CHAPTER 19

Snow Leopard Networking

The Mac is known for making it easy and safe to get online. Under the hood, Mac OS X has all the networking power of UNIX. The Internet and UNIX go way back, growing up together. You might even say they were made for each other. Like any UNIX system, Mac OS X comes with a full set of networking tools built in:

- **Firewall software**: For keeping your computer safe on the Internet in an effective, easy-to-use way
- **Monitoring tools**: For keeping an eye on what your computer is doing, online and off
- **Network utilities**: For inspecting your packets from the UI or the command line
- **AirPort utilities**: For setting up and managing wireless networks and shared resources

**Note** This chapter assumes you’ve already managed to connect your computer to the Internet. If you haven’t gotten that far, see Chapter 9.

Setting Up the Firewall

The Mac has a well-deserved reputation for being safe on the Internet, but that doesn’t mean you should be careless. The simplest thing you can do is set up the built-in firewall.

The firewall in Mac OS X arbitrates incoming connection requests based on the requested port, the source, and the intended recipient. It’s not unlike a lobby security guard in that it doesn’t limit the ability of packets to leave; it cares only about things trying to come in from the outside.

To change your firewall settings, launch System Preferences by selecting System Preferences... from the Apple menu. Then click the Security preference pane, and select the Firewall tab, as shown in Figure 19-1.

In order to be effective, security has to be simple. The firewall in Mac OS X is about as simple as a firewall can be, but it’s backed by Snow Leopard’s solid UNIX underpinnings.
On the BSD level, Mac OS X uses `socketfilterfw`. This is both simpler and more effective than older port-based filters. Aside from eliminating the hassle of manually configuring ports, the socket filtering method is more accurate, because it filters packets based on where they are going, rather than which port they are coming into.

Networking gurus might argue this approach is less flexible, and therefore less effective, than `ipfw`'s rulesets. With rulesets, it’s easy to block a specific protocol from a specific IP address.

As is typical of Mac OS X, the majority simple case prevails. The minority edge case is left to its own device. If you’re smart enough to care, you’re smart enough to install your own firewall.

**Note** There are a few times when it might be necessary to leave your firewall down. If you’re behind a dedicated firewall, it might be redundant. If you’re having trouble connecting to another machine, you might need to temporarily disable the firewall. Finally, your network administrator, who has the last word on network configuration, might ask you to keep it open.

Snow Leopard’s firewall requires no configuration. If you enable a network service on the Sharing panel in System Preferences, that service will automatically be added to the firewall’s list of allowed applications. Applications that have been code signed to prevent tampering are also allowed to access the network. Applications that have not been code signed will ask permission the first time they try to access the network, as shown in Figure 19-2.