Chapter 1: Networking Your Macs

In This Chapter

- **Creating a wired network**
- **Creating a wireless network**

If you have multiple Macs in the same place, you might find it convenient to connect your Macs to a network. A *network* allows multiple computers to share files and other resources like printers or backup hard drives. Although you could copy a file on a USB flash drive, plug it into another computer, and copy the files onto the second computer or print using the second computer's printer, such an approach (dubbed *sneaker net*) is tedious and inconvenient. However, when multiple computers connect to a network, they can share files almost as quickly and easily as copying a file from one folder to another.

Creating a Wired Network

The simplest wired network just connects two computers together using either a FireWire cable or a cable that conforms to a networking cable standard called *Ethernet*. Only the MacBook Air and two short-lived MacBook models shipped without a FireWire port. Every Mac (except the MacBook Air, again) has an Ethernet port, so if you plug a FireWire cable or Ethernet cable into the FireWire or Ethernet ports of two Macs, you'll have a simple network, as shown in Figure 1-1.

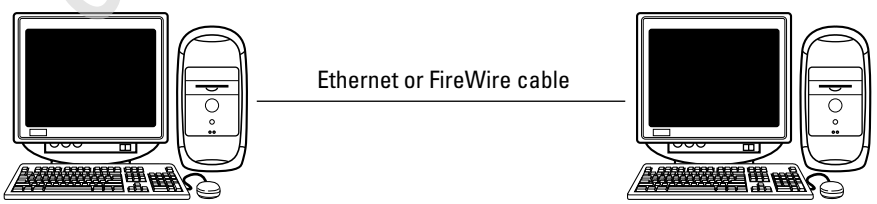

Figure 1-1: A simple network connects two Macs via a FireWire cable or an Ethernet cable.

Ethernet cables are often identified by the speeds that they can send data. The earliest Ethernet cables were Category 3 (or Cat 3) cables and could transfer data at 10 megabits per second (Mbps). The next generation of Ethernet cables was Category 5 (Cat 5) cables, which could transfer data at 100 Mbps. Category 6 (Cat 6) cables transfer data at 1,000 Mbps or one gigabit per second (Gbit/s). With networking, speed is everything and Category 6a (Cat 6a) and Category 7 (Cat 7) transfer data at 10 Gbit/s. Category 7a reaches transfer speeds of 100 Gbit/s.

Connecting two computers can be convenient for sharing files, but most networks typically consist of multiple computers connected together. Such a large network of multiple computers allows different computers to share files with each other.

Because it's physically impossible to connect more than two computers together with a single cable, networks typically use something called a *hub.* Each computer connects to the hub, which indirectly connects each computer to every other computer also connected to the hub, as shown in Figure 1-2.

An improved variation of a hub is called a *switch.* Physically, a hub and a switch both connect multiple computers in a single point (as shown in Figure 1-2).

With a hub, a network acts like one massive hallway that every computer shares. If a bunch of computers transfers data at the same time, the shared network can get crowded with data flowing everywhere, slowing the transfer of data throughout the network.

With a switch, the switch directs data between two computers. As a result, a switch can ensure that data transfers quickly regardless of how much data the other computers on the network are transferring at the time.

A variation of a switch is a *router,* which often adds a firewall. Because routers cost nearly the same as ordinary hubs and switches, most wired networks rely on routers. So if you want to create a wired network of computers, you need

- ✦ Two or more computers
- ✦ A network switch or router
- ✦ Enough cables to connect each computer to the network switch or router

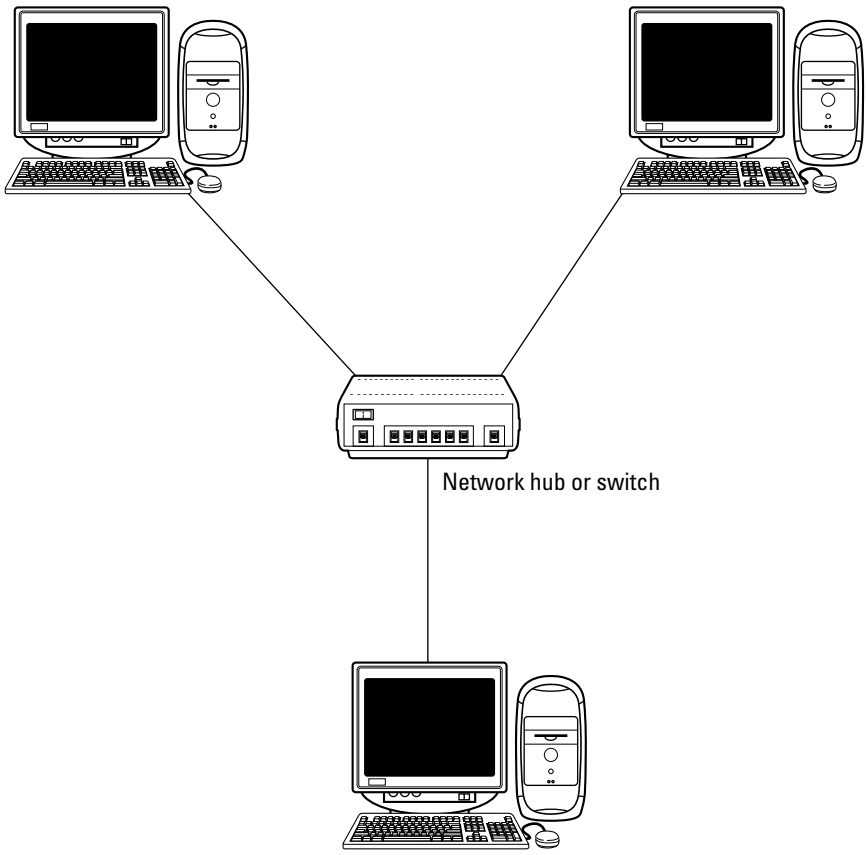

Figure 1-2: A hub or switch allows multiple computers to connect together in a network.

The speed of a wired network depends entirely on the slowest speed of the components used in your network. If you plan to use Cat 6 cables in your network, make sure your network switch is designed for Cat 6 cables. If not, you'll have the fastest Ethernet cables connected to a slow network switch, which will run only as fast as the slowest part of your network.

Creating a Wireless Network

Because wired networks can be inflexible, more people set up wireless networks instead. Essentially a wireless network is no different from a wired network, except (as the name implies) there are no wires. Wireless networks are generally a bit slower than wired networks.

Because of physical obstacles, wireless networks don't always reach certain parts of a room or building, resulting in "dead spots" where you can't connect wirelessly. Walls or furniture can disrupt the wireless signals.

All you need is a device called an *access point,* which can plug into your existing wired network. This access point broadcasts a signal that other computers can receive, creating a wireless connection to the network, as shown in Figure 1-3.

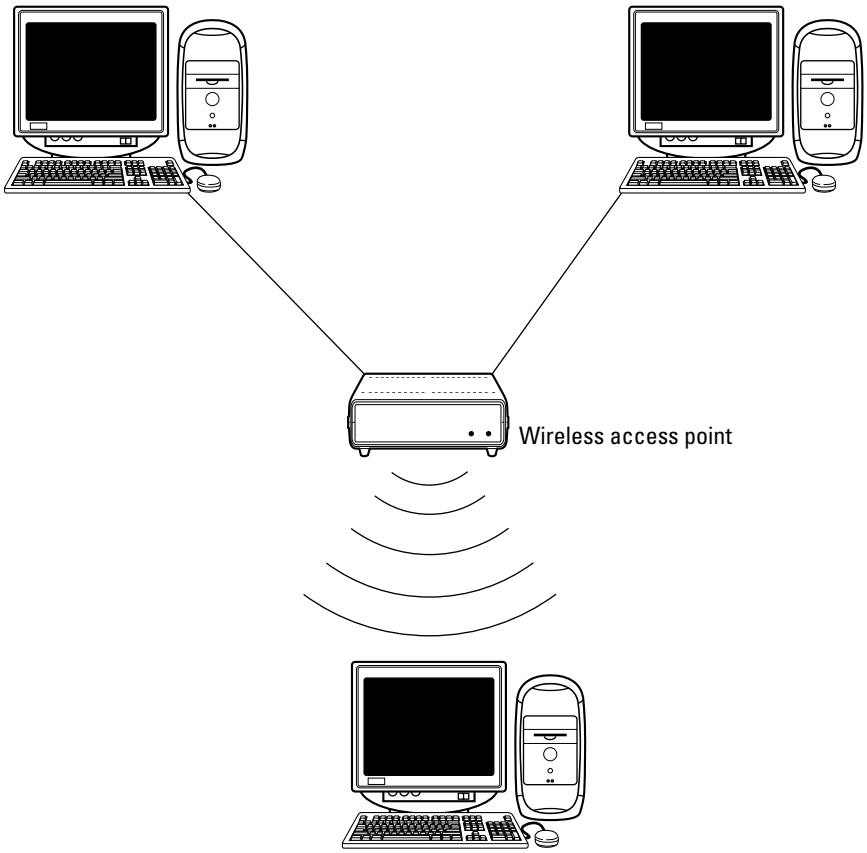

Figure 1-3: A wireless access point extends the reach of a wired network.

Your router may have wireless capabilities so you can connect the computer or printer that stays in one place to the router with an Ethernet cable but connect to the wireless network connection on your MacBook to work from your lawn chair in the garden, or from a desktop Mac located in another room in the house. Some cable and DSL modems come with built-in Wi-Fi transmitters, which means one device does the job of two if you choose to use a separate Wi-Fi router to connect to your cable or DSL modem.

The hazards of wireless networking

To access a wired network, someone must physically connect a computer to the network using a cable. However, connecting to a wireless network can be done from another room, outside a building, or even across the street. As a result, wireless networks can be much less secure because a wireless network essentially shoves dozens of virtual cables out the window, so anyone can walk by and connect into the network.

The practice of connecting to unsecured wireless networks with malicious intentions is *war driving* (also war flying, war walking, or war boating, depending on how you move around). The basic idea behind war driving is to drive around a city and keep track of which areas offer an unsecured wireless network. After getting connected to an unsecured wireless network, an intruder can wipe out files, capture personal information or interfere with the network's operation.

When creating a wireless network, you can make your network more secure by taking advantage of a variety of security measures and options. The simplest security measure is to use a password that locks out people who don't know the password. For further protection, you can also use encryption.

Encryption scrambles the data sent to and from the wireless network. Without encryption, anyone can intercept information sent through a wireless network (including passwords). Still another security measure involves configuring your wireless network to let only specific computers connect to the wireless network. By doing this, an intruder cannot gain access to the wireless network because his or her computer is not approved to access the network.

Ultimately, wireless networking requires more security measures simply because it offers potential intruders the ability to access the network without physically being in the same room, house, or building. Wireless networks can be as safe as wired networks — as long as you turn on security options that can make your wireless network as secure as possible.

The difference between an access point and a router is the router is at the center of the network, allowing the computers to share printers, Internet connections, and external hard drives. The access point is what allows the computers with wireless capabilities to connect to the network from across the room, from another room, or even outside on the porch, providing the wireless signal is strong enough to reach wherever you are with your Mac.

For more information about wireless networking, pick up a copy of *AirPort and Mac Wireless Networks For Dummies,* by Michael E. Cohen (Wiley).

Not all wireless networks are alike. The earliest wireless networks followed a technical specification called 802.11b or 802.11a. Newer wireless equipment followed a faster wireless standard called 802.11g, and the latest standard (at the time of this writing) is 802.11n.

When setting up a wireless network, make sure your router and/or wireless access point use the same wireless standard as the built-in wireless radio or wireless adapter plugged into each of your computers. All new and recent Macs connect to Wi-Fi routers that use one or up to all four types of the wireless network standards.

You can buy any brand of wireless access point or router to create a network, including Apple's Airport Extreme Base Station. Any router you choose will come with specific software and instructions for setting up your network. The basic steps are to

1. Name your network and base station so computers on the network can then find and connect to your Wi-Fi network.
2. Set up a password. (WPA2 provides the most security.)
3. Define how you connect to the Internet. (You may need information from your Internet Service Provider for this step.)
4. Add printers and/or external hard drives.

After you physically connect your wired network or configure your wireless network, you might still need to configure your Mac to work on your network if you want to share files and printers, which is the topic of Book VIII, Chapter 2.