Any computer—and more to the point, a Mac OS X Server—receives a barrage of traffic over the network interfaces. You can use two services in particular to control this traffic. The first is the router, and the second is the firewall. A router is a device on your network that chooses the paths between devices that network traffic takes; in short, a router connects networks and then manages the logic of how data is sent between them. A firewall, on the other hand, controls the various types of data that are allowed to communicate over those paths. In many cases, a firewall and a router are one device, although they can be two separate devices. This chapter first covers setting up the server as a router and then covers leveraging the firewall to restrict access to the server.

Before getting started, though, we’ll give you a very basic overview of what TCP/IP is. Short for “Transfer Control Protocol/Internet Protocol,” TCP/IP is the foundation of practically every modern network. TCP/IP is a collection of protocols that connect computers between one another in a modular (or layered) fashion. Computers each get an IP address, and each application or protocol that interconnects computers uses a unique port for communication.

Communications are then broken down into packets, which contain information about the sender, information about the recipient, and instructions for reassembling the original communication, in addition to the actual content of the communication, which is referred to as the packet’s payload. Packets also contain return information if the packet is traversing a router, meaning it is destined for a location outside your local network, or local area network (LAN). This becomes the foundation for NAT, which we will describe in further detail later in this chapter.

Using Mac OS X Server as a Router

One of the services that receives little to no attention in literature on Mac OS X Server is using the server as a default gateway for your environment. This primarily is because most environments don’t actually use Mac OS X Server as a router. A number of other
products are more suitable to the task because they are more feature rich and come at a much lower price point than an Apple computer running Mac OS X Server.

Before you decide to use Mac OS X Server as a router, it’s worth noting why you are going to do so. As a basic function, a Mac OS X Server is capable of acting as a router in order for other hosts on your local network to access systems outside your network, most notably web and mail servers on the Internet. But before you purchase Mac OS X Server as a dedicated gateway to the Internet, consider some of the tasks that a more advanced router makes more readily available:

- **Stateful packet inspection**: The inspection of packets to make sure that they conform to the standards of what should be in a packet and also do not contain any malicious content.
- **Failover**: Automated failover between multiple external network connections.
- **Logging**: Advanced logging facilities, such as a list of every connection that has been made on the device, open connections, and so on.
- **Accessible control options**: Granular control of port forwards from a graphical interface.

A number of other features are often leveraged for consumer- or prosumer-grade routing and firewalling appliances; although many environments lean on these features, if you don’t need them or if you have a specific use of the routing in Mac OS X Server, then you will find the gateway services in Mac OS X Server to be suitable. If this matches your need, then read on, because we’ll cover how to set up Mac OS X as a router, obtain basic functionality, and even forward a few ports.

### How Network Address Translation Works

Short for “Network Address Translation,” NAT is a core concept in understanding routing. NAT is the technology that hides all of your computers behind a single public IP address. Here are some basic concepts that will help you understand how NAT and routing work:

- **A subnet mask** (or netmask) on each computer instructs the network stack for that system as to what computers are on the local network. The subnet mask indicates the size of the network; anything within that subnet mask is considered local traffic, and anything outside the subnet mask is not.

- Traffic destined for computers on the local network does not traverse the **default gateway**, or router, and therefore does not use NAT. Network requests destined for IP addresses that are not on the local network use the default gateway to communicate with the computers that run those services.