opción y reemplazar un mensaje por su versión cifrada antes de enviarlo. Igualmente, podemos descifrar un mensaje entrante con una opción de menú. Si está interesado en utilizar PGP con frecuencia, busque utilidades que puedan facilitar su uso. Si hay un problema que siempre ha caracterizado a PGP, y a los sistemas de criptografía pública en general, es la dificultad de uso.

SSH (Shell seguro)

SSH se creó originalmente como un método para establecer sesiones de terminal que crean un túnel, una conexión extremo a extremo, entre un ordenador cliente y un servidor (vea la figura 6.8). SSH era necesario porque el protocolo telnet enviaba toda la información a las claras, permitiendo que cualquier espía en la red obtuviera los datos.

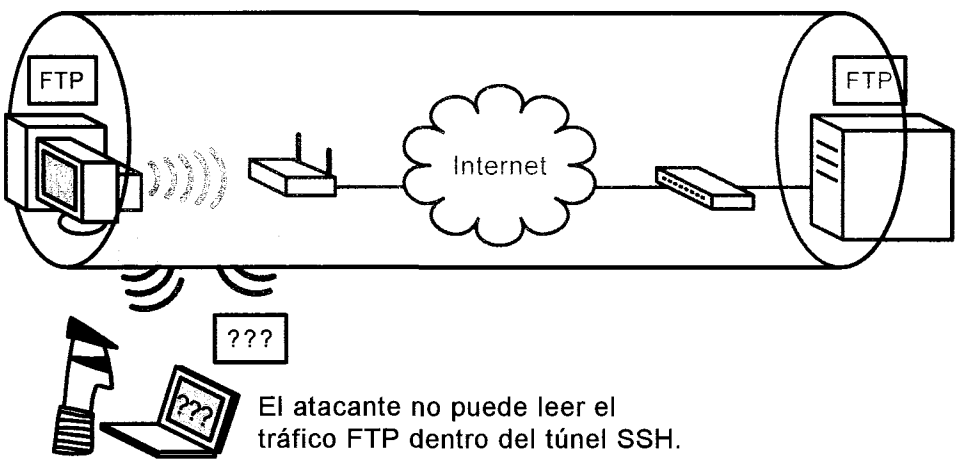

Figura 6.8. *Creando un túnel seguro con SSH protegemos los datos dentro del túnel.*

SSH se ha expandido mucho más allá de su propósito original. Ahora permite crear túneles para cualquier tipo de protocolo, ya sea POP y SMTP, FTP, Web o incluso Timbuktu Pro. Hace esto con un truco llamado *reenvío de puertos*, en el que se conecta un puerto local del ordenador con un puerto remoto del servidor.

Cómo funciona SSH

SSH cifra todo el contenido de cualquier sesión y está considerado como muy seguro. SSH, por omisión, no utiliza confianza externa: el intercambio inicial entre un servidor y un cliente para establecer una relación de confianza para sesiones futuras requiere confianza ciega o el uso de un código de confirmación, también llamado huella dactilar.

Nota *Un servidor SSH genera una huella dactilar para su clave de cifrado y, cuando conectamos por primera vez desde un cliente, podemos hacer una comprobación doble de que la huella dactilar que ve el cliente es idéntica a la del servidor. Si ejecuta su propio servidor, puede obtener usted mismo la huella dactilar (vea la documentación de OpenSSH). En caso contrario, pregunte al administrador de sistema.*

El reenvío de puertos con SSH implica conectar un puerto del ordenador local con un puerto de una máquina remota utilizando como conector un túnel SSH cifrado como conector. Por ejemplo, si queremos obtener el correo electrónico POP a través de un túnel SSH, primero establecemos el túnel entre el puerto POP (110) de la máquina y el servidor remoto. Después, configuramos el programa de correo electrónico para que recoja el correo de la dirección IP 127.0.0.1, que es un alias de la máquina local, en ese mismo puerto 110. El software SSH intercepta peticiones de conexión en ese puerto del programa de correo y envía esas conexiones, cifradas, al servidor de correo especificado; las respuestas pasan por el mismo túnel cifrado. El principal inconveniente de SSH es que hay que tener acceso a un servidor que pueda ejecutar SSH en su extremo de la conexión. Si ejecuta sus propios servidores equipados o ajustados a SSH o puede trabajar con un ISP o administrador de red que desee configurar la conexión, esto no será un problema.

Nota *Si no tiene la opción SSH en sus servidores, puede probar servicios como Anonymizer.com (www.anonymizer.com) que ofrecen servicios de túnel SSH a cambio de una cuota.*

Software SSH

Configurar una conexión SSH requiere software adicional para todos los usuarios de Windows y los usuarios de sistemas Mac con versiones del Mac OS anteriores a Mac OS X. Igual que con muchos otros tipos de software, puede probar en el mundo del software gratuito o compartido o comprar un software comercial totalmente desarrollado. En ambos casos, el software ayuda a configurar todos los puertos, nombres de host y demás detalles, y después sólo hace falta un clic en un botón para activar la conexión.

Para encontrar software gratuito y compartido, compruebe la lista www.openssh.com/windows.htm.

Para ver paquetes comerciales de SSH que pueden ser más fáciles de usar o tener mejor soporte, compruebe el software de SSH Communications Security (www.ssh.com), F-Secure (www.f-secure.com) y VanDyke Software (www.vandyke.com).

Terminal SSH

SSH forma parte de la mayoría de las distribuciones Unix y Linux y está integrado en el núcleo Unix de Mac OS X. Invocamos a SSH desde la línea de comandos escribiendo un comando en un cursor de terminal.

En un cursor o dentro de un script, escriba lo siguiente:

```
ssh -l nombreusuario -L puerto:host.dominio:puerto host.dominio -f -N
-C
```

Por ejemplo, si el usuario "billg" quisiera acceso SSH en su servidor de correo POP (que utiliza el puerto 110) "correo.ejemplo.com", el comando SSH sería:

```
ssh -l billg -L 110.correo.ejemplo.com:110 correo.ejemplo.com -f -N -
C
```

Nota

Para los aficionados a la tecnología, los conmutadores de línea de comandos (los guiones seguidos de letras) significan: -l = usuario, -L = puerto de reenvío, -f = no salir si se cierra la terminal, -N = no guardar en búfer o esperar la salida y -C = comprimir.

Podemos poner todos los comandos de reenvío de puertos en una sola línea añadiendo simplemente otro conmutador `-L`. En este ejemplo, también reenviamos los puertos 25 (SMTP) y 80 (Web).

```
ssh -l billg -L 110:correo.ejemplo.com:110 -L 25:correo.ejemplo:25 -L
80:correo.ejemplo.com:8080 correo.ejemplo.com -f -N -C
```

Fíjese en el último elemento, `80:correo.ejemplo.com:8080`. Reenvía las peticiones Web (puerto 80) al puerto 8080 en el otro extremo de la conexión donde, en este ejemplo, se encuentra un servidor proxy que recibe peticiones, las envía y las devuelve a la máquina solicitante. Para más seguridad, podemos reenviar peticiones de un puerto a otro completamente distinto en la máquina remota. Esto puede evitar ciertos ataques automatizados.

Cuando apagamos o hibernamos el ordenador o cambiamos de red inalámbrica, hay que reiniciar la conexión SSH. Quizá primero haya que detener las conexiones SSH activas. Para ello, Glenn ejecuta el pequeño script Perl que mostramos a continuación. Reemplace `nombrehost.dominio` con su nombre de host totalmente cualificado y sustituya `nombreusuario` con su nombre de usuario. Además, añada cualquier declaración `-L` que necesite para otros puertos que no sean el POP y el SMTP que utilizamos aquí:

```
#!/usr/bin/perl
$host = "nombrehost.dominio";
$user = "nombreusuario";
open (PS, "ps auxw | grep 'ssh -l' | grep -v grep | awk '{ print \$2
}' |");
while (<PS>) {
   chop;
   system ("sudo kill -9 $_");
}
close PS;
system ("sudo ssh -C -l $user $host -L 25:$host:25 -L 110:$host:110 -
p 23 -N -f -C");
```

También puede utilizar un script más simple. Fíjese que en la segunda línea y quinta líneas se utilizan acentos graves (`).

```
#!/usr/bin/perl
@jobs = grep(/ssh -C/, `ps auxw`);
foreach (@jobs) {
   (undef, $job) = split /\s+/;
   `sudo kill -9 $job`;
   print "Killed ssh job $job\n";
}
system("sudo ssh -C -l nombreusuario nombrehost \
  -L25:nombrehost:25 -L110:nombrehost:110 -p 23 -N -f");
```

Truco *Si nunca antes ha utilizado Perl, escriba el script en un editor de texto y guárdelo como archivo de texto sin formato (no como archivo de Word, por ejemplo) en su directorio principal con el nombre tunnel.pl (vea la figura 6.9). En un cursor de terminal, escriba* `chmod u+x`

`tunnel`. Después, cuando quiera ejecutarlo, navegue hasta el directorio que aloja el script y escriba el nombre del script precedido de un punto y una barra inclinada: `./tunnel`. (No escriba el punto que da fin a la frase en ninguno de los dos comandos).

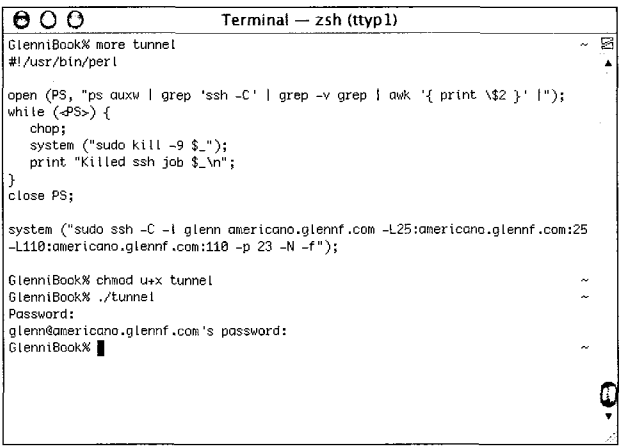

Figura 6.9. *Invocar el script de túnel.*

SSL (Capa de sockets seguros)

SSL fue desarrollado inicialmente para asegurar las transacciones financieras en la Web, pero ahora se utiliza mucho para asegurar transacciones de Internet de todo tipo.

SSL resuelve el problema del "problema compartido" de WEP utilizando una versión ampliada de criptografía de clave pública (vea la sección anterior "Cifrar contenido"). En lugar de requerir que la gente se ponga de acuerdo sobre un secreto (la clave de cifrado en WEP) por adelantado o que haya disponibles claves públicas, un navegador y un servidor equipados con SSL utilizan una tercera parte fiable, conocida como *autoridad de certificados*, para aceptar la identidad del otro.

Generalmente, SSL se utiliza para interacciones basadas en sesiones cortas, como enviar información de tarjeta de crédito a través de un formulario Web. Pero puede usarse para cifrar sesiones de correo electrónico (enviar y recibir), incluyendo todo el contenido del correo electrónico que va del cliente al servidor, FTP (en una forma generalmente conocida como FTP Seguro) y muchos otros tipos de transacciones. SSL es válido para cualquier servicio de

Internet que intercambia datos en fragmentos en lugar de hacerlo como información fluida. (Por ejemplo, se puede usar SSL para la mensajería instantánea pero no para reproducir música RealAudio.)

Como SSL es verificado por una tercera parte, no tenemos que utilizar la confianza (ciega o confirmada) como sucede en SSH.

Nota *SSL se utiliza mucho ahora porque las patentes subyacentes han caducado. Podemos encontrar SSL con nombres como EAP-TLS (Protocolo de autenticación encapsulada-Seguridad de capa de transporte, un tipo de PPP al que se añade seguridad), TLS/SSL u otras variaciones, pero todo es más o menos lo mismo.*

A diferencia de SSH, en el que podemos conectar dos puertos arbitrarios a través de un túnel (puerto a puerto), SSL funciona de programa a programa, con el cliente cifrando los datos y el servidor descifrándolos (vea la figura 6.10).

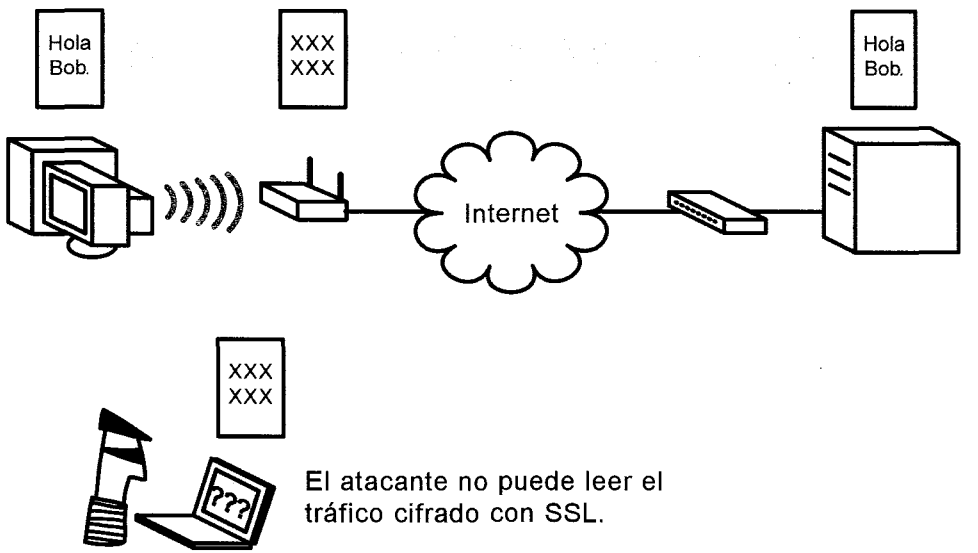

Figura 6.10. *Cifrando transacciones seleccionadas con SSL protegemos el contenido de esa transacción.*

Cómo funciona SSL

Cuando conectamos con una página Web protegida por SSL, el navegador y el servidor Web remoto deben negociar el intercambio de claves.

Primero, el navegador envía un mensaje que sólo el servidor puede leer, y el servidor utiliza la información del mensaje para empaquetar una clave de sesión pública junto con el certificado.

A continuación, el servidor envía la clave de sesión pública y el certificado al navegador, que entonces verifica que el certificado proviene de una autoridad de certificados fiable y que la clave de sesión del servidor es legítima. Dado que este primer intercambio es totalmente seguro y está verificado por una tercera parte, la clave de sesión puede utilizarse sin preocuparse porque pueda haber sido interceptada.

Habilitar SSL

A diferencia de PGP y SSH, cuando se trata de SSL raramente necesitamos introducir una contraseña, ejecutar un script o usar un programa independiente. El software cliente gestiona la comunicación y la autenticación como haría con una conexión no cifrada. En la Web, los navegadores y servidores modernos utilizan SSL cuando es necesario (asumiendo que los *webmasters* lo han configurado apropiadamente). Podemos saber que estamos viendo una página Web protegida con SSL porque a menudo aparece un pequeño icono de un candado cerrado en la esquina de la ventana. Además, podemos ver un signo indicador en el URL: en lugar de empezar con http, el URL empieza con https.

Muchos programas de correo electrónico prestan soporte a SSL y activarlo solamente requiere establecer una opción, a menudo oculta en el cuadro de diálogo de configuración avanzada. Desgraciadamente, no todos los servidores de correo prestan soporte a SSL y, aquellos que lo hacen, no todos gestionan SSL del mismo modo. Como resultado, algunos servidores de correo que admiten SSL no son compatibles con ciertos programas de correo que admiten SSL. Para saber si SSL es una opción válida para proteger su correo, consulte a su ISP o administrador de sistema o compruebe que instala un servidor de correo que es compatible con el software que ha decidido utilizar.

FTP puede asegurarse con SSL utilizando software gratuito y comercial. Para software gratuito, visite Glub Tech (www.glub.com) para encontrar un cliente FTP seguro basado en Java. Para software comercial, lea el artículo "Secure FTP 101" para ver una perspectiva general de FTP seguro y una lista de software comercial (www.intranetjournal.com/articles/200208/se_08_14_02a.html). Además, hay varias empresas de software en proceso de añadir soporte a SSL en su software cliente FTP.

Nota *Un paquete Windows y Unix llamado Stunnel (www.stunnel.org) permite a un administrador de sistema añadir SSL a prácticamente cual-*

quier servicio envolviendo con SSL el software de servidor existente en lugar de requerir un servidor FTP o de correo distinto.

VPN (Red privada virtual)

Como habrá notado, todas las soluciones de cifrado que hemos comentado hasta ahora son específicas para un tipo de servicio de Internet, para archivos o mensajes concretos, o para cierto software. ¿Por qué no cifrarlo todo? Para eso se necesita una VPN o red privada virtual. Las VPN son la solución definitiva para asegurar los datos porque en esencia crean un conducto cifrado, un túnel, entre el ordenador y un servidor VPN. Como los datos enviados o recibidos (correo electrónico, FTP, Web y demás) entre el ordenador y el servidor VPN están cifrados, no tenemos que preocuparnos por intrusos que puedan penetrar en la red inalámbrica. Si alguien entra en la red, no podrá descifrar el túnel que lleva toda la comunicación (vea la figura 6.11).

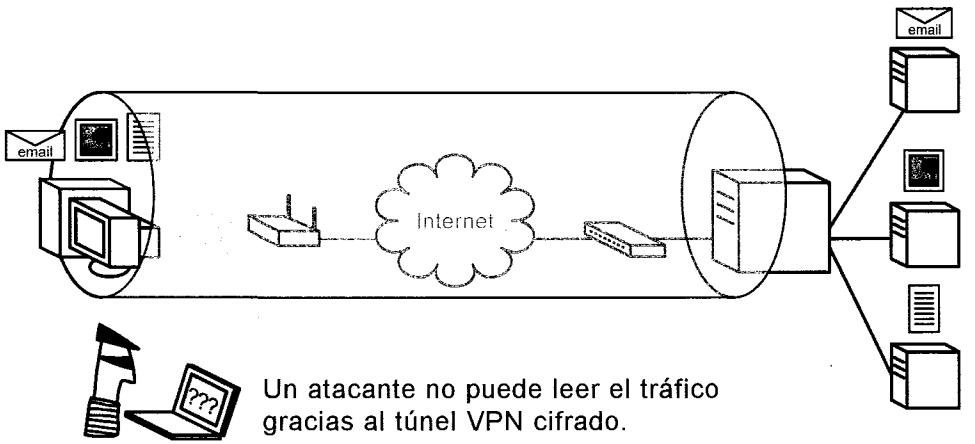

Figura 6.11. *Cifrado del tráfico dentro de un túnel VPN.*

El inconveniente de utilizar un VPN es que configurar un servidor VPN no es fácil actualmente. Requiere hardware dedicado y caro, y también control y mantenimiento continuo.

Han aparecido algunos puntos de acceso de nivel corporativo con servidores VPN integrados, que aseguran al menos las conexiones inalámbricas locales. Las pequeñas oficinas deben pensar en dispositivos de Colubris Networks (www.colubris.net) y otros.

Además, al menos un servicio casi ISP, Boingo Wireless, permite crear un túnel VPN utilizando sus servidores VPN. Boingo es un ISP inalámbrico de los EE.UU. que agrupa accesos de otras redes inalámbricas, proporcionando una sola cuenta de inicio de sesión y una sola factura, no importa cuál de las redes ISP inalámbricas de sus empresas asociadas se utilice (vea el capítulo 7). El software cliente Windows de Boingo incluye un cliente VPN integrado. Cuando conectamos a una red inalámbrica utilizando este cliente, el software VPN conduce por el túnel todo el tráfico al centro de operaciones de red de Boingo, donde es descifrado para atravesar el resto de Internet. Boingo piensa ofrecer también un cliente para sistemas Mac y solicitará una cuota mensual por usar su servicio VPN y el servidor de correo saliente SMTP AUTH.

Se utilizan dos protocolos populares para las VPN: PPTP (Protocolo de túnel punto a punto) e IPsec (seguridad IP). Microsoft desarrolló PPTP, de modo que el software cliente PPTP viene con la mayoría de las versiones de Windows. Además, PPTP está integrado en el Mac OS X 10.2 y hay clientes PPTP disponibles para Unix y Linux.

Los expertos en seguridad consideran a IPsec un estándar más robusto y el software cliente IPsec goza de amplia disponibilidad para Windows. Mac OS X 10.2 tiene soporte de línea de comandos para IPsec y varias compañías planean ofrecer también clientes IPsec gráficos. Los clientes gráficos serán bien recibidos, pues IPsec es bastante más complicado de configurar que SSH, requiriendo actualmente varios archivos de configuración y ajustes de línea de comandos.

Las VPN que utilizan IPsec a menudo no funcionan en redes inalámbricas que usan NAT (Traducción de direcciones de red) por cómo está cifrado el contenido. El servidor VPN necesita ver una dirección IP pública concreta asociada al cliente, pero como NAT rescribe los paquetes para incluir el número IP de la puerta de enlace NAT en lugar del perteneciente al verdadero cliente, no hay emparejamiento y la conexión no se puede iniciar. Sin embargo, muchas puertas de enlace y puntos de acceso han sido actualizados en el último año para prestar soporte a IPsec. Si su punto de acceso no presta soporte a IPsec, compruebe si el fabricante ofrece una actualización de firmware o compre un punto de acceso que pueda gestionarlo.

En resumen: si necesita utilizar una VPN existente, su compañía seguramente ofrecerá soporte interno que le ayudará a configurarla. Si desea configurar una VPN, debe investigar las opciones y ver si ofrecen suficientes ventajas que compensen el coste inicial y el de mantenimiento. Las organizaciones más grandes han adoptado las VPN como estrategia global de seguridad para los empleados que conectan desde ubicaciones remotas no seguras, como sus redes domésticas inalámbricas.

Proteger sus sistemas

Una parte de la seguridad es proteger los datos en tránsito; la otra parte es proteger los sistemas (los ordenadores, servidores de Internet en ejecución, puertas de enlace inalámbricas y demás) frente a los intrusos en línea. Dado que las redes inalámbricas pueden exponer los sistemas a los atacantes que nunca tendrían un tipo de acceso similar en una red convencional (a menos que entraran en la casa u oficina) hay que tener más cuidado para proteger los ordenadores de una red inalámbrica.

Nota *Podríamos entrar aquí en más detalles, pero este tema se aleja de las propias redes inalámbricas. Si está interesado en saber más del asunto, recomendamos que vea el libro "Internet Security for Your Macintosh: A Guide for the Rest of Us" de Alan Oppenheimer y Charles Whitaker. Aunque el libro está lleno de información para usuarios de Macintosh, las perspectivas generales se aplican a sistemas Mac, Windows, Linux y Unix.*

Podemos emplear dos métodos para asegurar los ordenadores frente a espionaje o ataques: un cortafuegos activo o traducción de direcciones de red. Podemos usarlos por separado o, para más seguridad, combinados. Pero antes, ¿por qué preocuparse?

¿Por qué preocuparse?

Quizá piense que no necesita proteger sus ordenadores, pero, desgraciadamente, hay miles de personas aburridas y amorales por el mundo que constante y automáticamente exploran grandes bloques de direcciones Internet buscando puntos débiles. Hoy día, pueden pasar sólo minutos entre el momento en que un ordenador recibe su primera dirección IP pública y el primer ataque lanzado contra él. La mayoría de estos ataques están totalmente automatizados mediante scripts desarrollados por piratas informáticos o proceden de crackers inexpertos que utilizan software prefabricado.

Los ataques se centran en problemas de programación conocidos del software que permiten a un programa remoto o a una persona infiltrarse en el ordenador y tomar el control del software o de todo el sistema operativo. Una vez que el atacante ha establecido ese nivel de control, puede destruir el siste-

ma o instalar software que ataque a otros ordenadores, convirtiendo nuestro sistema en lo que se llama un *zombi*.

La mayoría de los ataques están dirigidos a ordenadores que ejecutan alguna versión de Windows u otro software de Microsoft, como Outlook o Internet Information Server. Durante años, se han ido encontrando muchos problemas de programación que permiten a los atacantes hacerse con el control de una máquina; igualmente problemáticos son los gusanos y virus informáticos que pueden provocar daños, duplicarse a si mismos, convertir al ordenador infectado en un zombi o las tres cosas. Microsoft ha ido parcheando los agujeros conocidos, pero muchos usuarios de Windows no descargan e instalan los parches de seguridad, dejando sus ordenadores expuestos a la explotación e infección.

Aunque hay algunos virus que afectan a sistemas Mac, el número es una pequeña fracción de los dirigidos a Windows, reduciendo la preocupación de los usuarios de Macintosh. Además, como los sistemas Mac forman un porcentaje mucho más pequeño del mercado general, la mayoría de los crackers no se han interesado en exceso por atacar a estos ordenadores. Cuando se combina la falta de interés con los accidentes arquitectónicos que hicieron que el Mac OS 9 y anteriores fueran muy seguros, puede ver por qué los sistemas Mac no sufren tanto por la seguridad. Eso está cambiando ahora que Apple utiliza Unix por debajo del Mac OS X; aunque Unix no es inseguro en sí mismo, es un objetivo más probable para los piratas informáticos.

Algunos problemas no los provocan los sistemas operativos ni los programadores de aplicaciones, sino que los causa la persona que configura el sistema al cometer un error y permitir el acceso de forma inapropiada. Sólo hacen falta unos minutos de distracción o un ajuste mal configurado, como descubrió Glenn en 1994, cuando su archivo de contraseñas de Unix fue robado por primera vez (pero no roto). Y, recientemente, Adam se enfadó consigo mismo cuando su ISP le preguntó si sabía que cualquiera podía ver los archivos de uno de sus ordenadores Mac a través de AppleShare.

Otros ataques utilizan lo que se llama una estrategia de "denegación de servicio" (DoS), en la que el atacante envía tantos datos al ordenador que éste se sobrecarga. Los ataques DoS no provocan daños per se, pero impiden el funcionamiento normal del ordenador y pueden dificultar el apagarlo.

Una vez un ataque DoS saturó la conexión de Internet dedicada de Adam; sólo llamando a su ISP y pidiéndoles que bloquearan el tráfico ofensivo consiguió arreglar el problema. Glenn tuvo que pasar todo un día viendo su red saturada por un bombardeo de tráfico basura hasta que pudo convencer al ISP de cuya red provenía el ataque de que tenían un serio problema. Por último, después de un consejo informal del FBI, insinuó al ISP que no le quedaba más

remedio que demandarlos; después de eso, el ISP tomó medidas y desconectó al cliente DSL cuyo ordenador lanzaba el ataque (que probablemente había sido víctima de otro ataque que convirtió su ordenador en un zombi).

Todo el tema de proteger el ordenador se vuelve mucho más complicado cuando estamos en movimiento. Las propias redes inalámbricas podrían no ser fiables (¿está el técnico residente del café Internet sondeando el sistema?) o un cracker en la mesa de al lado podría sondear nuestro ordenador directamente. Recuerde, si alguien puede ver el tráfico de red no cifrado y robar las contraseñas, puede usar esas contraseñas para entrar en la propia máquina mientras está dentro de la red.

Unas pequeñas precauciones, como cifrar las contraseñas e instalar un cortafuegos, contribuyen en gran manera a impedir un océano de dolor y sufrimiento. Y más importante, siempre hay que hacer una copia de seguridad de los datos antes de llevarse de viaje el portátil: aún teniendo la seguridad absoluta de que ningún pirata informático puede entrar, siempre se nos puede caer el ordenador mientras pasamos el control de seguridad del aeropuerto o alguien puede robarlo mientras miramos para otro lado. Todo el mundo pierde datos en algún momento y los que tienen copias de seguridad son los que menos consecuencias sufren.

Cortafuegos activos

Un cortafuegos activo es un software de la puerta de enlace o los ordenadores individuales que controla los datos que entran y salen de un ordenador. Examina estos datos y bloquea bits determinados (a veces lanzando una advertencia) si los datos coinciden con ciertos criterios. Dentro de la red, utilizar un cortafuegos para que los servicios de entrada y salida necesarios estén abiertos sólo para los ordenadores locales es una buena forma de desalentar a los maleantes de intentar provocar estragos.

En un cortafuegos activo, podemos elegir permitir el paso a sólo ciertos protocolos, sólo conexiones que utilizan números de puerto concretos o sólo usuarios específicos.

En redes grandes, podemos combinar la autenticación de usuario con un cortafuegos para garantizar que únicamente determinadas personas pueden llevar a cabo ciertas tareas en la red.

Software de cortafuegos más avanzado identifica patrones de datos y, cuando reconoce un patrón de ataque, bloquea la dirección IP de la que proceden los datos y tiene la opción de lanzar una alerta. El hardware de cortafuegos muy caro puede reconocer miles de estos patrones de ataque.

Muchos cortafuegos también permiten establecer reglas de acceso que varían según el día de la semana y la hora del día. Así, si prestamos atención a la red, puede operar en un nivel de seguridad más bajo. Esto hace que sea más fácil llevar a cabo tareas rutinarias que serían tediosas si el cortafuegos estuviera a pleno funcionamiento.

Prácticamente todas las puertas de enlace que hemos visto incluyen un cortafuegos integrado, aunque estos cortafuegos tienden a ser rudimentarios. Vea el manual de la puerta de enlace para información sobre cómo se configura su cortafuegos.

Si está deambulando o desea un control más preciso, puede instalar software de cortafuegos personalizado en ordenadores individuales. Puede probar el cortafuegos integrado en Windows XP, pero recomendamos el cortafuegos ZoneAlarm (www.zonelabs.com) para Windows, un paquete potente y fácil de usar que es barato, goza de amplio soporte y tiene más funciones. Para los ordenadores Mac, Glenn se inclina por Intego NetBarrier X (www.intego.com/netbarrier/). Bajo Mac OS 9, Adam prefiere IPNetSentry de Sustainable Softworks (www.sustworks.com/site/prod_ipns_overview.html); en Mac OS X, utiliza el cortafuegos integrado. Si desea más control sobre el cortafuegos integrado de Mac OS X, compruebe la utilidad BrickHouse de shareware en http://personalpages.tds.net/~brian_hill/brickhouse.html.

Nota

Zone Labs tiene una versión de ZoneAlarm que funciona codo con codo con algunas puertas de enlace Linksys, como la EtherFast BEFW11S4 que hemos visto en el capítulo 5. Vea el sitio Web de Linksys en www.linksys.com para más detalles.

Configuración de cortafuegos integrado

El software de cortafuegos puede proporcionar más opciones y una interfaz mejor, pero el software de cortafuegos integrado en Windows XP y Mac OS X puede ocuparse de la tarea sin problemas. Los dos sistemas operativos hacen que configurar el cortafuegos sea fácil.

Nota

Al configurar un cortafuegos, la estrategia estándar es denegar todo el acceso y después abrir huecos concretos en el cortafuegos. De esa manera, es mucho más fácil averiguar qué está pasando en un ataque, pues el grupo de métodos posibles para atravesar el cortafuegos es pequeño. El único inconveniente es que hay que dedicar tiempo a determinar qué puertos abrir.

En Windows XP, siga estos pasos para configurar un cortafuegos:

1. Abra el Panel de control y haga doble clic en Conexiones de red.
2. Seleccione la conexión que desea asegurar (puede repetir esto en varias conexiones).
3. En el panel izquierdo, seleccione Cambiar la configuración de esta conexión en la sección Tareas de red.
4. Haga clic en la ficha Avanzadas.
5. Active la casilla de verificación Proteger mi equipo y mi red limitando o impidiendo el acceso a él desde Internet.

En Mac OS X, siga estos pasos para configurar el cortafuegos.

1. Abra Preferencias del Sistema y haga clic en Compartir.
2. Haga clic en la ficha Firewall y clic en **Iniciar**.
3. Seleccione los servicios que necesiten acceso desde el exterior.
4. Haga clic en **Nuevo** o **Editar** para modificar los servicios enumerados.

NAT (Traducción de direcciones de red)

Ejecutando NAT en la puerta de enlace eliminamos la posibilidad de muchas entradas no autorizadas porque las direcciones NAT suelen ser privadas (restringidas a la red local) y por tanto no pueden alcanzarse desde el mundo exterior (vea los capítulos 2 y 5 para más información sobre NAT). Siempre que un ordenador de la red local con una dirección privada solicita una conexión con otra máquina en Internet, la puerta de enlace NAT rescribe la solicitud para que parezca proceder de la propia puerta NAT, que debe ejecutarse en un ordenador al alcance del público. Si alguien intenta atacar a una red protegida por NAT, sólo está expuesta la puerta de enlace. Una puerta de enlace puede tener cierta vulnerabilidad, pero las puertas de enlace suelen ser más capaces de resistir ataques en parte porque su software es simple. Dado que las puertas de enlace no hacen muchas cosas, es difícil secuestrarlas. Algunas personas llaman a NAT cortafuegos pasivo y muchos fabricantes que anuncian puertas de enlace con cortafuegos en realidad hablan sólo de NAT.

NAT no nos protege de otros usuarios en la misma red, como en una cafetería u hotel, y puede provocar problemas en el software VPN IPsec (que requiere una dirección fija).

Conocer al enemigo

Entonces ¿quiénes son las personas que atacan a las redes y cómo lo hacen? Parafraseando los libros de Harry Potter, hay que conocer la magia negra para saber cómo defenderte de ella.

Las herramientas disponibles para vigilar e incluso forzar la entrada en redes inalámbricas no se han diseñado necesariamente pensando en causar algún mal. Como mucho, se desarrollaron para demostrar que las posibles debilidades eran en realidad agujeros en la seguridad. Los administradores de red necesitan este tipo de herramientas para entender cómo mejorar la seguridad de los datos que fluyen a través de las redes.

Estas herramientas entran en tres categorías. Algunas exploran constantemente para encontrar redes inalámbricas abiertas o cerradas. Otras interceptan datos de la red inalámbrica y los convierten en algo legible. Y, por si no nos ha creído cuando decíamos que era fácil romper las claves WEP, incluso hay una herramienta que hace eso sin esfuerzo.

Nota

Ni siquiera nos gustan las películas de abogados, pero le aconsejamos que averigüe si es legal o no utilizar cualquiera de estas herramientas en su país, estado, provincia, autonomía o ciudad. Hay un número creciente de leyes que ilegalizan la exploración en busca de redes, aunque sea pasivamente, a menos que la red sea de nuestra propiedad o dispongamos de permiso por escrito (en papel, no en correo electrónico).

Encontrar redes

Dado que un punto de acceso emite su identidad de red por omisión, una de las formas más simples de buscar redes abiertas en las cercanías es iniciar la utilidad de selección de redes y mirar la lista que muestra.

Herramientas más sofisticadas son NetStumbler (www.netstumbler.com) y MacStumbler (www.macstumbler.com). Ambas efectúan exploraciones continuas buscando todas las redes que producen señales perceptibles en las cercanías (vea la figura 6.12). NetStumbler funciona en Windows y en algunos dispositivos de bolsillo; MacStumbler sólo funciona en Mac OS X.

Las dos herramientas muestran los nombres de las redes y si está activado o no el cifrado WEP. Incluso si la red está cerrada, sigue apareciendo su nombre

y, con esa información, podemos conectar (aunque hay que tener en cuenta que conectar con una red cerrada ya es alejarse de la buena educación, como mínimo).

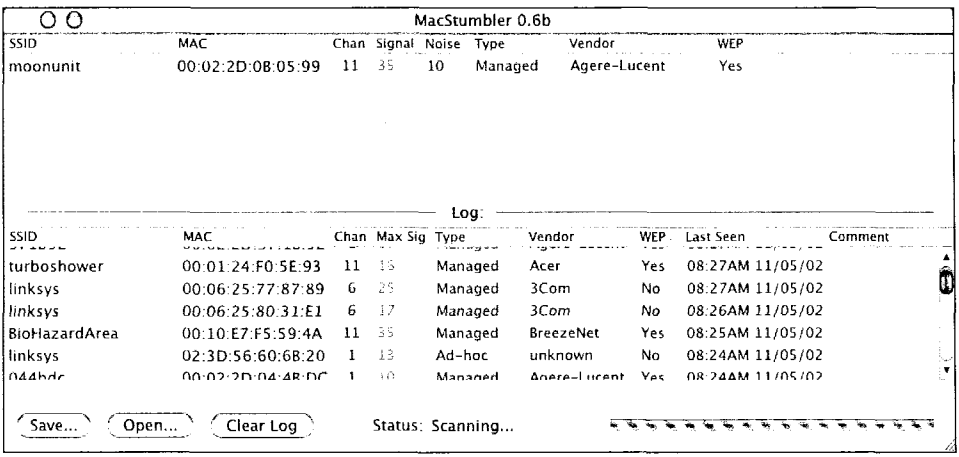

Figura 6.12. *Una exploración stumbler.*

El uso práctico de NetStumbler y MacStumbler aparece cuando estamos planificando la red. Para ello, ponemos el punto de acceso en un lugar que parezca adecuado y paseamos por la zona vigilando la fuerza de la señal. Si encontramos un punto muerto en un lugar en que es necesaria la conexión de red, movemos el punto de acceso y repetimos el proceso hasta encontrar la ubicación óptima.

Escuchar

Una vez conectados a una red inalámbrica, podemos escuchar todo el tráfico poniendo la interfaz de red en lo que se llama *modo promiscuo*. Un ordenador en modo promiscuo escucha todo el tráfico de la red, no sólo los paquetes dirigidos al aparato particular.

Una estrategia más gráfica de escucha la utiliza una herramienta Macintosh llamada EtherPEG (www.etherpeg.org), que extrae imágenes de paso de la visualización de una página Web y crea un collage aleatorio en pantalla (vea la figura 6.13).

Es una herramienta divertida para utilizarla durante una conferencia en la que la gente se aburre y empieza a navegar por la Web en lugar de prestar atención a las presentaciones. El objetivo de los creadores de EtherPEG era

demostrar lo fácilmente que alguien puede escuchar el tráfico de la red si no se toman las precauciones básicas activando el cifrado WEP.

Más cerca del nivel de red está tcpdump, una utilidad de línea de comandos que aparece en la mayoría de las distribuciones de Unix y Linux y también disponible en la línea de comandos de Mac OS X. La utilidad tcdump muestra las cabeceras de los paquetes TCP/IP que transitan por la red. Esto permite ver qué números IP están en uso y el tipo de tráfico de red que utilizan los usuarios. Es una útil herramienta para resolver problemas de red, pero no es fácil de usar.

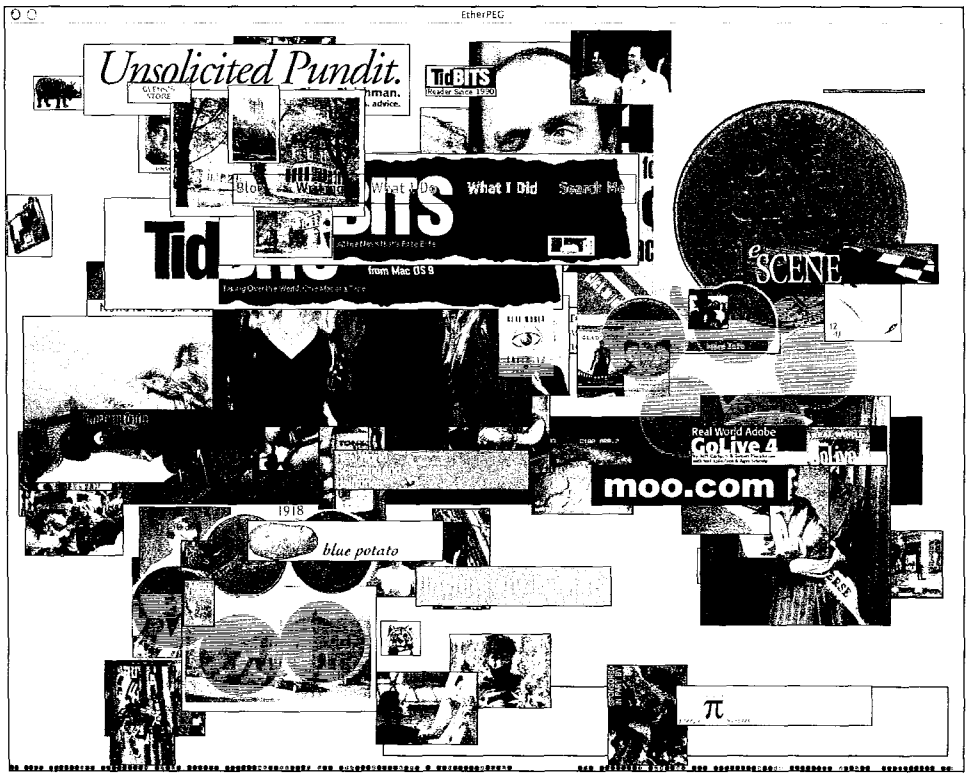

Figura 6.13. *EtherPEG observando los gráficos que pasan por la red inalámbrica.*

El prefijo war

Quizá haya leído artículos, algunos escritos por Glenn, acerca de wardriving, warflying, warwalking, warcycling y warchalking. Todos

estos términos describen en esencia diferentes modos de encontrar las redes inalámbricas de otras personas. El prefijo "war" de estas palabras no tiene nada que ver con verdaderos conflictos bélicos, sino que se ha tomado prestado de War Games (Juegos de guerra), un película de 1983 que mostraba el peligro de la guerra nuclear dirigida por ordenadores. Juegos de guerra fue una de las primeras películas de alto presupuesto que hablaba de los hackers informáticos.

En Juegos de guerra, el personaje representado por Matthew Broderick encontraba conexiones de módem abiertas haciendo que su ordenador marcara montones de números al azar hasta localizar un tono de respuesta. Una vez conectado, intentaba penetrar en el ordenador conectado a ese módem. Los hackers llaman a este proceso "wardialing".

El primero en despegar fue "wardriving", que es la técnica de ir conduciendo por una zona mientras se ejecuta NetStumbler o MacStumbler en el portátil dentro del coche. Durante la conducción, el programa recopila información sobre las redes inalámbricas que encuentra por el camino (vea la sección anterior). Warwalking, warcycling y warflying siguen la misma idea, variando sólo el medio de locomoción (andando, en bicicleta o volando, respectivamente).

Warchalking es una especie de palabra de segunda derivación. Matt Jones, un residente en Londres, decidió que el lenguaje de signos de tiza de los vagabundos utilizado a finales del siglo XVII y durante la Segunda Guerra Mundial por los agentes itinerantes podía ser adoptado como señales de información en el espacio físico cercano a puntos de acceso inalámbricos (www.warchalking.org).

Los medios saltaron sobre ello rápidamente (fue entonces cuando Glenn escribió una buena historia sobre el tema) y rápidamente resaltaron la noticia de que el warchalking se utilizaba para identificar redes que podían ser asaltadas. De hecho, no hay forma de determinar lo común que es el warchalking y nadie sabe decir si se está utilizando para mostrar redes comunitarias (puntos de acceso individuales que la gente comparte a propósito) o redes pensadas para ser privadas y seguras. En el momento de escribir esto, la mayoría de los informes de warchalking provienen de individuos que utilizan signos pintados con tiza para mostrar sus propios puntos de acceso. Algunos sospechan que la histeria de los medios puede haber sido alimentada por bromistas que dibujan signos por todas partes sin ningún sentido.

Ponemos objeciones a la desafortunada elección del término "war", pues lleva a que el público lo perciba como algo ofensivo en lo que

están involucrados los crackers. No es posible controlar la evolución del lenguaje, pero no parece positivo que propósitos legítimos y divertidos sean percibidos como ofensivos sólo por una mala elección del nombre.

La utilidad ntop (http://www.ntop.org) de Unix, Mac OS X y Windows recopila datos exhaustivamente, construyendo una base de datos durante su funcionamiento, y después presenta una interfaz Web con la que podemos examinar estadísticas de conexiones y tráfico. Como tcpdump, ntop puede resultar muy útil para buscar problemas de red.

Por último, aunque también tiene otros usos, la utilidad ettercap (http://ettercap.sourceforge.net) de Unix, Mac OSX y Windows es una rastreadora de tráfico de red optimizada para encontrar contraseñas de varios protocolos diferentes, como los de correo electrónico y FTP. El mejor uso de ettercap es convencer a la gente de que debe utilizar algún tipo de protección de contraseñas.

En una convención en la que estuvimos no hace mucho, un asistente estuvo ejecutando ettercap todo el tiempo y de vez en cuando decía en voz alta cosas como "Si alguien tiene el nombre de usuario ace, debe cambiar de contraseña y activar APOP".

Nuestro consejo es que no utilice ettercap, pues es difícil demostrar que los propósitos son legítimos.

Romper WEP

La utilidad Linux AirSnort (http://airsnort.shmoo.com) es una herramienta simple que escucha millones de paquetes que atraviesan una red y después produce la clave WEP. Sí, es así de fácil. No lo haga.

En realidad, la única razón válida para ejecutar AirSnort es determinar lo que tardaría un intruso en capturar suficientes datos para romper la clave WEP. Si sólo hacen falta 30 minutos, hay que tomar precauciones de seguridad adicionales; si tarda una semana, no hay que preocuparse porque alguien pueda romper la clave WEP.

Nota

Aunque ya hemos hecho antes la advertencia, la repetimos aquí: consulte con un abogado si tiene dudas sobre la legalidad de usar AirSnort. No se arriesgue a sufrir consecuencias inesperadas.

Redes desconocidas

Esperamos haberle proporcionado buenas sugerencias para proteger su red, sus datos y sus ordenadores. Si es un usuario doméstico y no tiene vecinos cercanos, probablemente sea suficiente con proteger las contraseñas. Si los factores de riesgo son más altos (vive o trabaja en zonas muy pobladas, sus datos son sensibles, ejecuta servidores de Internet), debe tomar más precauciones para asegurar los datos y la red.

Para aquellos que viajan con frecuencia, hay que tener en cuenta que los riesgos son altos siempre que se establece una conexión con una red desconocida. Hay que cifrar las contraseñas de correo electrónico y utilizar SSH o SSL si es posible; y ya que hablamos de esto, vea el siguiente capítulo, en el que ofrecemos consejos adicionales para utilizar redes inalámbricas durante los viajes.

7. De viaje

En esta era de Internet, quedar sin conexión durante los viajes parece muy frustrante. Los teléfonos móviles sirven de ayuda, por supuesto, pero para muchos de nosotros, el correo electrónico es el centro de la mayoría de nuestras comunicaciones. Y como nuestros clientes, colegas, amigos y familiares muchas veces no saben que estamos de viaje, esperan que comprobemos nuestro correo electrónico tan frecuentemente como siempre. Eso es difícil cuando vamos en un avión, o, como mínimo, caro; nunca hemos querido aceptar el coste de llamar a un ISP desde un teléfono en el asiento. Pero una vez que hemos aterrizado, podemos encontrar una red inalámbrica que esté a nuestra disposición para acceder a Internet y comprobar el correo electrónico, visitar los sitios Web necesarios o contactar con alguien a través de la mensajería instantánea. En su mayor parte, utilizar una red inalámbrica mientras estamos de viaje es exactamente igual que utilizar la de casa o la oficina. La principal diferencia es que recopilar toda la información que necesitamos para conectar con éxito con una red desconocida puede llevar tiempo y, en la mayoría de los casos, hay que averiguar la información antes de partir.

Truco *No importa lo fiable que pensemos que será la conectividad inalámbrica durante un viaje, siempre hay que garantizar que podremos utilizar*

Nota *también el módem del portátil para conectar con un ISP. Puede ser caro si hay que hacer una llamada a larga distancia, pero incluso un acceso a Internet caro es mejor que no disponer de acceso. Obtenga también números de acceso locales y busque opciones gratuitas de conexión. Glenn suele utilizar el servicio de número 800 de EarthLink que cuesta 6$ por hora cuando resulta más barato que las tarifas telefónicas locales del hotel o se encuentra en zonas alejadas.*

Redes en el camino

Debido a que cada día aparecen más y más puntos activos inalámbricos, es imposible encontrar ni un solo directorio actualizado con un listado exhaustivo de puntos activos. Es posible encontrar redes inalámbricas en lugares improbables y alejados (Glenn recibió un mensaje de correo electrónico de un lector de su sitio de noticias 802.11b Networking News comentándole que había encontrado un hotel con red inalámbrica en la India poco antes de que escribiéramos este capítulo), de modo que merece la pena dedicar algunos minutos antes de partir para determinar dónde hay redes inalámbricas en el punto de destino.

Nota *Un "punto activo" (hot spot) es una ubicación en la que hay una red inalámbrica a disposición del público.*

Directorios de puntos activos

Hemos encontrado sólo dos sitios Web que intentan hacer un seguimiento de los muchos puntos activos que hay en los EE. UU. y en el resto del mundo. En cualquier búsqueda de redes inalámbricas en el destino de un viaje, visite primero estos sitios.

- 802.11Hotspots.com (www.80211hotspots.com) permite encontrar puntos activos en ciudades de las que se sabe que disponen de ellos (ni siquiera se puede efectuar una búsqueda de una ciudad que no aparece en la lista). De cualquier forma, es posible obtener un listado con todos los puntos activos conocidos en cada estado de los EE. UU. y en un pequeño

número de otros países. En nuestras pruebas informales, 802.11Hotspots .com tenía más entradas que su principal competidor, WiFinder, y sus resultados eran algo más fáciles de usar porque muestran más resultados simultáneamente, en lugar de obligar a pasar de una página de resultados a otra.

- WiFinder (www.wifinder.com) proporciona un formulario de búsqueda más flexible que permite buscar por nombre de ubicación (por ejemplo, podemos buscar "airport" para encontrar todos los puntos activos disponibles en aeropuertos). Otros campos de búsqueda son Address (útil para encontrar una ubicación específica en una ciudad grande) y ZIP code (código de correos). WiFinder también permite seleccionar si queremos encontrar sólo puntos activos comerciales, redes comunitarias o las dos cosas, y podemos enumerar todos los puntos activos de algunas de las principales redes comerciales y comunitarias.

Aunque los dos sitios son útiles, 802.11Hotspots.com y WiFinder no incluyen todos los puntos activos ni mucho menos, de modo que no tenemos que asumir necesariamente que no hay puntos activos en un destino si no aparece en sus listados.

Truco

Los dos directorios de puntos activos aceptan informes enviados por usuarios, de modo que si conoce algún punto activo que no aparece en los listados, recomendamos encarecidamente que lo envíe a los dos directorios para ayudar a otros viajeros inalámbricos.

Redes inalámbricas gratuitas

Sorprendentemente, hay miles de lugares en los que podemos unirnos a una red inalámbrica para acceder a Internet gratuitamente. Naturalmente, no hay garantías del servicio y la velocidad de las conexiones puede variar desde un pequeño arroyuelo procedente de una conexión de llamada telefónica de 56 Kbps a las cataratas del Niágara de múltiples conexiones T-1. Para una rápida comprobación del correo electrónico, una red gratuita puede ser suficiente.

Lo único que hace falta para acceder a Internet a través de una de estas redes comunitarias es seleccionar el nombre de la red en la lista de señales disponibles. Algunas redes comunitarias redirigen la primera solicitud del navegador Web a una página que identifica el uso legítimo de la red y pregunta si está de acuerdo con las condiciones antes de proceder.

Truco *Si una red comunitaria requiere que hagamos clic en un acuerdo de uso antes de dar permiso para conectar, no es posible comprobar el correo electrónico hasta después de iniciar el navegador y aceptar las directivas de uso admitido.*

Redes inalámbricas comunitarias

Muchas comunidades tienen pequeñas, o incluso grandes, colecciones de redes agregadas libremente creadas por individuos de la comunidad. Estas redes comunitarias proporcionan puntos activos aislados en muchas ciudades, y en ciertos vecindarios el alcance es casi completo. Por ejemplo la zona Pioneer Courthouse Square en el centro de Portland, Oregon, tiene una excelente cobertura inalámbrica y acceso a Internet de alta velocidad gracias a que las empresas cercanas permiten el acceso a través de sus conexiones de Internet.

Aunque no hay una forma general de encontrar una lista actualizada con todos estos puntos activos, la mejor estrategia es buscar una red comunitaria inalámbrica en el punto de destino y ver si mantiene una lista de los puntos activos actuales.

Personal Telco, una organización de Portland dedicada a las redes de comunicaciones comunitarias, publica la lista más extensa de redes comunitarias inalámbricas en http://personaltelco.net/index.cgi/WirelessCommunities.

Bibliotecas

Muchas comunidades han añadido (o piensan añadir) acceso a Internet inalámbrico a sus bibliotecas públicas. La mujer de Adam, Tonya, colabora en la Tompkins County Public Library Board of Trustees en Ithaca, New York y, en el momento de escribir este libro, ayuda a la biblioteca a considerar qué será necesario para instalar y usar puntos de acceso que proporcionen acceso inalámbrico a Internet.

Nota *El acceso inalámbrico de red tiene muchas posibles ventajas en una biblioteca. Tonya espera que el acceso de red inalámbrico en la Tompkins County Public Library quite algo de trabajo a los ordenadores de mesa conectados a Internet y proporcione más movilidad y eficiencia a las operaciones de personal.*

El colega de Adam y Glenn Neil Bauman, empresario y capitán de Geekcruises.com, vive dentro del alcance de la red de su biblioteca local. (Neil

Bauman también tiene conexiones de Internet de cable, DSL y fibra óptica gracias a que vive en Palo Alto, California. ¡Qué envidia!)

De cualquier forma, encontrar acceso inalámbrico a Internet en una biblioteca pública durante un viaje puede implicar más esfuerzo del que merece la pena, a menos que conozcamos a gente de la comunidad. Las bibliotecas no suelen dar publicidad a sus servicios y pueden imponer restricciones al inicio de sesión o el acceso. Y más importante, puede ser difícil encontrar bibliotecas públicas en los parques empresariales de las ciudades que visitemos durante el viaje.

Colegas y universidades

Es probable que muchos institutos y universidades proporcionen acceso inalámbrico a Internet en este momento o en un futuro próximo. Si asiste a una convención cerca de una universidad (o en la propia universidad), merecerá la pena comprobar si ofrece acceso público. Desgraciadamente para los visitantes y viajeros, muchas universidades, como la Cornell University y la University of Washington, utilizan servidores de autenticación centralizados para permitir el acceso a sus redes inalámbricas sólo a estudiantes, profesores y personal.

Aunque es menos probable que las escuelas primarias tengan instaladas redes inalámbricas, también es posible que, en caso de tenerlas, restrinjan el acceso. Si termina en una reunión en la sala de conferencias de una escuela, abra el portátil y compruebe si puede conectar con una red inalámbrica.

Puntos activos aislados

El bajo coste de las conexiones de Internet de banda ancha y lo fácil que resulta configurar una red inalámbrica han provocado que muchas tiendas comerciales proporcionen acceso inalámbrico a Internet como un modo de atraer clientes y hacerles pasar tiempo en la tienda (y ver lo que venden, por supuesto). A lo largo de los años, hemos encontrado varios puntos activos excepcionales que ofrecen servicio gratuito. Por ejemplo, la cafetería Dana Street Roasting Company en Mountain View, California, tiene acceso gratuito porque un cliente que quería poder navegar por Internet mientras estaba allí pagó por él (www.live.com/danastreet/).

Estos puntos activos aislados pueden no aparecer nunca en los directorios, de modo que la única forma de encontrarlos por adelantado es buscar en Google (www.google.com). Por ejemplo, para encontrar redes inalámbricas en Rochester, New York, se pueden buscar términos como "wireless Internet access Rochester". A veces hay que esperar a llegar a la ciudad de destino, buscar un

lugar con buenas posibilidades (las cafeterías son una buena apuesta) y preguntar. Nuestro amigo y colega Jeff Carlson encontró una cafetería en su anterior ciudad de Renton, Washington, que ofrece acceso inalámbrico a Internet, pero sólo si se pide a algún empleado que active la red. ¿Por qué? No quieren que alguien aparque fuera y utilice la red sin ni siquiera pagar un café.

Convenciones y ferias comerciales

En muchas convenciones y ferias comerciales, especialmente las relacionadas con temas técnicos, los organizadores pueden preparar un área con acceso inalámbrico a Internet gratuito. El único inconveniente es que estas áreas suelen estar llenas de gente, provocando que el acceso a Internet sea a veces lento y dificultando el encontrar una silla libre.

Truco *Siempre merece la pena comprobar si hay redes ad hoc inalámbricas cercanas en los hoteles de convenciones. Como la mayoría de los hoteles ofrecen acceso a Internet de alta velocidad que se cobra por día, si alguien decide pagar la conexión, quizá también se ofrezca a ejecutar un punto de acceso de software para que el acceso a Internet esté disponible para otros usuarios inalámbricos dentro del alcance de la red. Una vez vimos una red llamada "Send beer to Rm 1471 for pwd" en la Macworld Expo: el propio nombre indicaba que si enviabas una cerveza a la habitación 1471 te darían la clave WEP. Desgraciadamente, recibíamos la señal inalámbrica de un hotel cercano a través de la ventana y no conseguimos averiguar a quién había que enviar la cerveza.*

Redes inalámbricas comerciales

Las redes inalámbricas gratuitas están muy bien, pero a veces merece la pena pagar por algo más. Las redes gratuitas raramente ofrecen soporte técnico formal si hay problemas para conectar, no garantizan el ancho de banda de la conexión a Internet (como las líneas T-1 a 1,544 Mbps que ofrecen generalmente las empresas) y no hay seguridad de que una red gratuita siga siendo accesible al día siguiente. Además, si hay que utilizar una VPN para conectar con la oficina, eso puede no ser posible a través de una red gratuita si utiliza una puerta de enlace NAT (Traducción de direcciones de red) incompatible. No es que sea difícil ofrecer soporte técnico, garantizar un cierto ancho de

banda y proporcionar fiabilidad en general, pero es caro. Las empresas que proporcionan acceso a Internet inalámbrico cobran entre 4 y 12$ por hora, de 5 a 10$ por día o tarifas planas de entre 25 y 75$ al mes, dependiendo siempre del nivel de uso.

Es tentador intentar atenerse a uno solo de los proveedores inalámbricos comerciales, pero eso sólo es válido si siempre nos movemos por un área muy específica que goza de cobertura por parte de ese proveedor. En su mayor parte, estas redes comerciales ofrecen acceso inalámbrico en distintas zonas, de modo que si el acceso inalámbrico a Internet es imprescindible, hay que firmar con varios proveedores inalámbricos. Una alternativa es un conglomerado como Boingo Wireless (hablaremos de los conglomerados en breve), que pretende reducir la confusa multiplicidad de proveedores de red inalámbricos ofreciendo una sola cuenta válida para varias redes.

Conectar con el portal cautivo

Si ha utilizado una red inalámbrica normal, quizá se pregunte cómo es posible forzar el pago en estas redes comerciales antes de que podamos conectar. La primera parte del proceso de conexión funciona de la forma esperada: encendemos el ordenador y seleccionamos la red en la lista de redes disponibles (o quizá la máquina la seleccione automáticamente). El ordenador se asocia con el punto de acceso y el punto de acceso le asigna una dirección DHCP. Pero todavía no está todo. Después hay que firmar el registro por medio de un *portal cautivo*. Para ello, hay que iniciar un navegador Web e intentar visitar cualquier sitio. El software de portal cautivo intercepta la solicitud y la redirige hacia la página de inicio de sesión, en la que introducimos la información de nuestra cuenta, acreditamos una cuenta o proporcionamos información de tarjeta de crédito para pagar el acceso.

Truco

Igual que en las redes comunitarias que utilizan software de portal cautivo para que aceptemos los términos de uso de la red, no podemos comprobar el correo electrónico ni utilizar software de Internet hasta haber iniciado la sesión en el portal cautivo con el navegador Web.

ISP inalámbricos

Los ISP inalámbricos, conocidos comúnmente como WISPs o wISP (un estilo algo irritante), existen en todo el mundo, ofreciendo acceso a sus redes

inalámbricas por una cuota. Sólo algunos ofrecen más que un puñado de puntos de acceso y la mayoría están especializados en cierto tipo de sitios, como hoteles o cafeterías.

Las redes WISP más grandes están en los EE.UU. y Canadá y son actualmente:

- **T-Mobile HotSpot (http://t-mobile.com/hotspot/):** T-Mobile USA, una división de Deutsche Telekom y una de las principales empresas de servicios de telefonía móvil en los EE.UU., compró los activos del servicio MobileStar que se había declarado en bancarrota a principios de 2002. A mediados de 2002, relanzó el servicio MobileStar bajo el nombre T-Mobile como asociado de Starbucks en más de 1.200 localidades, con planes para 2.000 localidades en 2003. En octubre de 2002, anunció un plan con Borders para poner puntos activos en las 400 librerías Borders para mediados de 2003, y en 100 salas de aeropuertos para finales de 2003. T-Mobile tiene un servicio con pago limitado por uso y planes para ofrecer servicio mensual.
- **Wayport (www.wayport.com):** El abuelo de los ISP inalámbricos, Wayport tiene varios centenares de puntos activos, principalmente en hoteles. Wayport también proporciona acceso inalámbrico en algunos aeropuertos, como Seattle-Tacoma y Austin. Wayport suele ofrecer una tasa diaria y una suscripción mensual.
- **Surf and Sip (www.surfandsip.com):** Surf and Sip se centra en el área de la bahía de San Francisco y tiene varias docenas de puntos activos, pero la compañía también tiene puestos de avanzada por los EE.UU. Surf and Sip ofrece acceso con pago por horas, tarjetas de prepago y planes de servicio mensual. Surf and Sip también vende un equipo de punto activo que permite a empresas de venta al por menor ofrecer acceso inalámbrico a Internet.
- **Concourse Communications Group (www.concoursecommunications .com):** Aunque Concourse sólo ofrece servicio actualmente en el aeropuerto Minneapolis-St. Paul (en la mayoría de las terminales), tiene el contrato para el servicio en Detroit y en los tres aeropuertos cercanos a New York City (JFK, LaGuardia y Newark). Concourse utiliza iPass, un servicio conglomerado, para gestionar la facturación y revender el acceso a otras redes, aunque ninguna de las que conocemos se ha unido todavía.
- **FatPort (www.fatport.com):** Esta firma de Vancouver, British Columbia, tiene varios puntos de servicio en el área de Vancouver y ofrece

servicio con pago por uso, tarjetas de prepago y planes de suscripción. Como Surf and Sip, FatPort vende un sistema de punto activo *plug-and-play* para pequeñas empresas que quieran ofrecer acceso inalámbrico a Internet sin esforzarse en exceso.

- **Airpath Wireless (www.airpath.com):** Airpath tiene un surtido aleatorio de puntos activos por los EE.UU.
- **SkyLink Internet Plus (www.skylink.ca):** SkyLink ofrece acceso inalámbrico a Internet en dos docenas de hoteles de Canadá con tasa por horas o suscripción mensual.

Muchos ISP inalámbricos permiten a los miembros de conglomerados de red utilizar sus redes siempre que utilicen cuentas de conglomerado existente (hablaremos más de los conglomerados en breve).

Aeropuertos

En el mundo posterior a los ataques terroristas del 11 de septiembre de 2001, la gente que viaja mucho se ve obligada a pasar en los aeropuertos bastante más tiempo que antes: tienes que llegar temprano, pasar los controles de seguridad y, después de un poco de tiempo, dedicar unas horas a esperar que llegue la hora del vuelo. Además, si hay que hacer un trasbordo y cambiar de avión, se necesita todavía más tiempo y el número de horas perdidas aumenta. Incluso viajando pocas veces al año, todas estas horas de inactividad se suman.

Es consecuencia natural que se proporcione acceso a Internet inalámbrico en los aeropuertos, ya sea en lugares especiales, cafeterías con puntos activos o en las terminales al completo. Desgraciadamente, el mercado de proveedores de servicios de Internet inalámbricos se ha plagado de bancarrotas y muchas de las empresas desaparecidas habían firmado acuerdos con las autoridades aeroportuarias para instalar el servicio inalámbrico. Estos acuerdos rotos, junto con las pobres cuentas de resultados de los aeropuertos que sí instalaron redes inalámbricas, han hecho dudar a las autoridades aeroportuarias y toda la industria está avanzando muy despacio.

¿Quiere convertirse en un punto activo?

Si está interesado en lanzar un servicio de punto activo desde su casa, empresa o centro comunitario, primero tiene que decidir si va a cobrar o no por el servicio. Si quiere ir por la vía gratuita, visite http://nocat.net,

www.bawug.org y www.personaltelco.net; todos tienen excelentes consejos y enlaces, también recomendamos el libro de Rob Flickenger, Building Wireless Community Networks.
Si quiere cobrar una cuota por el acceso a su red pero no desea tener que averiguar cómo reunir todas las piezas (las partes difíciles son la autenticación y las facturas), le recomendamos que compare distintas ofertas prefabricadas. Permiten comprar hardware preconfigurado por entre 500 y 1000 euros, configurar la conexión de red de banda ancha e introducir algunos ajustes para que la cosa empiece a funcionar. Quizá tenga que pagar por una conexión de Internet de nivel corporativo, pues muchos ISP cobran una tasa más alta por el ancho de banda si se revende la conexión.
El conglomerado o red que vende el sistema cobra las cuotas de los usuarios y paga un porcentaje dependiendo de las sesiones, el uso mensual u otros parámetros que debe negociar. En el momento de escribir esto, Surf and Sip, FatPort y Boingo ofrecen productos prefabricados; Boingo está asociada con varias otras redes inalámbricas, lo que la convierte en una buena elección si piensa que sus clientes van a desear acceso a Internet inalámbrico mientras viajan. Algunos sistemas de punto activo prestan soporte a varias redes, incluyendo Boingo, para mayor flexibilidad.

A pesar de los obstáculos, la demanda de acceso inalámbrico a Internet por parte de los viajantes empresariales es demasiado alta y hay muchas oportunidades para ofrecer este servicio a un público ya ansioso. Esperamos que para finales de 2003 los principales aeropuertos de los EE.UU. ofrezcan algún tipo de cobertura Wi-Fi, aunque esta cobertura puede ser tremendamente limitada en ciertas situaciones.

Muchas de las redes de aeropuerto forman parte de una red más grande. Por ejemplo, Austin, Seattle-Tacoma y San José tienen servicio de Wayport (y, por tanto, están disponibles también para los suscriptores de Boingo) y muchas salas vip de American Airlines tienen servicio T-Mobile HotSpot. T-Mobile planea ampliar su servicio a 100 salas de American, Delta y United Airlines para finales de 2003.

Nota *En varios aeropuertos, Wayport también gestiona pequeños pedazos de paraíso llamados Laptop Lanes (www.wayport.com/laptoplane), que compró a una empresa ISP que abandonó el asunto. Las Laptop Lanes*

son pequeñas salas autocontenidas, insonorizadas y con teléfonos y conexiones a Internet de alta velocidad por cable. Se paga una cuota bastante alta por hora, pero son tranquilas y privadas.

Ésta es una lista de los aeropuertos que actualmente tienen algún tipo de acceso inalámbrico a Internet, ya sea acceso limitado en puntos activos o cobertura completa en las terminales (omitimos las salas T-Mobile porque requieren ser miembro para entrar y los clubes a menudo están en lugares no muy accesibles):

- Austin,Texas (T-Mobile, http://locations.hotspot.t-mobile.com/page6a.asp?state=tx).
- Boston, Massachusetts (Airpath,http://isps.net/Directory.aspx).
- Chicago, Illinois (Airpath).
- Dallas, Texas (Airpath, Wayport).
- Dayton, Ohio (Airpath).
- Denver, Colorado (AT&T Wireless, www.attws.com/goport/).
- Flint, Michigan (Airpath).
- Greensboro, North Carolina (Airpath).
- Los Ángeles, California (Gate Escape, www.thegateescape.com).
- Louisville, Kentucky (T-Mobile).
- Miami, Florida (Airpath).
- Milwaukee, Wisconsin (Airpath).
- Minneapolis-St.Paul, Minnesota (Concourse Communications, www.concoursecommunications.com).
- Norfolk, Virginia (T-Mobile).
- Ottawa, Ontario (Nokia, no tiene sitio Web para puntos activos).
- San José, California (Wayport).
- Seattle-Tacoma, Washington (Wayport).
- Sioux Falls, South Dakota (T-Mobile).
- Tampa, Florida (Airpath).
- Toledo, Ohio (Airpath).

- Vancouver, British Columbia (Nokia, http://www.yvr.ca/guide/todo/internet_access.asp).
- Wichita, Kansas (Airpath).

En otras partes del mundo, puede encontrar acceso inalámbrico en muchos aeropuertos, incluyendo Schiphol en Amsterdam, partes de Heathrow en Londres y varias salas en aeropuertos en los que aterrizan aviones de las líneas aéreas SAS suecas. Merece la pena buscar en Google antes de partir para encontrar información acerca de acceso a Internet inalámbrico en los aeropuertos intermedios o de destino.

Hoteles

Cada vez más hoteles, reconociendo la creciente necesidad de sus clientes de conectar a Internet (y quizá admitiendo la naturaleza ridícula de las cuotas por minutos que aplican incluso a las llamadas de teléfono locales), ofrecen alguna forma de acceso Internet de banda ancha en las habitaciones.

Alentar los hoteles inalámbricos

Si desea ayudar a urgir a los hoteles a que instalen acceso inalámbrico, haga conocer su deseo preguntando cuando haga una reserva. Pregunte también al hacer uso de ella y, si el hotel ofrece acceso inalámbrico a Internet, agradézcalo. Además, rellene una carta de sugerencias, dando las gracias al hotel por proporcionar acceso inalámbrico a Internet o señalando que será más probable que visite de nuevo el hotel (o los hoteles de la cadena) en el futuro si instalan el acceso inalámbrico. Este tipo de respuesta directa, incluso en pequeña cantidad, influye en la toma de decisiones de las cadenas hoteleras.

Los hoteles empezaron poniendo cables en cada habitación, que funciona bien, pero es una propuesta cara y puede requerir que el cliente lleve un cable Ethernet (algunos hoteles también proporcionan los cables necesarios). Sin embargo, más recientemente, algunos hoteles se han asociado con un proveedor de servicios de Internet inalámbricos, principalmente Wayport, para ofrecer acceso inalámbrico a Internet en ciertas habitaciones, zonas públicas o salas de reuniones.

Típicamente, los hoteles cobran alrededor de 10€ por día, definiendo el día de forma molesta como de medianoche a medianoche. De modo que sí, si permanece dos noches en el hotel y desea acceso continuo a Internet, le cobrarán

tres días: el de llegada, el día completo que pase allí y el día de partida. El conglomerado Boingo Wireless ha intentado solucionar esta molestia de las formas de cobro con una cuota de suscripción mensual que concede acceso al servicio inalámbrico en hoteles igual que en otros puntos activos. No está claro si el intento tendrá éxito, pues aunque puede aumentar el uso general del servicio en los hoteles, también reducirá los beneficios de éstos, al menos a corto plazo.

Los hoteles se muestran preocupados ante la próxima generación de teléfonos móviles, que podrán acceder a Internet a velocidades decentes, variando entre 10 Kbps y 150 o hasta 200 Kbps (vea el capítulo 10 para más detalles). Los viajantes empresariales que es más probable que utilicen el teléfono de la habitación y el acceso a Internet de banda ancha, también comprarán seguramente los nuevos modelos de teléfonos móviles, haciendo difícil justificar la inversión en poner cables en las habitaciones e instalar puntos de acceso inalámbricos.

Starbucks

La cadena de cafeterías Starbucks lo dice una y otra vez: no son cafés de Internet. En Starbucks quieren que llevemos nuestro caro portátil y compremos sus caras bebidas mientras usamos su, bueno, ligeramente cara red. Starbucks tiene más de 3.500 establecimientos en los EE.UU. y primero se asoció con MobileStar, que terminó en bancarrota, y después con T-Mobile para construir puntos activos de alta calidad basados en T-1 en sus tiendas en los EE.UU. y en otras partes del mundo.

A mediados de 2002, Starbucks y T-Mobile anunciaron acceso a Internet inalámbrico total en 1200 establecimientos en varias ciudades y áreas metropolitanas: Atlanta, Austin, Boston, Buffalo, Dallas, Denver, Fort Worth, Hartford, Houston, área metropolitana de New York City, Newark, Philadelphia, Portland (Oregon), Rochester (New York), Sacramento, San Antonio, área de la bahía de San Francisco, Seattle, Southern California y Tacoma (Washington). También están experimentando en algunos establecimientos en Londres y Berlín, y tienen planes para añadir el servicio gradualmente en Europa.

Puede ver la lista actualizada en http://locations.hotspot.t-mobile.com/starbucks.htm. T-Mobile actualmente ofrece un plan regional que permite usar servicio ilimitado dentro de ciudades o áreas metropolitanas por 30$ al mes.

Starbucks y T-Mobile han dicho que tendrán más de 2000 establecimientos conectados a principios de 2003. Eso está cerca del plan original que decía ir a conectar alrededor del 70 por ciento de los establecimientos Starbucks dependiendo de la densidad de población y las estadísticas de usuarios empresariales

de un área. Pero dado que Starbucks abre cientos de nuevos establecimientos cada año, es más que probable que llegue a 3000 establecimientos con conexión inalámbrica para el 2004.

Borders

Starbucks no es la única cadena que se ha decidido por lo inalámbrico. Justo cuando estábamos acabando de escribir este capítulo, T-Mobile anunció que se asociaba con Borders para instalar puntos activos inalámbricos en 400 tiendas Borders para mediados de 2003, ésas son todas las tiendas Borders en los EE.UU.

Borders le dijo a Glenn que empezarían por California e irían llevando el servicio a otros lugares durante unos seis meses, aunque no harían un anuncio formal hasta que todas las tiendas estuvieran listas. Una vez que la cadena Borders esté totalmente conectada, se podrá utilizar el localizador Borders Store Locator (www.bordersstores.com/locator/locator.jsp) para encontrar una tienda en los lugares de los EE.UU. a los que piense viajar.

Schlotzsky 's Deli

Aunque Schlotzsky 's Deli ha decidido instalar acceso gratuito y ofrecerlo sólo en algunos lugares de Texas y Georgia, evidentemente es para ellos parte de un experimento para averiguar cómo utiliza la gente las redes inalámbricas (www.cooldeli.com/wireless.html).

Conglomerados para los viajantes

Como queda dicho, ninguna de las redes inalámbricas comerciales es lo bastante extensa para que los que viajan fuera de ciertos pasillos, digamos de Seattle a San José, paguen cuotas mensuales por acceso ilimitado a una red dada. Wayport y T-Mobile tienen las redes más grandes, pero ni siquiera ellos pueden ofrecer conexiones en todos los lugares de destino.

Problemas como éstos presentan oportunidades para compañías ambiciosas y algunas han saltado al nuevo campo asociándose con varios WISP para formar un conglomerado de servicio. La mayoría de esas compañía empezaron agregando acceso telefónico de Internet en todo el mundo para los viajantes empresariales.

Lo atractivo de trabajar con un conglomerado es que pagamos una sola factura y sólo tenemos que recordar la información de un inicio de sesión, todo

para utilizar distintos WISP. Como bonificación, los conglomerados suelen ofrecer software cliente que proporciona seguridad adicional para aquellos de nosotros que no estamos preparados para usar software VPN.

Boingo Wireless

Aunque Boingo Wireless (www.boingo.com) es el más nuevo conglomerado, ha desarrollado la red de puntos activos más grande asociándose con otros proveedores. Boingo tiene tarifas fijas bastante aceptables y un cliente de última línea para gestionar las conexiones por cuota y las configuraciones inalámbricas (para cualquier red, no sólo las comerciales).

En el momento de escribir este libro, Boingo tiene alrededor de 800 puntos activos, unos 400 de los cuales son manejados por Wayport, el mayor asociado de Boingo. Boingo ha anunciado asociaciones con varias otras compañías y el fundador de la empresa, Sky Dayton (la misma persona que fundó EarthLink), predijo 4000 puntos activos para el final de 2002. (¡Para cuando lea esto podrá saber si tenía razón!) Boingo también incluye puntos activos comunitarios gratuitos y visitar su directorio de puntos activos (www.boingo.com/search.html) bien merecerá la pena.

Boingo cobra el servicio por día y cada día cuesta 8$. También ofrece servicio ilimitado por 75$ al mes o un plan de 25$ al mes que incluye 10 conexiones mensuales (cobra 5$ por conexión adicional).

Boingo tiene su propio software cliente de red inalámbrica que incluye una lista de localizaciones y una herramienta para almacenar claves de cifrado WEP. Cuando estamos cerca de un punto activo de uno de los socios de Boingo, el software puede enviar un aviso para que nos conectemos si lo deseamos. No es necesario utilizar una página de puerta de enlace o portal cautivo para iniciar una sesión.

El software Boingo incluye un cliente VPN (Red privada virtual) que permite dirigir por un túnel todo el tráfico de la máquina hacia el centro de operaciones de red de Boingo antes de que sea descifrado y enviado a través de la Internet pública. (Para más información sobre las VPN, vea el capítulo 6.)

Boingo también incluye un servicio de correo electrónico de salida con SMTP autenticado, que requiere que reconfiguremos el software de correo electrónico temporalmente con el nombre y la contraseña de la cuenta Boingo. Este servicio ayuda evitar toda una categoría de problemas de correo electrónico de salida, que comentaremos en una sección posterior del capítulo.

El software de Boingo está disponible para Windows y a finales de 2002 se ha anunciado una versión para sistemas Macintosh que estará disponible para el primer semestre del 2003.

iPass

iPass (www.ipass.com) empezó como una forma de permitir a las compañías dar a un viajante solitario una sola cuenta que le permite acceder a una conexión de llamada telefónica de Internet desde cualquier parte del mundo. Con ISP asociados en más de 150 países y con 15.000 puntos de presencia, iPass ha conseguido su propósito. El acceso telefónico a Internet de iPass cuesta unos 18$ por hora, dependiendo de la cantidad de servicio comprado, de si se trata de una compañía o un individuo y de si se llama o no a un número gratuito.

Las ofertas inalámbricas de iPass son relativamente recientes, pero iPass ofrece acceso a una sola cuenta gracias a asociados en varios países por entre 7 y 20$ por un periodo de 24 horas. iPass está asociado con Wayport en los EE.UU. y también gestiona la facturación de Concourse Communications.

iPass requiere que los usuarios ejecuten un software cliente especial, disponible para Windows, Macintosh y varios ordenadores de bolsillo. Desgraciadamente, iPass todavía no ha actualizado la versión Macintosh para el Mac OS X y la versión actual no puede gestionar las conexiones de banda ancha o inalámbricas.

GRIC Communications

GRIC (www.gric.com) ofrece servicios parecidos a los de iPass, aunque sólo hemos podido averiguar que se ha asociado con Wayport para el acceso inalámbrico a Internet.

El sitio Web de la compañía señala 20.000 puntos de presencia, pero no proporciona información sobre coste y otros detalles. GRIC también requiere su propio software cliente, disponible sólo para Windows.

Otra preparación

Aunque buscar redes inalámbricas que podamos utilizar durante los viajes y en el destino es la preparación más importante que se puede hacer, también hay que recopilar otro tipo de información. Además, hay que comprobar que el portátil está listo para partir; también vamos a ofrecerle algunos consejos para eso. No ocuparse de esta preparación por adelantado no impedirá necesariamente que utilice una conexión inalámbrica con Internet mientras está fuera, pero quizá le obligue a dedicar un tiempo a descargar y configurar software.

Cuentas de acceso

La mayoría de las redes con cuotas que hemos visto durante el capítulo requieren cuentas y varias de ellas requieren software propio. Algunas, como Boingo, ofrecen la posibilidad de descargar gratuitamente el software junto con una configuración de cuenta también gratuita. Las cuotas se pagan sólo cuando accedemos a una sesión del servicio o aceptamos un plan de suscripción.

Pero estas descargas son largas y afiliarse a una cuenta siempre es molesto cuando intentamos efectuar una conexión rápida. Recomendamos que lo prepare todo por adelantado: descargue e instale el software necesario, inicie una sesión y cree cuentas en los sitios Web de las empresas y suscriba planes de servicio si cree que los va a necesitar en el futuro.

Truco

Si le preocupa olvidar su nombre de usuario y contraseña, escríbalos, pero guarde el papel en un lugar seguro. Recuerde que la mayoría de las contraseñas se roban porque están escritas en un papel.

Correo electrónico

El aspecto más frustrante del correo electrónico durante los viajes es enviar respuestas y mensajes nuevos. La frustración nace de que, para impedir que alguien dedicado al envío de correo basura asalte sus servidores de correo saliente, muchas compañías e ISP han restringido severamente cómo se puede enviar correo electrónico a través de sus servidores.

Desgraciadamente, hay poca diferencia técnica entre lo que hace una persona que envía correo basura para asaltar un servidor de correo y lo que hacemos cuando conectamos con una red inalámbrica cualquiera e intentamos enviar correo a través de nuestro servidor de correo saliente usual. (En ambos casos, la acción se llama "retransmisión" y casi todos los servidores de correo bien configurados rechazan en la actualidad la retransmisión.)

Hay varias formas de sortear este problema y debe reflexionar sobre todas ellas antes de partir. Siempre es importante comprobar el funcionamiento de tales cambios antes de salir de viaje.

- **Correo ISP Web:** Muchos ISP ofrecen una interfaz de correo electrónico basada en Web que permite olvidarse del problema durante los viajes. Utilizando un cliente de correo Web para leer y enviar los mensajes de

correo electrónico, perdemos la ventaja de trabajar en nuestro programa de correo usual, y sólo es posible trabajar estando conectados a Internet, pero como el programa de correo Web se encuentra en realidad en el ordenador del ISP, puede enviar el correo electrónico a través del servidor SMTP del ISP sin problemas. Una ventaja de utilizar un cliente de correo Web basado en ISP es que funciona en el buzón existente en los servidores del ISP, facilitando la integración de lo que hacemos en el cliente de correo Web con nuestro programa de correo electrónico usual a la vuelta.

Nota *La mayoría del correo Web no utiliza SSL, que significa que el correo electrónico se envía a las claras mientras lo leemos. Si eso le preocupa, lea el capítulo 6. Cierto correo Web permite una firma SSL para proteger al menos el nombre de usuario y la contraseña.*

- **Correo Web genérico:** Varios servicios independientes permiten obtener el correo electrónico existente a través de un cliente de correo Web. Estos programas de correo Web utilizan nuestra información de cuenta POP para obtener el correo entre bastidores y después lo presentan con una interfaz Web. Muchos de estos servicios permiten asignar nuestra verdadera dirección de correo electrónico, no la que utilizamos en el servicio, a la dirección de retorno para que las respuestas vayan a nuestro buzón correcto. Algunos de estos servicios son gratuitos, como Yahoo! Mail (http://mail.yahoo.com); otros, como FastMail (www.fastmail.fm), cobran cuotas, pero eliminan las restricciones de espacio de almacenamiento, no contienen anuncios publicitarios y ofrecen más funciones.

Truco *Si tiene un servicio de reenvío de correo en su ISP, puede también reenviar su correo directamente a la dirección de correo en el servicio de correo Web mientras está de viaje.*

- **Primero POP después enviar:** Varios ISP permiten enviar el correo electrónico de salida sólo después de haber recogido el correo de la cuenta POP. Al recoger el correo electrónico vía POP se abre una ventana, generalmente de 30 minutos, durante la que el servidor de correo del ISP aceptará correo de la red que estamos utilizando. Esta estrategia resulta ligeramente problemática en la práctica y a veces requiere varias recuperaciones de POP y después esperas de algunos minutos. Aunque ese funcionamiento no es universal, muchos programas de correo electróni-

co populares prestan soporte a la comprobación de una cuenta POP antes de intentar enviar el correo.

- **Transmisión extendida (XTND XMIT):** El protocolo POP se utiliza para obtener el correo, pero tiene una opción, llamada XTND XMIT, que permite también enviar correo a través de POP. Aunque XTND XMIT evita algunos problemas del envío de correo con redes inalámbricas aleatorias, el soporte a XTND XMIT no está muy extendido entre los programas de correo electrónico y los servidores de correo y hay que preguntar al ISP si presta soporte a XTND XMIT y buscar en las opciones del programa de correo alguna casilla de verificación que permitan activarlo. Hemos tenido resultados variables con XTND XMIT y recomendamos que compruebe el resultado de su configuración antes de suponer que funcionará durante un viaje.
- **SMTP autenticado (SMTP AUTH):** Un creciente número de servidores de correo impiden que la gente no autorizada envíe correo electrónico gracias a una técnica llamada SMTP autenticado o SMTP AUTH. Para poder enviar mensajes, nuestro programa de correo electrónico debe autenticarse con un nombre de usuario y una contraseña (no necesariamente los mismos que los de la cuenta POP) para poder después enviar correo a través de ese servidor. SMTP AUTH puede cifrar el nombre de usuario y la contraseña para que no puedan ser rastreados; vea el capítulo 6 para más información acerca de SMTP AUTH.

Nota

SMTP autenticado es probablemente la mejor solución, suponiendo que el servidor de correo y el programa de correo le presten soporte. De nuevo, configúrelo antes de partir de viaje. Un problema posible es que algunos ISP bloqueen todo el tráfico procedente de sus redes en el puerto 25, el puerto que utiliza SMTP, impidiendo que enviemos correo a cualquier servidor que no sea el del propio ISP. Un administrador de red puede solucionar esto para los usuarios viajeros asignando como puerto de salida en el servidor de correo principal un puerto por encima del 1024.

- **Túnel de shell seguro (SSH):** Si utilizamos la técnica comentada en el capítulo 6 para crear túneles SSH cifrados, generalmente podemos enviar correo electrónico a nuestro servidor usual. El túnel SSH engaña al servidor de correo para que piense que estamos en la misma máquina en que se ejecuta el servidor de correo, solucionando totalmente el problema remoto.

- **Red privada virtual (VPN):** Si utilizamos un cliente VPN para conectar con nuestra oficina, no debemos tener problema alguno para enviar correo. La VPN nos autentica en la red local y también cifra todo lo que enviamos.

Archivos

Todos intentamos llevarnos de viaje los archivos que sabemos que vamos a necesitar (presentaciones, informes, software de demostración, etc.), pero, en un momento u otro, todos terminamos descubriendo que nos faltan archivos importantes, porque los hemos olvidado o por pura mala suerte. Todavía peor es que le suceda algo al portátil o que, al llegar, descubramos que no podemos conectar nuestro portátil al proyector necesario ni copiar la presentación en un ordenador que sí pueda conectar con el proyector.

Afortunadamente, con sólo un poco de previsión, podemos garantizar que estas situaciones no van a frustrarnos. Pruebe los métodos que describimos antes de partir, especialmente los de conexiones, para garantizar que medidas de seguridad que no dejan de ser razonables no le van a impedir acceder los archivos que necesita.

- **Servidores de archivos IP:** Muchos servidores de archivos, incluido el software para compartir archivos integrado en Windows, Mac OS 9 y Mac OS X, permite conectar con ellos a través de Internet. Sin embargo, a menudo los administradores de sistema bloquean el acceso a los servidores de archivos para los usuarios no locales; hay que comprobar que podemos entrar y, si la máquina que necesitamos está detrás de una puerta de enlace NAT, garantizar que está configurado el reenvío de puertos apropiados.
- **Servidores FTP, Web y WebDAV:** Si tenemos una cuenta IPS en cualquier sitio o podemos acceder a servidores locales, seremos capaces de cargar archivos que nos pueden ser útiles para acceder a ellos posteriormente a través de FTP, WebDAV o la Web.
- **Timbuktu Pro:** Los dos utilizamos el software de Netopia (www.netopia.com) Timbuktu Pro de intercambio y control remoto para copiar archivos y comprobar software en ejecución en nuestros sistemas locales mientras estamos de viaje. Funciona en Mac y Windows.
- **Almacenamiento en línea:** Si es usuario de Macintosh, puede suscribirse a los servicios Web de pago .Mac (www.mac.com) de Apple, por 100$

al año. .Mac incluye 100 MB de almacenamiento en línea, al que puede acceder directamente desde un ordenador Mac o a través de la función Carpetas Web integradas en las versiones recientes de Windows. (Vea la página iDisk en .Mac para encontrar instrucciones de acceso a iDisk desde distintas plataformas.) Otros servicios orientados a Windows ofrecen acceso y tasas similares, incluyendo Xdrive Technologies (www.xdrive.com), la división IBackup de Pro Softnet (www.ibackup.com) y My Docs Online (www.mydocsonline.com).

- **Enviar mensajes de correo electrónico a la dirección propia:** Si utiliza uno de los métodos de correo Web comentados anteriormente en este capítulo, puede pensar en enviarse un mensaje a su propia dirección con los archivos que puede necesitar. Si es necesario, después podrá descargarlos utilizando un navegador Web en cualquier ordenador.

Copias de seguridad

Es fácil crear nueva información importante durante un viaje y, al estar lejos del sistema de copia de seguridad usual, resulta más probable perder datos importantes si le sucede algo al portátil. Recomendamos:

- **Hacer copias de seguridad antes de partir:** Haga una copia de seguridad completa de su portátil y su ordenador de mesa justo antes de partir. De ese modo, incluso si le roban el portátil o le sucede algo, podrá restaurar los archivos en un nuevo portátil cuando vuelva a casa.
- **Enviar archivos a casa:** Todos los métodos anteriores para obtener archivos durante un viaje ofrecen una buena forma de trasladar archivos a un lugar seguro.
- **Copiar un CD:** Muchos portátiles modernos tienen copiadora de CD. Con unos cuantos discos en blanco, será fácil hacer copias de seguridad de toda la nueva información. Es mejor guardar los CD de copia de seguridad en otra maleta que no sea la del portátil, por supuesto, pues es más fácil que un ladrón intente hacerse con la bolsa del portátil que con una maleta normal.
- **Utilizar una unidad USB RAM:** Ahora se pueden comprar pequeñas unidades USB RAM que caben incluso en el llavero. Utilizan memoria flash y proporcionan entre 32 MB y 1 GB de espacio. Todavía mejor, cuando las conectamos al puerto USB del ordenador Mac o el PC, se montan igual que los discos duros. Como estas unidades USB RAM son

lo bastante pequeñas para llevarlas en el bolsillo, incluso si el portátil desaparece podemos conservar los archivos críticos.

- **Utilizar un programa de copia de seguridad remota:** Algunos programas de copia de seguridad, como el potente Retrospect de Dantz Development (www.dantz.com, disponible para sistemas Mac y Windows), permiten guardar copias de seguridad en un servidor FTP o cualquier otro servidor remoto.

Todavía mejor, para cualquier archivo de datos verdaderamente importante, haga varias copias de seguridad con distintos métodos.

VPN

Una VPN (red privada virtual) puede resolver varios de estos problemas de los viajes, que es una de las razones por la que muchos viajantes empresariales acceden a los servidores de correo y archivos de su compañía a través de una VPN.

Sin embargo, hay que comprobar que dispondremos de toda la información necesaria para conectar con la VPN durante el viaje. La mayoría de las compañías ofrecen acceso de llamada telefónica en sus VPN y, aunque siempre hay que comprobar que tenemos los números apropiados, toda va mucho mejor si podemos usar una conexión inalámbrica de Internet de alta velocidad.

El principal miedo que puede asaltar a los usuarios de VPN es que muchas redes inalámbricas y otras conexiones Internet de banda ancha pueden usar NAT. Dependiendo de la puerta de enlace NAT, el uso de NAT puede impedir que nuestro software VPN conecte con la oficina. Este problema es especialmente común cuando se utilizan redes comunitarias gratuitas.

Nota *Surf and Sip, T-Mobile y Wayport nos han dicho que utilizan direcciones estáticas que se pueden redirigir para evitar estos problemas en sus redes.*

Desgraciadamente, probar las conexiones VPN puede ser peliagudo, pues no hay modo de conocer las limitaciones de las redes que utilizaremos en un momento dado. Compruebe que dispone del número de teléfono del servicio de ayuda de la oficina y pida consejo para resolver problemas, averiguando si hay que establecer permisos de acceso especiales u otros detalles antes de abandonar la ciudad.

Trabajar durante el viaje

Utilizar una conexión inalámbrica a Internet durante un viaje no es muy distinto de utilizarla cuando estamos en casa o la oficina. De todas formas, hemos encontrado algunas rarezas a lo largo del año y podemos proporcionarle algunos consejos útiles.

Conectar a una red

Para conectar a una red inalámbrica, hay que encontrarla y tener la configuración de red apropiada. Si se necesita una cuenta, también hay que proporcionar autenticación.

Encontrar una red

Incluso si llevamos a cabo un estudio antes de partir y pensamos que sabemos dónde hay una red inalámbrica, encontrar el lugar preciso en el que obtener acceso puede ser más difícil de lo previsto. A menudo hay zonas muertas en las terminales de aeropuertos que tienen "cobertura total" y hemos llegado a ser conocidos por ir paseando mirando la pantalla del portátil en busca de redes inalámbricas en los alrededores de los lugares en que se suponía que tenía que haber un café con acceso inalámbrico.

Hay tres opciones principales a la hora de encontrar una red que pensamos hay en las cercanías o para investigar si existe una red:

- **NetStumbler y MacStumbler:** Estas herramientas, que puede encontrar en www.netstumbler.com y www.macstumbler.com (las hemos descrito en detalle en el capítulo 6), rastrean redes locales en las cercanías y muestran los nombres de red, la fuerza de la señal y si están protegidas con cifrado WEP. Puede pasear viendo si la fuerza de la señal aumenta o disminuye, consiguiendo acercarse al lugar en el que la señal es más fuere. Tenga en cuenta que utilizar estas herramientas puede molestar a la gente, pues se utilizan tanto para propósitos válidos como para atacar redes.
- **Signos de tiza:** El warchalking es el acto de escribir signos con tiza que indican a otras personas que hay una red cercana disponible (vea la figura 7.1). Algunos WISP han desarrollado versiones más pulidas de los signos de tiza para utilizarlas como símbolos de sus tiendas; ejemplos

son las tiendas FatPort y, como informaron a Glenn recientemente, Schlotzsky 's Deli. Para más información sobre warchalking (y una explicación del nombre), vea el capítulo 6.

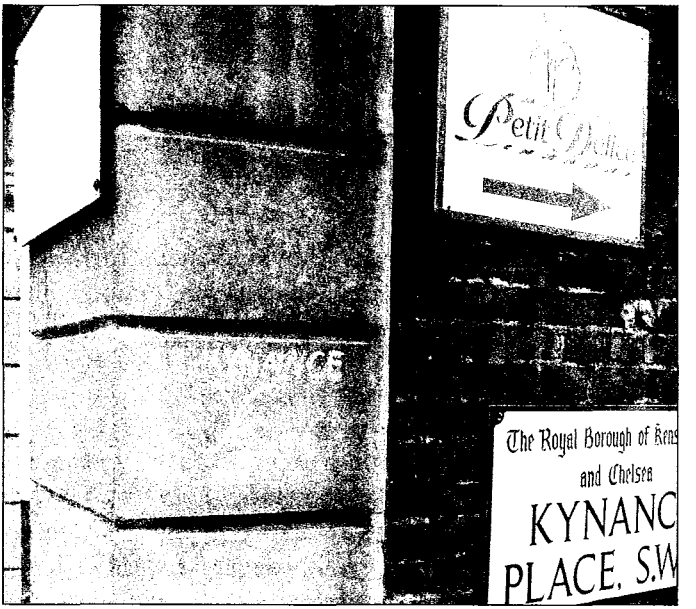

Figura 7.1. *Un signo de tiza típico del warchalking.*

- **Preguntar:** Sabemos que es orgulloso, también lo somos nosotros. Por eso ponemos aquí este punto, la opción más obvia en el último lugar de la lista. Pero igual que nos vemos obligados a preguntar cuando nos perdemos conduciendo, la forma más fácil de encontrar una red es preguntar a la gente. Aunque la persona a la que preguntemos no sepa dónde hay una, puede ser capaz de indicarnos la dirección correcta.

Configurar la red

La mayoría de las redes inalámbricas proporcionan automáticamente una dirección IP y otros detalles de red a través de DHCP. Por ello, la configuración de red para los viajes debe estar establecida para obtener una dirección IP automáticamente.

Truco *Encontrará información sobre la configuración de la conexión de red para trabajar con DHCP en el capítulo 4.*

Después de garantizar que el portátil utiliza DHCP, todo lo que falta es seleccionar la red inalámbrica que haya al alcance y la máquina negociará automáticamente una dirección IP para proporcionar acceso a la red.

Truco

Prácticamente ninguna red pública utiliza WEP evitando así procedimientos de inicio de sesión complicados. Como WEP no protege los datos frente a otras personas que se encuentren dentro de la misma red, el cifrado WEP no es útil en las redes públicas.

Acceso de inicio de sesión

Algunas redes gratuitas o con cuotas pueden requerir que naveguemos hasta una página de portal cautivo antes de acceder a la red. Inicie el navegador e intente visitar cualquier página Web; la página de portal cautivo aparecerá y solicitará que acepte los términos de uso o que introduzca la información de inicio de sesión o los detalles de pago por tarjeta de crédito.

Trucos prácticos

Como hemos señalado al principio de este capítulo, utilizar una conexión de red inalámbrica durante un viaje una vez conectado es casi igual que hacerlo en casa o en la oficina, pero podemos ofrecer algunos trucos que nos ha enseñado la práctica.

- **Compruebe el correo electrónico siempre que pueda:** Nunca se sabe si podremos conectar en el futuro; cuando haya presente un acceso inalámbrico a Internet, aproveche la oportunidad para ponerse al día.
- **Desactive las tarjetas de red para ahorrar energía:** Aunque los portátiles actuales han mejorado mucho, la corta vida de las baterías sigue siendo su principal problema. Junto con otras medidas de ahorro de energía que pueda tomar (oscurecer la pantalla, reducir la velocidad del disco duro o la del procesador), compruebe que desactiva la tarjeta de red inalámbrica si no hay un acceso en las cercanías. Eso es especialmente adecuado en los aviones, donde no se permite el uso de ningún transmisor de ondas de radio.

Truco

Hemos probado una bonita PC Card inalámbrica Com HomeConnect que tiene una antena dipolo plegable. El controlador puede configurar-

se para desactivar la tarjeta inalámbrica cuando plegamos la antena, que es un acto satisfactorio. Además, cuando la antena está plegada, no estorba.

- **Navegar fuera de línea:** Varios navegadores y otras utilidades permiten almacenar páginas Web como grupo local de archivos para verlas posteriormente. Adobe Acrobat ofrece una opción que transforma Web en PDF para guardar páginas Web e imágenes, incluyendo ciertos tipos de multimedia, convirtiendo las páginas en archivos Acrobat PDF. Estas funciones son útiles porque es probable que el acceso a Internet sea esporádico; descargando páginas Web para verlas posteriormente, podemos acceder a la información cuando no hay una red activa en las cercanías.
- **Usar un kit de seguridad.** El problema de las sesiones largas en una cafetería es que beber tanto café significa que tarde o temprano tendremos que visitar el aseo. ¿Qué hacemos con el portátil? Si estamos solos, la estrategia más segura es guardarlo todo y llevarlo con nosotros, perdiendo sólo algo de tiempo y quizá un buen sitio en el que sentarse. Otra alternativa es hacer lo que hacemos nosotros: usar un kit de seguridad para encadenar el portátil y la bolsa a la mesa. Puede comprar varios tipos de kits de seguridad, incluyendo algunos con alarma que producen un fuerte sonido si se mueve el ordenador. Nosotros utilizamos los kits de seguridad de Kensington Technology Group (visite www.kensington.com/html/1434.html para ver los modelos actuales).

Redes a distancia

Poca gente quiere trabajar mientras está de viaje, pero en el mundo actual a menudo es necesario. Esperamos que los consejos de este capítulo le ayuden a ser más funcional en su próximo viaje.

A continuación, vamos a abordar el tema de las conexiones inalámbricas de gran alcance; aunque dudamos que la mayoría de la gente quiera instalar una antena para alcanzar una señal de red inalámbrica que proviene de una torre a kilómetros de distancia, estas conexiones de largo alcance pueden ser una buena alternativa a comprar un acceso a Internet DSL o de módem de cable.

8. A distancia

Probablemente esté familiarizado con la advertencia que acompaña a muchas piezas de equipamiento de red 802.11b, algo como "Rendimiento máximo 11 Mbsp hasta 500 metros". Y si lleva un tiempo usando redes inalámbricas, sabrá que 500 metros es una estimación a menudo optimista. Poniendo una pared o dos en el camino, el alcance de la red inalámbrica bajará a 100 ó 150 metros.

Estos descargos de responsabilidad no significan que haya una limitación particular en el alcance efectivo de las redes inalámbricas 802.11b estándar. Con el equipo apropiado, principalmente una antena de alta ganancia que aumente la fuerza de la señal inalámbrica, podemos configurar una red inalámbrica 802.11b con un alcance que no se mida en metros, sino en kilómetros.

De hecho, con otras variantes de redes inalámbricas que utilizan salto de frecuencias más lento pero más robusto, esas distancias pueden ampliarse más allá de lo posible con 802.11b. Hay un proveedor de servicios de Internet inalámbricos (WISP) en Maine que despliega sus enlaces entre 30 y 60 kilómetros, incluyendo un enlace de 35 kilómetros desde la costa hasta una isla con 300 residentes.

Los residentes de esta isla antes tenían conexiones de llamada telefónica muy lentas que costaban varios centavos por minuto. Con el enlace inalámbrico

de gran alcance, los residentes locales pueden conectar directamente a alta velocidad con la torre de la isla y recibir un ancho de banda de entre 1 y 3 Mbps; o pueden establecer una conexión por módem con la torre y no pagar nada por minuto. La conexión de red inalámbrica de gran alcance ha sido todo un cambio para estas personas.

Nota *Vaya por delante una aclaración: nosotros conocemos muy bien los ordenadores, no las radios, y suponemos que el lector también está más familiarizado con los ordenadores que con las radios. Los comentarios siguientes están basados en nuestra experiencia, investigación y objetivo de explicar el tema sin entrar en detalles sobre la física y las matemáticas que definen exactamente lo que sucede en una conexión inalámbrica de largo alcance.*

¿Por qué elegir el largo alcance?

El caso del WISP de Main es especialmente adecuado, porque ilustra los dos usos de las redes inalámbricas de largo alcance en situaciones en que los cables pueden no funcionar: conectar con Internet y ampliar una red existente.

Los dos hemos trabajado algo en establecer conexiones de Internet de largo alcance y en extensión de redes, y hemos aprendido que cada situación individual es distinta. Por tanto, nuestra intención aquí es describir las posibilidades, comentar qué hardware puede ser necesario y darle ideas. No ofrecemos instrucciones detalladas porque es imposible imaginar por adelantado qué será necesario en las situaciones particulares.

Nota *Ya desee conectar con Internet o ampliar el alcance de su red existente, es importante saber por adelantado que una conexión inalámbrica de largo alcance enlaza el sitio remoto con un solo aparato en su lado. No suponga que todos los ordenadores con capacidad inalámbrica podrán de pronto utilizar la conexión de largo alcance sólo porque ha puesto una antena de alta ganancia. Igual que con los módem de cable o DSL, hay que usar una puerta de enlace para redistribuir la conexión en el resto de la red local.*

Conectar a Internet

Casi todo el mundo tiene teléfono en la actualidad y puede conectar con un proveedor de servicios de Internet a través de un módem estándar. Pero los módems tardan un tiempo en efectuar la llamada, su rendimiento es lento y no son muy robustos en general, que es una de las razones por las que las conexiones de Internet de alta velocidad, también llamadas "conexiones de banda ancha de consumidor", a través de líneas de teléfono o cable se han vuelto tan populares.

La gente que vive bastante cerca de una oficina central telefónica bien equipada o cuyas empresas de televisión por cable ofrecen acceso a Internet siguen siendo una pequeña fracción de la población mundial, y sigue siendo muy probable que una persona cualquiera viva en un lugar en el que el acceso de banda ancha tiene un precio prohibitivo o es imposible de conseguir de ningún modo.

La dificultad de encontrar acceso a Internet de banda ancha es especialmente común en áreas rurales poco pobladas, donde es posible que las compañías de teléfono o cable no inviertan en el equipamiento de última línea necesario o el desarrollo sea lento.

Nota

Incluso cuando el acceso de alta velocidad a Internet está disponible, a menudo la base no es muy resistente. Unos amigos de Glenn de una pequeña cuidad de Maine tuvieron la suerte suficiente para conseguir un servicio de módem de cable... durante un tiempo. La compra de la compañía local por un proveedor de servicios de Internet más grande provocó que el servicio de módem de cable dejara de funcionar con fiabilidad.

Cada vez en más lugares de esas características, los proveedores de servicios de Internet se están decidiendo por redes inalámbricas de largo alcance como método de proporcionar conectividad con Internet a clientes alejados sin utilizar cables telefónicos ni desplegar nuevos cables. Al no necesitar cables, el coste de añadir un cliente es bajo tanto para el ISP como para el propio cliente, y el rendimiento estándar de 1 Mbps (la menor de las velocidades del estándar 802.11b) es generalmente igual al de las mejores conexiones de cable o DSL.

Nota

Algunos ISP incluso se asocian con pequeñas compañías de teléfono que todavía operan en zonas rurales de los EE.UU. El ISP proporciona

Internet de alta velocidad al punto de intercambio local a través de una conexión inalámbrica de largo alcance y la compañía de teléfonos lo redistribuye por medio de DSL.

El largo brazo de la ley

Hay restricciones legales a la potencia que se puede transmitir por radio, incluyendo las redes inalámbricas. Estas restricciones varían entre países y estados dentro de los EE.UU. y en algunos estados las conexiones inalámbricas de largo alcance están totalmente prohibidas. Compruebe los estatutos legales antes de suponer que puede configurar una red inalámbrica de largo alcance.
En los EE.UU., las restricciones sobre las redes inalámbricas de largo alcance las establece la Federal Communications Commission (FCC) en lo que se llama "Regulaciones de la parte 15". La parte 15 especifica limitaciones de potencia, limitaciones de equipamiento, requerimientos de certificación y gestión de interferencias. Puede leer toda la parte 15 en http://www.access.gpo.gov/nara/cfr/waisidx_01/47cfr15_01.html. Para ver un análisis de la parte 15 y qué significa al establecer conexiones inalámbricas de largo alcance, recomendamos que lea el artículo de Tim Pozar sobre el tema, disponible en www.lns.com/papers/part15/. Aunque Pozar no es abogado, es ingeniero de radio que actúa como consultor en temas de comunicaciones y también es miembro fundador del Bay Area Wireless Users Group (www.bawug.com), uno de los principales grupos de usuarios inalámbricos del mundo.

Igual que la conexión de Internet inalámbrica de largo alcance puede ser la única opción para mucha gente, otros las utilizan para obtener conexiones redundantes.

Por ejemplo, la conectividad Internet es esencial para el trabajo de Adam como escritor y editor, de modo que cuando se mudó desde las afueras de Seattle, Washington (donde estaba pensando en establecer su propio servicio de Internet inalámbrico desde su casa encima de Tiger Mountain) hasta Ithaca, New York, suscribió una conexión a Internet por módem de cable y también instaló una conexión inalámbrica de largo alcance con un ISP diferente. Si le sucediera algo en alguna de las conexiones o a uno de los ISP, podría pasar a la otra conexión en todos los ordenadores en cuestión de minutos.

Ampliar la red

Otro de los principales usos de las redes inalámbricas de largo alcance es ampliar una red existente hasta una ubicación remota. Quizá nuestra compañía tenga oficinas en edificios distintos en un parque empresarial y queramos unirlas. La distancia puede ser excesiva para desplegar un cable Ethernet y el coste de alquilar una línea digital de alta velocidad de una compañía de teléfonos quizá sea prohibitivo, pero por menos de 1.000€ y algunos días de trabajo, es posible añadir nuevas oficina a la red existente sin pagar costes a la compañía de teléfono.

Y todavía más que en las conexiones Internet inalámbricas de largo alcance, los detalles aquí dependen de la red particular y lo que se quiera conseguir, de modo que nos vemos forzados a hablar más en general en cuanto a ampliar las redes inalámbricas.

Asuntos básicos de las antenas

La principal pieza de hardware implicada en una red inalámbrica doméstica o de pequeña oficina que nace de una red inalámbrica de largo alcance es una antena. Todos los adaptadores de red inalámbrica y los puntos de acceso tienen antenas integradas, pero en su mayor parte se han diseñado para que sean pequeñas más que para aumentar la fuerza de la señal (vea la figura 8.1). La mayoría de los adaptadores de red inalámbrica PC Card tienen embutida toda la antena en la parte de unos 50 cm que sobresale del portátil cuando la tarjeta está conectada.

No hay necesidad de que las antenas sean tan pequeñas y ofrezcan tan mínima mejora de la fuerza de la señal, y, de hecho, desde el lanzamiento de su tecnología de red inalámbrica AirPort, Apple ha construido antenas más potentes dentro de los ordenadores Mac. Con la excepción del Titanium PowerBook G4, eso ha originado que los sistemas Mac tengan un alcance de red inalámbrica mucho mejor que los portátiles que sólo usan las antenas integradas en sus adaptadores de red PC Card. Afortunadamente, muchos fabricantes de portátiles PC han captado la idea y están siguiendo la idea de Apple.

Nota

Adam tiene un estudio apartamento para invitados sobre su garaje y, a pesar de que está todo lo cerca posible de la ubicación de su punto de acceso dentro de la casa, dos invitados con portátiles PC y adaptadores

de red PC Card y otro con un Titanium PowerBook G4 fueron incapaces de conseguir una señal de la red inalámbrica. Sin embargo, el iBook de Adam recibe las cinco barras de fuerza de la señal exactamente en el mismo punto. Las buenas antenas son la diferencia.

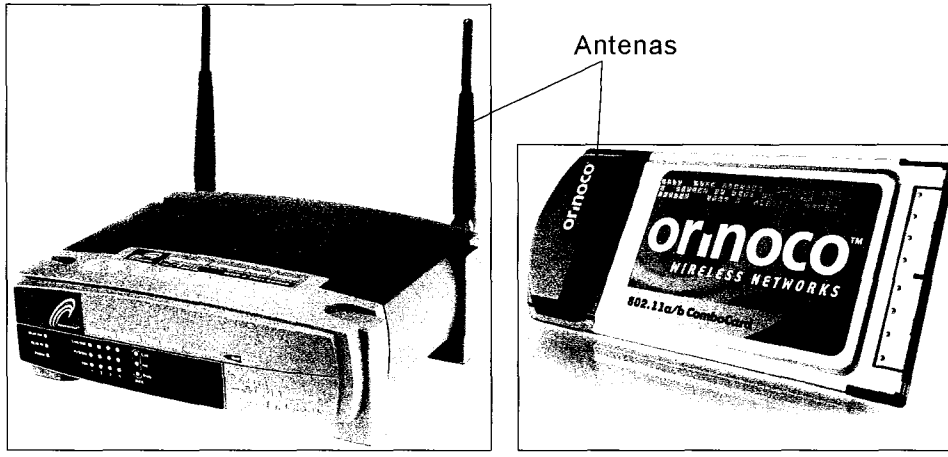

Figura 8.1. *Antenas integradas normales.*

De cualquier forma, para redes inalámbricas de largo alcance, las antenas integradas nunca serán suficiente y hay que buscar antenas externas más grandes. Afortunadamente, gracias al crecimiento de la comunidad inalámbrica, cada vez es más fácil y más barato comprar una antena externa. Para encontrar un buen vendedor de antenas después de leer nuestro debate sobre las antenas, visite sitios de redes comunitarias como http://nocat.net y vea sus recomendaciones.

Preocupación por la salud

¿Hay problemas de salud relacionados con las redes inalámbricas? Sí y no. En la mayoría de las situaciones, la potencia implicada está muy por debajo de la cantidad de radiación emitida por un teléfono móvil y los estudios no han encontrado relaciones concluyentes entre el uso de teléfonos móviles y el cáncer, y los móviles a menudo están en contacto con el propio cuerpo humano.

Como veremos más adelante, la fuerza de las señales transmitidas a la antena es muy débil y, por supuesto, el hecho de utilizar la antena no

significa que recibamos más radiación que todas las demás personas que hay en la zona. Todos estamos constantemente bajo el bombardeo de radiación electromagnética de baja potencia. Además, la intensidad de las señales transmitidas baja muchísimo en cuanto nos separamos un poco de la antena. Dicho eso, si configuramos un enlace inalámbrico de largo alcance que utiliza el extremo superior del espectro de potencia permitido, sólo hay que utilizar el sentido común y colocar las cosas para que nadie tenga que pasar mucho tiempo delante de la antena direccional de alta ganancia.

Antenas y fuerza de la señal

La parte más difícil de la planificación de una conexión de red inalámbrica de largo alcance es determinar la cantidad de ganancia, mejora de fuerza de la señal, necesaria en la antena para enviar y recibir señales de la ubicación remota. Es peliagudo porque hay que tener en cuenta cierto número de variables y algunas no son fáciles de determinar sin ser un experto en antenas. Veamos un cálculo utilizando la conexión a Internet inalámbrica de largo alcance de Adam como ejemplo.

Nota

Hay que hacer este cálculo en las dos direcciones porque aunque las antenas mejoran la fuerza de la señal tanto para transmitir como para recibir, no todas las radios tienen la misma calidad recibiendo datos y enviándolos.

Truco

Es posible encontrar en la Web calculadoras que se ocupan de resolver los números, pero nuestra experiencia nos dice que muchas de ellas piden más información de la que es posible determinar, siendo más precisas que en nuestro debate siguiente, pero casi inútiles si uno no conoce todos los detalles. Vea la calculadora de Green Bay Packet Radio en http://www.gsl.net/n9zia como ejemplo de lo que decimos.

Potencia transmitida

El primer número a encontrar es la potencia transmitida del transceptor de radio en el aparato que queremos conectar a la antena. Afortunadamente, los

fabricantes casi siempre publican ese número en las especificaciones técnicas del aparato y es fácil de encontrar. Adam alimenta su conexión inalámbrica utilizando una PC Card Lucent WaveLAN (sacada de una Estación Base AirPort) conectada a un PowerBook G3 de Apple (vea la figura 8.2). Un breve examen de las especificaciones técnicas de la Estación Base AirPort en la base de conocimiento en línea de Apple revela que tiene una potencia transmitida de 15 dBm (en la siguiente nota encontrará una explicación de la abreviatura dBm). Otra búsqueda en Google (www.google.com, el mejor motor de búsqueda de Internet) utilizando "Lucent WaveLAN transmit power dBm" muestra varios otros recursos que confirman el valor de 15 dBm.

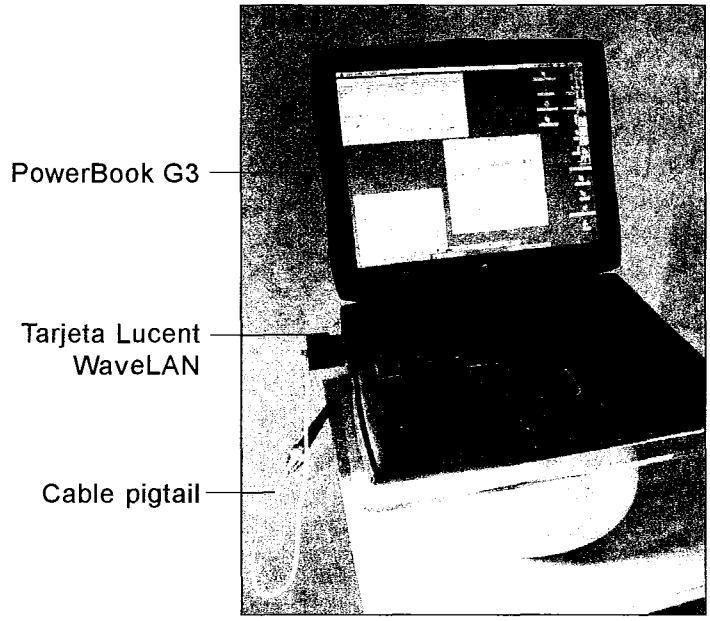

Figura 8.2. *La tarjeta WaveLAN de Adam en un PowerBook G3.*

Nota

dB significa decibelios, la unidad utilizada en estos cálculos; dBm significa decibelios relativos al nivel de referencia de 1 milivatio (mW). Hablando sin mucha precisión, 1 mW es igual a 0 dBm y cada vez que se doblan los milivatios, se suma 3 a los decibelios. La radiación máxima emitida por una antena (que puede terminar muy por encima de los vatios de entrada) que admite la FCC en los EE.UU. es 1 vatio, equivalente a 30 dBm. En Europa, es de sólo 250 mW o 24 dBm. HyperLink Technologies ofrece una tabla de conversión de decibelios a vatios en

www.hyperlinktech.com/web/dbm.html y el artículo de Tim Pozar en www.lns.com/papers/part15/ explica la limitación con más detalle.

También hay que calcular la potencia transmitida de la radio remota, que podemos determinar comprobando las especificaciones técnicas del hardware, si sabemos exactamente cuál es, o preguntando al WISP. En el caso de Adam, su WISP, Lightlink, utiliza un Cisco AP340 y una rápida búsqueda revela que también tiene una potencia transmitida de 15 dBm. Si no puede determinar este número, apueste por 15 dBm, el equivalente de un transmisor de 30 mW, que es común. Es posible comprar transmisores de 100 mW y de hasta 250 mW, pero son menos comunes y se acercan peligrosamente a los límites de potencia permitidos.

Pérdida de señal en el cable

Para conectar una antena a un adaptador de red inalámbrico, se necesita un pequeño cable fino llamado *pigtail* cuyo propósito es conectar la pequeña toma del adaptador de red con el grueso cable coaxial de la antena. Ampliaremos el tema de los cables de antena en un momento; veamos primero la posible pérdida de señal.

En todos los cables hay pérdida de señal y cuanto más fino es el cable, más señal se pierde. Como los cables pigtail siempre son finos, tienden a tener mayor pérdida de señal; hemos visto estimaciones de unos 1,2 dB o más por metro. Pero la calidad del cable constituye una gran diferencia, de modo que la pérdida puede ser mayor o menor dependiendo del cable pigtail que compre. El fabricante puede indicarle la pérdida de señal del cable y si no, puede intentar adivinarla. Siendo conservadores, vamos a suponer que en los 40 cm de cable pigtail de Adam se pierde alrededor de 1 dB.

Otra fuente de pérdida de señal son los conectores, de manera que hay que reducir el número de conectores tanto como sea posible. De nuevo, hemos visto estimaciones de 1 dB de pérdida por conector. Típicamente, los conectores baratos tendrán más pérdida que otros más caros. Como Adam tiene tres conectores en su configuración (uno de la tarjeta Lucent WaveLAN al cable pigtail, uno del cable pigtail al cable de la antena y uno del cable de la antena a la propia antena) vamos a suponer que se pierden 3dB.

La última parte de la ecuación de cables viene de la longitud del cable desde la antena al cable pigtail. La pérdida de señal varía mucho dependiendo del tipo de cable, pero es algo que el fabricante publica en las especificaciones técnicas o al menos puede decirnos cuál es. Adam utiliza 4,5 metros de cable

LMR400, con 0,22 dB de pérdida por metro, y un rápido cálculo muestra que pierde alrededor de 1 dB de fuerza de la señal en el cable.

Sumando todos los números (1 dB del cable pigtail, 3 dB de los conectores y 1 dB del cable de la antena) obtenemos un total de 5 dB de pérdida de fuerza de la señal debido al indispensable cableado.

Desgraciadamente, es probable que calcular la pérdida de señal en los cables del lado remoto sea sólo una conjetura, pues sólo la persona que instaló el equipo sabrá qué cable de antena y cable pigtail utilizó y cuántos conectores fueron necesarios. Si no consigue averiguarlo, puede conjeturar que la pérdida será también de 5 dB.

Ganancia de antena

La potencia principal del sistema proviene de la propia antena, por supuesto, y es fácil determinar la ganancia de una antena porque sólo depende de dos variables (junto con el tipo de antena) que vemos cuando miramos las antenas en la tienda. Igual que los otros números de este cálculo, la ganancia de la antena se mide en decibelios, expresados en este caso como dBi o decibelios relativos a lo que se llama una antena isotrópica.

Aquí es necesaria una explicación. Las antenas son útiles porque dan forma a la señal de radio y la enfocan en una dirección determinada. La peor antena de larga distancia imaginable irradiaría la señal con forma esférica, siendo la antena el centro de la esfera; eso es una antena isotrópica. El diseño de una antena permite dar forma a la señal y enfocarla en la dirección deseada, aumentando la fuerza de la señal en esa dirección y reduciéndola en las otras. Comentaremos los distintos diseños de antenas en un momento; por ahora, baste con saber que el diseño de la antena afecta directamente al aumento de la fuerza de la señal. En el caso de Adam, primero compró una antena yagui de 14 dBi, pero cuando vio que no funcionaba, la cambió por una antena parabólica de 24 dBi que funciona perfectamente (vea la figura 8.3). (No se preocupe si estos nombres de antena le resultan desconocidos, los describiremos más adelante en este capítulo.)

Tenga en cuenta que el otro lado de la conexión también tiene una antena y hay que sumar eso a la ecuación; la única forma de conocer esa información es preguntar. La antena del WISP de Adam es una omnidireccional de 14 dBi.

Pérdida en el aire

La parte más fácil de entender, si no de calcular, en la ecuación de fuerza de señal es la pérdida que se produce mientras viaja por el aire entre la antena

doméstica y la antena remota. Nadie tiene problemas para aceptar que cuanto mayor es la distancia entre un transmisor y un receptor más débil es la señal. Las razones de esta pérdida de señal en el aire son que las ondas se dispersan de forma proporcional al cuadrado de la distancia que recorren y que el aire absorbe parte de la fuerza de la señal, especialmente si hay moléculas de agua en un día lluvioso.

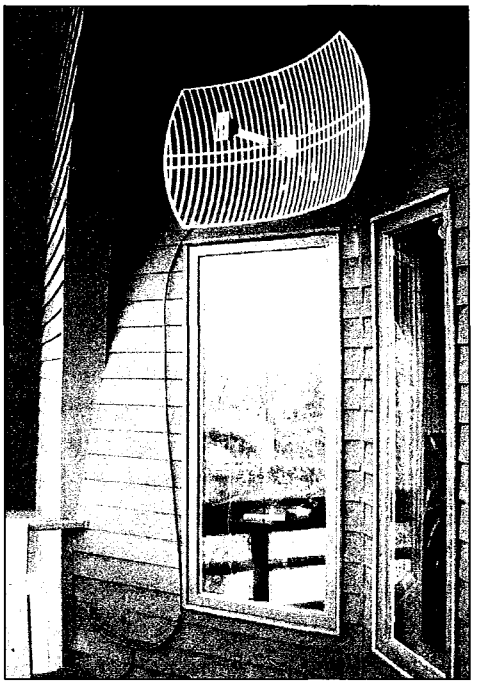

Figura 8.3. *La antena parabólica de 24 dBi de Adam.*

Nota

El WISP de Maine con el que habló Glenn le comentó que la nieve que frecuentemente cae en Maine parece mejorar la calidad de la señal y Adam descubrió una vez que su iBook podía recibir la señal remota utilizando sólo su antena interna durante una tormenta de nieve. La moraleja de la historia es que las precipitaciones afectan a la fuerza de la señal de modo impredecible, por la reflexión de la señal en gotas de agua o copos de nieve individuales.

Puede usar una calculadora en línea para determinar la pérdida en el aire (la que encontrará en www.comsearch.com/satellite/tools_fsl.jsp es fácil de

usar; otras que hemos visto no eran tan sencillas). O, si no le gusta la opción, puede calcular la pérdida en aire con la siguiente ecuación:

```
-L = C + (20 x log(D)) + (20 x log(F))
```

En la ecuación, -L es la pérdida de señal, C es una constante que vale 36,6 si se mide la distancia D en millas o 32,5 si se mide D en kilómetros y F es la frecuencia en megahercios (2400 MHz para el estándar 802.11b).

Truco *Que no le intimiden las letras y logaritmos de la ecuación, es fácil resolverla con una calculadora corriente que resuelva logaritmos. De cualquier forma, tenga cuidado de multiplicar lo que hay dentro de los paréntesis antes de hacer la suma final.*

Lo único que hay que determinar para resolver esta ecuación es la distancia entre la antena doméstica y la remota. Puede ponerse quisquilloso y utilizar un aparato GPS para determinar su posición y la de la antena remota, pero no es necesaria tanta precisión porque al usar el logaritmo de la distancia se minimiza el efecto de ésta en la ecuación general. La casa de Adam está a unas 2 millas de la antena remota, de modo que la ecuación para su conexión es:

```
-L = 36,6 + (20 x log(2)) + (20 x log(2400))
```

Calculando los logaritmos (escriba el número y pulse el botón log de la calculadora) resulta:

```
-L = 36,6 + (20 x 0,301) + (20 x 3,38)
```

Y resolviendo las multiplicaciones entre paréntesis, queda:

```
-L = 36,6 + (6,02) + (67,60)
```

Por último sólo falta hacer la suma:

```
-L = 110,22
```

Es decir, que la distancia entre la antena de Adam y la antena remota produce una pérdida de señal de unos 110 dB.

Nota *¿Recuerda que dijimos que la precisión en la distancia no tiene mucho efecto en el resultado? si la casa de Adam estuviera a 3 millas de la antena remota, la pérdida de señal aumentaría sólo a 113 dB. No es que sea un salto insignificante, pero se necesita un margen mayor de 3 dB para que una conexión funcione correctamente.*

Sensibilidad de recepción

El cálculo anterior determina la fuerza de la señal a su llegada, pero hay un detalle más que determinar para saber si es probable que la conexión funcione: la sensibilidad de recepción de las dos radios. La sensibilidad de recepción es una medida de lo fuerte que debe ser una señal para que la radio receptora sea capaz de decodificarla.

Como la potencia transmitida, se mide en dBm, pero los números son muy pequeños, a menudo alrededor de -85 dBm.

En nuestro lado, podemos mirar en las especificaciones técnicas de la tarjeta inalámbrica o el punto de acceso. Algunos fabricantes de equipamiento de red inalámbrica incluyen la sensibilidad de recepción en las especificaciones técnicas, pero otros la omiten. También es posible encontrar los valores de sensibilidad de recepción de muchos aparatos de red en http://freenetworks.org/moin/index.cgi/ReceiveSensivity.

A menos que nos encarguemos de la instalación en ambos lados de la conexión, el único modo de determinar la sensibilidad de recepción en el lado remoto es preguntar al ISP o buscar información acerca de los equipos que utiliza el ISP. Si no es posible averiguar el valor de la sensibilidad de recepción, una buena apuesta son valores entre -75 y -90 dBm.

En el caso de Adam, buscando en Google "Lucent WaveLAN receive sensivity dBm" se obtienen algunas páginas que muestran que su tarjeta tiene una sensibilidad de recepción de -90 dBm. Otra búsqueda sobre "Cisco AP340 receive sensivity dBm" revela que la radio remota tiene también la sensibilidad de recepción -90 dBm.

Reunirlo todo

Ha llegado el momento de reunirlo todo, sumar los números que representan la fuerza de la señal y restar los que representan la pérdida de señal. Recuerde que tenemos que hacer los cálculos en las dos direcciones: envío de información a la ubicación remota y recepción desde la ubicación remota. Para la conexión de largo alcance de Adam, obtenemos lo siguiente para el envío de datos al WISP (vea la tabla 8.1).

Truco

Este cálculo incluye un margen de 15 dB para tener en cuenta los cambios de tiempo. Si la conexión inalámbrica está en el límite de tener suficiente fuerza de señal con buen tiempo, una tormenta puede provocar que desaparezca la conexión totalmente.

Tabla 8.1. Cálculo de la fuerza de señal enviada a la ubicación remota.

Variable	Ganancia o pérdida
Potencia transmitida local	+15 dBm
Pérdida en cables locales	-5 dB
Ganancia de antena local	+24 dBi
Pérdida en el aire	-110 dB
Ganancia de antena remota	+14 dBi
Pérdida en cables remotos	-5 dB
Margen para cambios de tiempo	-15 dB
Fuerza de señal en la ubicación remota	**-82dBm**

Como la sensibilidad de recepción en el lado remoto es -90 dBm, el cálculo muestra que Adam debe tener una fuerza de señal de 8 dBm en el caso del peor tiempo (los 8 dBm son la diferencia entre los -90 dBm de sensibilidad de recepción y los -82 dBm de fuerza de la señal que calculamos en la tabla 8.1). Con buen tiempo, terminamos con 23 dBm (8 dBm más los 15 dBm que hemos utilizado como margen para el mal tiempo). Teniendo en cuenta que la potencia transmitida en la mayoría del equipamiento de red inalámbrica está entre 15 y 20 dBm y funciona bien en situaciones de corto alcance, ser capaz de enviar entre 8 y 25 dBm a la ubicación remota debe ser suficiente para que la conexión funcione bien.

Ahora llevaremos a cabo el cálculo inverso, para ver la fuerza de la señal que recibe Adam procedente de su WISP (vea la tabla 8.2).

Tabla 8.2. Cálculo de la fuerza de señal recibida en la ubicación local

Variable	Ganancia o pérdida
Potencia transmitida remota	+15 dBm
Pérdida en cables remotos	-5 dB
Ganancia de antena remota	+14 dBi
Pérdida en el aire	-110 dB

Variable	Ganancia o pérdida
Ganancia de antena local	+24 dBi
Pérdida en cables locales	-5 dB
Margen para cambios de tiempo	-15 dB
Fuerza de señal en la ubicación local	**-82dBm**

Como el equipo de Adam y el del WISP resultan ser idénticos en términos de potencia transmitida y sensibilidad de recepción, la fuerza de la señal es la misma en las dos direcciones.

Nota

La fuerza de la señal transmitida y recibida no siempre es la misma. En otras situaciones, será probable que la radio del ISP tendrá una potencia transmitida superior, quizá de 24 dBm,y la radio local puede no tener una sensibilidad de recepción tan alta, tal vez sólo sea de -75 dBm. Desarrollando el cálculo con estos valores, la fuerza total de la señal recibida resulta ser -73 dBm, que deja sólo 2 dBm entre eso y los -75 dBm de sensibilidad de recepción de la radio teórica. Como el cálculo tiene en cuenta la posibilidad de tormentas, es probable que esta configuración proporcione suficiente fuerza de señal para la conexión durante las épocas de buen tiempo, pero puede perderse la conexión en días lluviosos.

Variables cambiantes

En el ejemplo anterior de la conexión de Adam, sabíamos o podíamos conjeturar fácilmente todos los valores porque es una conexión existente. Pero hay que efectuar este cálculo antes de comprar el equipamiento (y si hubiera sabido entonces lo que sabe ahora, Adam también lo habría hecho).

Por tanto, nuestro consejo es que prepare una hoja de cálculo sencilla parecida a las tablas anteriores e introduzca todos los números que pueda conjeturar para el sitio remoto (suponiendo que no está configurando los dos extremos de la conexión usted mismo) y después incluya la pérdida en el aire. Una vez hecho eso, puede introducir valores del equipamiento que piense que necesita para comprobar si va a funcionar. Si Adam hubiera hecho este cálculo antes de configurar su conexión inalámbrica de largo alcance, habría averiguado que la

antena yagui de 14 dBi que compró al principio no iba a funcionar porque la fuerza de señal efectiva iba a ser de sólo -2 dB con mal tiempo o 13 dB con buen tiempo. Naturalmente, eso no explica por qué la antena yagui de 14 dBi no funcionaba con buen tiempo, pues la fuerza de la señal debería haber sido suficiente para el funcionamiento. El hecho de que no funcionara pone en evidencia que el cálculo descrito es sólo aproximativo y hacer el cálculo real conllevaría tener en cuenta muchas variables adicionales. Las calculadoras Web pueden servir de ayuda y también se puede utilizar hasta cierto punto, como hizo Adam, la estrategia de prueba y error.

Truco *No hemos mencionado una forma más de aumentar la fuerza de la señal: utilizar un amplificador. No son baratos (algunos cientos de euros) y hay que tener cuidado para no violar límites de regulación de potencia, pero pueden ser útiles. No hemos experimentado con ellos, pero tenemos informes de que no carecen de inconvenientes, pues amplifican el ruido además de la señal.*

Tipos de antena

Ya hemos mencionado los tres principales tipos de antenas de largo alcance (omnidireccional, yagui y parabólica), pero es necesaria más información sobre ellas. Además, queremos mencionar otros tipos que pueden ser útiles.

Truco *Con algunas antenas, como las parabólicas y las antenas panel, es importante montarlas con la orientación adecuada que coincida con la polarización de la antena remota. Si no está seguro de cuál es la polarización apropiada, pregunte al ISP y, si no hay respuesta, pruebe con la vertical.*

Antenas ominidireccionales

Como puede imaginar por el nombre, una antena omnidireccional, también llamada una antena de fuste vertical, es útil principalmente si queremos que la señal sea irradiada desde la antena en todas las direcciones. Eso no es del todo exacto, pues una antena omnidireccional suele tener la forma de una vara vertical y la señal irradia hacia los lados en círculos, pero no va hacia arriba o

hacia abajo, creando las ondas una especie de disco aplanado (vea la figura 8.4). En su mayor parte, se utilizan antenas omnidireccionales para crear una conexión punto a multipunto, esto es, cuando queremos que la antena reciba muchas conexiones. Los ISP utilizan a menudo antenas omnidireccionales en sus torres para no tener que instalar una antena de haz enfocado para cada cliente. Otro uso de las antenas omnidireccionales sería para proporcionar acceso de red inalámbrica en el campus de un instituto o universidad. El problema de las antenas omnidireccionales es que funcionan mejor en situaciones de alcance relativamente corto en las que todos los que establecen la conexión están más o menos a la misma altura que la antena (pues el haz no sube ni baja mucho).

Figura 8.4. *Una antena omnidireccional.*

Truco

Si quiere montar una antena omnidireccional (o cualquier otro tipo de antena externa) en el exterior donde puede ser alcanzada por un rayo, será buena idea instalar un supresor de saltos de tensión para proteger el punto de acceso. Adam decidió no añadir un supresor de saltos de tensión porque su antena parabólica está montada en la pared de la casa, debajo del alero. Añadir un supresor de salto de tensión reduce ligeramente la fuerza de la señal.

También se puede utilizar una antena omnidireccional de baja potencia para aumentar la fuerza de la señal de una red interior. En tal instalación, se monta-

ría la antena aproximadamente en el centro del espacio para aprovechar su patrón de radiación circular.

Dado que no se enfoca mucho el haz, la máxima salida de las antenas omnidireccionales está alrededor de 15 dBi de ganancia. También son baratas, fáciles de instalar y duraderas.

Antenas de sector

Como las antenas omnidireccionales, las antenas de sector se utilizan en conexiones punto a multipunto. Sin embargo, a diferencia de las antenas omnidireccionales, las antenas de sector irradian sólo en una dirección específica y a menudo se combinan para cubrir un área. Los vendedores de antenas de sector siempre describen la extensión de la cobertura de la antena, normalmente entre 60 y 180 grados.

La ventaja de utilizar múltiples antenas de sector en lugar de una antena omnidireccional es que podemos inclinar las primeras para solucionar el problema de la altura que afecta a las segundas. También ofrecen mayor ganancia, alrededor de 22 dBi. Suelen parecerse a pequeñas cajas estrechas, a veces sin centro (vea la figura 8.5).

Las antenas de sector cuestan mucho más que las omnidireccionales y, como se necesitan varias para cubrir los 360 grados completos, el coste todavía aumenta más. Merece la pena tenerlas en cuenta principalmente en ubicaciones específicas en las que una antena omnidireccional no resuelva el problema.

Figura 8.5. *Una antena de sector.*

Una cosa más sobre eso. Quizá encuentre antenas de baja potencia más baratas que se venden también para extender el alcance de la red en interiores. La ventaja que tienen frente a las antenas omnidireccionales cuando se utilizan

para este propósito es que se puede montar una antena en la pared para aprovechar su patrón de cobertura para aumentar la fuerza de la señal en una sola dirección.

Antenas de panel

Las antenas de panel son paneles planos sólidos que se utilizan para conexiones punto a punto enfocadas, como las antenas yagui y las parabólicas, que comentaremos a continuación. Las antenas de panel son baratas, tienen una buena ganancia de más de 22 dBi y pueden mezclarse con el entorno mejor que las antenas parabólicas de rejilla o plato. No parecen una antena, son como pequeñas cajas planas (vea la figura 8.6).

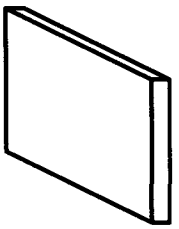

Figura 8.6. *Una antena de panel.*

Como inconveniente, dado que las antenas de panel deben estar dirigidas hacia la antena remota, a menudo no es posible montarlas planas sobre una pared. Y si no están planas sobre la pared, un viento fuerte puede moverlas o dañarlas.

Para el uso en interiores, las antenas de panel de baja potencia a menudo funcionan bastante bien, aunque hay que montarlas de forma que cubran bien el área de interés.

Antenas yagui

Si las antenas omnidireccionales se visualizan fácilmente gracias a su nombre, con las antenas yagui pasa justo lo contrario. Desde fuera, una antena yagui es como un tubo grueso de plástico y en el interior tienen una serie de círculos o barras de metal que van disminuyendo de tamaño según se llega al final de la antena (vea la figura 8.7). Una antena yagui proporciona un haz bastante enfocado, junto con una ganancia máxima de unos 21 dBi, siendo más común el valor de 15 dBi. Debido a lo enfocado del haz, hay que montar una antena yagui dirigiéndola a la ubicación remota.

Truco *Por el modo en que radian las antenas yagui, a menudo es mejor dirigir la antena yagui ligeramente hacia la derecha o hacia la izquierda de la ubicación remota. Igual que con todas las antenas direccionales, pruebe dirigiendo la antena hacia distintos puntos antes de bajar al suelo.*

Las antenas yagui son populares porque proporcionan una ganancia bastante decente al tiempo que resultan poco prominentes. Si monta una yagui en su casa, no tendrá que preocuparse demasiado porque un vecino paranoico piense que quiere espiarle. Aunque no son tan poco llamativas como las antenas de panel, las antenas yagui se ven menos afectadas por la fuerza del viento (aunque la nieve y el hielo que se acumule en invierno pueden perjudicar a la señal).

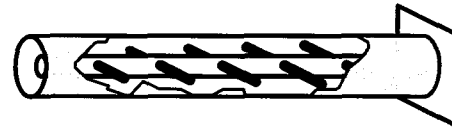

Figura 8.7. *Una antena yagui.*

Antenas parabólicas

Una antena parabólica es la más potente que se puede comprar y generalmente tiene la apariencia de una rejilla metálica curvada o un pequeño plato de satélite (vea la figura 8.8). Cuanto mayor sea la distancia que haya que cubrir, será más probable que sea necesaria una antena parabólica. Con una antena parabólica, se puede disfrutar de un haz enfocado y una ganancia de 27 dBi. El principal inconveniente de las parabólicas es que pueden ser bastante grandes (la de Adam mide 60 x 90 cm y las antenas de 27 dBi pueden tener un diámetro de 1,8 m).

Afortunadamente, la mujer de Adam, Tonya, piensa que una gran antena blanca colocada en el lateral de la casa le da mucho estilo. El hecho de que proporcione mejor conectividad a Internet también es una gran ventaja. Algunas otras esposas pueden no ser tan comprensivas.

Las antenas parabólicas son bastante asequibles y las que tienen una rejilla no sufren por la fuerza del viento ni acumulan nieve, siendo más apropiadas para situaciones más extremas en que se necesita alta ganancia.

Truco *Si no le preocupa la apariencia de la antena y no quiere complicarse, una antena parabólica de alta ganancia quizá sea la mejor opción.*

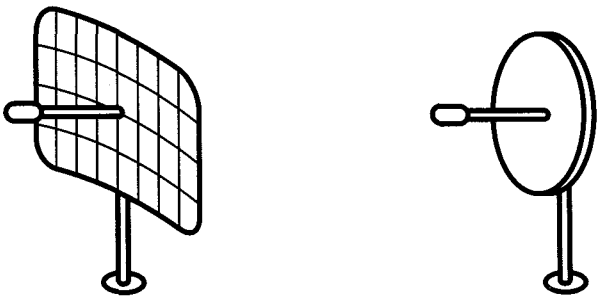

Figura 8.8. Antenas parabólicas.

Antenas dipolo

Aunque las antenas dipolo no son útiles para las redes de largo alcance (porque su ganancia es sólo de unos 2,2 dBi), a menudo se añaden a puntos de acceso para ampliar el alcance en interiores. Muchos puntos de acceso con antenas dipolo externas tienen un par de ellas, que pueden utilizarse para diversidad de señales, con ambas antenas emitiendo y recibiendo combinando el resultado (como la visión estereoscópica) o en un modo en que una antena emite y la otra recibe (vea la figura 8.9).

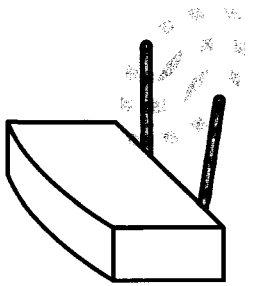

Figura 8.9. Antenas dipolo.

Nota

Las antenas dipolo son en esencia como las antenas de cuernos utilizadas para la recepción de televisión hace años, excepto que las antenas dipolo utilizadas en las redes inalámbricas son mucho más pequeñas. Son más pequeñas porque el estándar 802.11b utiliza frecuencias en la banda de 2,4 GHz (o 2400 MHz) del espectro de radio,

mientras que las de televisión usan frecuencias de la banda de 100 MHz. Al aumentar la frecuencia, disminuye la longitud de onda y, por tanto, el tamaño de las antenas.

La principal utilidad de un punto de acceso con antenas dipolo desmontables (no todos son así) es que es mucho más fácil añadir una antena externa más potente. La vida es más fácil si no hay que taladrar agujeros en el punto de acceso ni que soldar conexiones entre el punto de acceso y la antena externa.

Construir nuestra propia antena

Ningún libro que hable de las redes inalámbricas de largo alcance estará completo sin mencionar esto: sí, podemos construir una antena sin gastar prácticamente nada de dinero. El tipo de antena más popular entre las que uno se puede construir es la de "lata de Pringles", que es una antena yagui.

Truco *Aunque las latas de patatas fritas Pringles han resultado ser populares para hacer antenas, hay gente que ha conseguido mejores resultados con otros tipos de lata. Puede ver una comparación realizada por Greg Rehm en www.turnpoint.net/wireless/cantennahowto.html.*

¿Por qué construir una antena? La diversión es una de las primeras razones de la lista y, aunque las antenas no son caras, construir una antena combinando piezas es más barato que comprarla. Sin embargo, también hay buenas razones para preferir comprarla en lugar de construirla. La antena casera tendrá propiedades aleatorias, puede tener mayor o menor ganancia de la que resultaría ideal para la situación. Si la ganancia es mucho mayor de lo esperado, pueden violarse regulaciones de limitación de potencia. También es probable que emita ondas de radio en direcciones imprevistas o frecuencias ilegales, que pueden provocar problemas para otras personas de las cercanías. Y, naturalmente, decorar la casa con una lata no tendrá la aprobación de una esposa con la misma probabilidad que una antena comercial. Para más información sobre la construcción de antenas, haga una búsqueda en Google o visite la explicación de Rob Flckenger sobre cómo construir una antena yagui con una lata de Pringles en www.oreillynet.com/cs/weblog/view/wlg/448 (figura 8.10).

Nota *Rob es también autor del libro Building Wireless Community Networks, que resultará útil si quiere conectar con sus vecinos para construir una red comunitaria.*

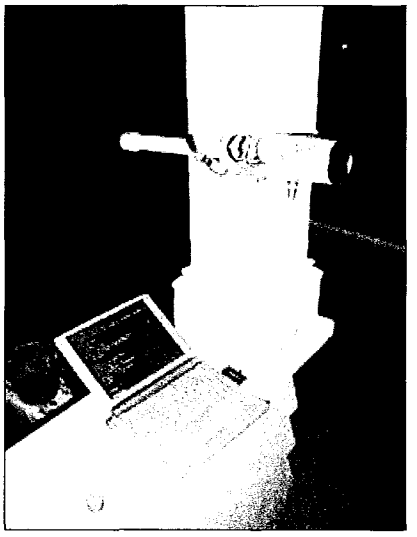

Figura 8.10. La antena con una lata de Pringles de Rob Flickenger.

Cables y conectores de antena

Para aquellos cuya experiencia reside en el mundo de la informática, enfrentarse con los cables de antena es un problema, porque hay poco conocimiento basado en ordenadores que se pueda utilizar. Las conexiones de antena a menudo requieren tipos de cable poco familiares y, en muchos casos, cada cable tiene un conector diferente. Los cables suelen ser gruesos y resulta difícil trabajar con ellos (o en el caso de los cables pigtail, son delgados y frágiles) y la longitud del cable siempre tiene importancia.

Truco

¿Nuestro consejo? No intente construir cables usted mismo a menos que tenga mucha experiencia (o desee dedicar mucho tiempo y muchos cables al aprendizaje) e intente comprar todos los cables de la misma marca. En lugar de hacer un pedido por Internet, llame a la tienda y hable con alguien para comprobar que todas las piezas que quiere son apropiadas y podrán ser conectadas entre sí.

Cables pigtail

Para conectar el punto de acceso o el adaptador de red inalámbrica a una antena externa se necesita un cable pigtail, que es un trozo de cable delgado y

flexible con conectores en los dos extremos (vea la figura 8.11). Los cables pigtail existen por dos razones. Primero, resuelven un problema de tamaño: algunas tarjetas de red inalámbrica tienen una toma de antena muy pequeña (quizá de un cuarto del diámetro de un lápiz normal, por ejemplo), haciendo que sea imposible conectar un cable de antena que es mucho más grueso (de dos veces el grosor de un lápiz). Segundo, pueden doblarse; como los cables de antena suelen ser gruesos y rígidos, la flexibilidad de los cables pigtail facilita la conexión con el grueso cable de antena.

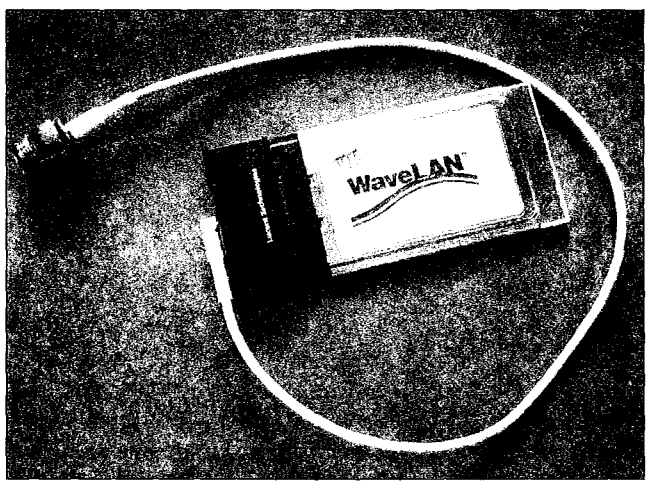

Figura 8.11. *Un cable pigtail.*

A pesar de que los cables pigtail son indispensables, tienen varios atributos molestos. Tienden a ser muy caros, costando entre 20 y 60€ o más. El precio es alto en parte porque el mercado no tiene alternativas, pero también porque un buen cable pigtail utiliza alambres y conectores de alta calidad y se construyen cuidadosamente. Eso es importante porque el cable fino no transmite la señal bien y porque cada conector que se añade a un sistema de antena provoca pérdida de señal. Como el objetivo es siempre evitar la pérdida de señal, merece la pena pagar un poco más por un cable pigtail de buena calidad.

Truco *Para reducir la pérdida de señal, compre un cable pigtail tan corto como parezca razonable para la instalación, generalmente entre 15 y 40 cm.*

El último inconveniente de los cables pigtail es que hay muchos tipos de conector distintos de diferentes fabricantes de equipamiento de red inalámbrica.

El equipamiento Orinoco es distinto del equipamiento Linksys, por ejemplo; hay que tener cuidado para solicitar un cable pigtail compatible con el hardware.

Nota

Esta última dificultad está regulada: la FCC no desea que los usuarios pongan antenas en su propio equipamiento y lo desalienta requiriendo que los fabricantes utilizan conectores únicos no ajustados a un estándar.

Los cables pigtail solían ser difíciles de encontrar y todavía más caros, pero el crecimiento de las redes comunitarias ha hecho que aumentara el interés y, por tanto, la provisión de suministros. Para información adicional sobre los cables pigtail, incluyendo enlaces con vendedores, visite la página Seattle Wireless Pigtails en www.seattlewireless.net/index.cgi/PigTail.

Cable

Aunque los cables delgados utilizados en los pigtail son flexibles y es fácil trabajar con ellos, la pérdida de señal en tales cables es problemática. Como resultado, el cable más largo a desplegar desde la antena debe ser bastante más grueso que el pigtail. Es posible comprar cables de distintos diámetros para las antenas externas, el truco está en determinar la cantidad de dinero que estamos dispuestos a gastarnos en relación con la pérdida de señal. La parte incómoda de este equilibrio es que cuanto más largo deba ser el cable, más preocupante resultará la pérdida de señal y el coste aumenta porque se necesita más cable y el cable debe ser más grueso.

Truco

Tome las medidas de la forma más precisa posible para determinar exactamente cuánto cable necesita antes de solicitar un cable de antena, pues tener un cable más largo de lo necesario provoca que haya más pérdida de señal.

El cable que más se utiliza parece ser el LMR400, donde el 400 indica el diámetro del cable. Proporciona una buena comunicación de bajo precio, poca pérdida de señal y flexibilidad aceptable para facilitar la instalación. La mayoría de los cables de antena, si no todos, están diseñados para ser instalados en el exterior y pueden resistir la luz ultravioleta procedente del sol que atraviesa la cubierta plástica de los cables diseñados para el uso en interior. También se puede comprar un cable de antena que puede ser enterrado directamente en el suelo sin necesidad de poner un conducto protector.

Truco *Igual que con otras partes de un sistema inalámbrico de largo alcance, recomendamos investigar por adelantado qué será necesario para después llamar al vendedor elegido y hacer el pedido. Pregunte al vendedor si las piezas solicitadas sirven para el uso que tiene pensado y si son compatibles entre sí. Otra razón para pedir ayuda es que algunos vendedores tienen sus propios nombres y descripciones de algunas piezas. Por ejemplo, el cable LMR400 puede tener un nombre de marca como Commscope WBC-400; la única forma de asegurarse de que un cable es el que necesitamos es preguntar.*

Igual que con los cables pigtail, encontrar el cable apropiado va siendo más fácil que en el pasado y muchas empresas que venden antenas y cables pigtail también venden cable de antena.

Conectores

Todavía más confusos que los cables pigtail y de antena para los que provienen del mundo de la informática resultan los muchos tipos distintos de conectores que podemos encontrar unidos a los extremos de estos cables. No vamos a comentar todos los tipos posibles de conectores que hay, sino que nos vamos a centrar en los tipos que es más probable que utilice.

Truco *No confíe en la comparación visual entre conectores, pues algunos parecen idénticos cuando en realidad tienen el género o la rosca invertidos. Verifique siempre que los cables que compra tienen conectores que son compatibles uno con otro.*

- Los conectores N son grandes conectores con rosca utilizados comúnmente para conectar el cable de antena (especialmente el cable LMR400 o mayor) con antenas y pigtails. Tienen una pérdida de señal bastante baja y crean conexiones muy seguras, pero simplemente son demasiado grandes para utilizarlos con tipos de cable más pequeños.
- Los conectores TNC son similares a los BNC utilizados en los cables Ethernet 10Base2 (vea el capítulo 2 en el que comentamos 10Base2 y lo conectores BNC), pero añadiendo una rosca para que las conexiones sean más seguras. La pérdida de señal es aceptable, aunque mayor que en los conectores N. También son más pequeños que los conectores N.

- Los SMA son conectores pequeños a rosca y se suelen usar para cables más pequeños que los LMR400. Otras variantes son los SMB, que es un tipo de conector a presión, en lugar de a rosca, y SMC, que son todavía más pequeños.

Visite http://nocat.net/connectors.html para más información sobre estos conectores y otros.

Nota *Los conectores N y BNC en los que se basan los conectores TNC se diseñaron durante la Segunda Guerra Mundial para aplicaciones militares.*

Instalación de antena

Cuando llegue la hora de instalar la antena, probablemente no haya tantas opciones, porque hay muchas limitaciones.

Línea de visión

La limitación más importante en la instalación de antena es que debe haber una línea de visión sin obstáculos hasta la antena remota. Aunque las radios utilizadas en las redes inalámbricas son bastante sensibles, casi cualquier obstáculo bloqueará la señal, incluyendo las hojas de los árboles.

Truco *Si está preparando una conexión inalámbrica de largo alcance en invierno o primavera antes que broten las hojas de los árboles, tenga esto en cuenta o la conexión resultará estacional.*

En algunos casos, como en el de Adam, puede resultar fácil determinar la línea de visión porque la torre de la antena remota puede ser visible a simple vista (la antena del ISP de Adam está montada en la torre de radio WVBR, que es fácil de ver). Si no puede ver la antena remota, pruebe a utilizar unos prismáticos o un telescopio.

Nota *Las ondas de radio de la banda de 2,4 GHz del espectro no están enfocadas como un haz láser. De hecho, se dispersan y ocupan un área elíptica en las dos direcciones de la línea de visión. Esta área se llama zona de Fresnel y en realidad se necesita una línea sin*

obstáculos también en la zona de Fresnel, de modo que los árboles que no obstaculizan la línea visual pueden todavía interferir con la conexión inalámbrica (vea la figura 8.12). Utilice la calculadora de http://gbppr.dyndns.org/fresnel.main.cgi para ver el margen de flexibilidad que necesita la línea de visión de radio.

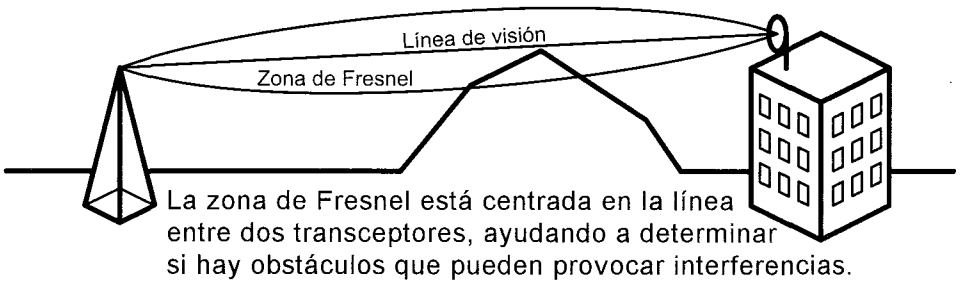

Figura 8.12. *La zona de Fresnel.*

Si simplemente no puede encontrar la antena remota visualmente, quizá todavía pueda crear una conexión de red inalámbrica, pero es casi seguro que necesitará una antena de alta ganancia. La única forma de saberlo seguro es hacer la prueba. Siga adelante algunas páginas para encontrar más información sobre cómo probar una conexión.

En general, la elevación ayuda a conseguir una línea de visión de radio. Intente, pues, encontrar una ubicación para la antena que esté más elevada. Siendo realistas, una antena termina montada en el tejado o incluso en un mástil que la eleva por encima del tejado del edificio.

Despliegue de cable frente a facilidad de acceso

Como ya sabe, queremos minimizar la longitud del cable desplegado para evitar la pérdida de fuerza de la señal. Ese deseo ha provocado que la gente haya intentado averiguar cómo colocar un punto de acceso justo al lado de la antena. La dificultad aquí consiste en construir un receptáculo a prueba de agua (pruebe los receptáculos que se utilizan para los controles de aspersores que puede encontrar en tiendas de utensilios de jardinería), conectar el punto de acceso al resto de la red con un cable Ethernet (o un puente inalámbrico) y proporcionar corriente al punto de acceso, quizá con un dispositivo PoE (Potencia a través de Ethernet, también conocido como Ethernet Activa).

Nota

Potencia a través de Ethernet funciona transportando voltajes bajos por pares no usados del cable Ethernet estándar. Se necesita un "inyector" que introduce el voltaje DC en los hilos no utilizados del cable y, a menos que el punto de acceso sea compatible con PoE, se necesita también otro aparato para sacar la electricidad del cable y dársela al punto de acceso. Para más información, vea www.hyperlinktech.com/web/what_is_poe.html.

Truco

La mayoría de los cables Ethernet estándar no están preparados para el uso en exteriores y se romperán debido a la luz ultravioleta. El cable para exteriores puede ser difícil de encontrar, pero si piensa desplegar cable Ethernet fuera de la casa, llame a tiendas de suministros de electricidad y pregunte si tienen cable Ethernet preparado para el uso en exteriores o incluso para ser enterrado directamente.

Algunos grupos de redes inalámbricas comunitarias han renunciado a intentar reducir la longitud del cable de antena a toda costa. Resulta que poner el punto de acceso en un receptáculo a prueba de agua en el tejado hace que sea más difícil acceder a él en caso de que haya un problema (por ejemplo, si hay que reiniciarlo por algún motivo) y nadie quiere trepar por una escalera todos los días para reestablecer el punto de acceso.

Aviso

¡Tenga cuidado si sube al tejado! Es muy fácil resbalarse y caer y la altura puede ser considerable. Nuestro colega Rob Flickenger sufrió una caída a principios de 2002 y su comentario a Glenn en una convención hace poco fue: "Hay una razón para que la gente tenga dos riñones". Rob se recuperó y ahora es un acérrimo defensor de la seguridad. "Alguien que te vigile, sentido común y arneses", dice.

Nuestro consejo es que intente utilizar un cable de antena lo más corto posible pero colocando el punto de acceso en una ubicación en el interior razonable.

Durabilidad

Lo último a tener en cuenta al instalar la antena es si va a estar expuesta a las inclemencias del tiempo día sí y día también. Sol, viento, lluvia, nieve, hielo, niebla, plagas de langostas... queremos que la antena resista todo lo que la naturaleza pueda enviarle. Al decir "resista" nos referimos a que no se mue-

va o deje de funcionar. Si un viento fuerte hace girar una antena panel o una tormenta de hielo cubre una antena yagui, el acceso a Internet puede dejar de funcionar. Ya hemos comentado cómo responden los distintos tipos de antena al viento; si en su zona hay vientos fuertes frecuentemente, compruebe la resistencia al viento al comprar la antena. Igualmente, cuando la instale, móntela de la forma más segura posible. Si la monta sobre un mástil redondo, compruebe que puede girar sobre el mástil; es mejor que la antena gire si hay viento que caiga completamente.

También preste atención al cable y los conectores. La mayoría de los cables de antena están diseñados para el uso en exteriores y los conectores con rosca proporcionan conexiones más seguras que los conectores a presión. Los conectores con rosca pueden ser bastante resistentes al agua, pero sigue siendo buena idea cubrirlos con cinta impermeable, pues el agua tiene la mala costumbre de filtrarse en las conexiones, incluso en las más seguras. Si el establecimiento en que compra el equipamiento de antena no dispone de cinta aislante impermeable, puede encontrarla en Radio Shack (www.radioshack.com). Si es posible, compruebe que la cinta también resiste la radiación ultravioleta.

Truco *Varias compañías venden receptáculos resistentes como los que utilizan las compañías de teléfono para la caja de conexiones en el exterior de las casas. Se pueden utilizar estas cajas para instalar equipamiento de red inalámbrica en el exterior. Naturalmente, los aparatos electrónicos generan calor y el calor en una caja cerrada, especialmente en días calurosos, puede provocar fallos en el hardware.*

Si piensa instalar la antena en el tejado del edificio, compruebe que todo queda bien sujeto. En muchos casos, puede no haber un lugar evidente en el que montar soportes o es posible que no le den permiso para hacer tales modificaciones. Si el tejado es plano, piense en construir un armazón de madera (vea la figura 8.13).

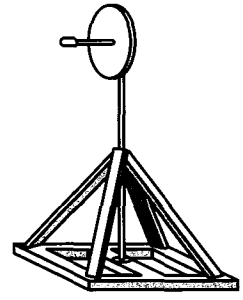

Figura 8.13. *Diseño de armazón para antena.*

Si sujeta bien con bloques de cemento o sacos de arena, el armazón sujetará la antena (pero tenga cuidado de no dañar la superficie del tejado).

Hacer conexiones inalámbricas a larga distancia

Hemos hablado de antenas, cables, pigtails y conectores, pero ¿a qué hay que enchufar el pigtail? Si conectamos con un WISP o extendemos la red existente, el dispositivo inalámbrico debe actuar como cliente; esto es, como un ordenador normal con capacidad inalámbrica que conecta con un punto de acceso. De hecho, si queremos conectar un solo ordenador a un WISP, podemos instalar un adaptador de red inalámbrica que tenga una toma de antena y conectarlo con el cable pigtail. Más difícil es conectar a una conexión inalámbrica de largo alcance toda una red; para ello tenemos dos opciones:

- *Conectar un adaptador de red inalámbrica a un ordenador, conectar la antena (con el cable pigtail) al adaptador de red inalámbrica y ejecutar en el ordenador el software que le convierte en una puerta de enlace. En Windows XP, podemos usar su capacidad integrada para compartir una conexión de Internet, como hemos visto en el capítulo 5. En Mac OS X puede probar la utilidad de shareware BrickHouse de Brian Hill que cuesta 25$ (vea http://personalpages.tds.net/~brian_hill/brickhouse.html) para configurar la función integrada de Mac OS X Compartir Internet. En Mac OS 9, pruebe el IPNetRouter de 89$ de Sustainable softworks (www.sustworks.com/site/prod_ipr_overview.html). Después tendrá que conectar el ordenador a un concentrador Ethernet utilizando una red Ethernet de cable convencional. Y si quiere proporcionar también acceso de red inalámbrico interno, en lugar de un concentrador normal, utilice una puerta de enlace inalámbrica que integre un punto de acceso y un concentrador Ethernet. El inconveniente de esta estrategia es que la conexión sólo está activa cuando el ordenador está encendido y funcionando, de modo que es una tarea que gestionará mejor un ordenador que no utilice nadie para el trabajo normal (los ordenadores viejos, especialmente los portátiles que ahorran energía y no ocupan espacio, a menudo funcionan bien en esta situación).*
- *Usar un puente inalámbrico Ethernet como el Linksys WET11 (www.linksys.com/Products/product.asp?grid=22&prid=432) o*

el airBridge de smartBridges (www.smartbridges.com/products/wireless/airbridge.php); ambos aceptan antenas externas y pueden hacer de puente entre una conexión inalámbrica de largo alcance y una red Ethernet convencional (encontrará detalles en el capítulo 5). De nuevo, si desea proporcionar acceso de red inalámbrica interno, debe conectar también el puente Ethernet inalámbrico a la puerta de enlace inalámbrica. (Sólo porque una puerta de enlace inalámbrica diga que puede hacer de puente entre redes convencionales e inalámbricas no significa que pueda hacer de puente con una conexión inalámbrica de largo alcance. Eso es porque la mayoría de las puertas de enlace inalámbricas pueden ejecutar sus radios inalámbricas sólo como puntos de acceso, actuando como un concentrador para una red inalámbrica, más que como cliente que se conecta a otro punto de acceso.)

En cualquier caso, probablemente querrá usar NAT y DHCP para proporcionar direcciones IP privadas a los ordenadores. En el capítulo 5 encontrará más información.

Conectar a Internet

La información que hemos mostrado hasta ahora en este capítulo proporciona lo básico que hay que saber para establecer una red inalámbrica de largo alcance. Ahora nos vamos a centrar en una de las dos principales razones para crear tal red: establecer una conexión inalámbrica a Internet de largo alcance.

Encontrar un WISP

El primer paso para configurar una conexión inalámbrica a Internet de largo alcance es determinar si hay un ISP inalámbrico (WISP) que preste servicio a la zona. Como el acceso inalámbrico a Internet es todavía un servicio poco usual, no siempre es fácil encontrarlo, ni siquiera cuando está disponible.

El recurso más útil es ver el directorio de WISP mantenido por Broadband Wireless Exchange Magazine en www.bbwexchange.com/wisps/. Incluye cientos de WISP de todo el mundo, aunque no es un listado exhaustivo, en parte porque Broadband Wireless Exchange Magazine cobra 250$ al año a los WISP por ser incluidos en sus listas.

Si la búsqueda en el directorio de Broadband Wireless Exchange Magazine no produce resultados, mire en la más barata lista de Open Directory Project en http://dmoz.org/Business/Telecommunications/Wireless/Service_Providers/Internet/Fixed_Broadband/. La última opción en línea es una búsqueda en Google, aunque parece difícil encontrar términos de búsqueda que funcionen de forma fiable. Empiece buscando algo como "wireless Internet access *ciudad*" (reemplazando ciudad por el nombre de su ciudad") o y añada otros términos como "802.11b" y "WISP" si es necesario. Si en su zona hay grupos de noticias o listas de correos Usenet, pruebe a preguntar también ahí.

Hemos visto que hay interés por promover asociaciones de WISP en varios grupos comerciales, pero parece que no se ha establecido ninguna asociación todavía. Merece la pena comprobar si algún grupo se ha consolidado después de la escritura de este libro, pues proporcionarán listas de los miembros en distintas zonas.

Aunque resulta difícil recordarlo en la era actual de Internet, a veces la mejor estrategia es utilizar métodos tradicionales para encontrar empresas. Compruebe las páginas amarillas, pregunte a amigos que sepan de Internet y llame a los ISP normales para preguntar si saben de alguien que ofrezca acceso inalámbrico a Internet en su zona. La mayoría de los ISP conocen a las otras compañías de acceso a Internet y nuestra experiencia dice que no se sienten molestos por dirigir a los clientes que no pueden atender hacia otras empresas.

Truco

Si la búsqueda de WISP no produce resultados y no tiene otras alternativas para conseguir acceso a Internet de alta velocidad, puede intentar convencer a alguien que sí disponga de acceso a Internet de alta velocidad para que mantenga el lado remoto de una conexión inalámbrica a Internet de largo alcance. Lea la sección posterior "Extender la red" para información sobre cómo establecer tal conexión.

Truco

Si tiene vistas del cielo sur, el acceso a Internet basado en satélites de StarBand Communications (www.starband.com) es otra posibilidad.

Comprobar el sitio

Una vez encontrado un WISP y determinado que es concebible que haya una línea de visión para acceder a la antena del WISP, el siguiente paso es

pedir al WISP que haga una comprobación de sitio. Los WISP pueden cobrar por las comprobaciones de sitio, pues tales comprobaciones implican llevar una antena de alta ganancia montada en un trípode a la ubicación solicitada, conectarla a un portátil y probar si la fuerza de la señal es suficiente. También pueden tener equipos especializados, como aparatos GPS y telescopios, que pueden ayudar a determinar exactamente dónde se encuentra la antena remota para dirigir de forma óptima la antena.

La comprobación de sitio debe llevarse a cabo aunque no sea posible ver la antena remota, pues puede ayudar a determinar qué tipo de antena será necesaria. Si la fuerza de la señal es buena, con una antena pequeña menos molesta puede ser suficiente, mientras que si la comprobación de sitio muestra que está en el límite de poder recibir la señal, necesitará una gran antena parabólica de alta ganancia.

Truco *Compre una antena con mayor ganancia de la que parezca necesaria; la fuerza de señal extra siempre será bienvenida, especialmente porque las condiciones climáticas pueden afectar a la pérdida de señal. No hay manera de saber lo representativas que serán las condiciones climáticas el día de la comprobación de sitio, de modo que es mejor dejar un margen de error.*

Direcciones IP

Una vez establecida la conexión inalámbrica, conectar el ordenador o red a un WISP no es distinto de hacerlo a cualquier otro proveedor de servicios de Internet en términos del resultado: se proporciona conectividad a una o más direcciones IP (estáticas o dinámicas) de la red local.

- Los ISP normalmente pasan en la actualidad direcciones IP dinámicas porque así su servidor DHCP puede controlar quién está en línea en un momento dado y distribuir direcciones IP del bloque de direcciones disponibles del ISP. La asignación dinámica de direcciones es más fácil de gestionar para los ISP y a muchos usuarios no les importa en absoluto porque no necesitan (ni quieren) que sus ordenadores estén disponibles para la conexión directa desde Internet. Si no desea ejecutar servidores de Internet, la asignación dinámica de direcciones está bien.

  Si no puede evitar la asignación dinámica de direcciones, pero desea ejecutar servidores, mire en DNS dinámico, que permite a alguien de

Internet conectar con www.ejemplo.com, pongamos por caso, y conseguir que se asigne a ese dominio la dirección IP dinámica que tenga el ordenador en ese momento. Vea el capítulo 5 para más información sobre DNS dinámico.

- Con una dirección estática, se recibe una dirección IP permanente que siempre corresponde al puente Ethernet inalámbrico o al ordenador que actúa como puente. Eso es ideal para ejecutar servidores, pues los servidores están siempre disponibles en la misma dirección IP (que a su vez puede ser asignada a un nombre de dominio). Si desea una dirección IP estática, puede pedirla al WISP. Quizá tenga un coste algo mayor.
- Si desea varias direcciones IP estáticas, el servicio seguramente costará más, necesitará un enrutador (aunque algunas puertas de enlace baratas también pueden actuar como enrutadores) y el WISP debe ayudarle a configurarlo todo.

Ampliar la red

Cuando configuramos una conexión inalámbrica a Internet de largo alcance, tenemos una gran ventaja: los técnicos del WISP probablemente sabrán mejor que nosotros qué hay que hacer y seguro que están deseando ayudar. Eso no es cierto si lo que queremos es ampliar la red hasta una ubicación remota, en cuyo caso todo el trabajo recae sobre nuestros hombros. Pero eso no significa que sea una sola persona la que se encargue de todo, de hecho es casi imposible ampliar una red utilizando una conexión de largo alcance sin ayuda.

La mayoría de lo que necesita saber con respecto a la ampliación de redes aparece al determinar dónde colocar las antenas en ambos lados de la conexión, pues ya hemos comentado todo lo demás.

Determinar la ubicación de la antena

Si queremos conectar dos edificios en un parque empresarial, por ejemplo, determinar la línea de visión y dónde colocar las antenas en los dos extremos de la conexión probablemente resulte bastante fácil.

La tarea se vuelve más difícil según aumenta la distancia o si simplemente determinamos que no hay modo de conseguir una línea de visión sin una antena intermedia.

Largas distancias

Al intentar establecer los dos extremos de la línea de visión de una conexión a través de una gran distancia, empiece por estudiar mapas topográficos detallados (vea la figura 8.14).

Los mapas en papel de buena calidad probablemente resulten más manejables, pero quizá encuentre los detalles necesarios en un sitio Web como TopoZone.com en www.topozone.com.

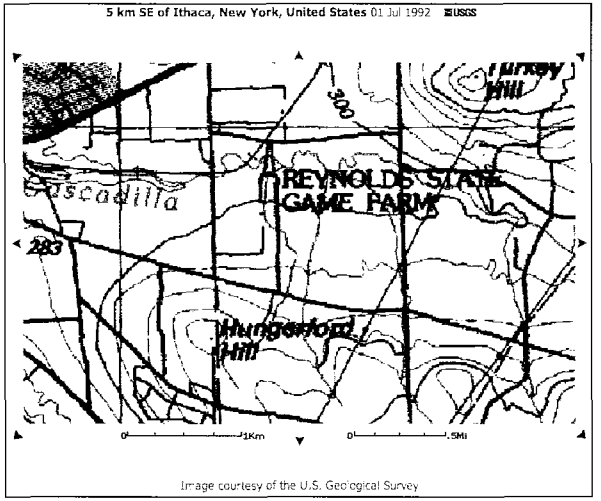

Figura 8.14. *Un mapa topográfico del área que rodea la casa de Adam.*

Pero los mapas topográficos tampoco nos llevan demasiado lejos, pues muestran sólo la elevación del suelo, mientras que también nos interesan los objetos que hay por encima del suelo, como árboles o edificios. Una vez identificadas las posibles áreas en que colocar las antenas en el mapa, es el momento de utilizar los prismáticos o, mejor, un telescopio.

Aquí es donde es indispensable que alguien nos ayude, preferiblemente con un teléfono móvil para poder retransmitir la posición de cada antena si es necesario.

Piense en comprar globos de helio baratos y atarlos con una cuerda muy fina para poder dejar flotar el globo y que la otra persona pueda encontrarlo con el telescopio; una vez lo haya encontrado, tire de él hacia abajo para señalar su posición. Una vez identificado un punto que tenga buenas perspectivas de ser válido, márquelo con algo como un trozo de plástico de color que sea fácilmente visible desde lejos para poder utilizarlo como guía mientras monta la antena.

Truco

Preste atención a los obstáculos que estén cerca del camino, pues el efecto Fresnel puede provocar problemas aunque la línea de visión esté libre.

Una vez identificadas las ubicaciones de las antenas, es el momento de probar con verdaderas antenas. Resuelva los cálculos mostrados anteriormente en el capítulo para determinar qué tipo de antenas es probable que necesite, pues a menos que pueda tomar prestadas antenas de un WISP o de alguien que tenga antenas sin montar, es probable que tenga que comprar las antenas que piense que va a necesitar. Adelante, instale las antenas, pero comprobando que puede ajustar sus posiciones si es necesario.

Sea su propio WISP

Supongamos por un momento que vive en el quinto pino, pero no excesivamente lejos de donde la compañía de teléfonos deja de proporcionar acceso a Internet basado en DSL. Quiere acceso a Internet de alta velocidad, pero no tiene una buena visibilidad del cielo sur para usar StarBand, aunque sí puede ver algunos tejados de los vecinos. ¿Por qué no pagar a un vecino para que ponga una conexión a Internet y utilizar una conexión inalámbrica de largo alcance para llevar la conexión hasta su casa?

No hay razones técnicas que impidan hacer eso, pero se requiere una buena planificación y ser un buen relaciones públicas, pues hay que determinar por adelantado qué vecinos se encuentran en un lugar en el que se puede conseguir la conexión DSL que al mismo tiempo esté en la línea de visión para la conexión inalámbrica. Hay que utilizar con pericia los prismáticos y el telescopio, investigar la compañía telefónica local y ser persuasivo con el vecino identificado. No es inusual toparse algunas veces con personas poco comprensivas. Intente buscar a alguien que no es probable que vaya a mudarse, no es fácil que nadie quiera explicar la situación a posibles compradores de la casa y un nuevo vecino podría acabar con la conexión inesperadamente.

Hay algunos inconvenientes en esta estrategia. Además de cargar con el coste mensual de la conexión a Internet, hay que comprar dos antenas, dos puentes Ethernet inalámbricos y probablemente una puerta de enlace para que la persona que hospeda la conexión de Internet pueda compartirla. (Evidentemente, si puede encontrar una persona o negocio que ya tenga una conexión a Internet de alta velocidad y quie-

ra compartirla, el coste baja bastante.) También es probable que resulte necesario proporcionar soporte técnico al huésped de Internet y se crea una situación en que depende de alguien más para la conectividad con Internet, incluyendo la resolución de problemas si algo va mal. Hablando en plata, es verdaderamente una buena idea, pero no resulta barata y puede implicarle en la vida de otro más de lo que le gustaría. Por otra parte, si la cosa funciona, puede ser un primer paso para construir su propia comunidad de red inalámbrica.

Si le preocupa comprar más equipamiento en este punto, el método más barato para realizar pruebas probablemente es usar un par de portátiles con adaptadores de red inalámbrica PC Card y cables pigtail que conecten con las antenas. (Tal vez tenga que comprar un cable pigtail extra, pero si la conexión simplemente no funciona, no habrá hecho falta comprar los puentes Ethernet inalámbricos.) Configure una sencilla red ad hoc y vea si un portátil puede conectar con la red del otro. De nuevo, tener a alguien con un teléfono móvil es esencial para recibir informes de la fuerza de la señal y ajustar la posición de las antenas.

Por otro lado, si no le preocupa el coste, compre los puentes Ethernet inalámbricos que necesite en los dos extremos de la conexión inalámbrica de largo alcance. Instale y configure uno de ellos, después utilice un portátil en la otra ubicación para verificar que las antenas pueden recibir las señales de cada extremo.

Una vez verificado que todo funciona, asegure las antenas, confirme que todo sigue funcionando y despliegue los cables necesarios para unir las dos redes.

Red de dos saltos

¿Hay que abandonar toda esperanza si el mapa topográfico muestra que no hay modo de encontrar una línea de visión entre dos ubicaciones? Todo depende de lo indispensable que resulte la conexión inalámbrica de largo alcance. Para resolver el problema, se podría intentar construir una conexión de dos saltos con un par de antenas en el centro.

El proceso de determinar las ubicaciones de las antenas en una conexión de dos saltos es aproximadamente el mismo que en una conexión de largo alcance normal, pero con la dificultad añadida de encontrar una posición visible desde los dos extremos. Los mapas topográficos son indispensables en esta tarea, y también varios ayudantes con teléfonos móviles, globos y telescopios.

Tenga en cuenta que la ubicación intermedia debe disponer al menos de energía y, si es posible, algún tipo de sitio cerrado en el que poner un par de puentes Ethernet inalámbricos (uno para cada antena intermedia).

Sin rodeos, crear una red de dos saltos no es imposible ni mucho menos, pero es difícil, caro y lleva tiempo. Si la alternativa es una conexión digital de alta velocidad de una compañía telefónica que cuesta miles de euros al mes, el esfuerzo de establecer una red de dos saltos puede merecer la pena, pero quizá también merezca la pena encontrar y contratar profesionales que se ocupen del trabajo.

Cuando las cosas van mal

Con la información de este capítulo, tiene todo lo necesario para poner en marcha su propia conexión de largo alcance. Ciertamente es más complicado que construir una red inalámbrica normal de corto alcance, pero también es más divertido y hemos intentado proporcionar trucos y consejos para los aspectos de las redes inalámbricas específicos de las conexiones de largo alcance. Las redes de corto alcance pueden ser más fáciles, pero tienen sus propios problemas, de modo que en el próximo capítulo vamos a ver los problemas generales que puede encontrar en redes inalámbricas y a ofrecer varios trucos para aislar y resolver problemas comunes.

9. Las cosas pueden chocar en la red

No tiene sentido fingir que no aparecen problemas. La vida puede ser vista como una combinación de problemas y soluciones. Lo que siempre nos ha sorprendido es que tanta gente con poca experiencia técnica asuma que será imposible para ellos resolver problemas de los ordenadores. Aunque el conocimiento especializado evidentemente ayuda, resolver problemas es una habilidad universal. Si podemos averiguar por qué las bisagras chirrían o la máquina de coser se atasca, también podremos solucionar problemas relacionados con los ordenadores. A pesar de lo que mucha gente piensa, no hay verdadera diferencia. Para aquellas personas que se sienten intimidadas ante la perspectiva de averiguar cuál es el problema y cómo solucionarlo, mostramos aquí una guía que le ayudará a resolver problemas de todos los tipos. Después, pasaremos a ver problemas y soluciones específicos de las redes inalámbricas. No pretendemos decir que nosotros podemos resolver todos los problemas, pero nuestros ordenadores y redes funcionan bien la mayor parte del tiempo.

Cómo resolver problemas

La mayoría de la gente no tiene dificultad para notar que algo va mal. Pero percibimos (y el experto en facilidad de uso Don Norman lo dice a menudo)

que los nuevos usuarios suponen que son ellos los que están haciendo algo incorrectamente en lugar de ser un fallo relacionado con los ordenadores que puede (y debe) ser eliminado. Si se descubre a sí mismo efectuando rutinariamente los mismos pasos para sortear un problema, recomendamos que dedique algunos minutos a estudiar las guías que mostramos aquí para ver si puede solucionar el problema y simplificar su vida.

Nota *A veces, los pasos complejos para sortear un problema reflejan fallos de un programa o el sistema operativo. Determinar si es un error de programación, un malentendido o algo que falta es la clave para resolver el problema.*

El consejo más importante que podemos dar en esta sección es: sea metódico. Si empieza a probar soluciones en un problema sin reflexionar sobre la causa del problema y el efecto que puede tener la solución, terminará complicando toda la situación. La mejor forma de fomentar la estrategia metódica es preparar un cuaderno de notas e ir apuntando todo lo que vemos (especialmente los mensajes de error), lo que hacemos y los efectos que tiene lo que hacemos. No hace falta ser obsesivos con las notas, pero compruebe que al menos describe el orden de los sucesos, por si posteriormente tiene que volver atrás.

Describir el problema

El primer paso es identificar el problema y reunir información sobre él. Eso parece fácil y normalmente lo es, pues la mayoría de los problemas no son especialmente sutiles. Quizá no pueda enviar correo electrónico o uno de los ordenadores de la red convencional no sea visible para los ordenadores de la red inalámbrica.

Es importante determinar si el problema se reproduce continuamente o es intermitente. Aunque un problema intermitente puede resultar menos molesto que uno que se reproduce continuamente, como pueden permitir que continúe el trabajo, los problemas intermitentes son mucho más difíciles de controlar, pues una de las variables tiene que ver con un hecho relacionado con el tiempo o el estado del sistema. Los problemas continuos exigen su resolución, pues no se puede continuar trabajando hasta haber resuelto el problema.

También hay que prestar atención a cualquier indicador visible que pueda proporcionar información acerca del problema. Por ejemplo, la mayoría de los adaptadores de red tienen LED que se mantienen encendidos si el adaptador

está funcionando y pasan a estar intermitentes cuando fluye el tráfico. Si esos LED no funcionan de la forma esperada, es un dato importante que hay que añadir a la descripción.

Por último, hay que vigilar los mensajes de error cuando algo falla, o incluso el hecho de que no aparezcan mensajes de error. Apunte los mensajes exactamente según aparezcan o tome capturas de pantalla, pues cada dígito o letra en un número de error puede ser importante.

Desarmar el sistema

Una vez bien agarrado el problema a resolver, hay que empezar a desarmar el sistema relacionado con el problema en pasos o piezas discretas. Después puede empezar a analizar las distintas partes del todo. Lo más difícil aquí es saber cuáles son las distintas partes del sistema, que dificulta entender cuál puede ser la que falla. Pongamos por caso el ejemplo de una red inalámbrica que también tiene conectado un ordenador con un cable Ethernet. En esta red, el ordenador con cable se utiliza como servidor de archivos informal. Estamos utilizando uno de los ordenadores inalámbricos y de repente no es posible conectar con una carpeta compartida. ¿Cuáles son las variables implicadas aquí? Determinemos lo que debe cumplirse para que la situación funcione correctamente; después podemos empezar a probar cada uno de los componentes. Esto es lo que debe cumplirse:

- En nuestro ordenador, necesitamos tener correctamente instalado un software cliente para compartir archivos.
- El ordenador debe tener en funcionamiento una conexión con el punto de acceso.
- El punto de acceso debe permitir ver un ordenador conectado a través de Ethernet de cable.
- El ordenador conectado con Ethernet debe tener en funcionamiento una conexión con el punto de acceso.
- El software de servidor de archivos compartidos debe estar en ejecución en el ordenador conectado con cable Ethernet.
- Debe haber una carpeta compartida explícitamente en el ordenador conectado con cable Ethernet.

Ciertamente, estas piezas podrían dividirse en otras más pequeñas, pero con esto debe ser suficiente para empezar.

Tenga en cuenta que lo que acabamos de describir es sólo un sistema en funcionamiento, que es importante, porque si hay otros sistemas en funcionamiento (otros ordenadores inalámbricos que pueden ver el servidor de archivos) eso nos ayudará a enfocar el problema rápidamente.

Apunte brevemente todas estas variables en el cuaderno de notas y, si le gusta dibujar, cree un diagrama de cómo se unen las piezas; los diagramas pueden resultar útiles si al final hay que separar de verdad las piezas del sistema desconectando cables o reordenando el equipamiento.

Hágase preguntas

Ahora que ya están identificadas todas las partes del sistema, es el momento de estudiar cuidadosamente cada parte, imaginando una posible razón para que un fallo en ese punto pueda ser el responsable de todo el problema. Tomemos en nuestro ejemplo cada variable y analicémosla, planteándonos preguntas:

- El software cliente de archivos compartidos es necesario, por supuesto, pero como antes hemos podido conectar, podemos suponer que está bien instalado. ¿Está activado? ¿Ha cambiado algo desde la última conexión con éxito que pueda proporcionar una pista? ¿Se ha reiniciado el sistema? (Siempre merece la pena intentarlo.) ¿Qué hay de los otros ordenadores? ¿Puede su software cliente de archivos compartidos ver el ordenador conectado con cable?
- ¿Funciona la conexión con el punto de acceso? ¿Funciona para otras tareas de red al mismo tiempo que no funciona la conexión con el ordenador de cable?
- ¿Está el punto de acceso configurado correctamente de modo que los ordenadores inalámbricos puedan ver el ordenador de cable? Dado que antes funcionó bien, es probable que ésta no sea la fuente del problema. ¿Ha cambiado algo en el punto de acceso desde la última conexión que pudiera estar relacionado?
- ¿Puede el ordenador de cable conectar con el punto de acceso a través de Ethernet? Nunca subestime los problemas que un cable roto, suelto o mal conectado pueda provocar.
- ¿Está activada y bien configurada la opción de compartir archivos en el ordenador de cable? ¿Ha cambiado algo en ese ordenador que pueda haber provocado que se desactive o reconfigure la opción de compartir archivos? ¿Se ha reiniciado recientemente el ordenador de cable?

- ¿Sigue compartida la carpeta en cuestión? ¿Puede haber cambiado alguien cuáles son las carpetas compartidas? ¿Se ha movido la carpeta o ha cambiado de nombre o ha sido modificado de alguna manera que pueda haber modificado su estado?

Hemos mencionado la diferencia entre los problemas intermitentes y continuos; si hay un problema intermitente al conectar con el ordenador con cable Ethernet, eso genera preguntas adicionales.

- ¿Sucede el problema en todas las horas del día? ¿Aparece justo después de haber hecho alguna otra cosa? ¿Está relacionado el problema con la presencia o ausencia de cualquier otro ordenador en la red?

Apunte estas preguntas en el cuaderno de notas, numerándolas para poder volver a ellas fácilmente cuando empiece a responder las cuestiones haciendo pruebas.

Responder preguntas

Una vez enumeradas las preguntas, vuelva a ellas y reflexione sobre qué pruebas debe llevar a cabo para obtener una respuesta a cada cuestión. Separe las cuestiones por categorías: fácil, moderada y difícil (puede escribir en el margen al lado del número de cada cuestión la letra F, M o D correspondiente).

También dé una oportunidad a la intuición. Si tiene la persistente impresión de que su esposa puede haber dejado a su sobrino de 4 años jugar en el ordenador de cable Ethernet, empiece por esa máquina. O, si acaba de restablecer en el punto de acceso los ajustes predeterminados de fábrica por alguna otra razón, empiece por él.

Empiece por donde empiece, comience por hacer pruebas que eliminen primero las cuestiones más fáciles. Por ejemplo, es trivial comprobar si el sobrinito desconectó el cable de Ethernet al pisarlo sin darse cuenta; no hay razón para empezar a pensar en reinstalar todo el sistema operativo de la máquina hasta haber agotado las opciones más sencillas.

Nota

Glenn ha sufrido lo de reinstalar el sistema sin necesidad: como comentaremos más adelante en el capítulo, hace poco reinstaló Windows XP Profesional antes de saber que sólo necesitaba restablecer un oscuro servicio del sistema.

Trabajar metódicamente es esencial en este punto y, si cambia algo de un modo que se modifican significativamente las variables, es mejor (si es posi-

ble) devolver el sistema a la misma situación en que se encontraba al analizar el problema. Por ejemplo, si había estado pensando en instalar un nuevo punto de acceso que acaba de comprar, no lo haga durante el proceso de resolver un problema o corre el riesgo de que todo sea más confuso.

Compruebe que anota las preguntas solucionadas en el cuaderno e incluya cualquier cosa interesante que haya sucedido al llevar a cabo una prueba. No le decimos que haga esto porque vaya a olvidar lo hecho durante la resolución del problema, sino porque le será útil si el problema vuelve a aparecer. Además, si termina necesitando pedir ayuda a alguien, tendrá una prueba de que ya ha intentado una comprobación determinada con resultados negativos.

En la mayoría de las situaciones, la solución al problema aparecerá durante este proceso de contestar preguntas. Quizá sea verano y al poner una persiana se haya bloqueado la señal de la red inalámbrica, o tal vez su esposa haya reconfigurado el ordenador de una forma especial para que el sobrino pueda jugar. Es posible que el punto de acceso haya perdido los ajustes que hacen de puente para el paso de la red convencional a la inalámbrica o tal vez sólo sea necesario reiniciar el ordenador.

Conseguir ayuda de expertos

¿Y si después de todos estos pasos, el problema sigue sin solucionarse? Que no consigamos resolver un problema nosotros mismos no es razón para rendirse, pues normalmente no entendemos el sistema lo bastante bien para dividirlo en las piezas apropiadas. O es posible que no se nos hayan ocurrido las pruebas necesarias. Por ejemplo, siguiendo con nuestro caso, si no hubiéramos dado cuenta que todo el tráfico tenía que pasar a través del punto de acceso y un restablecimiento de los ajustes de fábrica (quizá provocado por una subida de voltaje a causa de la caída de un rayo) había desactivado el puente Ethernet de cable-Ethernet inalámbrica, sería fácil probar todo lo demás sin caer en la cuenta de dónde estaba el problema.

Aquí es donde entran los expertos. A veces pueden haber resuelto tantos problemas que saben automáticamente la solución simplemente oyendo una descripción. Pero es más frecuente que dividan el problema en más partes, una de las cuales proporciona la solución.

En esto es cuando los problemas intermitentes pueden volvernos locos. Aunque un experto puede ofrecernos sugerencias acerca de dónde mirar, si tenemos un sistema que funciona a veces, es muy difícil determinar si estamos comprobando las variables equivocadas o las variables correctas en el momento equivocado o las dos cosas.

A dónde dirigirse

Necesita ayuda. ¿A dónde acudir primero? Debe reflexionar sobre el orden en que salta de un experto a otro, pues el objetivo debe ser encontrar la solución del problema con el menor esfuerzo y coste.

Antes que cualquier otra cosa, pruebe a buscar en la Web, tanto en las bases de datos de empresas cómo más en general en Google (www.google.com). Lo único difícil es encontrar los términos de búsqueda apropiados, pero cinco minutos de búsqueda merecen la pena si muestran las respuestas necesarias. No creería el número de cuestiones que hemos recibido a lo largo de los años cuyas respuestas se encontrarían fácilmente en Google (que es donde también nosotros miramos primero).

Si dispone de libros o revistas que tocan el tema, mire también en ellos, pero nosotros normalmente preferimos buscar primero en la Web, pues es más rápido que buscar en un índice o entre varios números de una revista.

Nota

Naturalmente, para problemas de redes inalámbricas, el resto de este capítulo resultará útil, junto con los capítulos apropiados de este libro.

Si una búsqueda en la Web no proporciona la respuesta o, como mínimo, algunas pruebas más a intentar, lo más rápido, barato y fácil es pedir ayuda a un amigo experto. Si tiene tal amigo, le recomendamos que le pida ayuda. Pero tenga cuidado, pues utilizar en exceso el deseo de responder cuestiones técnicas de otras personas para resolver nuestros problemas puede estropear las amistades más sólidas. Y si el amigo es más que un conocido, hay que tener todavía más cuidado para no provocarle molestias. Si es posible, intente hacerle favores equivalentes para que no se sienta explotado. Adam y su esposa tienen un modo personal de consultar a los amigos sobre problemas de informática: invitarlos a cenar. De ese modo, la consulta se convierte en una reunión social y todo el mundo se siente gratificado. Glenn fue invitado a un almuerzo con sushi que incluyó hablar sobre un nuevo teléfono móvil.

Truco

Si siempre se siente confuso sobre qué tipo de hardware comprar, hasta el punto que no se decide por un PC o un ordenador Mac, una forma de romper el bloqueo es elegir la opción ya decidida por su mejor amigo experto. Dicho de otra forma, averigüe a quién puede llamar un sábado por la mañana y compre el sistema que tiene o recomienda esa persona. Naturalmente, ese amigo podría recomendar la plataforma contraria si se imagina en dónde se va a meter.

Si no tiene un amigo experto, la siguiente mejor opción es contactar con el soporte técnico del fabricante del aparato en cuestión. Si no lo ha hecho todavía, visite su sitio Web y compruebe si tiene en línea una base de datos de problemas y soluciones que pueda servirle.

Si el sitio Web no sirve de ayuda, envíe un mensaje de correo electrónico o llame por teléfono. Los ingenieros de soporte técnico a menudo no están muy bien pagados y la rotación de la plantilla es rápida, y eso significa que no es poco común que la persona de soporte técnico sepa aún menos que nosotros. (En ese caso, pregunte con mano izquierda si el problema puede pasar a un segundo nivel de soporte técnico.)

Algunas compañías cobran por el soporte técnico y, aunque sea gratuito, las llamadas raramente lo son. Eso no sería malo si no fuera común tener que pasar 30 minutos colgado del teléfono esperando para hablar con una persona, y no hay nada más frustrante que saber que la cuenta del teléfono sigue aumentando 10 céntimos por minuto mientras estamos sentados sin hacer nada.

Por último, algunos ingenieros de soporte técnico pueden conocer bien sus productos, pero si el problema nace de la interacción de varios productos, pueden no ser capaces de ver toda la figura o quizá intenten pasar la culpa a otra compañía (que a su vez, en los casos más molestos, dirá que el problema proviene de la primera). Suponiendo que el soporte técnico de Sony tendría una excusa menos que alegar en caso de un problema, Glenn recomendó una vez a un amigo que comprara la versión Sony Vaio de la PC Card Orinoco para su portátil Vaio.

Si el soporte técnico falla o le parece que no merece la pena intentarlo por el coste de la llamada y los excesivos tiempos de espera, el siguiente lugar en que buscar ayuda es un foro de Internet apropiado. Lo difícil aquí es identificar el lugar correcto en el que preguntar, pues hay muchísimos grupos distintos. Busque listas de correos, grupos de noticias Usenet, foros de soporte basados en Web e incluso canales IRC apropiados. Cuando decimos "apropiados" lo hacemos en todo su sentido. Observe brevemente el foro antes de poner su pregunta para garantizar que lo que plantea encaja con el debate en marcha, pues plantear solicitudes apartadas del tema pidiendo ayuda puede molestar innecesariamente a la gente y no le proporcionarán la solución necesaria. Además, hace que se pierda un tiempo precioso.

Truco *No sea demasiado exigente al pedir ayuda en foros de Internet. Funcionan sólo porque hay personas que desean dar su tiempo y conocimientos por el bien del público; si quiere que los foros prosperen, sea comprensivo y ayude también a otros cuando pueda.*

Si todo lo demás ha fallado o no tiene tiempo o paciencia para las estrategias anteriores, piense en contratar a un consultor. La vía del consultor es la más cara y no es necesariamente rápida, dependiendo de los horarios del consultor y de lo familiarizado que esté con la situación concreta. Pero si el problema es lo bastante grave o molesto, el tiempo y el dinero merecerán la pena.

Cómo reportar problemas

Cuando llega el momento de informar del problema a alguien más, las notas son inapreciables, pues, sin ellas, terminaríamos repitiendo pruebas sólo para verificar los resultados una vez más. Evidentemente, cómo se reporte un problema varía dependiendo de a quién se está informando, pero esta estrategia funcionará en la mayoría de las situaciones.

Primero, cree un perfil del ordenador que incluya:

- El modelo de ordenador, cuanta memoria tiene, el sistema operativo que utilice, el número o tipo de versión (Windows XP Pro) y los parches (el .1 en Mac OS X 10.2.1 o el Service Pack 1 para Windows XP).
- Cualquier cambio reciente en el sistema, como la actualización del propio sistema operativo o la instalación de nuevos controladores.
- Extensiones especiales o añadidos instalados, como un cortafuegos de terceras partes o, en Mac OS 9, extensiones del sistema.
- Cualquier aparato añadido, como un segundo monitor, una tarjeta de vídeo de terceras partes, una tarjeta SCSI, hardware de audio o vídeo, escáner, etcétera.
- Números de versión del software o los controladores relacionados con el problema. A menudo, los controladores antiguos o demasiado nuevos pueden provocar problemas.

Truco

En Windows, busque un programa llamado Información del sistema (generalmente se encuentra en la carpeta Herramientas del sistema dentro de Accesorios), y en los sistemas Mac, busque Perfiles de sistema Apple en el menú de la manzana en Mac OS 9 o en la carpeta Utilidades en Mac OS X. Estas utilidades generan perfiles del ordenador que puede guardar y enviar junto con el informe del problema.

Una vez desarrollado un perfil que pueda presentar en caso necesario, es el momento de reportar el verdadero problema. Describa el problema brevemente

y señale que ya ha llevado a cabo los intentos de resolución estándar. Después relate brevemente lo que ya ha intentado, pero no entre en muchos detalles, pues el hecho de que pida ayuda significa que lo intentado no resultó útil. Cómo continúe depende de lo interactivo que sea el medio de soporte.

Para situaciones de soporte de interacción rápida (en persona, a través del teléfono o con mensajería instantánea), deje que la persona de soporte técnico le haga preguntas y le guíe durante el proceso, pues es probable que tenga alguna idea del origen del problema. Si se lanza a contarle lo que ya ha intentado, puede abrumarle con detalles innecesarios. No se ofenda si le pregunta si hay corriente o si el aparato está enchufado, puede parecer irritante, pero es su versión de resolver un problema metódicamente.

Cuando se pide ayuda con interacción lenta (mensajes de correo electrónico, listas de correo, grupos de noticias Usenet o foro de soporte Web), complemente su breve resumen de lo que ha intentado con una lista de las pruebas llevadas a cabo y su configuración de sistema. No hay necesidad de explicar qué sucedió en las pruebas que han fallado intentando aclarar la situación, pero es importante incluirlas todas para que la gente que intenta ayudar no termine sugiriendo pruebas ya efectuadas (en estas formas de comunicación de interacción lenta, un intercambio de información puede llevar uno o dos días, de modo que el numero de mensajes debe ser el menor posible).

En cualquier situación, intente responder preguntas a los expertos tan rápida y completamente como sea posible. Desde nuestra perspectiva después de haber ayudado a gente durante muchos años, no hay nada peor que recibir una respuesta incompleta a las preguntas, que obliga a repetir la pregunta de una forma ligeramente distinta alargando todo el intercambio.

Enfrentarse a lo irresoluble

Nos gustaría decir que si sigue todos los pasos que hemos perfilado podrá resolver cualquier problema. Desgraciadamente, hay un pequeño número de problemas que resisten todos los esfuerzos, tanto los propios como los de los expertos. Eso es porque todo lo que intente lleva tiempo y esfuerzo, y hay un límite a la energía y el dinero que se debe invertir para resolver un problema dado. A veces lo mejor es rendirse y comprar nuevo hardware o software que elimine completamente el problema, Por supuesto, la esperanza es tomar este nuevo camino antes de dedicar demasiado esfuerzo al intento de solucionar las cosas.

Pero no deje que el hecho de que algunos problemas no pueden resolverse con un esfuerzo razonable le impida intentarlo. En la inmensa mayoría de los casos, recorrer metódicamente los pasos mencionados dará resultado.

¡Sea amable!

En realidad, hay algo peor que proporcionar respuestas incompletas a las cuestiones, aunque resulta un poco difícil decir esto: no sea maleducado. Le resultaría increíble la cantidad de gente que asume que el problema es, de alguna forma, culpa del personal de soporte técnico. De acuerdo, se siente frustrado y quizá hasta enfadado porque ha comprado una pieza de hardware o software que no funciona, pero si quiere ayuda, será más probable que la obtenga si se comporta de forma educada y profesional al hablar con el soporte técnico.

Aunque la mayoría de la gente es más amable cuando pide ayuda en una lista de correos independiente o en un foro en línea, todavía hay una tendencia a quejarse o amenazar con no volver a comprar productos de la compañía. Mala idea, pues a la gente que es más probable que pueda ayudar seguramente le gustan la empresa y sus productos, y cuanto más despotrique menos interesados estarán en responderle. Además, si es demasiado molesto, preferirán que compre productos de la competencia a que siga acosándoles.

Hablando en plata, hay un tiempo y un lugar para las quejas, pero hay que separarlas de las peticiones de ayuda. De ese modo conseguirá el máximo efecto con sus quejas y tendrá la mejor oportunidad de obtener ayuda.

Problemas de redes inalámbricas

En casi todos los casos con redes convencionales, o tenemos una conexión o no la tenemos. Son binarias (activas o inactivas) y eso tiene sentido para nosotros que nos hemos acostumbrado a los ordenadores. Las redes inalámbricas son distintas. Son difusas. A veces puedes recibir una señal fuerte sentado en el sofá; otras veces no recibes nada en el mismo sitio. Francamente, eso nos vuelve locos y, a juzgar por los problemas que hemos ayudado a resolver a otras personas, vuelve locos a casi todo el mundo. Afortunadamente, la falta de claridad de la recepción inalámbrica desaparece cuando se miran los extremos de la red: cualquier problema que haya con el adaptador de red inalámbrica o con obtener los servicios de red locales o llegar a Internet obedecen a las más comprensibles reglas de la resolución de problemas informáticos.

En esta sección, hemos identificado un pequeño número de problemas comunes ofreciendo una gran cantidad de soluciones o pruebas posibles para cada uno. En su mayor parte, nuestras soluciones son generales, aunque si conocemos una solución específica para un dispositivo o sistema operativo determinados, también la presentamos.

Truco *Apple tiene una detallada guía de resolución de problemas para su tecnología de red inalámbrica AirPort, pero como AirPort es simplemente el estándar 802.11b, merece la pena leerla aunque utilice otra plataforma. La encontrará en http://docs.info.apple.com/article.html?artnum=106858. Pruebe también la página de Wireless Networks Troubleshooting en www.practicallynetworked.com/support/troubleshoot_wireless.htm.*

Truco *Microsoft integra una guía interactiva de resolución de problemas de red con algunos consejos para las redes inalámbricas en el sistema de ayuda de Windows XP (vea la figura 9.1). Puede guiarle paso a paso por problemas comunes y aconsejarle para reconfigurar sus ajustes.*

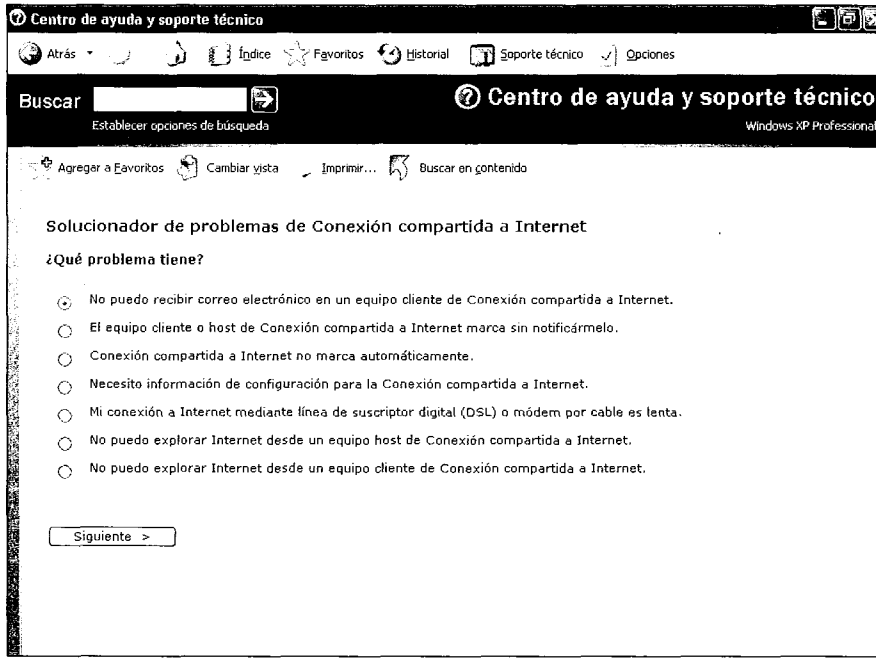

Figura 9.1. *Solucionador de problemas de red de Windows XP.*

Problema: el adaptador de red no funciona

P: Mi software cliente de red inalámbrica no funciona en absoluto. ¿Qué puedo hacer para convencerle de que la tarjeta de red está instalada?

R: Cuando se trata de problemas relacionados con un dispositivo periférico, como un adaptador de red inalámbrica que no funciona, puede intentar varias cosas, aunque algunas quizá sólo le acerquen a la resolución del problema:

- ¿Se pone intermitente el LED de actividad o al menos se enciende? Si no, la tarjeta o tal vez la ranura o puerto a la que conecta la tarjeta pueden estar estropeados. También es posible que se necesite corriente externa.
- Desconecte y vuelva a conectar el adaptador de red inalámbrica. Le sorprendería cuántos problemas se solucionan restableciendo las conexiones físicas.

Truco

Si el adaptador es una PC Card, quizá tenga que decirle al sistema que suspenda la tarjeta para poder quitarla. Sin embargo, si el sistema ni siquiera reconoce la tarjeta, tendrá que sacarla aunque técnicamente siga activa. Compruebe tres veces antes de hacerlo o, todavía mejor, apague primero el ordenador totalmente. En Windows, se suspende una tarjeta haciendo clic derecho en su icono en la bandeja del sistema y eligiendo el elemento apropiado del menú; en un ordenador Macintosh, quizá tenga que hacer ***Control-clic*** *en el icono de la tarjeta en el escritorio y seleccionar* ***Expulsar****.*

- Si es posible, conecte el adaptador de red a otro ordenador y vea si funciona en él. Si no, puede estar roto y habrá que comprobar la garantía. (Pruebe en una tercera máquina, si puede, sólo para estar más seguro.)
- Compruebe que dispone del software de cliente de red (que reside en el ordenador) y el firmware (que reside en el propio adaptador) más modernos. Si no tiene las versiones apropiadas, actualícelas. A veces la incapacidad para actualizar controladores o firmware indica problemas más profundos del sistema que no tienen relación con lo inalámbrico.

- Si está utilizando un software cliente de red inalámbrica de terceras partes, reinstálelo con el CD-ROM original.
- Bajo Windows, pruebe a desinstalar todos los controladores de adaptador inalámbrico y después instale sólo el que necesita.
- En Windows XP, compruebe que el servicio Configuración inalámbrica rápida está iniciado.
- En Mac OS 9 o anterior, reinicie utilizando el grupo de extensiones "Mac OS completo" para eliminar un conflicto con alguna extensión de terceras partes (vea la figura 9.2). Si el adaptador de red funciona bajo el grupo de extensiones "Mac OS completo", hay que averiguar qué extensión de terceras partes provoca el conflicto. Una vez identificado el conflicto, puede desactivar la extensión problemática o comprobar si una actualización de la extensión resuelve el problema. La utilidad Conflict Catcher de Casady & Greene (www.conflictcatcher.com) puede ayudarle a localizar extensiones conflictivas.

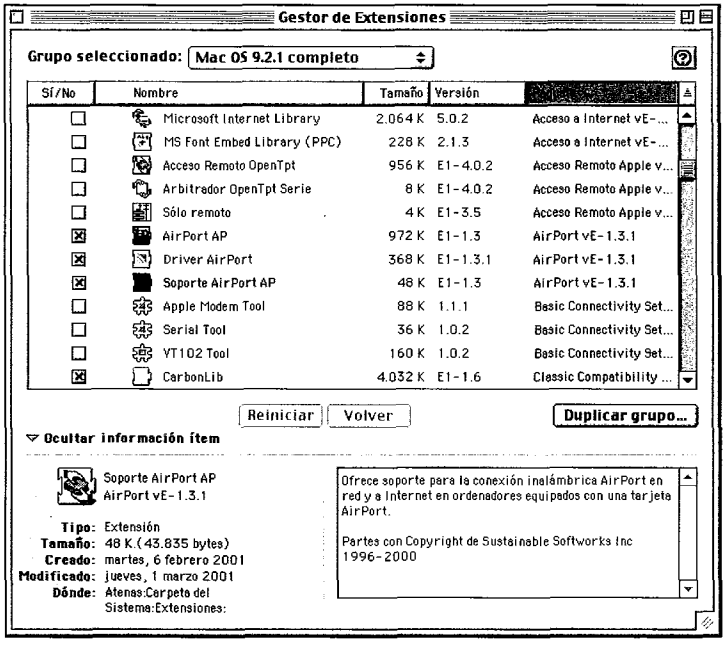

Figura 9.2. *El grupo "Mac OS completo" del Gestor de Extensiones.*

- Si tiene instalados Mac OS 9 y Mac OS X, pruebe en los dos sistemas operativos para determinar si el adaptador de red funciona en uno pero no en el otro.

- En un ordenador Mac, si dispone de un disco duro externo que pueda iniciar el ordenador, pruebe a iniciar el sistema desde ese disco para ver si el problema está relacionado con el disco de inicio normal o si sucede lo mismo con los dos discos.
- Bajo Windows, puede intentar iniciar en modo seguro con funciones de red, para deshabilitar otros servicios y subsistemas. Reinicie el ordenador y, una vez que aparezca el texto "Iniciando Windows" durante el proceso de inicio, mantenga pulsada la tecla **F8**. Si el problema desaparece, puede concluir que es probable que esté relacionado con algo que no se carga en el modo seguro. El siguiente paso podría ser reinstalar el sistema operativo o probar otro software de red para ver si está provocando el problema.
- Si es posible, verifique que el puerto o ranura en la que conecta el adaptador de red inalámbrica funciona. Puede hacerlo probando en ese puerto o ranura otro controlador de red que sí funcione.
- Si está seguro de que todo el hardware funciona, piense en reinstalar todo el sistema operativo. Tenga cuidado para no borrar datos en el proceso y compruebe siempre que dispone de una copia de seguridad reciente antes de proceder con este paso.

Conexiones de red inalámbrica Windows XP inhabilitadas

Glenn se enfrentó una vez a un molesto problema en el que un portátil con Windows XP, un Sony Vaio, dejó de funcionar con sus tarjetas inalámbricas de Linksys y Proxim (Orinoco).
Después de los intentos estándar de resolución del problema, Glenn contactó con el soporte técnico de todas las compañías implicadas: Sony, Linksys, Proxim e incluso Boingo, cuyo software, que estaba en ejecución, no podía reconocer ninguna de las tarjetas. No llamó a Microsoft, y eso pudo haber sido un error, pero utilizó su ayuda en línea y también el extenso solucionador de problemas de red de Windows XP. Nada sirvió de ayuda al principio.
Al final, descubrió que desinstalando todos los controladores Linksys y Orinoco podía conectar la tarjeta Orinoco y obtener una red.
Pero la tarjeta Linksys seguía sin funcionar. Después, recibió un mensaje de correo electrónico de Proxim que apuntaba la raíz del problema. Hay una pieza de software, un "servicio" en la jerga de Windows, que se ocupa de configurar las conexiones inalámbricas cuando se

instala una tarjeta o se añade un adaptador. Ese servicio había que iniciarlo; ¿por qué se había detenido? Glenn todavía no puede imaginarlo. Si se encuentra con una situación similar, siga estos pasos:

1. *En el escritorio, haga clic derecho en Mi PC y seleccione Administrar.*
2. *En la lista de elementos que aparece en la consola de administración, expanda la sección Servicios y aplicaciones en el lado izquierdo y seleccione Servicios (vea la figura 9.3).*

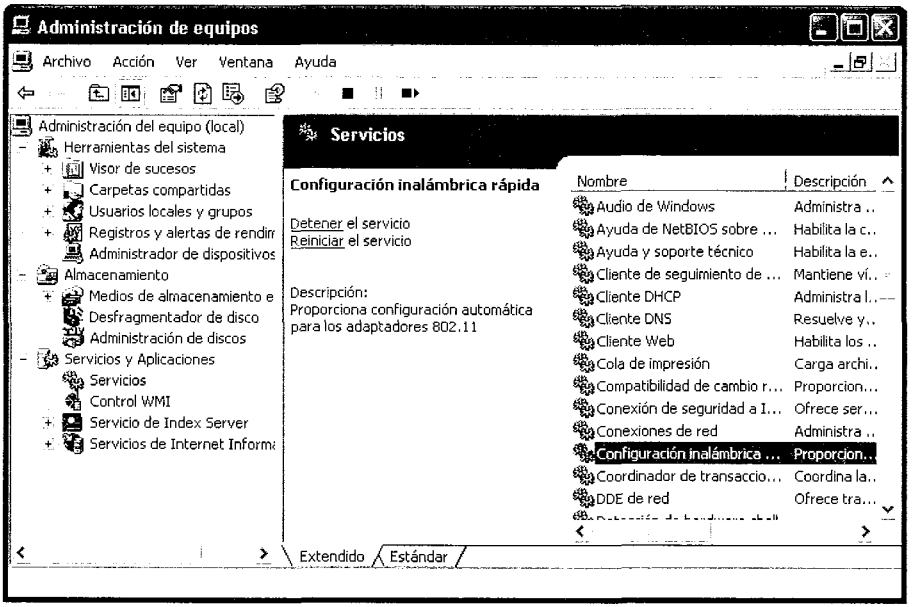

Figura 9.3. *Consola de administración.*

3. *En el panel de la derecha, desplácese hasta Configuración inalámbrica rápida y haga doble clic en su icono.*
4. *En la ficha General del cuadro de diálogo que aparece, compruebe que se asigna Automático al Tipo de inicio y que el Estado del servicio es Iniciado (vea la figura 9.4).*
5. *Si el servicio no está iniciado, haga clic en* ***Iniciar****.*

Glenn ha tenido que iniciar el servicio Configuración inalámbrica rápida en su sistema varias veces desde entonces, aunque antes nunca había necesitado hacerlo.

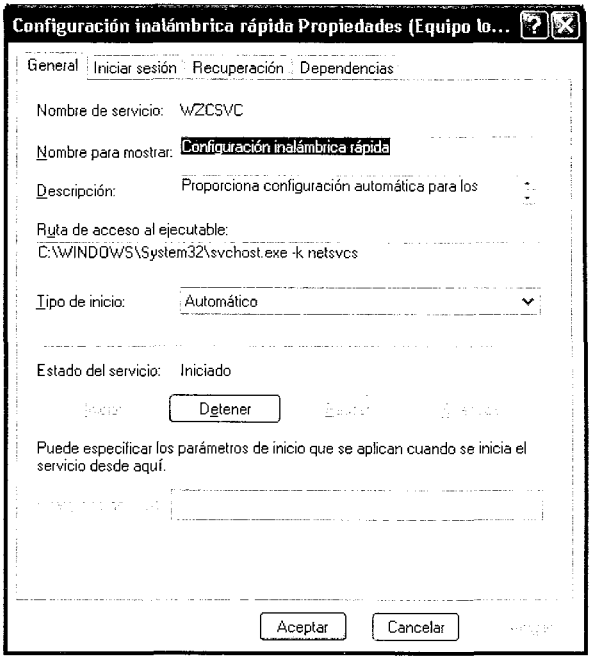

Figura 9.4. *Cuadro de diálogo Configuración inalámbrica rápida.*

- Gire 90 grados. En serio. A veces es lo único que se necesita para mejorar la fuerza de la señal lo suficiente para que siga funcionando la red. Es como en los viejos tiempos cuando la gente tenía que subir al tejado para ajustar la posición de la antena de TV y mejorar la recepción de la señal el día del gran partido de fútbol.
- Pruebe otros ángulos en otros planos. Incluso las antenas de punto de acceso bien diseñadas envían ondas en todas las direcciones. Citando a Mr. Spock en Star Trek II, "No está pensando en tres dimensiones".
- Si el ordenador tiene una antena interna, compruebe que la antena está bien conectada a la tarjeta de red inalámbrica.
- Esto es penosamente obvio, pero tenemos que decirlo. Intente acercarse al punto de acceso. Como solución, es fácil, barato y, sí, ya sabemos que debería poder trabajar desde donde quiera. Si no quiere dejarse ganar por los duendes de la radio, siga con las próximas sugerencias.
- Piense en llevar el punto de acceso a un lugar más centrado. Esto puede no ser posible sin desplegar un largo cable de Ethernet y, aunque sabe-

mos que el objeto de las redes inalámbricas es deshacerse de los cables, en ocasiones no hay más remedio que utilizar uno.

- Añada una antena al punto de acceso. Puede comprar pequeñas antenas omnidireccionales para interiores que aumentan la fuerza de la señal, aunque muchos puntos de acceso no permiten conectar una antena externa.
- Piense en comprar un nuevo punto de acceso que tenga tomas para antenas externas o que incluyan una antena más potente (muchos puntos de acceso, incluyendo la Estación Base AirPort, sólo utilizan la pequeña antena de la PC Card interior).

Problema: la señal es intermitente

P: La mayor parte del tiempo, no tengo problema para mantener una conexión con mi punto de acceso, pero a veces desaparece y vuelve más tarde. ¿Qué puede estar pasando?

R: Cuando vea este tipo de problemas, piense en posibles interferencias:

- ¿Tiene un horno microondas que pueda estar emitiendo radiación y provocando interferencias? Haga una prueba vigilando el indicador de fuerza de la señal en el ordenador mientras funciona el microondas. Puede resolver este problema colocando el microondas más lejos de los aparatos de red inalámbrica.
- ¿Tiene un teléfono inalámbrico de 2,4 GHz o, peor, lo tienen sus vecinos en un edificio de apartamentos? Estos teléfonos son cada vez más comunes y como funcionan en la misma frecuencia que las redes inalámbricas 802.11b, puede haber interferencias. Probablemente no oiga nada más que cierto chisporroteo en el teléfono, pero la red puede dejar de funcionar completamente. Intente separar la base del teléfono del punto de acceso y los ordenadores. Si va a comprar un nuevo teléfono inalámbrico, los de 900 MHz ofrecen la misma calidad de sonido y tienen un alcance similar al de los modelos de 2,4 MHz, a pesar de lo que dicen los fabricantes.
- Busque otros aparatos que puedan usar la frecuencia de 2,4 GHz, como cámaras espía X10 o dispositivos de transmisión de audio o vídeo en un equipo estéreo o de televisión. Adam probó una vez un aparato que transmitía el audio de su ordenador al equipo estéreo; tan pronto como encendía el aparato, la red inalámbrica se paraba en seco.

Problema: la recepción es imposible

P: En mi lugar de trabajo, un muro de cemento impide que mi red inalámbrica cubra toda la oficina. ¿Cómo puedo extender la red inalámbrica hasta los puntos muertos actuales?

R: Suponemos que ya ha probado el consejo anterior sobre aumentar la fuerza de la señal. Recolocar el punto de acceso o añadir una antena (especialmente si puede tomar una prestada para hacer pruebas) son soluciones fáciles. Si no funcionan, hay otro par de opciones:

- ¿De verdad es necesario el acceso inalámbrico al otro lado del muro? Si no, probablemente sea más fácil taladrar un agujero para que pase un cable Ethernet. Sólo porque las redes inalámbricas sean atractivas no significa que nunca se puedan usar cables.
- Si el acceso inalámbrico al otro lado del muro es indispensable, taladre un agujero, pase un cable Ethernet y conecte otro punto de acceso. Como este punto de acceso no tiene otra cosa que hacer aparte de proporcionar acceso de red inalámbrico, puede ser un punto de acceso sencillo, sin necesitar funciones de puerta de enlace inalámbrica.

Comprar un nuevo punto de acceso

Cuando se mudó a su nueva casa, Adam comprendió que el módem de cable debía instalarse en la esquina noreste del piso bajo de la casa, donde llegaba el cable de la conexión. Desgraciadamente, eso significaba que su punto de acceso, que había que conectar al módem de cable, también debía estar instalado en ese lugar. Al principio, utilizando una Estación Base AirPort grafito, podía proporcionar acceso de red inalámbrico en todas las habitaciones de la casa excepto la oficina de su esposa, que se encontraba en la esquina suroeste del segundo piso.

Utilizando como punto de acceso un iBook (que tiene una antena mejor que la Estación Base AirPort) con el software Estación Base resolvió el problema, excepto que el iBook quedaba anclado. A continuación, Adam decidió desplegar un cable Ethernet a través del techo hasta el segundo piso, donde había verificado que un punto de acceso tendría el alcance necesario para llegar a la oficina de su esposa. Como muchos trabajos que implican cables, fue fatigoso y difícil, pero resolvió el problema.

La recepción seguía sin ser tan buena en toda la casa como le hubiera gustado, de modo que después de sacar la PC Card Lucent WaveLAN de la Estación Base AirPort para aprovecharla en su conexión inalámbrica de largo alcance, Adam compró una puerta de enlace Linksys EtherFast con un par de pequeñas antenas dipolo que proporcionaba una mejor fuerza de señal. Todavía vive en el armario de Adam en el dormitorio.

- Taladrar agujeros no siempre es factible. Si es ésa la situación, piense en usar un par de puentes Ethernet HomePlug o HomePNA a cada lado del muro, con un segundo punto de acceso en el otro lado de la pared. Evidentemente, HomePlug es ideal si tiene las conexiones eléctricas y el voltaje apropiado; si puede usar cables de teléfono, tal vez HomePNA sea la solución.
- Derribe el muro. (Suponiendo que no es un muro de carga: es mala idea coger un martillo hidráulico y derribar un muro de carga, a menos que quiera tirar todo el edificio.)

Problema: no hay conectividad inalámbrica

P: Mi adaptador de red inalámbrica parece ver el punto de acceso, pero no me deja conectar. ¿Alguna idea?

R: En este tipo de situación, el problema suele estar relacionado con ajustes de seguridad demasiado rígidos, aunque también puede haber otras razones:

- Si es posible, compruebe si otros ordenadores pueden conectar. Si es así, el problema es específico del ordenador. Saber que el problema está relacionado con el ordenador reduce el campo de las posibles pruebas y soluciones futuras.
- Es posible que esté demasiado alejado para conectar de forma fiable, a pesar de que el software del adaptador reporte que puede ver el punto de acceso. Muchos indicadores de fuerza de señal del software no se corresponden de forma proporcional con la calidad de la señal. Intente acercarse al punto de acceso para comprobar si desaparece el problema o descargue NetStumbler o MacStumbler, comentados en el capítulo 6, para recoger más datos sobre la fuerza de la señal.

- Vuelva a comprobar que ha introducido correctamente la clave WEP. Es fácil cometer un error, especialmente si hay que escribir 26 caracteres; con un solo error queda invalidada toda la clave. Cierto software no avisa que la clave WEP es incorrecta, haciendo difícil solucionar problemas relacionados con WEP.
- Desactive el cifrado WEP y el filtrado de direcciones MAC en el punto de acceso para comprobar si impiden la conexión.
- Compruebe que el nombre de red es exacto y no tiene espacios o caracteres especiales.
- Reinicie el punto de acceso o apáguelo y enciéndalo después de 30 segundos.
- Si los ordenadores que utilizan Windows XP pueden conectar, pero los que usan otros sistemas operativos no, el problema puede estar relacionado con un administrador que haya habilitado la autenticación 802.1x, que hemos descrito en el capítulo 6. La autenticación 802.1x es una buena herramienta en organizaciones grandes, pero sólo goza de soporte en Windows XP. Algunos administradores pueden intentar habilitarla sin tener en cuenta sus limitaciones.

Nota

Compruebe que no hay usuarios de la red en medio de un trabajo importante antes de apagar y encender el punto de acceso. Al hacerlo, se deshabilita el acceso a todo el mundo y el servicio DHCP puede asignar nuevas direcciones.

Problema: hay que reiniciar el punto de acceso con frecuencia

P: Cada pocos días o semanas, mi punto de acceso parece quedarse congelado: no puedo conectar con él y tengo que reiniciarlo. ¿Qué le sucede a la puerta de enlace?

R: Algunas puertas de enlace y puntos de acceso parecen requerir ser reiniciados con regularidad:

- Si tiene un WAP11 Linksys de primera generación, tenga en cuenta que muchos informes y nuestra propia experiencia muestran que requiere encenderlo y apagarlo regularmente, por lo demás funciona bien. Poste-

riores versiones del firmware sirven de ayuda (la 1.4i es la última para ese modelo) y la versión 2 de WAP11 actualizada no sufre ese problema, Las primeras versiones de la puerta de enlace EtherFast Linksys también tenían el mismo problema.

- La primera generación de Estaciones Base AirPort, la versión grafito, tenía la reputación de requerir ser reiniciada regularmente, aunque no frecuentemente. Las unidades grafito posteriores y las nuevas Estaciones Base AirPort versión nieve no tienen este problema.
- Si observa el problema en otras puertas de enlace, piense en las soluciones usuales: añada un protector contra saltos de tensión; utilice un sistema de alimentación ininterrumpida (SAI o UPS en sus iniciales inglesas) para prevenir problemas provocados por breves cortes de corriente que no llegan a reiniciar la puerta de enlace; y piense en llevar la puerta de enlace a reparación si todavía está dentro del periodo de garantía.

Problema: no hay enlace entre la red inalámbrica y la convencional

P: Mis ordenadores de cable e inalámbricos no pueden verse entre sí. ¿Qué falla?

R: En la mayoría de los casos, este tipo de problemas puede estar provocado por ajustes incorrectos en el puente entre la red de cable y la inalámbrica o por cables dañados:

- Compruebe el punto de acceso para garantizar que el puente entre la red convencional y la inalámbrica está configurado correctamente y activo.
- Si está utilizando un punto de acceso de software, compruebe que los ajustes de red del ordenador siguen siendo correctos y que un reinicio o cualquier otro cambio no deshabilitó el puente.
- Verifique que los cables de los ordenadores de la red convencional están bien conectados. No subestime la posibilidad de que un cable haya resultado dañado porque alguien lo haya pisado o un ratón lo haya roído.
- Si tiene varios ordenadores conectados con cables, compruebe que se ven entre sí.
- Si la puerta de enlace inalámbrica tiene un conmutador para restablecerla, presiónelo para limpiar errores.

- Desenchufe la puerta de enlace inalámbrica, espere 30 segundos y vuelva a enchufarla. A veces así se limpian errores que no desaparecen con el conmutador de restablecimiento.
- Si el problema está relacionado con un servicio específico, como compartir archivos o impresoras, compruebe que el software está correctamente instalado y configurado en todos los ordenadores en cuestión.

Problema: no hay conexión a Internet

P: Mi red inalámbrica funciona bien básicamente, pero no puedo ver Internet a través de mi conexión de módem, DSL, cable o banda ancha. ¿Qué puede estar mal?

R: Desgraciadamente, hay muchos problemas diferentes que podrían provocar la desaparición de una conexión a Internet y algunos de ellos no dependen de nosotros:

- Si está utilizando asignación dinámica de direcciones, verifique que se ha asignado una dirección DHCP al ordenador. Si no, el problema puede estar en el servidor DHCP de la puerta de enlace o de la red.
- DHCP puede no estar emitiendo a través de todos los puntos de acceso: la mayoría de los servidores DHCP en puntos de acceso tienen que tener habilitada una opción para hacer de puente de DHCP a la red de cable.
- Un punto de acceso "bribón" puede estar ofreciendo direcciones IP que no son enrutadas al resto de la red. Hemos visto este problema en nuestras propias redes y en una convención reciente.

Efectuar una prueba ping

Una de las formas más básicas de probar la conectividad entre ordenadores es hacer una prueba ping, que es como un sónar para ordenadores. Un ordenador envía un ping a otro ordenador o dispositivo y espera una respuesta. Si vuelve la respuesta, el ordenador remoto está conectado y en funcionamiento; si no, el problema está relacionado con la conexión o con un software de red de bajo nivel. Para efectuar una prueba ping, lo único que hay que saber es la dirección IP del ordenador que se quiere probar. Para determinar la dirección IP de un ordenador en Windows, haga clic en el menú Inicio y seleccione MS-DOS

(Windows 98) o Símbolo del sistema (Windows XP) en el menú jerárquico Programas. (Microsoft ha movido a veces este comando con el tiempo; si no lo encuentra en Programas, mire en Accesorios en Windows XP.) Después, escriba `ipconfig` *para encontrar la dirección IP. En sistemas Mac, busque en el panel de control TCP/IP (Mac OS 9) o en el panel de preferencias Red (Mac OS X) la dirección IP.*
Una vez encontrada la dirección IP, puede efectuar una sencilla prueba ping en Windows seleccionando Ejecutar en el menú Inicio y escribiendo `ping 192.168.1.1` *(reemplace la dirección IP con la de la máquina que quiera probar). En Mac OS X, abra una terminal y escriba el mismo comando. En Mac OS 9, necesita una utilidad como IPNetMonitor de Sustainable Softworks (www.sustworks.com/site/prod_ipmonitor.html) o Interarchy de Stairways Software (www.interarchy.com).*
La prueba ping ha tenido éxito si ve una serie de líneas con números consecutivos, cada una con una hora al final. Si hay muchos intervalos en los números consecutivos, puede haber algo mal en el enlace de la red local, el enlace de la red con Internet o la conexión de Internet entre el ISP y redes de nivel más alto.
Quizá tenga que pulsar ***Control-C*** *en Mac OS X y Windows para detener la prueba ping; en algunos sistemas operativos, los pings continúan indefinidamente hasta que los detenemos. Si funciona la prueba ping, pase a otras pruebas de resolución de problemas. Si no funciona, busque cables en mal estado o compruebe que los ajustes de red básicos están configurados correctamente. Algunos módems DSL que permiten conexiones telnet también tienen incorporadas utilidades ping que pueden ayudar a eliminar la red local como fuente del problema.*
Una advertencia: el software de cortafuegos Intego NetBarrier que utiliza Glenn en todos sus ordenadores Mac OS X ¡tiene una opción para proscribir direcciones IP que emiten pruebas ping! Se puede desactivar esta opción, pero si se olvida hacerlo, puede resultar muy misterioso, pues inadvertidamente quedan proscritas las máquinas propias. Otro software de cortafuegos puede deshabilitar totalmente las respuestas ping (de modo que es buena idea efectuar algunas pruebas ping aunque todo funcione bien, sólo para recopilar datos que sirvan de punto de partida).

- Compruebe los ajustes de cortafuegos. Para asociarse con la mayoría de puntos de acceso, el ordenador u otro dispositivo debe aceptar emisiones DHCP y un cortafuegos demasiado estricto puede restringir las emisio-

nes DHCP, incluso desde una red local. (Glenn ha sufrido por este asunto durante varios meses cuando viajaba hasta que descubrió su propio exceso de celo.)

- Si su puerta de enlace inalámbrica tiene un conmutador para restablecerla, presiónelo para limpiar errores, pero sólo después de advertir a otros usuarios de la red (vea la nota anterior en "no hay conectividad inalámbrica"). Si eso falla, desenchufe la puerta de enlace inalámbrica, espere 30 segundos y vuelva a enchufarla. A veces esto elimina errores que no se corrigen con el conmutador.
- Verifique que el cable de la conexión de Internet (ya sea de módem o enrutador) está correctamente conectado. No menosprecie la posibilidad de que el cable haya sido dañado por alguien al pisarlo o por un roedor.
- Restablezca su módem, enrutador, módem DSL o módem de cable o, si no tienen conmutador para reiniciar, desenchufe el aparato, espere 30 segundos y vuelva a enchufarlo. (Y repetimos de nuevo, ¡avise antes a los otros usuarios de la red!)
- Restablezca o apague y encienda el módem o enrutador *de nuevo*, pero primero apague la puerta de enlace, para encenderla después de reiniciar el módem.

La puerta de enlace EtherFast Linksys se confunde

El principal punto de acceso inalámbrico de Adam es un EtherFast Wireless AP + Cable/DSL Router w/4-Port Switch y, en gran parte, funciona bien. Cuando estaba recién comprada, aproximadamente una vez al mes, la conexión a Internet por módem de cable quedaba fuera del alcance a pesar de que la conexión inalámbrica con la puerta de enlace seguía siendo sólida. Resultó que había dos problemas ligeramente distintos. Uno se resolvía pulsando el conmutador de reinicio; el otro requería desenchufar y enchufar la puerta de enlace. Después de sufrir estas molestias durante unos meses, Adam actualizó el firmware de la puerta de enlace con la versión más reciente y los problemas desaparecieron totalmente.

Después, investigando el cifrado WEP para escribir este libro, Adam estuvo activando y desactivando el cifrado WEP y cambiando las claves, hasta que de algún modo llegó a poner la puerta de enlace Linksys en un estado en que todo parecía estar bien (y nada había cambiado en la conexión con Internet), pero ninguno de los ordenadores podía

acceder a Internet. Para solucionar el problema, Adam primero verificó que la conexión con Internet seguía funcionando conectando directamente un iBook al módem de cable. Después apuntó todos sus ajustes personales de la puerta de enlace Linksys y restableció los ajustes de fábrica. Después de introducir de nuevo sus propios ajustes, todo volvió a funcionar perfectamente.

- Si es posible, pruebe la conexión con un solo ordenador conectado directamente al módem o enrutador. Si el problema persiste, contacte con el soporte técnico de su ISP y pida ayuda.
- Apunte los ajustes personales de la puerta de enlace o el punto de acceso inalámbricos y restablezca los ajustes predeterminados. Vuelva a introducir sus ajustes.
- Pruebe con otra puerta de enlace o punto de acceso inalámbrico distinto.

Problema: no hay acceso a la red o Internet estando fuera

P: Cuando estoy fuera de la oficina, puedo conectar con los puntos de acceso y el servidor DHCP me asigna una dirección IP, pero no puedo ver la red ni alcanzar Internet. ¿Qué ajuste falla?

R: Si son puntos de acceso con los que no tiene una conexión directa, hay algunas explicaciones probables:

- Si está de visita en el campus de una universidad o en otra oficina, es posible que la red no ofrezca acceso a los visitantes. El adaptador de red inalámbrica puede asociarse a los puntos de acceso pero, al carecer de credenciales, no puede enviar ni recibir tráfico. Algunas de estas redes tienen códigos de acceso para visitantes, pero no muchas.
- Si está en un punto activo gratuito o de pago, quizá no ha pagado el acceso o no ha aceptado las directivas de uso. Inicie el navegador e intente visitar una página Web cualquiera para ver si aparece la página de portal cautivo en la que obtener acceso.
- La conexión del punto de acceso con el resto de la red o la conexión a Internet de la red pueden estar inactivas y no hay nada que pueda hacer, excepto llamar al soporte técnico (si existe tal cosa en la red a la que intenta acceder).

- Si está jugueteando intentando conseguir acceso, ¡déjelo! ¡No obtiene acceso real por una buena razón, caray!

Una mirada a la bola de cristal

Solucionar problemas es algo que sucede mucho en la actualidad, pero ahora que ya ha leído este capítulo, cambiemos de chip y miremos el futuro de lo inalámbrico, tanto en términos de avances técnicos que prevemos a corto y largo plazo como de los desafíos a los que se enfrenta el mundo de las redes inalámbricas.

10. El futuro de lo inalámbrico

Vivimos en un mundo en el que aceptamos no sólo que la tecnología cambia constantemente, sino también que la velocidad de esos cambios aumenta cada vez más. En muchas tecnologías, los cambios afectan sólo al uso de la propia tecnología, no al mundo en general. Procesadores más rápidos significa que los programas se ejecutan más velozmente. Monitores más grandes permiten ver más cosas en pantalla simultáneamente. Adaptadores de red más rápidos reducen el tiempo que se tarda en copiar archivos desde un servidor. Pero ninguno de estos muy bienvenidos avances tecnológicos afectan significativamente a nuestro mundo social, económico o político.

No sucede eso con las redes inalámbricas. Más que las otras tecnologías, las redes inalámbricas afectan a cómo viajamos y usamos Internet. Además, puede resultar que el acceso inalámbrico a Internet afecte a cómo, dónde y cuándo trabajamos, y eso afecta significativamente a su vez a nuestro modo de vida. Puede cambiar nuestra relación con los jefes y con las compañías que proporcionan acceso a Internet. Y como el espectro de radio está gobernado por organismos reguladores en todo el mundo, construir y utilizar redes inalámbricas puede afectar a nuestras relaciones con el gobierno.

Dicho esto, todas las tecnologías están destinadas a la obsolescencia, algunas mucho antes que otras. Nuestras oficinas son prácticamente museos de

ideas fallidas; ¿serán las redes inalámbricas una más? Nada de eso. Pero aunque las redes inalámbricas están aquí para quedarse, eso no significa que algunas tecnologías de red específicas no vayan a hundirse en el pozo de la historia. Lo pronto que nuestros tipos actuales de redes inalámbricas caigan en ese pozo depende de cómo interactúen con los desafíos sociales políticos y técnicos.

En este capítulo, pues, veremos algunos de estos desafíos y las actualizaciones y cambios a corto plazo de las tecnologías que hemos comentado a lo largo del libro. También nos permitiremos un pequeño vistazo a la bola de cristal basándonos en ideas que se están probando en el laboratorio o aparecen por sí mismas.

Desafíos que encara lo inalámbrico

Aunque gran parte del futuro parece de color rosa para las redes inalámbricas, una gran variedad de desafíos acecha en el horizonte. La duda que nos corroe a todos al pensar en gastar nuestro duramente ganado dinero en un aparato o dispositivo es si quedará obsoleto: ¿lamentaré haberme comprado un dispositivo Wi-Fi en lugar de esperar a que aparezca algo más, quizá basado en la red de móviles? Si decidimos instalar y usar una red Wi-Fi, no dejan de surgir más cuestiones. Como hemos debatido en el capítulo 6, el estándar 802.11b ha sufrido de huecos en la seguridad bien conocidos, añadiendo una nueva preocupación a cualquiera que transmita datos sensibles a través de conexiones de red inalámbrica. Podemos encontrarnos lidiando con reparos morales o incluso legales sobre si es o no admisible compartir conexiones de Internet a través de una red inalámbrica. Ése es un tema importante en redes comunitarias públicas. Aunque estas redes comunitarias pueden parecer algo bueno, los proveedores de servicios de Internet cuyas conexiones están siendo utilizadas más de lo previsto no se sienten muy inclinados hacia esa tendencia.

Obsolescencia inalámbrica

Puede ser difícil sobreponerse al temor ante la obsolescencia con cualquier tecnología, pero la angustia es mayor cuando se trata de redes inalámbricas, en parte debido al número de aparatos implicados. Por ejemplo, generalmente no basta con comprar un adaptador de red inalámbrica para el ordenador, sino

que también hay que comprar un punto de acceso. Y si queremos añadir varios ordenadores, eso hace crecer la inversión en tecnología. ¿Debe preocuparnos que el equipamiento de red 802.11b recién comprado sea inútil mañana? Y si todavía no lo hemos comprado, ¿tiene sentido esperar? En ambos casos nos complace decir que la respuesta es un resonante "¡No!"

La tecnología Wi-Fi tiene sentido por varias razones:

1. Wi-Fi (los dos tipos 802.11a y 802.11b) ha sido la tecnología que ha ganado claramente. Es demasiado tarde para que competidores como HomeRF desplacen un estándar ya tan aceptado.
2. Todos los estándares en desarrollo para las bandas de frecuencia de 2,4 y 5 GHz, de los que hablaremos en la próxima sección, no atacan a Wi-Fi, sino que la mejoran de varias formas manteniendo la compatibilidad con lo anterior.
3. A la gente le preocupaba que hubiera una división entre los estándares 802.11a y 802.11b, que utilizan bandas de frecuencia distintas. Esa división no se ha producido, principalmente gracias a que aparecieron adaptadores duales y puntos de acceso que prestaban soporte a los dos estándares al mismo tiempo que salía el 802.11a. Prácticamente todos los fabricantes de chips y equipamiento han hecho sus planes para vender equipamiento dual.

A pesar de las razones a favor de Wi-Fi, no podemos ofrecer soluciones para el problema de los remordimientos del que compra tecnología: siempre se paga más ahora de lo que valdrá en el futuro. Todavía peor, los precios seguirán bajando mientras que la funcionalidad mejorará. Si compramos hoy una PC Card 802.11b por 75€, podemos terminar maldiciendo nuestro mal sentido de la oportunidad cuando veamos la semana que viene una tarjeta Wi-Fi que combina 802.11a y b por sólo 80€.

De igual forma, si esperamos, siempre habrá algo mejor en el horizonte. El estándar 802.11g, que es en esencia una versión del 802.11b más rápida y compatible con lo anterior, está previsto para mediados de 2003. Dado que el equipamiento 802.11g debe costar prácticamente lo mismo que el 802.11b, no vemos ninguna razón para comprar equipamiento 802.11b a partir de ese momento.

Todo se reduce a la respuesta estándar que nos hemos acostumbrado a dar a nuestros amigos y familiares: hay que comprar la tecnología que se necesite hoy haciendo caso omiso de que los precios bajarán y la funcionalidad aumentará en el futuro. No hay nada malo en esperar, pero no se prive de una tecnología que necesita ahora porque será mejor y más barata dentro de seis meses.

Cambios en la regulación

Quizá haya visto la cita de algún entendido: "La industria de los móviles acabará con Wi-Fi". Seguro. Y ningún estudiante universitario copiará nunca música sin el permiso de la industria discográfica.

Hemos oído continuamente a los columnistas, analistas del campo, encargados de tecnología de la información y usuarios individuales predecir que las compañías de telefonía móvil utilizarían su capacidad de presión para obligar a la FCC a cambiar la regulación que gobierna el espectro sin licencia, haciendo imposible el uso de Wi-Fi en espacios públicas y quizá incluso en interiores. Estas especulaciones ignoran la realidad fundamental:

- La regulación Parte 15 de la FCC que permite el uso de Wi-Fi también está dirigida a otro equipamiento inalámbrico. Cualquier cambio en la regulación Parte 15 afectará a muchos fabricantes de aparatos electrónicos, como los vendedores de teléfonos inalámbricos.
- Se han vendidos millones de adaptadores de red inalámbrica y cientos de miles de puntos de acceso a consumidores individuales y empresas.
- Algunas corporaciones de servicio nacional, como IBM Global Services, ganan decenas de millones de dólares al año instalando y manteniendo redes para proveedores de punto activo y grandes empresas.
- Las compañías de telefonía móvil en realidad están empezando a probar Wi-Fi. El Sprint PCS Group ha invertido en el conglomerado inalámbrico Boingo Wirelles, T-Mobile USA opera la red T-Mobile HotSpot y AT&T Wireless opera una red inalámbrica en el aeropuerto de Denver.
- Microsoft, Intel, Proxim, 3Com, Cisco Systems, Dell Computer, Gateway, Siemens, Motorola, Nokia, Agere Systems, Apple Computer y muchas otras grandes compañías tecnológicas fabrican directamente o venden grandes cantidades de equipamiento Wi-Fi a pequeños consumidores y empresas, y también equipamiento relacionado con la banda de frecuencias de 2,4 GHz.

Los ingresos procedentes de ventas y servicios de Wi-Fi, otros estándares de red inalámbrica y aparatos electrónicos ajustados a la Parte 15 representan miles de millones de dólares para la industria. En unos pocos años, se espera que la cantidad se doble o triplique. Cuando hay tales cantidades de dinero implicadas, las compañías son grandes y tienen interés en mantener la prosperidad del negocio. Dicho a las claras, es casi impensable que la FCC pueda

cambiar la regulación Parte 15 de forma que impida el tipo de redes inalámbricas a que nos hemos acostumbrado.

A pesar de esa cantidad de dinero, a muchas personas les preocupa que las redes inalámbricas terminen como el mundo del contenido digital, donde industrias por valor de seiscientos mil millones de dólares han desaparecido al enfrentarse a las poco razonables restricciones de los derechos digitales que las industrias de los medios (música, películas, vídeo y televisión), cuyo valor no sobrepasa los treinta y cinco mil millones de dólares, han conseguido que fueran legisladas a su favor. En el caso de las redes inalámbricas, la preocupación es que las grandes compañías de telecomunicaciones de voz y datos se enfrenten a las baratas redes inalámbricas.

No se preocupe. Ya estamos viendo como compañías de ordenadores y aparatos electrónicos dan un paso adelante para defender las redes inalámbricas frente a posibles amenazas de legislación. Por ejemplo, dos compañías de radio digital por satélite han intentado recientemente que se pusieran restricciones a la banda de 2,4 GHz utilizada por las redes inalámbricas del estándar 802.11b y muchos otros aparatos, como los teléfonos inalámbricos.

Estas dos firmas, XM Satellite Radio y Sirius Satellite Radio, alegaron que la fuga de señal fuera de la banda (la pequeña parte de la señal que puede extenderse fuera del espectro asignado por varias condiciones) interferiría con la capacidad de sus receptores de automóviles para captar las distantes emisiones de satélite. XM y Sirius intentaron que la FCC regulara la materia y, durante los estudios preliminares, antes siquiera que la FCC aceptara considerar la petición, Intersil y Motorola escribieron devastadores (y cómicos) expedientes técnicos oponiéndose a la petición.

Intersil escribió, "Si los proveedores DARS (radio digital por satélite) tienen problemas para prestar servicio a sus clientes, la culpa no es de la regulación Parte 15. Más bien, parece que los proveedores DARS han construido un sistema frágil y ahora se dirigen a la Comisión para solucionar los puntos débiles de su propio trabajo de ingeniería". Intersil continuaba, "Sirius declara que el nivel de interferencia máximo tolerable en sus receptores es -152,6 dBW/MHz. Este nivel está en realidad unos 8 dB por debajo del ruido térmico". Esto significa que el calor en el aire crea más ruido que el nivel de señal objetado por las compañías. El informe de Motorola señalaba, "Es bastante interesante que en el informe de XM la principal fuente de interferencia no es el equipamiento que utiliza la banda de 2,4 GHz sino el ruido de ignición del vehículo". Las redes inalámbricas están aquí para quedarse y, dado que hay compañías cuyo valor es de miles de millones de dólares que comparten nuestros intereses, no nos deben preocupar qué cambios en la regulación afecten al statu quo.

Compartir

Al leer las anécdotas repartidas por el libro, quizá haya notado que a veces hemos saltado alegremente a una red inalámbrica abierta para utilizar la conexión de Internet de la red. ¿Es ético? Después de todo, no teníamos modo de saber si al propietario de la red le importaba que cualquier visitante aprovechara la conexión de Internet.

Además, no podíamos pedir permiso porque los estándares de red no proporcionan una forma de consultar esa información, como a quién pertenece la red.

Acceder a redes inalámbricas de otras personas

En un nivel, podría argüirse que uno nunca debería usar una red inalámbrica que no haya de alguna forma dejado claro que todo el mundo tiene permiso para acceder a ella. Ciertamente, nunca habrá problemas si nos atenemos a ese punto de vista. Pero este enfoque olvida un par de hechos importantes.

Primero, no hay una forma sencilla de identificar como abierta una red inalámbrica, mientras que es muy fácil cerrarla a los visitantes casuales. Por tanto, se puede suponer que si una red inalámbrica está abierta es porque se acepta su uso por cualquier persona. Ésa es la estrategia que sigue Adam con su red inalámbrica: mientras nadie abuse de ella, le satisface permitir que cualquiera dentro del alcance pueda utilizarla.

Segundo, la Internet fue construida con el espíritu de compartir y, durante muchos años, se asumía que si alguien te daba una conexión de Internet, era tu deber compartirla con otros. Para aquellos de nosotros que hemos estado utilizando Internet desde los primeros tiempos, la propagación de redes inalámbricas disponibles para el público es un poco como volver a los viejos tiempos.

Proporcionar acceso a la red inalámbrica

También merece la pena ver la situación de red compartida desde el punto de vista de la persona que ejecuta la red. Algunos proveedores de servicios de Internet venden el servicio para un solo ordenador, pero si el cliente compra e instala una puerta de enlace de banda ancha (a menudo como parte de un punto de acceso inalámbrico), no hay opción técnica para impedir que la conexión sea compartida entre varios ordenadores.

Éste es un tema peliagudo, pues si el ISP prohíbe expresamente compartir la conexión con varios ordenadores y lo hacemos de todas formas, estamos violando los términos de servicio. De todas formas, mucha gente no se preocu-

pa por esto porque saben que es algo indetectable y además no ven razón por la que usar varios ordenadores pueda perjudicar de algún modo al ISP.

El hecho de que mucha gente haga caso omiso de los deseos de los ISP nace porque los términos de servicio que prohíben el uso de múltiples ordenadores aplican una restricción legal donde no hay limitación técnica alguna. Además, la gente que entiende cómo funciona Internet sabe que los gastos del ISP corresponden a la cantidad de tráfico que atraviesa la conexión, no al número de ordenadores conectados. Se puede alegar que los ISP deberían cobrar las conexiones de Internet basándose en su uso, reflejando con precisión los gastos correspondientes. De ese modo no importaría el número de ordenadores o personas que utilizaran la conexión, porque el cliente sería responsable de pagar las cuotas de uso.

Nota

Algunos ISP por fin están captando la idea, permitiendo explícitamente compartir las conexiones de cierta forma, incluyendo varias máquinas (¡Verizon acaba de asociarse con Linksys para promover máquinas compartidas que utilizan puertas de enlace inalámbricas!) o incluso compartir el ancho de banda entre vecinos o en una comunidad.

Truco

La Electronic Frontier Foundation mantiene una lista de ISP que toleran o al menos no prohíben explícitamente compartir el ancho de banda en www.eff.org/Infra/Wireless_cellular_radio/wireless_friendly_isp_list.html.

No es asunto nuestro decirle qué debe pensar, ya sea como usuario potencial de redes inalámbricas abiertas o como alguien que puede compartir su conexión de Internet con otros a través de una red inalámbrica.

Baste decir que generalmente nos inclinamos por compartir conexiones y por modelos de empresa que reflejen los costes reales, pero cada situación es distinta; si comparte redes inalámbricas y cómo lo hace es una decisión que debe tomar usted.

Disputas por el territorio I: usuarios sin licencia y con licencia

Los estándares de redes inalámbricas que hemos debatido en este libro utilizan todos el espectro sin licencia disponible para el uso general de individuos

y empresas siempre que la potencia siga siendo lo bastante baja. (Vea los capítulos 3 y 8 para más información.)

Estos usos sin licencia de varias bandas del espectro podrían toparse con un pequeño problema: la FCC y otros cuerpos reguladores internacionales tienen usuarios autorizados con licencia, que pagan o al menos tienen garantizada la prioridad de acceso a la banda del espectro para sus propios propósitos.

Estos usuarios con licencia no pueden expulsar a otros usuarios arbitrariamente, pero si pueden demostrar que los equipos sin licencia producen interferencias con sus propios propósitos con licencia, la FCC o los cuerpos reguladores internacionales pueden requerir a los usuarios sin licencia que desconecten o modifiquen su uso.

La principal preocupación en esta área recae en la banda de 2,4 GHz del estándar 802.11b. Los radioaficionados son usuarios con licencia de la parte más baja del espectro y sus equipos de radio y también los nacientes servicios de televisión independiente que utilizan las mismas frecuencias, pueden interferir o requerir la desconexión de las redes inalámbricas.

Hasta ahora, sólo ha habido un incidente entre los usuarios sin licencia y con licencia de la banda de 2,4 GHz, que fue hace mucho tiempo y no está muy claro, implicando a un proveedor de servicios de Internet ahora difunto. De cualquier forma, el posible conflicto sigue estando presente y es una de las razones por las que las personas que establecen redes inalámbricas de largo alcance tienen que tener cuidado para no sobrepasar las limitaciones de potencia establecidas por la FCC. Eso no es difícil si nos atenemos al equipamiento de red estándar, pero no suponga que puede aumentar la potencia a su gusto sin sufrir ninguna consecuencia.

Disputas por el territorio II: aceptar interferencias

Un problema relacionado con el uso sin licencia del espectro es que la FCC no garantiza nada. Los aparatos que utilizan las bandas sin licencia no sólo deben procurar no provocar interferencias, sino que también deben ser muy tolerantes ante interferencias o conflictos con otros usos legítimos.

Dado que el equipamiento de red inalámbrica ofrece sólo opciones limitadas para configurar qué frecuencias se utilizan, hay una alta probabilidad de que surjan conflictos cuando las instalaciones aumenten en densidad. Hablando en plata: personas, compañías u organizaciones próximas pueden querer usar la misma banda del espectro. Esto no es un problema teórico: ya está empezando a suceder.

En agosto de 2002, el socio inalámbrico de espacio público de Starbucks, T-Mobile USA, se encontró dos veces en una situación embarazosa cuando un nuevo despliegue de red entró en conflicto con redes vecinas. En Portland, Oregon, la instalación predeterminada de T-Mobile utilizó el mismo grupo de frecuencias que había estado utilizando un grupo de red comunitaria establecido ya hacía tiempo. En San Francisco, en un establecimiento Starbucks donde T-Mobile, Starbucks y Hewlett-Packard pensaban hacer un gran anuncio acerca de servicios de red ampliados, hubo un conflicto con una franquicia de Apple vecina.

En ambos casos, los problemas se resolvieron. En Portland, T-Mobile instaló un software mejor que escogía canales no utilizados. En San Francisco, la franquicia de Apple no tuvo inconveniente en cambiar de canales para la conferencia de prensa de modo que su red no apareciera como opción predeterminada.

Estas anécdotas pueden parecer de poca importancia, pero perfilan un problema que puede terminar siendo más importante: sin una coordinación central, los conflictos de canales pueden reducir la calidad de los servicios de red inalámbrica. Nuevas versiones de especificaciones de red, así como nuevos tipos de redes seguramente reducirán el problema, como debatimos en la siguiente sección.

Redes comunitarias ¿bienes públicos o robo de servicios?

Fomentadas por los bajos precios del equipamiento de red inalámbrica, las redes comunitarias están surgiendo en todo el mundo, encontrándose algunas de las más conocidas en San Francisco Bay Area, New York City y Seattle. Es asunto personal de cualquiera dejar abierta una red inalámbrica para que todo el mundo que disponga de un portátil con el equipamiento apropiado pueda entrar si lo desea. ¿Pero cuál es la diferencia cuando se reúne mucha gente para hacer esto en beneficio público más en general?

Principalmente hay una diferencia: el área cubierta aumenta muchísimo y es posible utilizar la red inalámbrica en muchos otros lugares, no sólo en unos pocos. También empieza a ser posible que algunos hogares decidan utilizar sólo el acceso inalámbrico a Internet en lugar de usar módem, DSL o cable. Muchas de estas redes inalámbricas comunitarias tienen el objetivo de proporcionar una alternativa gratuita a los monopolios de comunicación que controlan el acceso a Internet.

Los grandes ISP más afectados por estas redes comunitarias difusas no ven con complacencia que sus clientes compartan las conexiones violando los términos de servicio, pero dudan en ser demasiado estrictos temiendo la mala publicidad y la insatisfacción de los clientes. Sin embargo, al aumentar el alcance de las redes comunitarias, los grandes ISP pueden reaccionar negando el acceso a clientes que les parece que están abusando de sus redes. Como queda dicho, una estrategia mejor sería cobrar cuotas basadas en uso, pero los ISP se resisten a hacerlo porque los clientes recelan de las facturas impredecibles.

Algunos analistas predicen que las redes comunitarias dirigidas por voluntarios no durarán mucho, pues cuando la gente se acostumbre a utilizarlas, empezarán a solicitar mejor calidad de servicios, aumentando los costes significativamente. Eso podría abrir un nuevo mercado para modelos de empresa que quisieran proporcionar acceso inalámbrico a Internet de forma fiable, aunque varias empresas que se lanzaron al campo pronto no consiguieron sobrevivir a la implosión de las punto com.

Estándares futuros

En el capítulo 3, presentamos varios estándares, incluyendo 802.11a, 802.11b, Bluetooth y HomeRF. Pero siempre hay más estándares a punto de surgir, a menudo ampliando y mejorando las ideas existentes. Aquí vamos a valorar algunos protocolos casi terminados de los que oirá hablar mucho en el futuro.

Nota *El objetivo de los estándares, naturalmente, es evitar que haya muchas soluciones incompatibles al mismo problema. Sin embargo, con el crecimiento de Internet, provocado en gran parte por estar basada en unos pocos estándares importantes, los estándares han surgido como hongos, provocando un comentario jocoso: "Los estándares son importantes y es magnífico que haya tantos entre los que elegir".*

Más rápido y compatible: 802.11g

Aunque el estándar 802.11b a 11 Mbps ofrece un rendimiento decente, los ingenieros implicados en el desarrollo del 802.11a pensaron que podía ser mejor e idearon el estándar 802.11g más rápido. El objetivo del 802.11g era usar la banda de 2,4 GHz y alcanzar al menos 22 Mbps de velocidad bruta. Todavía

más importancia tuvo en el 802.11g el objetivo de mantener la compatibilidad con el equipamiento 802.11 existente. Recuerde, el 802.11a utiliza la banda de 5 GHz y es por tanto incompatible con el estándar 802.11b de 2,4 GHz.

El estándar 802.11g, todavía en revisión a finales de 2002, se enfrentó a esas pruebas, aunque las disputas políticas en 2001 retrasaron su desarrollo. Dos grandes fabricantes de chips, Intersil (que hace la mayoría de los chips del equipamiento 802.11b) y Texas Instruments (un antiguo diseñador de chips, pero recién llegado al espacio 802.11b) se enfrentaron alegando que su método para introducir 22 Mbps de datos en un grupo de señales era mejor que el de su competidor. Al final, se alcanzó un compromiso por el que el método utilizado para codificar datos en señales de 802.11a a 54 Mbps fue adoptado como codificación obligatoria para 802.11g, mientras los métodos de Intersil y Texas Instruments se convertían en añadidos opcionales. Nadie cree que la codificación 802.11a pueda producir velocidades de 54 Mbps en la banda de 2,4 GHz, pero por razones políticas resultó un buen compromiso.

Texas Instruments ya ha lanzado su codificación como parte de una variante de set de chips que algunas compañías, incluyendo D-Link, están vendiendo, pero representantes de Texas Instruments le han dicho a Glenn que este set de chips (el ACX100) no será adaptable al estándar 802.11g cuando sea ratificado a mediados de 2003.

Nuestro consejo es que espere a la ratificación real y no compre equipamiento "turbo" o de "doble velocidad" que sólo funcione con otros dispositivos de la misma línea de productos. Además, debido al reciente cambio de la Wi-Fi Alliance del sello de compatibilidad de Wi-Fi, esperamos que se incorpore la interoperabilidad con 802.11g en el próximo sello Wi-Fi. Puede merecer la pena esperar a que aparezcan productos que incluyan el certificado Wi-Fi antes de decidirse a gastar mucho dinero en equipamiento 802.11g.

Calidad, seguridad y adaptabilidad: 802.11e, 802.11i y 802.11h

Tres de los muchos comités de los grupos de trabajo IEEE 802.11 también es probable que den a conocer los frutos de sus labores en 2003, solucionando varios problemas inherentes a los estándares 802.11a y 802.11b.

- 802.11e mejora la Calidad de servicio (QoS), que es la capacidad de una red inalámbrica para garantizar la transmisión coherente de los datos, como es necesario para enviar vídeo fluido o prestar soporte a voz a través de llamadas de teléfono IP.

- 802.11i corrige el sistema de cifrado WEP incompleto del 802.11b. Hemos explicado los problemas de WEP en el capítulo 6. Hasta que el 802.11i no esté implementado en muchos dispositivos, nuestras sugerencias del capítulo 6 le ayudarán a evitar problemas de seguridad.
- 802.11h garantiza que 802.11a sea legal en zonas de Europa que tienen restricciones en la banda de 5 GHz distintas de las que hay en los EE.UU. El 802.11h garantiza que sólo se emitirá en las frecuencias que no están siendo utilizadas por otros transmisores y que utilizará sólo la cantidad de potencia necesaria para transmitir un mensaje, en lugar de usar una potencia fija.

Estos tres estándares podrán ser integrados en los mismos dispositivos y es probable que los fabricantes de chips empiecen a prestarles soporte antes incluso de que sean ratificados formalmente.

Nota *Es posible que en el futuro podamos comprar equipamiento con la etiqueta "presta soporte a 802.11a, b, e, f, g, h e i". ¡Que Dios nos ayude!*

Tipo Bluetooth: 802.15.1-2002

Al debatir Bluetooth en el capítulo 3, mencionamos que el IEEE ha desarrollado un subgrupo de Bluetooth con interoperabilidad con la especificación de Bluetooth. La primera versión de este subgrupo se llama IEEE 802.15.1-2002. Intente decirlo rápido.

La presidencia del comité 802.15 confirmó a Glenn que las compañías podrán crear equipamiento que actuara como el de Bluetooth utilizando la especificación 802.15.1-2002 sin tener que pagar por los derechos o recibir la aprobación del Bluetooth Special Interest Group, que controla el estándar Bluetooth, la marca registrada y el logotipo. Dicho de otra forma, podremos encontrar equipamiento tipo Bluetooth que no utilice el nombre Bluetooth, pero que funcionará con otros aparatos Bluetooth existentes.

Camino de salida

Aunque algunos aspectos de las redes inalámbricas pueden parecer ya de ciencia ficción, las verdaderamente nuevas formas de pensar o trabajar deben

ser imaginadas antes de que se conviertan en realidad. No queremos presentarle productos de nuestra febril imaginación, sino que queremos mostrarle algunas ideas que empiezan a salir a la luz. Si estas ideas fructificasen, podrían transformar parte de lo comentado en el libro, si no todo. Pero no se inquiete, la mayoría de estos cambios no se producirán hasta dentro de unos años, si se producen.

Nuestras previsiones pueden no ser acertadas

¿Es muy probable que lo que decimos en esta sección sea cierto? Llevamos un tiempo prediciendo cosas y, como todo el mundo, hemos tenido razón y nos hemos equivocado. Aunque la mayoría de los que se dedican a hacer pronósticos no confiesan errores pasados, nosotros preferimos admitir nuestros errores e intentar evitar el adagio de George Santayana: aquellos que olvidan el pasado están condenados a repetirlo.

Glenn creyó una vez que:

- ***Las unidades Zip no tenían futuro:*** *¿Cómo podían las lentas, ruidosas e inclinadas a los errores unidades Zip de 100 MB de Iomega esperar competir con las fiables unidades de 45 MB SyQuest, que utilizaban rápidos y sólidos discos duros desmontables? Pues vaya. Iomega apenas pudo conseguir mantener la financiación para fabricar las unidades que estaba vendiendo por la gran demanda: el precio del éxito. Unos pocos años después de la aparición de las unidades Zip, SyQuest Tecnology estaba en bancarrota y Zip ha dominado desde entonces. Tal vez Glenn iba adelantado a su tiempo: la combinación de copiadoras de CD-ROM y DVD, la alta capacidad de las tarjetas de memoria CompactFlash y las conexiones a Internet de alta velocidad han provocado que el mercado de almacenamiento desmontable empiece a decaer. Ya ni siquiera recordamos dónde están nuestras unidades Zip.*
- ***El servicio DSL y de módem de cable llegará lentamente y será caro:*** *En 1997, Glenn predijo en Adobe Magazine que el alto coste de proporcionar a los clientes servicios DSL y de módem de cable con gran ancho de banda y alta velocidad evolucionaría gradualmente en áreas limitadas. Pensó que habría muchos problemas y el precio sería alto. Naturalmente, se equivocó en el*

despliegue: cerca del 15 por ciento de los hogares en los EE.UU. tienen ahora acceso de banda ancha por DSL o módem de cable. Pero tenía razón en el coste: de tres compañías DSL nacionales, dos cerraron sus puertas y una se recuperó por los pelos de la bancarrota. La mayoría de las compañías de teléfono y cable en los EE.UU. están en graves dificultades debido a fraudes o grandes recortes en los beneficios.

A favor de Glenn, también creyó que:

- ***La Web sería muy grande:*** *Glenn estaba codificando HTML en mayo de 1994 y fue cofundador de una de las primeras compañías de desarrollo Web al mes siguiente, con clientes en funcionamiento para octubre de ese año.*
- ***Que Sony eMarker fracasaría:*** *El eMarker era un dispositivo USB mal desarrollado. He aquí cómo funcionaba. Se suponía que lo tenías que llevar contigo en todo momento para que, cuando oyeras en la radio una canción que te gustara, pulsaras un botón en el eMarker. Todo lo que hacía el aparato era grabar la hora en que habías pulsado el botón para que cuando sincronizarás el aparato con el ordenador, pudieras saber qué canción había sonado. Además de la casi total inutilidad del producto, sólo funcionaba con las estaciones de radio Top-40..., no estaban incluidas las emisoras públicas o de música clásica. Glenn escribió sobre ello en una columna de un diario antes de la aparición de eMarker, con el título: "¿Obsolescencia? ¡Garantizada!".*

Adam pensó una vez que:

- ***Métodos de introducción de datos alternativos destronarían al teclado:*** *Ya fuera por reconocimiento de voz o de escritura manual o por un nuevo diseño, Adam pensó que el teclado tradicional estaba abocado a la desaparición. Pero ninguno de estos métodos de introducción de datos ha avanzado mucho. En retrospectiva, tiene sentido. Un nuevo diseño de teclado requeriría que hubiera nuevo hardware y la gente aprendiera a escribir de forma totalmente nueva; casi todo el mundo escribe rápido en el teclado tradicional. El reconocimiento de la escritura manual tiene problemas de precisión, siempre es más lento que escribir en el teclado tradicional (incluso en pequeños teclados) y requiere*

el uso de un stylus que se pierde fácilmente. ¿Y el reconocimiento de voz? Bueno, si ni siquiera otras personas entienden a veces lo que decimos, ¿cómo podemos esperar que lo haga un ordenador? Y encima está la cuestión del idioma.

- ***Los teléfonos móviles eran juguetes para ejecutivos:*** *Durante años, Adam no podía imaginar por qué alguien llevaría el teléfono móvil a todas partes. Sólo después de visitar a unos amigos en Australia, donde los teléfonos móviles los utiliza un porcentaje de la población mucho mayor (debido a la estrategia "el que llama paga" que hace que las llamadas entrantes sean gratuitas) cayó en la cuenta que cuando combinas un teléfono móvil con buena cobertura local, cuotas razonables y suficientes amigos que también tienen uno, terminas con un nuevo y útil método de comunicación. El punto de inflexión se produjo cuando sus amigos utilizaron los teléfonos móviles para concertar una cena en grupo con 11 personas en menos de 90 segundos.*

A favor de Adam, también pensó que:

- ***Internet cambiaría la vida de millones de personas:*** *En septiembre de 1993 se publicó el libro de Adam Internet Starter Kit for Macintosh, siendo el quinto libro publicado en el mundo que trataba de Internet. Terminó siendo autor (y coautor) de cuatro ediciones dedicadas a los sistemas Mac y tres a los sistemas Windows durante los siguientes tres años, vendiendo unos 600.000 ejemplares. Fue traducido al japonés, francés, alemán, chino y checo, y, a juzgar por los miles de mensajes de correo electrónico que Adam recibió durante los años en que el libro estuvo al día, cambió la vida de muchos de sus lectores.*
- ***Cue:Cat era una mala idea:*** *Hace varios años, Adam recibió por correo un explorador de códigos que tenía la forma aproximada de un gato. Intrigado por el aparatejo promocionado por una gran revista, investigó en qué consistía. La idea era que cuando leías una revista y te encontrabas con un anunció de un producto que te interesaba, pasabas el Cue:Cat por el código de barras del anuncio y el navegador cargaba automáticamente la página Web de la empresa en cuestión. La pura falta de comprensión de cómo funciona el mundo real por parte de la compañía que desarrolló el producto y lo envió a cientos de miles de usuarios desprevenidos*

era apabullante. Dejando de lado la suposición errónea de que la gente se interesa lo bastante por los anuncios para molestarse en coger el Cue:Cat para leer el código de barras en lugar de escribir un corto URL, ¿cuánta gente lee revistas sentada delante de un ordenador? Estamos hablando de una pérdida de millones de dólares de capital de riesgo.

Redes de datos celulares

El servicio de telefonía móvil está ampliamente disponible en áreas pobladas y los teléfonos móviles se han convertido en algo normal en casi todas las ciudades. Imagine que estas redes celulares pudieran gestionar datos, no sólo llamadas de voz. En lugar de estar limitados a puntos activos inalámbricos, podríamos enviar y recibir datos prácticamente en todas partes.

Naturalmente, las redes celulares ya llevan datos: la inmensa mayoría de redes celulares en todo el mundo gestionan ya llamadas digitales de voz con la "segunda generación" de tecnología de móviles (la primera generación era analógica). Con adaptadores especiales, muchos inconvenientes y paciencia, y una gran tolerancia a la facturación por tiempo de uso, podemos conseguir una velocidad de algunos miles de bits por segundo en estas redes celulares digitales.

Sin embargo, las redes de segunda generación se ven limitadas por el concepto de conexión: el servicio está disponible sólo cuando conectamos con él y hay que mantener una conexión continua para intercambiar datos (o hablar con alguien). Este concepto de conexión es estándar en las redes telefónicas, que generalmente reciben el nombre de *red de conmutador de circuito*, porque es como tener el propio cable (circuito) desde nuestro teléfono al de la persona a la que estamos llamando.

Teléfonos móviles: la próxima generación

Una tercera generación de redes celulares, a veces llamada 3G, pretende convertir los datos digitales en la principal aplicación de los aparatos celulares, con voz, multimedia y acceso a Internet entremezclado en distintos dispositivos, incluyendo teléfonos y adaptadores de red de ordenador, y también cabinas y nuevos aparatos electrónicos de consumidor y para automóviles. En el mundo 3G, los datos estarán disponibles en todo momento. Como la red celular pasa de ser una red de conmutador de circuito a una *red de conmutador de paquetes* como Internet (en la que los datos a transferir se dividen en paque-

tes que recorren distintos caminos), los teléfonos móviles y otros aparatos siempre podrán estar conectados a la red.

3G promete velocidades de entre una docena de kilobits y algunos megabits por segundo. Habrá disponible conexión de baja velocidad en áreas metropolitanas, autopistas y prácticamente en todas partes, mientras que las conexiones de velocidad más alta se alcanzarán sólo en las partes más pobladas de las ciudades o tal vez sólo dentro de edificios de oficina con transmisores internos.

Como los aparatos 3G están siempre en la red, la baja velocidad tampoco será obstáculo cuando, por ejemplo, se transmitan nuevos mapas al sistema direccional del automóvil o se descarguen los titulares de noticias al PDA. Estos servicios que envían información aprovecharán la ubicuidad de la red no exigiendo que nos mantengamos atentos mientras se transfieren los datos.

3G es tanto una realidad como una tecnología futura, pues hay empresas que ya están desplegando diferentes versiones en todo el mundo, principalmente en ciudades grandes. El precio sigue siendo demasiado alto, con las compañías de telefonía móvil deseando cobrar según la cantidad de datos transferidos en lugar de usar una tarifa plana.

El despliegue a escala nacional en los EE.UU. costara miles de millones de dólares y muchas compañías de telefonía europeas están haciendo equilibrios para no caer en bancarrota después de haber pagado colectivamente cien mil millones de dólares por el espectro gubernamental de licencias para operar servicios 3G, y eso antes de que esos servicios hubieran sido construidos.

Nota

Los EE.UU. y el resto del mundo no se han puesto de acuerdo sobre qué frecuencias usar para 3G, que significa que los teléfonos 3G de los EE.UU. no funcionaran en Europa o Asia y viceversa, a menos que los teléfonos presten soporte a las ocho bandas de frecuencias diferentes que utilizan todas las posibilidades. Algunos teléfonos actuales que aceptan transmisiones analógicas y digitales (uno de los varios tipos de 2G) pueden gestionar tres o cuatro bandas.

Medio paso atrás

Como puente para saltar el intervalo que hay entre donde nos encontramos en la actualidad y un sistema 3G totalmente desarrollado, se ha creado una versión intermedia de 3G, llamada 2,5G, que ofrece funciones que se encuentran entre las que ofrecen las generaciones segunda y tercera. No puede proporcionar las velocidades más altas de 3G, pero podrá llegar a decenas o centenares de kilobits por segundo, aunque usando todavía las frecuencias ya

pagadas y la mayoría de los equipos que constituyen las redes celulares actuales. El precio de 2,5G tiende además a ser menor, ya que las velocidades son demasiado bajas para provocar aumentos en los precios.

Los ingresos previstos en 2,5G y 3G se han visto amenazados por la proliferación de puntos activos inalámbricos. Muchos de estos puntos activos ofrecen un buen ancho de banda con tecnología Wi-Fi ya existente y tarifas planas en entornos humanos densamente poblados en los que quieren prosperar 2,5G y 3G. Los puntos activos no pueden ofrecer ubicuidad, pero ese puede ser el pequeño precio a pagar por las otras ventajas.

¿No podemos tenerlo todo?

Las compañías de telefonía móvil, cuando terminaba 2002, empezaron a enfrentarse con este dilema deseando impulsar la convergencia entre las redes celulares y las redes de puntos activos. Sprint PCS fue un temprano inversor de Boingo Wireless y T-Mobile USA ejecuta más de 1200 puntos activos en Starbucks, mientras que la sueca Telia opera varios cientos de puntos activos llamados colectivamente HomeRun en Escandinavia. En Japón y Corea del Sur, las compañías telefónicas dominantes piensan instalar miles de puntos activos en el próximo año.

Al mismo tiempo que se producen estas inversiones, pruebas y despliegues, se produce el continuo desarrollo de un adaptador de red ajustado a múltiples estándares llevado a cabo por muchos fabricantes de aparatos de redes inalámbricas. Este adaptador puede hablar 802.11a y 802.11b, y también lenguajes de datos celulares, como GSM (Sistema global de comunicaciones móviles) y GPRS (Servicio de radio de paquete global), dos estándares internacionales que están abriéndose paso en los EE.UU.

Una sola PC Card, probablemente con un módulo de autenticación personal parecido al de los móviles, podría permitir el paso de una red celular a un punto activo y de nuevo a la red celular sin interrumpir el acceso. O, quizá, el portátil conectará con el teléfono (probablemente a través de Bluetooth) para acceder a Internet.

Redes malla

Hemos mencionado las redes malla en el capítulo 2 como una de las topologías de red estándar. Las redes malla no establecen una conexión entre los nodos y un concentrador central ni encadenan los nodos uno con el siguiente. En realidad, surgen como efecto colateral de las transmisiones de radio,

pues cada transceptor de ondas de radio puede "ver" y "oír" a otros transceptores. Las redes malla pueden crear rutas oportunistas, en las que el enrutador del nodo envía los datos de la forma más eficiente entre los distintos nodos que puede ver. Esto no sólo reduce los puntos de atasco, también añade redundancia, garantizando que el corte de un solo nodo no provoca problemas en la red.

Nota

Se supone que Internet debe funcionar de ese modo, y a veces lo hace, pero el número de rutas posibles de Internet está limitado por las conexiones físicas reales entre redes y máquinas.

El equipamiento de red en malla hace posible ampliar una red inalámbrica o aumentar su ancho de banda general simplemente añadiendo más puntos de acceso a la malla. Siempre que uno de los puntos de acceso de malla tenga una conexión a Internet, todos los ordenadores conectados a la malla pueden usarla. Con las redes malla, tanto las comunidades remotas como las áreas urbanas muy pobladas pueden disfrutar de conectividad Internet más fiable, robusta y barata.

Hemos probado las redes malla al utilizar WAP11 y WET11 de Linksys como puentes de red. Aunque no incluyen protocolos de enrutamiento en malla para encontrar modos eficientes de dividir los datos, permiten crear redes totalmente inalámbricas con algunas estructuras con concentrador o en cadena, ampliando redes pequeñas para hacerlas más grandes sin usar cables o compañías telefónicas.

La logística detrás de las redes malla ha interesado a muchas mentes académicas brillantes y empezamos ya a ver que hay empresas que lanzan productos que se pueden usar para redes malla:

- **Nokia** (www.wbs.nokia.com): El sistema RoofTop de Nokia, diseñado para WISP, permite poner unidades en cualquier número de ubicaciones de suscriptor que pueden proporcionar ancho de banda al hogar o la organización y permitir el paso de tráfico entre varias unidades similares. RoofTop elimina la necesidad de una línea de visión entre el transmisor del WISP y cada casa conectada.
- **FHP Wireless** (www.fhpwireless.com): Un conjunto recién anunciado de productos de esta empresa se ha diseñado para reemplazar los caros enlaces punto a punto para proporcionar ancho de banda a cúmulos de red en lugares como campus universitarios o parques empresariales. Los enrutadores SmartPoint de la compañía encuentran la mejor ruta entre unos y otros y pueden cambiar automáticamente la ruta si falla una co-

nexión. Es posible conectar estos enrutadores a conexiones de alta velocidad y el sistema puede agregarse y distribuir ancho de banda como fondo común de recursos.

- **RoamAD** (www.roamad.com): Una pequeña compañía de Nueva Zelanda ha encontrado una forma de cubrir tres kilómetros cuadrados en el centro de Auckland con acceso 802.11b utilizando una combinación de puntos de acceso colocados inteligentemente, un fondo inalámbrico basado en malla (ancho de banda de una conexión de cable distribuido a los puntos de acceso) y un software especial que permite deambular sin que se interrumpa el acceso. RoamAD garantiza un mínimo de 330 Kbps, pero los lectores del registro Web de Glenn en Auckland reportan que generalmente obtienen mucho más de 330 Kbps. RoamAD espera tener en ejecución una demostración de 100 kilómetros cuadrados pronto.

Cuando la tecnología necesaria para convertir un punto de acceso inalámbrico normal en un punto de acceso capaz de participar en una red malla empiece a estar ampliamente disponible, esperamos que cada vez más puntos de acceso la incluyan. Eso a su vez provocará que los esfuerzos en redes comunitarias se muevan todavía más rápido, pues el esfuerzo de añadir un nodo a la red comunitaria será significativamente menor de lo que es ahora.

Ancho de banda inalámbrico aerotransportado

Como habrá visto si leyó nuestro debate sobre las redes inalámbricas de largo alcance, establecer una línea de visión es un gran problema. Encontrar una vista clara desde donde nos encontramos hasta una antena en algún edificio o torre altos a menudo es difícil y, en el caso de los propios ISP, averiguar dónde deben colocarse las antenas a menudo es frustrante, pues el objetivo es maximizar el número de posibles clientes que reciben la señal. Pero ¿y si la señal procediera de lo alto? Todo lo que se necesitaría sería entonces una antena con una vista del cielo para recibir las señales inalámbricas. No estamos hablando de utopías: tres compañías intentan que esto sea una realidad.

- **Angel Technologies** (www.angeltechnologies.com) planea operar su red HALO con aviones especiales de gran altitud que trazarán círculos sobre las áreas de servicio a 52.000 pies, muy por encima del tráfico aéreo comercial. Los aviones de Angel tendrán pilotos y despegarán y aterrizarán con horarios solapados para evitar la interrupción del servicio.

- **AeroVironment** (www.skytowerglobal.com) está colaborando con la NASA para desarrollar un aeroplano llamado Helios que puede actuar como una estación de telecomunicaciones aerotransportada móvil. A diferencia de los aviones de Angel Technologies, los aviones Helios no utilizarán pilotos y se alimentarán con energía solar, y volarán a una altitud de 60.000 pies. Se espera que los aviones Helios puedan permanecer en el aire unos seis meses o más (y para responder la pregunta obvia, utilizan células de combustible recargables para proporcionar energía durante la noche). Actualmente es un prototipo Helios el que mantiene el récord mundial de altitud para aviones propulsados por jet o hélice en 96.500 pies.
- **SkyStation International** (www.skystation.com) planea una estrategia diferente, optando por grandes zepelines sin tripulantes que volarán sobre una ciudad a 69.000 pies de altitud. También utilizará la energía solar para el equipo de red que proporcione la conectividad a los clientes.

Aunque estas compañías anuncian que empezarán a prestar servicio el año que viene (en el caso de SkyStation en 2002), parece que sus planes se van a retrasar, en parte por la pérdida de capital de riesgo en la industria de telecomunicaciones y en parte porque sigue habiendo cuestiones sin respuesta (algunas ni siquiera han sido planteadas). Por ejemplo, aunque los dos servicios sin tripulantes utilizan materiales muy ligeros, en ambos casos tienen que cargar con entre 250 y 1000 kilos de equipamiento, que es mucha carga para caer a tierra sobre una ciudad en caso de catástrofe. De cualquier forma, la idea de proporcionar servicios de red inalámbrica permanentes utilizando aviones o globos a gran altitud es innovadora y, si tiene éxito, será un gran cambio en el modo en que muchos nos conectamos con Internet.

¿Por qué no satélites?

Aunque la altitud de 52.000 ó 69.000 pies (16 ó 21 kilómetros) por encima de la superficie de la tierra que proponen estas compañías parece mucha, no es nada comparada con la altura que necesita un satélite geoestacionario, que debe orbitar en torno a la tierra a 36.000 kilómetros para mantener su posición fija (respecto al suelo; eso significa geoestacionario).

Nota

Glenn siempre recuerda que 36.000 kilómetros (22.300 millas) es la altura de la órbita geoestacionaria porque era la altitud a la que orbitaba

el satélite de la Liga de la Justicia de América. Todos los números de la Liga de la Justicia de DC Comics mencionaban esa distancia al presentar escenas en las que aparecía el satélite.

Si recuerda el papel de la pérdida de señal en el aire, puede ver por qué es más atractivo volar más bajo. Incluso los satélites no geoestacionarios deben orbitar a unos 320 kilómetros de altitud y se necesitan varios satélites de órbita baja para proporcionar cobertura constante.

Además, el largo viaje que deben hacer los paquetes desde el ordenador hasta el satélite, de nuevo a tierra hasta su destino, la respuesta hasta el satélite y desde allí abajo otra vez puede provocar que el rendimiento sea pobre.

Algunas compañías ofrecen o planean un servicio satélite-avión y Tenzing Communications (www.tenzing.com) permitirá que se use un servicio de satélite en aerolíneas o jets privados. Las velocidades que ofrece Tenzing serán bastante bajas (entre 56 y 128 Kbps por avión) pero no se necesita infraestructura adicional.

Banda ultraancha (UWB)

Las radios de hoy día funcionan de forma muy parecida a como lo hacía la primera radio de Marconi, utilizando una banda específica de frecuencias del espectro. Debido a esta realidad técnica, agencias gubernamentales de todo el mundo han establecido reglas que dictaminan quién puede usar qué partes del espectro, en qué áreas geográficas se permite la transmisión, cuánta potencia se puede usar y para qué propósitos. Estas regulaciones afectan a individuos, organizaciones privadas, ramas militares y agencias gubernamentales.

Detengámonos aquí un momento. Un concepto de las ciencias dela información llamado Ley de Shannon define las hasta ahora inmutables ideas sobre la cantidad de información que se puede codificar en un trozo de ancho de banda, que es, casi literalmente, la anchura de las bandas de frecuencias de radio utilizadas para la transmisión, medida en hercios, acoplada con el tamaño de la longitud de onda (frecuencias más altas proporcionan más espacio para codificar).

La Ley de Shannon dice que cuanto más ancho de banda se utiliza o mayor es la potencia de emisión, más información se puede introducir. Sin embargo, aumentar la potencia de emisión es un problema, pues nadie quiere verse frito si pasa delante de una antena.

Nota

El estándar 802.11a va una velocidad bruta de 54 Mbps: funciona en la banda de 5 GHz, frente a la banda de 2,4 GHz del 802.11b, y una frecuencia superior significa la capacidad de codificar más información por hercio. El estándar 802.11g puede al final ser capaz de obtener hasta 54 Mbps de la banda de 2,4 GHz, pero los expertos piensan que la banda de 5 GHz podría proporcionar espacio para futuros protocolos que ofrezcan más rendimiento incluso que el "modo turbo" registrado de 108 Mbps de algunas tarjetas 802.11a.

La comunicación de banda ultraancha (UWB) utiliza la Ley de Shannon para aprovechar la estrategia de espectro disperso tradicional, proporcionando gran ancho de banda para datos al tiempo que evita obstrucciones. En lugar de emitir continuamente pequeños trozos del espectro (entre 1 y 22 megahercios en los estándares que hemos comentado) saltando entre muchas frecuencias, un transmisor UWB emite millones de pequeños pulsos de picosegundos (un picosegundo es una billonésima de un segundo) de muy baja potencia a través de enormes franjas de ancho de banda: cientos o incluso miles de megahercios. El receptor extrae el contenido de la transmisión decodificando el ritmo de los pulsos.

Los defensores de UWB dicen que puede coexistir con todos los usos actuales, pues el equipamiento actual no será capaz de detectar las señales; las señales están muy por debajo del umbral del equipamiento actual y aparecerá como ruido incluso si se traspasa el umbral. UWB puede atravesar prácticamente cualquier objeto físico porque algunas de las frecuencias que utiliza son muy bajas y pueden penetrar en casi todo (este tipo de frecuencias es el que se utiliza para la comunicación con submarinos sumergidos). El equipamiento UWB también podrá coexistir consigo mismo, pues sería mucha casualidad que dos dispositivos transmitieran simultáneamente.

Como el receptor sólo tiene que determinar el ritmo de los pulsos, en lugar de decodificar las ondas de ninguna forma, UWB puede usar muy poca potencia, algo útil desde muchos puntos de vista, no siendo el menos importante el aumentar la vida de las baterías de portátiles. Una última ventaja es que, como los pulsos son tan rápidos, la comunicación UWB es muy segura; gran parte del interés que ha atraído UWB durante años ha procedido de aplicaciones militares.

El inconveniente de UWB es que, aunque ha sido probada en laboratorios, varios cuerpos reguladores del mundo, incluyendo la FCC, ven discutible que se pueda utilizar sin mucha más investigación. A los detractores de UWB les preocupa que las transmisiones puedan interferir con una gran variedad de

usos existentes, por la estrategia que utiliza UWB de transmitir en grandes bandas del espectro simultáneamente.

En 2002, la FCC dio un pequeño paso aprobando una versión de corta distancia, baja potencia y banda estrecha de UWB que podría presionar a Bluetooth, llevando 100 Mbps (o más) en lugar del rendimiento de 1 Mbps de Bluetooth. Pero es más probable que los transceptores UWB simplemente reemplacen a los transceptores Bluetooth con salto de frecuencias de 2,4 GHz, pero el resto de la estrategia de Bluetooth de nivel más alto permanezca igual.

Si se demuestra que puede funcionar, el potencial de UWB es enorme. Imagine que, en lugar de un alcance de unos cientos de metros y transferencias de datos de entre 11 y 54 Mbps de 802.11b y 802.11a, ¡pudiéramos tener un alcance de casi un kilómetro y transmitir datos a 1 gigabit por segundo! Si sucediera esto, el IEEE probablemente extendería su grupo de trabajo dedicado a lo inalámbrico para aplicar protocolos tipo Ethernet a UWB igual que ha hecho con tantos otros medios de transporte físicos. Una vez que tenemos rendimientos de gigabits por segundo, no hay razón para que las redes de área local sigan utilizando cables.

UWB también podría ayudar a los fabricantes de aparatos electrónicos proporcionando servicios de gran ancho de banda como vídeo y audio a cortas distancias. Imagine lo que sería poner un plato de televisión por satélite en el tejado con varios televisores recibiendo la señal dentro de la casa, ¡y sin usar cables!

No aguante la respiración mientras llega o no UWB, pero si lo hace, será algo grande. Para más información, visite el sitio Web Ultra Wideband Working Group en www.uwb.org.

Futuras sorpresas

No podemos predecir con certeza si cualquiera de las tecnologías o ideas que hemos comentado en este capítulo tendrá una oportunidad para sustituir al pan cortado en rebanadas como lo mejor que hay en el mundo, pero sí sabemos que el deseo de comunicarse con otras personas ha propulsado avances inimaginables en el pasado y volverá a hacerlo en el futuro.

Sean cuales sean las cuestiones específicas, siempre somos optimistas cuando se trata de tecnologías de la comunicación y tenemos la esperanza de que, en ediciones futuras de este libro, alguna sección de este capítulo desaparecerá porque habrá pasado del mundo de la fantasía a ser una realidad que tenemos en el salón de nuestra casa.

Índice alfabético

D

E

F

G

H

I

R

S

T

U

V

W

X

Y

Z

Introducción a las Redes Inalámbricas

802.11a, 802.11b, AirPort y AirPort Extreme de Apple

Adam Engst y Glenn Fleishman

El atractivo de las redes inalámbricas está en la combinación de flexibilidad, ubicuidad y distancia entre nodos que hace que dichas redes superen al prosaico mundo cableado.

Conectando un hardware sencillo y activando una conexión podemos caminar por nuestra casa u oficina, salir al patio o visitar un café manteniendo el acceso a la red todo el tiempo. De repente estamos utilizando las redes de una forma que hace una década parecía ciencia ficción.

Este libro ofrece todo lo necesario para preparar y poner en funcionamiento redes inalámbricas y convencionales, con detalladas instrucciones paso a paso y trucos para resolver problemas.

En esta obra encontrará:

- Una sólida base de conocimientos sobre el trabajo en redes tanto inalámbricas como convencionales.
- Información detallada sobre 802.11b, 802.11a, 802.11g, y otras tecnologías.
- Detalles específicos para usuarios de Windows y Macintosh (AirPort).
- Prácticos consejos sobre la protección de las redes inalámbricas.
- Sugerencias y trucos para encontrar y utilizar redes inalámbricas durante los viajes.

ANAYA MULTIMEDIA
http://www.AnayaMultimedia.es

NIVELES: Iniciación; Básico; ✓ Medio; ✓ Avanzado; Profesional/Experto

TIPO DE LIBRO: Referencia / Aprendizaje

TEMÁTICA: Internet

2315503
ISBN 84-415-1561-1
9 788441 515611