point's settings. The setup page is protected by a username and password, but the username and password are initially set to default values that are easy to guess. Anyone who gains access to your network can then log in to the administrative page and take control of your network.

- **Hide the SSID.** A simple step you can take to secure your wireless network is to disable the automatic broadcast of your network's SSID. That way, only those who know of your network's existence will be able to access it. (Securing the SSID isn't a complete security solution, so you shouldn't rely on it as your only security mechanism.)
- **Disable guest mode.** Many access points have a guest-mode feature that enables client computers to specify a blank SSID or to specify "any" as the SSID. If you want to ensure that only clients that know the SSID can join the network, you must disable this feature.
- **Use MAC address filtering.** One of the most effective ways to secure a wireless network is to use a technique called *MAC address filtering.* MAC address filtering allows you to specify a list of MAC addresses for the devices that are allowed to access the network or are prohibited from accessing the network. If a computer with a different MAC address tries to join the network via the access point, the access point will deny access.

  
  TIP

  MAC address filtering is a great idea for wireless networks with a fixed number of clients. If you set up a wireless network at your office so that a few workers can connect their notebook computers, you can specify the MAC addresses of those computers in the MAC filtering table. Then other computers won't be able to access the network via the access point.

  MAC address filtering isn't bulletproof, but it can go a long way toward keeping unwanted visitors off your network. Unfortunately, MAC address filtering is also pretty inconvenient. Whenever you want to grant access for a new device, you'll have to find out that device's MAC address and add it to the list of permitted devices.
- **Place your access points outside the firewall.** The most effective security technique for wireless networking is placing all your wireless access points *outside* your firewall. That way, all network traffic from wireless users will have to travel through the firewall to access the network.

  As you can imagine, doing this can significantly limit network access for wireless users. To get around those limitations, you can enable a virtual private network (VPN) connection for your wireless users. The VPN will allow full network access to authorized wireless users.

  Obviously, this solution requires a bit of work to set up and can be a little inconvenient for your users, but it's an excellent way to fully secure your wireless access points.