Take Control of Your AirPort Network

by Glenn Fleishman

Table of Contents (Version 1.0)

Check for Updates
Click Here to Look for
Updates to This Ebook

Help a Friend Take Control!
Click Here to Get 10% Off
for You and Your Friend

$5

TidBITS Electronic Publishing

Take Control of Your AirPort Network

Published by:

TidBITS Electronic Publishing
50 Hickory Road
Ithaca, NY 14850 USA
http://www.tidbits.com/takecontrol/

July 2004. Version 1.0

Take Control ebooks help readers regain some measure of control in an oftentimes out-of-control universe. Take Control ebooks also streamline the publication process so information about quickly changing technical topics can be published while it's still relevant and accurate. Send comments about this, or any, Take Control ebook to tc-comments@tidbits.com.

This ebook does not use copy protection because copy protection makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. (Use the Help a Friend offer on the cover page of this ebook to give your friend a discount!) Your support makes it possible for future Take Control ebooks to hit the Internet long before you'd find the same information in a printed book. Plus, if you buy the book, we will contact you should a free update become available.

Although the author and TidBITS Electronic Publishing have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this ebook is distributed "As Is," without warranty of any kind. Neither TidBITS Electronic Publishing nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

Any trademarks, service marks, product names or named features that appear in this ebook are assumed to be the property of their respective owners.

INTRODUCTION

Apple introduced wireless networking to the world with AirPort in 1999. Although corporations had been using forms of wireless networking for warehouse tracking and to connect buildings in a large campus, the cost was high, speeds were low, and complexity was manifest. Other companies were selling similar wireless hardware in 1999, but Apple's product shot off the shelves due to its extremely low initial price—especially in comparison to the competition, its simple configuration interface, and its excellent performance.

AirPort came out of the same approach that allowed Apple to ship the iMac the year before: taking parts that were available and standard, and combining them in a unique package that provided more value than any of the parts.

The AirPort Card fit into a special slot in Macs; its stand-alone, central coordinating hub was called the AirPort Base Station. The original AirPort line was superceded and supplemented in 2003 with AirPort Extreme, a faster but backward-compatible version. Most recently, Apple added its least-expensive base station ever, the AirPort Express, which bundles several features into a unique package for home and traveling users.

Despite Apple's 5-year history with wireless networking and the general excellence of their software and support, I still find the same questions asked again and again. This book addresses these concerns and gives you tips that should save time, improve security, extend range, and give you a technical edge when working with AirPort networks.

Although the title of this book references AirPort, the book not only covers AirPort, AirPort Extreme, and AirPort Express equipment, but also includes many tips about comparable equipment or connecting to non-AirPort networks or from non-AirPort equipment.

I start with purchasing decisions, move through installation and configuration, give advice on the common task of extending the range of a home or small-office network, and finish with how-to information on security for those who want to make their AirPort networks free from interception.

AirPort Networking Quick Start

This book takes you through the process of deciding which equipment to purchase and configuring it to meet your needs, including how to set up larger networks and how to secure your networks against snooping and interception.

Wireless basics:

- Get a quick grounding in wireless terminology and technology. See Wireless Basics.

Pick a base station:

- Consider whether an AirPort Extreme Base Station or AirPort Express Base Station is the best choice for the money. See Choosing AirPort Extreme or AirPort Express.
- Disregard buying an older AirPort Base Station. See Don't Buy Older AirPort Base Stations.
- Learn the pros and cons of using a software-based base station. See Consider a Software Base Station.
- Pick a cheaper alternative wireless gateway if you don't need AirPort's unique features. See Use a Wireless Gateway Alternative and Buy Subsequent Access Points More Cheaply.

Install your base station:

- Pick the Right Place by testing signal strength.
- Successfully configure the base station to connect to your ISP. See Solve Common Internet Connection Problems.
- If desired, set up dynamic addressing. See Take Control of Dynamically Assigned Addresses.

Improve coverage area and range:

- Add access points for roaming. See Add Additional Access Points for Roaming.
- Bridge Wirelessly among access points, in order to avoid wiring.

- Extend your network with a data network over your home electrical system. See Extend with HomePlug.
- Consider adding an antenna. See Add an Antenna.
- Learn how to Solve the Titanium PowerBook Range Problem.
- Solve interference problems by talking to your neighbors. See Talk to Your Neighbors.

Secure your network:

- Decide if you need encryption. See Likelihood, Liability, and Lost Opportunity.
- Apply encryption using an older or a newer method. See Protect with WEP and Protect More Easily with WPA.
- Choose to encrypt just data from applications instead of the whole wireless network. See Deploy Application Security.

Future Updates

TidBITS Electronic Publishing may publish minor updates to this ebook to account for errata, software updates, new information, or other reasons. Such updates will be offered at no extra charge; notification will go to the email address you gave at the time of purchase. You can also click here to check for updates.

WIRELESS BASICS

Let's quickly run through some wireless basics to set the stage for what follows.

You might have heard of AirPort and AirPort Extreme by the name Wi-Fi, which is a certification guarantee for which The Wi-Fi Alliance trade group owns the rights and controls the testing. Wi-Fi loosely means *wireless fidelity*, in the sense of *faithfulness*: devices with Wi-Fi stamped on them work with other Wi-Fi devices, or are faithful to one another. I use the terms, "AirPort," "AirPort Extreme," and "Wi-Fi" interchangeably unless the distinction is important.

AirPort and Wi-Fi networks need two parts: a wireless adapter that connects inside or outside a computer or a handheld device, and a wireless hub, like an Ethernet switch, that's known generically as an "access point" or "wireless gateway" depending on its features, but is called a "base station" in the Mac world.

The wireless adapter uses client software on the computer or handheld device to connect to a specific base station after a user selects the base station from a list or enters its name. Mac OS X allows base-station selection from the AirPort menu in the menu bar, the AirPort tab of the Internet Connect program (located in the Applications folder), and the AirPort tab assigned to the AirPort adapter in the Network preference pane. (If you're using a non-AirPort card, you may have to use a separate preference pane supplied by the card's maker or a third-party company providing a Mac OS X driver.)

When a wireless card connects to a base station, it's called *association*. If a base station has encryption enabled, then you must enter an encryption key exactly as it was entered on the base station in order to join the network after associating with the base station.

Once a card associates with a base station, Mac OS X can carry out its next steps, such as automatically requesting an Internet protocol (IP) address using DHCP, and sending data over the wireless network.

TIP If you have no background in Wi-Fi and need more fundamentals, you can turn *to The Wireless Networking Starter Kit*, a 500-plus-page book written by Adam Engst and me that's available in electronic and print editions from http://wireless-starter-kit.com/.

Early Airport

The original, slower form of AirPort and Wi-Fi is known as IEEE 802.11b. It sounds less technical when you learn that IEEE is the Institute of Electrical and Electronics Engineers; 802 is the number of their group that makes standards for local area networks (LANs); 11 covers wireless LANs; and, finally, "b" is the name of the task group that created the 11 megabit-per-second (Mbps) standard.

The original AirPort system comprises an AirPort Card, which fits into an internal card slot in all AirPort-capable Macs (the slot looks almost exactly like a PC Card slot); and an AirPort Base Station, which looks like a small, gray ("graphite" original) or white ("snow" revision) flying saucer. It has three status lights on its front top.

The "graphite" base station has a single Ethernet port and a built-in modem. The "snow" base station added a second Ethernet port, which increased security and flexibility by allowing you to separate a LAN from a broadband connection via a cable or DSL modem.

Airport Extreme and Airport Express

In 2003, Apple added the AirPort Extreme system. Airport Extreme uses an AirPort Extreme Card (it fits in a mini-PCI-like internal slot) and the AirPort Extreme Base Station (**Figure 1**), which now comes in two configurations, discussed in the next section, Pick a Base Station.

FIGURE 1

The AirPort Extreme card (left) and the AirPort Extreme Base Station (right).

AirPort Express, released in July 2004, is similar to AirPort Extreme, but it supports fewer users and can stream music to your stereo.

AirPort Extreme and AirPort Express both use the 802.11g standard, which is also part of the Wi-Fi specification. 802.11g is backward compatible: it incorporates the entire 802.11b spec and adds speeds up to 54 Mbps.

TIP There's another IEEE standard that's part of some Wi-Fi devices, too, called 802.11a. Where 802.11b and g operate in the 2.4 gigahertz (GHz) part of the electromagnetic spectrum and are compatible forward and backward with one another, 802.11a uses the 5 GHz band. Because of this, you can't use 802.11a and b/g together. Some manufacturers sell combined a/b/g cards that can use any of the Wi-Fi standards, but you'll be hard pressed to find 802.11a in use.

With the basics out of the way, let's work through picking the best base station for your needs.

Pick a Base Station

"You can paint it any color as long as it's black," is allegedly (but apparently not in actual fact) Henry Ford's statement about choice with the Model T. Apple's similar quotation on Wi-Fi before June 7, 2004, was, "You can have whatever you want as long as it costs $200 or more." Then Apple introduced AirPort Express, and changed the face of home Wi-Fi.

In this section, you can find out whether you really need the AirPort Extreme or AirPort Express Base Station, or whether older or alternative models could serve you better for less cost—or whether an old Mac can avoid the problem altogether. (I'll foreshadow the answer: it's often "yes.")

Choosing AirPort Extreme or AirPort Express

Apple has always charged a premium for their AirPort gear because of its ease of use and unique features. That premium was hard to swallow in 2003 and early 2004 when an Extreme base station cost $200 or $250, whereas comparable equipment ran for as little as $50 to $80 from companies other than Apple.

In the initial, unreleased draft of this book, I listed many reasons why you shouldn't choose Apple's hardware to build your AirPort network unless you had a few very particular needs. Apple's announcement of the AirPort Express Base Station changed all that. With a price tag of $129, the Express has all the features needed by home users with a few extras you can't get anywhere else or at anywhere near the same price.

Note AirPort Express didn't ship while I was writing this edition of the book, but I had plenty of details about the product. When the base station ships in July 2004, I plan to release a free update to this book as quickly as possible. If you're still reading an older version of this title, please click the Check For Updates button on the cover of this book or click here to access update information.

The AirPort Extreme Base Station now comes in two models which, as is Apple's unfortunate wont, have no model numbers. (You can find their part numbers if you hunt.) The AirPort Express Base

Station comes in a single model with an extras kit you can purchase separately. AirPort Express replaced the least-featured AirPort Extreme model. **Table 1** explains how to tell them apart.

Table 1: Differentiating Current AirPort Base Stations

Model	What distinguishes it	Users	Price
AirPort Express	Audio jack (controlled via iTunes); barely larger than a power adapter; one Ethernet port	10	$129
AirPort Extreme (modem)	Dial-up modem; antenna jack; two Ethernet ports	50	$199
AirPort Extreme (plenum)	Plenum rating for fire safety; Power over Ethernet (PoE); antenna jack; two Ethernet ports	50	$249

Commonalities

All current AirPort base stations have a USB port that allows you to share any of a long list of supported printers among connected Macintosh users with at least Mac OS X 10.2.7 or Windows users running XP or 2000.

NOTE Some TidBITS readers have asked me if the USB port could share a hard drive with a USB interface. For now, no: it handles printers only. And it's likely that, for cost reasons, the port supports only the USB 1.1 interface, which has a maximum speed of 12 Mbps.

If you'd like to connect a USB hard drive to a network, consider the Linksys Network Storage Link (NSLU2). It hooks a USB 1.1 or 2.0 drive—including USB memory drives—to an Ethernet network for $99. Mac OS X 10.2 and 10.3 can connect to it using Samba, as can Linux and Windows.

If you're using older networked printers or Macs, you may need AppleTalk support. These base stations offer that, but so do some other manufacturers, including long-time Apple supplier Asanté. Most users have weaned themselves off pure AppleTalk, and so this probably isn't a determining factor when you're deciding what to buy.

The AirPort base stations support wireless bridging, which allows them to connect to each other without wires to form a larger network. Apple's units are some of a handful of devices that can serve wireless clients while bridging to other base stations. (See Bridge Wirelessly.)

Now let's look at the differences.

AirPort Express

In features, AirPort Express is broadly similar to AirPort Extreme: it runs at the same speed, but only supports 10 users per base station whereas Extreme's recommended maximum is 50 users. AirPort Express has three jacks: the USB printer sharing port; a single Ethernet port; and an audio-out jack that can handle analog or digital outputs with adapters.

The single Ethernet port offered by Airport Express limits you in one important way if you also use wired computers on your network.

You can plug the base station into your cable or DSL modem and share the incoming Internet connection to wirelessly connected computers. But, you cannot simultaneously share that connection with your wired computers. For such sharing with wired computers, you need at least one separate WAN (wide area network) Ethernet jack, which the broadband modem connects to, and one LAN (local area network) port to hook to an Ethernet hub or switch for wired computers. These ports are offered either by an AirPort Extreme Base Station or a similar device from another maker, which I talk about later.

The audio jack on the AirPort Express is its truly unique feature. It lets you plug Airport Express directly into your stereo system and then stream music to it using iTunes 4.6 or later (on Macintosh or Windows) as a controller. For example, if you have an AirPort Express Base Station in the living room, basement, and bedroom, with each connected to a stereo or powered speakers, you can have three separate copies of iTunes that control one set each simultaneously, or one copy of iTunes can select which single set of speakers to control at any given time.

Although you can purchase stand-alone streaming audio adapters that work with Wi-Fi networks, these cost from $125 to $300 and require you to use a different interface—typically a small LCD screen and a remote control—to select and play music.

NOTE The AirTunes system works on a one-to-one basis: one copy of iTunes can control one set of speakers at a time. You can't stream from iTunes to several sets of speakers—yet.

Apple sells a $39 AirPort Express Stereo Connection kit that includes both analog and digital optical (Toslink) adapters for its audio plug, along with a separate power cord to make it easier to use the Express farther from a power outlet. Otherwise, it plugs straight in and hugs the wall.

TIP You can purchase a mini-to-Toslink cable separately from any online audio store for $20 or less.

AirPort Extreme

AirPort Extreme is meant for wireless networks with wired computers and more users than an Express network. Both Extreme models can handle up to a recommended 50 users at a time, and they have robust management tools and built-in features designed to work on complex corporate and academic networks. Never mind that Apple was selling Airport Extreme models to home users (and still does); Extreme is now more firmly aimed at an audience that needs a bit more and is willing to pay for it.

AirPort Extreme's two Ethernet ports means that you can use a single base station as your link to both a broadband modem via the WAN port and your local Ethernet network via the LAN port.

AirPort Extreme's modem model is practically the only Wi-Fi gateway available that includes a modem for connecting to a dial-up Internet connection. If you're using a modem connection and want to use Wi-Fi at home, this pretty much determines your choice. It can even dial America Online on behalf of individual users—it's the only shared gateway that can handle that. Because it has Ethernet ports, you can upgrade simply to broadband later, too.

NOTE The modem model of the AirPort Extreme Base Station also lets you call your network remotely using PPP if you set up the base station to answer the phone line. This is handy for some people who have networks that they either can't or don't want to access over the Internet using static addressing or dynamic DNS.

The Plenum/PoE model was designed specifically to be placed in out-of-the-way places, like drop ceilings or within walls or closed compartments. The Plenum rating means that the unit meets fire-safety guidelines for off gassing in the event of a conflagration. Power over Ethernet (a.k.a. IEEE 802.3af) pushes DC (direct current) over unused wires in an Ethernet cable, eliminating the need to plug the device into a nearby electrical outlet.

Also, AirPort Management Tools 1.0, discussed in Appendix A: AirPort Management Tools, enables you to configure several or even hundreds of AirPort Extreme—but not AirPort Express—base stations at once, a feature that can save enormous amounts of time in the case of large installations.

Decide which one and whether to buy

Buy the AirPort Extreme base station if you need a modem, a Plenum rating, Power over Ethernet, or to configure many base stations at once. All these features are uniquely inexpensive (or just plain available) in AirPort Extreme models; other models with these features cost several hundred dollars each.

AirPort Express is a cheaper option, perfect for homes without wired computers sharing the same network as wireless ones. But if you need to put wired and Wi-Fi computers on the same network, AirPort Express is useful only to extend the range of your wireless network (and perhaps to integrate your music with your stereo wirelessly), not as the main base station. Also, if you don't need USB printer sharing or audio output, the AirPort Express base station costs about $40 more than a comparable unit with several LAN Ethernet ports from other manufacturers. Later in this section, I offer specific suggestions for cheaper alternatives from other manufacturers that work with Mac OS.

Many of my colleagues have been discussing using AirPort Express as an adjunct to AirPort Extreme: their main base station is AirPort

Extreme for its benefits and configurability; the satellites near stereos or remote parts of the house will be AirPort Express for the audio output and lower cost.

TIP On the client side, it makes the most sense to equip most machines with an AirPort Card or AirPort Extreme Card if that's the only available slot or if you use Bluetooth constantly alongside Wi-Fi. But if you have a Power Mac with a free PCI slot or a PowerBook with an empty PC Card slot, you can shave $30 to $70 off the card cost, too, through alternatives mentioned throughout the book and surveyed fully in Appendix B: Connect without AirPort Adapters.

Don't Buy Older AirPort Base Stations

If you're keen to stick with Apple at a lower price, you might consider buying a used original AirPort Base Station—but let me talk you out of it.

You can't get them cheap: eBay auctions consistently show completed sales of the graphite and snow models at $70 to $125, which is the same price as or even higher than a new 802.11g, 54 Mbps wireless gateway with a three- or four-port 10/100 Mbps Ethernet switch! The original base station works at just 11 Mbps (802.11b), and the graphite model included only a single Ethernet port, with no extras for connecting any other wired computers.

You could get a dud: Apple had a lot of duds in the early batches of graphite base stations, and to a lesser extent in the snow series. Many graphite units gave up the ghost a year or two into their lives. Apple didn't offer an extended warranty or recall for this well-known problem, and you don't know if the unit you buy might fry. If they were cheaper, perhaps around $35, you could buy two and have a backup. But they're not (yet).

They lack the faster 802.11g: You want 802.11g speeds for faster streaming media and sending files among machines on your network. The amount of data you send and receive will only increase, especially as home broadband speeds have started to ratchet up.

Take my advice—move forward, buying a used modern wireless gateway, rather than the slower, problematic original model. It was much loved, but its time has passed.

Consider a Software Base Station

One the sneakiest ways to save money on a Wi-Fi network is to use software that Apple built into Mac OS 8.6/9.x, and then omitted from Mac OS X 10.0 and 10.1. The software returned in Mac OS X 10.2 Jaguar and continued to improve in Mac OS X 10.3 Panther.

NOTE Mac OS 8.6/9.x calls this feature "Software Base Station," whereas Mac OS X builds it into its more robust "Internet Sharing." I use the term "software base station" generically to talk about this set of features in any Mac OS or Windows version.

With Mac OS X's Internet Sharing, you connect to a local network, a dial-up service, or a broadband modem using one connection method, like Ethernet, a dial-up modem, or even FireWire daisy-chained to another computer. You then share that connection to one or more other methods of connection.

Mac OS 9's Software Base Station works the same way, but is limited to an Ethernet or dial-up connection being shared over Wi-Fi only instead of the broader Mac OS X options.

In the most typical use, you convert a Mac into your base station, and other computers on the network connect to it just as they would to any regular Wi-Fi gateway. Once you know how to set up a software base station, you can use it on the fly whenever and wherever you need to connect two kinds of networks. For instance, my office-mate Jeff Carlson and I used software base station in a hotel in San Francisco that had free, wired Ethernet connectivity. One of us would hook up via Ethernet and turn on Internet Sharing, and the other would connect over Wi-Fi.

TIP You can do interesting things in Mac OS X with Internet Sharing, such as connecting via Wi-Fi to a base station and then sharing that connection via FireWire. Or, more practically, if you lack a wired Internet feed, you could use Bluetooth or USB to connect to a cellular data connection and then share it via Wi-Fi to a small group.

Although a software base station saves you money and reduces the number of devices you need to manage, you should also consider the drawbacks of a software base station:

- **Range:** The built-in antennas used with AirPort and AirPort Extreme cards often lack the range of the more advanced or higher-gain antennas found in dedicated base stations.
- **Availability:** Making a Mac into a software access point turns it into something you must monitor and maintain. Stand-alone equipment tends to be more robust than most desktop operating systems, and although even hardware access points can become confused, they require less maintenance and fiddling than the computers that run software access points.
- **Electrical power:** If you're the sort of person who likes to turn off the lights when you leave a room, the extra wattage used by a computer turned on all the time may irritate you. A hardware access point burns maybe 50 watts, while a Mac—even with Energy Saver settings set correctly—could run at 150 watts with its monitor turned on. The cost savings is probably minimal, but the principle of not wasting power unnecessarily is what matters. Of course, if you're already running a Macintosh server, turning it into a software base station actually *saves* energy over having another device turned on.
- **Intermittent connectivity:** I don't recommend using a software access point in conjunction with an intermittent dial-up Internet connection, particularly if you want your computers to communicate with one another when you're not connected to the Internet. The reason is that when you're connected to the Internet, your software access point will hand out one set of IP addresses. But when you're not connected to the Internet, your computers will revert to self-assigned IP addresses in the 169.254.0.0 range. This

switching of IP addresses is likely to cause irritating problems that go away if you rely on a hardware access point to connect to the Internet and dole out a single set of IP addresses.

NOTE You can bypass this address assignment problem by setting up your own dynamic address server. See Take Control of Dynamically Assigned Addresses.

- **Limited encryption:** A software base station can use only WEP (Wired Equivalent Privacy) encryption as an option. This is fine for home use, but a bad idea for business. I discuss WEP's weakness and alternatives in Secure Your Network.

NOTE If you want to share files between two wireless computers, you can create an ad hoc wireless network. I discuss the details of this in Chapters 12 and 13 of *The Wireless Networking Starter Kit, Second Edition* (http://wireless-starter-kit.com/).

I explain how to set up a software base station in Appendix D: Configuring Software Base Station.

Use a Wireless Gateway Alternative

Depending on the features you need, a $30 to $120 base station from a company other than Apple could fulfill your needs completely. Even compared with the newer, cheaper AirPort Express model, you could still save $50 to $120 by buying from another manufacturer.

I first make a general recommendation if you don't need specific features, and then I move into more specific recommendations for AppleTalk support and for wireless bridging for building a network of more than one access point.

Generic alternatives

It's true that practically any 802.11b or 802.11g Wi-Fi gateway will do. Most of the equipment that's sold by major brands like Linksys, Buffalo, NetGear, and D-Link uses underlying chips, firmware, and even hardware designs from a few chip makers.

If you want the greatest odds of full compatibility and no surprises with Apple's gear, buy a gateway from Belkin, Buffalo, or Linksys. All three companies use the same chips Apple chose for AirPort Extreme, and all three sell inexpensive wireless gateways that include Internet connection sharing, Ethernet ports, and Web-based configuration, along with full security support for WEP and WPA (see Secure Your Network).

For some people, having a three- or four-port Ethernet switch built into a wireless gateway saves the $30 to $50 required for a similar device—additional savings over the AirPort Extreme and AirPort Express Base Station.

In particular, you might consider the gateway that has sold more units than any other piece of Wi-Fi equipment, Linksys's solid WRT54G. It costs about $80 from Amazon.com as this ebook goes into production. I cover how to configure its features in some depth in *The Wireless Networking Starter Kit, Second Edition*, but the basics, such as setting up dynamic address assignments with DHCP and adding security keys, are straightforward.

TIP A problem you might run into with equipment not made by Apple that uses a Web browser for configuration is that you might be unable to upgrade the firmware with a browser running on a Mac. Before you dig up a PC or leave old firmware on the system, try a few different browsers other than Safari and Internet Explorer 5.2, if those fail. Try Mozilla, Camino, OmniWeb 5, or Opera—one of them will probably have the right secret sauce.

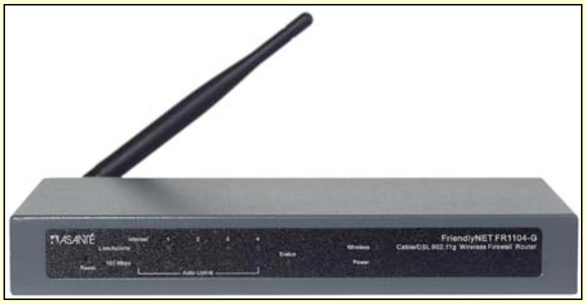
AppleTalk

As noted earlier, AppleTalk is the primary stumbling block for most Mac networks: some routers from Buffalo, Belkin, SMC, and Linksys appear to fully handle the older, plain AppleTalk standard used in Mac OS 9 and earlier (and supported in Mac OS X) when sending traffic between your wired and wireless networks.

TIP AppleTalk support can be confusing because most gateways handle all protocols, including AppleTalk, just fine across one kind of network media. So your Wi-Fi segment or your Ethernet segment can see other AppleTalk devices fine. The real problem is routing the protocol between Wi-Fi and wired; only a few devices offer that.

The $90 Asanté FR1104-G (http://www.asante.com/products/routers/FR1104-G/) seems to be the most Mac-friendly wireless gateway with full support for AppleTalk (**Figure 2**).

FIGURE 2



The Asanté FR1104-G.

TIP If you buy an FR1104-G, make sure that you install the G1.1 firmware upgrade if it didn't ship with the upgrade installed. That upgrade adds WPA security and AppleTalk support, and it was released in April 2004.

Bridging

Many home and small-office networks now take advantage of a feature called Wireless Distribution System (WDS) that's found in most 802.11g gateways, including AirPort Extreme. I explain WDS in full in Bridge Wirelessly, but in short, it's an easy way to create a larger network without using Ethernet cables to connect the wireless access points.

The most flexible inexpensive gateway that supports WDS comes from Buffalo. An AirStation WBR2-G54 (http://www.buffalotech.com/wireless/products/airstation/WBR2G54.html) costs $80 to $90 and is a full-featured gateway with Ethernet ports and WDS support.

It may be possible to use an AirPort Extreme Base Station as your main Internet connection and the Buffalo unit as remotes: I had this working last year when I had Buffalo gateways on loan from the company. Recent reports from users who read my article on the subject (http://www.oreillynet.com/pub/a/wireless/2003/08/28/wireless_bridging.html) said that they saw spotty or no performance after firmware upgrades changed both Buffalo's and Apple's equipment.

802.11b instead of 802.11g

I’m a big proponent of the faster 54 Mbps 802.11g standard because it’s more robust and has already dropped to a pretty decent price. But slightly older, 11 Mbps 802.11b-only equipment is incredibly cheap. I’ve seen new base stations with all the trimmings for $30 or less. Often these are sold with limited-time rebates to help clear out inventory.

If you don’t need AppleTalk, bridging, or all the speed of 802.11g, search for bargains or used devices.

Cheap adapters

I can’t finish this section without explaining how you could save $50 to $100 on a Wi-Fi adapter for your Mac, too.

If you own an iMac, an iBook, or an eMac, you’re stuck: if you want reasonably priced Wi-Fi with reliable performance, buy an AirPort or AirPort Extreme Card, as appropriate to your situation. (Although there are a couple of USB-based Wi-Fi adapters for no-slot models, they tend to cost more than even a used AirPort Card.)

Also, if you use Bluetooth extensively on or near your Macintosh, the AirPort Extreme Card and Apple’s Bluetooth adapters coordinate their frequency use. Bluetooth and Wi-Fi both use the 2.4 GHz spectrum band. Mac OS X can coordinate the two wireless technologies so that both work at their highest available speeds. This coordination isn’t yet available in any other combination of Bluetooth and Wi-Fi on the Mac.

But if you own a PowerBook or a Power Mac running the latest Apple AirPort software (3.3 or later), or are willing to use a third-party driver, you can typically buy an 802.11b card for $30 or less or an 802.11g card for $50 or less.

I cover the options extensively in Appendix B: Connect without AirPort Adapters. Flip forward to that before you buy a card.

Buy Subsequent Access Points More Cheaply

A little-known secret to saving money in building a Wi-Fi network is that when you try to cover a larger area and need to use more than one base station, only one of them has to be *smart*. That is, only one needs Internet sharing, and PPPoE support, and all the rest of the doodads that let you connect to your ISP.

The other base stations can be *dumb*. In fact, it's better if they're dumb, because you don't want them also assigning addresses and generally interfering with the Internet-connected gateway.

So even if you decide that you want to use an AirPort Extreme Base Station as your main unit, you can purchase $50 to $120 access points that have no features except a radio and an Ethernet port, or inexpensive gateways on which you can turn off all the smart features. If you need to hook in a printer or audio output for those other units, that's the time to use the $130 AirPort Express base station as a satellite.

TIP Adam Engst once found a deal on an 802.11b-based access point such that he paid $33… and got $30 back after a rebate. It's hard to go wrong for $3. Many companies are trying to clear out their inventories of older 802.11b, so these rebates aren't uncommon. For deals like this, subscribe to announcements from http://dealnews.com/.

It's also true that unless you often move large files around your network, you might opt for older, cheaper 802.11b gateways as your remotes.

The section Improve Coverage Area and Range explains how to connect remote and satellite base stations to a main one in a simple network.

Install Your Base Station

Installing your Base Station can be as simple as plopping it next to your broadband connection or phone line, powering it on, and making a few configuration changes. Right. And memorizing the capitals of all the states and composing a song about them may be simple too, but only for those with a particular odd bent.

What I have found from hard experience is that the little things can make you crazy. In this section, I discuss the fine details in locating and setting up a base station that typically are hard to find and figure out.

Pick the Right Place

When you walk around with a cell phone, the number of bars showing signal strength varies with the quality of signal that the phone can currently "see." These bars reflect the strength of signals received from nearby cellular network transmitters on towers and roofs. It's the same issue over a much smaller space with a Wi-Fi gateway. Depending on where you place the base station, its signal may or may not penetrate with enough strength to be useful.

First, decide where you want service: do you want to work in your backyard? Upstairs and downstairs?

Second, think about the number of obstacles in the places you want to work. Walls, ceiling, floors, and even metal exercise bikes can all absorb and reflect Wi-Fi signals, reducing their range and quality.

Pick a spot that is near the middle of where you want your signal to reach and test to see if it's a good location for your base station. You want to get the best average signal in all the places from which you want to connect. To run the test, just power up the base station: its default settings, no matter what the maker, will provide a name and a signal. If you already have a laptop equipped with Wi-Fi (or can invite a friend with one to help), you can use it as a signal-strength testing device; otherwise, you might use a handheld $30 Wi-Fi sniffer. (I talk more about these options just ahead.)

TIP If the spot you want to use is far from your broadband connection or modem line, see the next section, Improve Coverage Area and Range, for tips on bringing your connection to your base station or adding base stations to cover more area.

General testing advice

Here are some general tips for finding your ideal location:

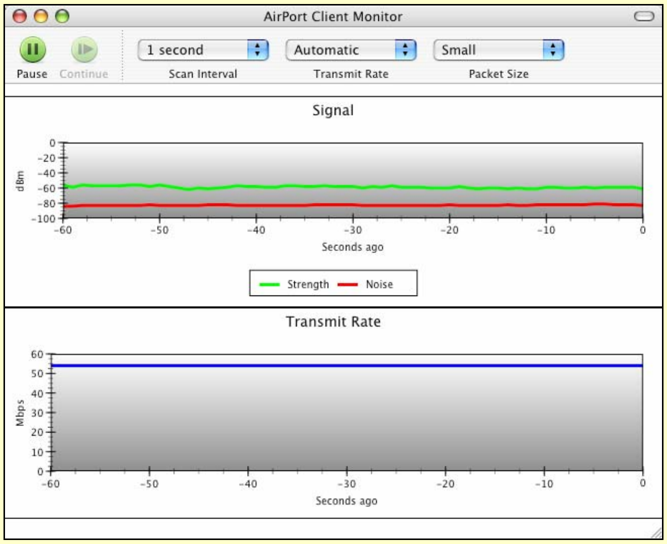
- Leave the base station in one place while you try all the areas you want to use it in.
- Spend up to 30 seconds in one spot to see if the signal strength varies.
- Use sticky notes to mark signal strengths at the locations where you work most regularly or would like to spend most of your time. Mark the current location of the base station and the signal strength you're seeing at that location so it's easy to sort out the ideal placement of the base station later.
- When you move the base station, make sure to keep its orientation the same. The antenna in a base station is *omnidirectional*—all directions—but any antenna has better performance in a bubble that parallels its longest vertical side. Putting it vertically on the wall might dramatically change where signals reach.
- If you find you need to put your base station in an odd location for best performance, read Improve Coverage Area and Range for tips on locating your base station far away from the rest of your wired network or Internet connection.

Testing with an AirPort or AirPort Extreme Card or compatible varieties

If you have Apple's Wi-Fi adapter or any of the compatible cards I talk about later in the book along with the latest AirPort Software (version 3.4 or later), you can download and install AirPort Management Tools 1.0 (go to http://www.apple.com/support/airport/ and look in the Resources section at the upper right). Once installed, run the AirPort Client Utility and choose your network from the AirPort menu.

This tool is nifty because it provides ongoing monitoring of signal and transmit rate. The signal (green) and noise (red) lines show how much useful information you're getting. The higher the signal the better, but noise has to remain somewhat below that line for the data on the signal to be filtered out and reconstituted (**Figure 3**).

FIGURE 3



Scan Interval: 1 second
Transmit Rate: Automatic
Packet Size: Small

The top shows signal-to-noise ratio; the bottom shows the transmit rate.

The lower half of the tool shows the speed at which your card has connected to the wireless gateway. This is useful to know because you can have decent signal strength but be connected at a lower speed than the 11 or 54 Mbps maximum for 802.11b or 802.11g, respectively.

NOTE Both flavors of Wi-Fi have slower speeds for mixed networks or adapters more distant from the central transceiver.

Testing with other cards

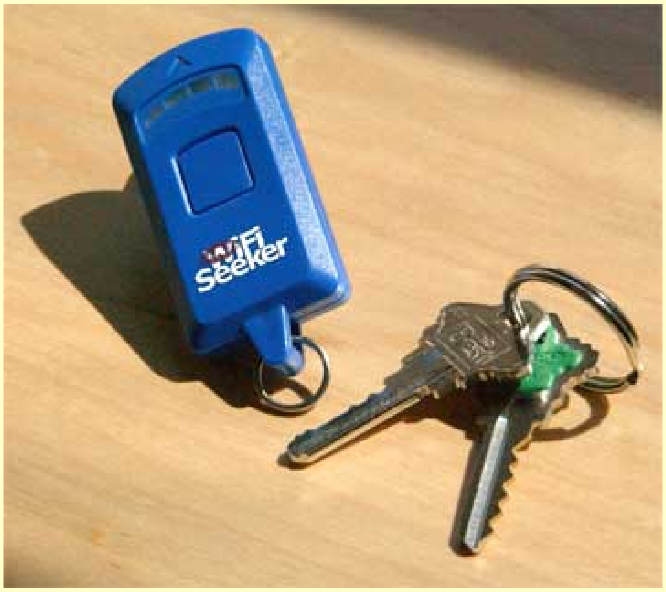
Most other wireless adapters on the Mac have primitive interfaces that lack the monitoring tool support provided with the AirPort family. With other adapters, you're restricted to a signal strength meter, which might show as little information as zero to five bars or dots.

You can also download and install software such as MacStumbler (http://www.macstumbler.com/) or iStumbler (http://www.istumbler.com/). These utilities work with a variety of adapters and can provide more detailed signal strength information plotted over time.

Testing with handheld sniffers

If you'd like to have a laptop-free way to plan a network, you can use one of several compact Wi-Fi sniffers that cost about $30 each. The sniffers have a built-in signal detector and use LEDs to display how much signal they can detect in a given area. I recommend a new device, the WiFi Seeker from Chrysalis Development (http://www.wifiseeker.com/). The Seeker is extremely small, quite sensitive, and responds only to Wi-Fi networks (**Figure 4**).

FIGURE 4



The WiFi Seeker's four LEDs show signal strength of Wi-Fi networks while the button is held down.

NOTE The WiFi Seeker detects all Wi-Fi networks in the vicinity, so if there are other networks operating you can't discriminate which network it's measuring.

Solve Common Internet Connection Problems

To put your wireless network on the Internet, you must use the settings your ISP gave you to get on the Internet with a single computer or a set of computers. Here's how to handle situations that might arise, depending on the kind of connection you make to your ISP.

Plug your broadband modem into your WAN port

The simplest and best way to put your base station on a broadband network is to connect its WAN (Wide Area Network) Ethernet port to your cable or DSL modem. Then plug any local wired devices (or an Ethernet hub or switch) into the LAN port or ports.

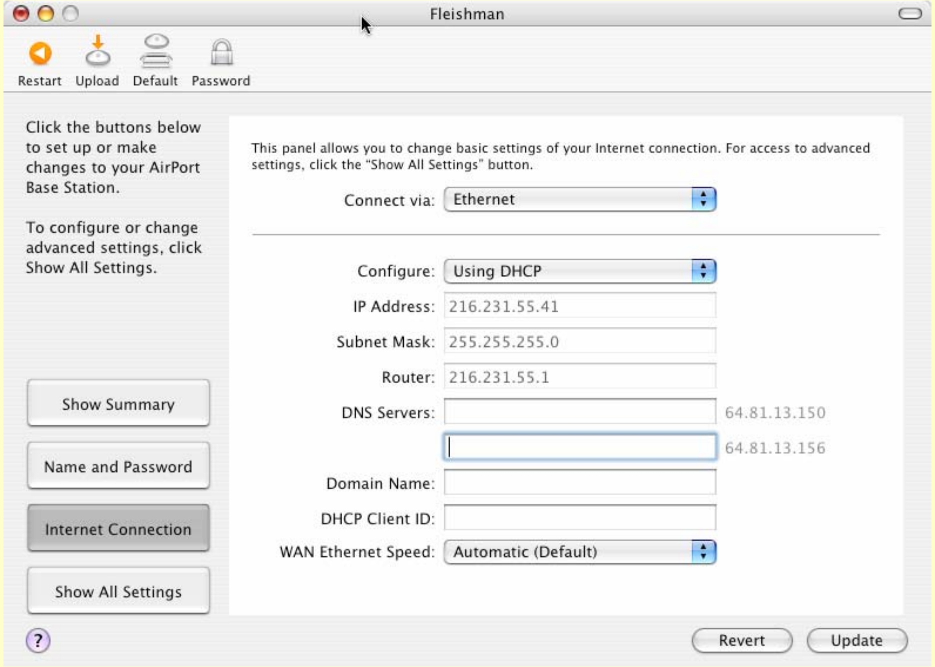
It used to be a rule that if you connected two devices directly together, you had to use a special crossover Ethernet cable that flipped some of the wires at either end. Fortunately, almost all new equipment comes with a feature called auto-MDI/MDI-X, which is also known as auto-sensing. This feature allows an Ethernet port to reconfigure itself without intervention for pass-through or crossover purposes. Most WAN ports are either set by default to connect to a broadband modem with a regular Ethernet cable or to have auto-sensing.

Receive a dynamic address over broadband

Many home users with DSL and cable-modem service receive one or more dynamically assigned addresses using DHCP. If your ISP tells you to set up dynamic addressing or DHCP, use the simplest settings, which you can usually find under an Internet heading in your configuration software as DHCP or Configure Using Dynamic IP.

If you run AirPort Admin Utility and click the Internet Connection button, you can enable DHCP just by selecting Using DHCP from the Configure menu (**Figure 5**).

FIGURE 5



Click the buttons below to set up or make changes to your AirPort Base Station.

To configure or change advanced settings, click Show All Settings.

This panel allows you to change basic settings of your Internet connection. For access to advanced settings, click the "Show All Settings" button.

Connect via: Ethernet

Configure: Using DHCP

IP Address: 216.231.55.41

Subnet Mask: 255.255.255.0

Router: 216.231.55.1

DNS Servers: 64.81.13.150

64.81.13.156

Domain Name:

DHCP Client ID:

WAN Ethernet Speed: Automatic (Default)

The Using DHCP setting causes the base station to obtain its Internet address automatically.

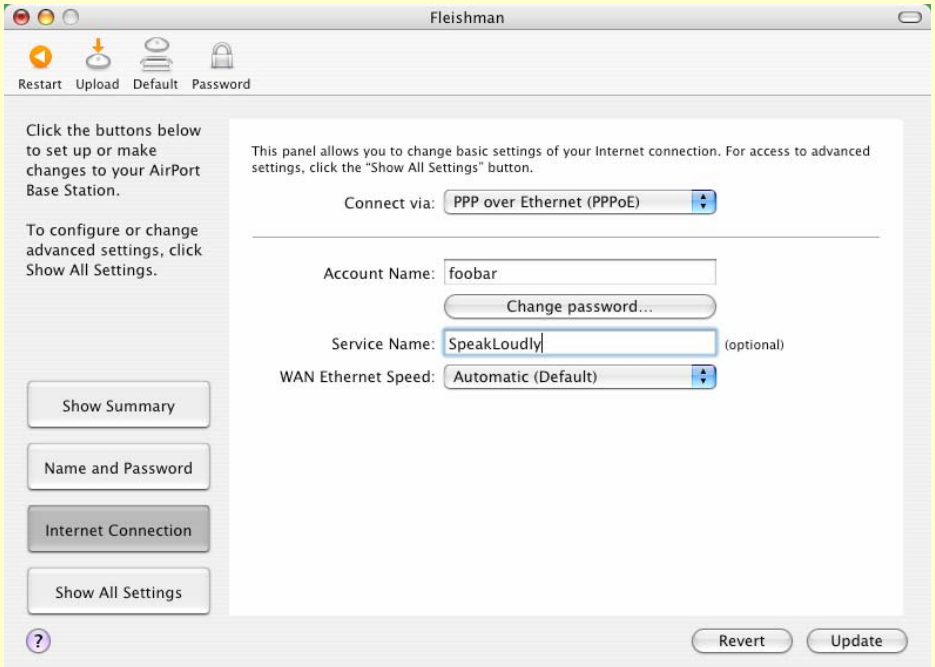
With dynamic addressing, your gateway may never have the same address twice (or it might hold on to the same IP address for days or weeks; there's no way to predict), but that shouldn't matter as you almost never need to connect from outside the local network.

NOTE *Do you want to know more about DHCP?* Flip ahead to Take Control of Dynamically Assigned Addresses.

Log in via PPPoE over broadband DSL

For security and tracking purposes, many DSL providers require you to use a technology called *PPPoE* (PPP over Ethernet) when connecting to their network. With PPPoE, you log in with a user name and password to your ISP over your DSL connection, at which time you are automatically assigned an address and the connection works just like any other broadband connection. If you need PPPoE, configure it in the Internet Connection screen of the AirPort Admin Utility (**Figure 6**).

FIGURE 6



Click the buttons below to set up or make changes to your AirPort Base Station.

To configure or change advanced settings, click Show All Settings.

This panel allows you to change basic settings of your Internet connection. For access to advanced settings, click the "Show All Settings" button.

Connect via: PPP over Ethernet (PPPoE)

Account Name: foobar

Service Name: SpeakLoudly (optional)

WAN Ethernet Speed: Automatic (Default)

PPP over Ethernet connects using a login name and password.

Virtually all wireless gateways support PPPoE, as it's a routine part of many ISPs' services now.

Deal with MAC address restricted cable broadband

To prevent multiple machines from accessing a single cable-modem connection, some providers have restricted access to a single MAC address, which is a unique number assigned to a Ethernet or Wi-Fi adapter, including individual ports on a switch or gateway (see the sidebar What and Where is a MAC Address?).

TIP ISPs use two common methods for restricting access by MAC address. The more annoying method requires that you register your computer's MAC address with the ISP manually or through an automatic installation process; read ahead for how to deal with that situation.

The less annoying method involves the cable modem locking on to the MAC address of the device connected to it when the modem powers up. In this second case, you can switch between devices (such as computer and a gateway) simply by powering down the cable modem before you connect the new device.

To work around MAC limitations, most wireless gateways let you extract the MAC address from the one that your cable-modem connection has locked onto and then modify the WAN port MAC address to match it; this is called *cloning*.

WARNING! No release of AirPort base station firmware contains this cloning feature, which may make it impossible to share a network connection on a cable-modem service using any Apple gateway.

Typically, the process works as follows, starting with setting up your cable-modem service:

1. Connect your computer to the cable modem and use the software provided by your cable modem provider to activate your high-speed service.
2. Obtain the MAC address from that computer. (The sidebar What and Where is a MAC Address? explains how to obtain it.)
3. Connect via a Web browser to your wireless gateway.
4. Find the MAC cloning settings, usually found in an Advanced tab.
5. Enter the MAC address and click Update or Restart to apply the setting.
6. Disconnect the computer that set up your cable-modem connection, and plug your wireless gateway into the modem instead.
7. Plug your computers into the wired LAN ports or connect via Wi-Fi to the gateway.

Once you've cloned a MAC address, you can never use that computer and the wireless gateway on the same network segment again. The gateway segregates its WAN port (to the broadband service) and LAN ports (to local wired computers) to avoid MAC address conflicts.

Set a static address over broadband

If you arranged with your ISP to obtain one or more static addresses to use with your account, you configure your wireless gateway with what it might call its manual or static IP settings. Enter the information provided by your ISP exactly, since your ISP's servers won't fill in missing values such as DNS server addresses.

If your ISP provided a range of static addresses that you plan to use on your wireless and/or wired LAN, you can't use your base station as an intermediary between the ISP's network and your own because most base stations won't allow you to even manually assign static addresses to machines connected via its LAN port or ports.

You can work around this limitation in three ways:

- Assign a static address to the base station, and connect its WAN port to a LAN that contains only computers that have their addresses assigned statically. Any wired machines that need a dynamic address can be connected to the LAN ports. Wi-Fi-connected computers will have to receive a shared, dynamic address.
- If you have a WAN port or a single port, use that connection to hook into your wired network, but don't use the gateway's LAN ports (if it has one) except for computers that are obtaining non-routable private addresses via DHCP and NAT, explained in Take Control of Dynamically Assigned Addresses.
- Install the gateway with a static address and have it assign addresses to wired and wireless machines via Wi-Fi and its LAN port or ports from a static range. The AirPort Extreme Base Station offers this option, but many wireless gateways can only assign private NAT routed addresses.

Configure a dial-up connection

If your wireless network connects to an ISP through a dial-up modem, make sure to include alternate phone numbers for the dial-up connection so that you don't have to reconfigure the gateway if one number is often busy.

You may also want to make sure that your base station is set to dial when an Internet service is requested instead of a manual process, such as connecting via the AirPort Admin Utility and clicking a button to dial.

Take Control of Dynamically Assigned Addresses

Most of us have broadband connections that arrive via a DSL or cable modem. The Ethernet port on these modems is designed, typically, to connect to a single computer. Ha! If you're reading this book, you almost certainly have at least two computers.

All home gateways, whether they have Wi-Fi or not, are designed to address this little missing piece. As discussed earlier, gateways typically have a single WAN port to connect to a broadband modem and at least one LAN port for hooking up Ethernet-connected computers or hubs and switches.

Gateways use a combination of Dynamic Host Configuration Protocol (DHCP), the technical name for dynamic Internet address assignment, and Network Address Translation (NAT) to create private addresses and assign them on demand to computers that connect to the LAN through Wi-Fi or Ethernet. Whenever you power up a computer, an address is instantly and automatically assigned to your computer with no involvement on your part—that's DHCP.

DHCP and NAT work together to take the single dynamic address that most ISPs assign each customer and multiply it transparently on your LAN. But there are scenarios in which a gateway's built-in DHCP/NAT combo doesn't cut it:

- If you have a single Ethernet port on your gateway, as with the AirPort Express Base Station, you cannot use its Internet sharing because it will pollute your ISP's DHCP service. See Don't get your service canceled for details and solutions.
- You want to assign fixed, private addresses to specific computers based on their MAC addresses or DHCP client IDs.
- The limitations of which addresses can be used or other irritations with your gateway mean that you want to configure your own DHCP settings.
- You're running a combination of static and dynamic addresses on one network, and the gateway can't handle both in exactly the way you want it to (as described previously in Set a static address over broadband).

Fortunately, you have options. Let's first make sure you don't make your ISP mad by polluting their DHCP service, and then look at four options for dynamically assigning addresses outside a Wi-Fi gateway.

TIP It's important—nay, critical!—to run only a single DHCP server on your local network: you need only one device assigning IP addresses to avoid confusion among machines and gateways.

Don't get your service canceled

Many ISPs, especially cable modem providers, bridge your network connection directly onto their network: your Ethernet network is just an extension of their larger pool. This is a stupid design for a variety of reasons, but it's standard practice. (ISPs could use filtering to keep DHCP from leaking upstream, for instance.)

As a result, if you turn on DHCP service on your local Ethernet network and it's not separated by your gateway onto the LAN ports of that gateway—or if your gateway lacks a LAN port at all, like the AirPort Express—then your DHCP service pushes out to other machines in your ISP's network. When other machines use your DHCP-assigned addresses, they probably won't be able to connect to the Internet at all, and some ISPs will cancel your service in retribution for the trouble you've caused.

If you're assigned a static pool of Internet addresses by your provider and your own subnet mask, then this problem doesn't happen: The DSL modem or digital service router that sits between your network and the ISP won't pass the DHCP service messages. On my office network, for instance, we have a small pool of 64 routable, static IP addresses, and we also run a DHCP service; no conflict there. (In fact, in that scenario, we plug our LAN into the WAN port of the base station because the base station's "wide" network is our local LAN.)

If you purchase a single Ethernet port base station, like the AirPort Express, then you can feed DHCP and NAT only to Wi-Fi clients. The only way around this limitation is to purchase a wired gateway, which I describe later in this section, in Non-wireless broadband gateways.

If you have a LAN and a WAN port on your base station, or don't need to provide access to wired computers, then you don't need to worry about this problem with polluting your ISP's DHCP pool.

Configuring DHCP with AirPort

The AirPort Extreme Base Station (probably true also for the AirPort Express Base Station; see the Note just ahead) intertwines its DHCP and NAT options, making it sometimes difficult to set up precisely what you want. The primary choice depends on whether you want the base station to share an IP address with your entire network by using both DHCP and NAT, or you want it to assign static, routable addresses using only DHCP.

NOTE All examples in this book that show the AirPort Admin Utility are demonstrating the settings for an AirPort Extreme Base Station. At the time of this writing, AirPort Express hadn't shipped, and Apple hadn't clarified which precise settings will be available in an AirPort Express Base Station, or whether the AirPort Admin Utility's appearance will change.

Also, the AirPort Express Base Station will come with a setup assistant to make entering ISP settings and security much simpler. AirPort Express will ship in mid-July; click here to check for a free update that will contain AirPort Express details.

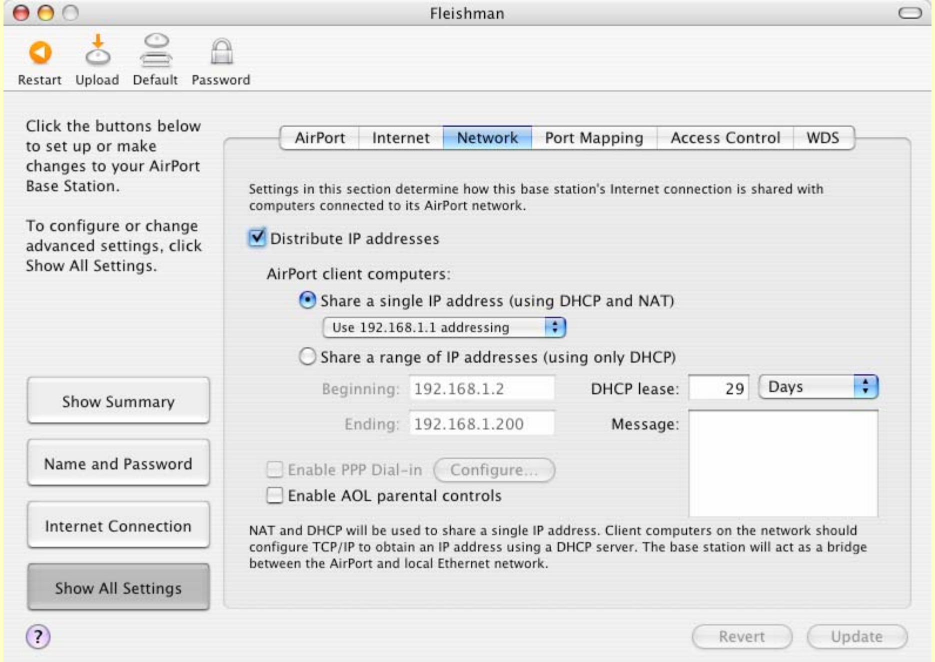
DHCP addresses are assigned to all wireless devices that ask to have their address assigned automatically, and similarly to any wired devices connected to network segments that are plugged into the LAN port of the base station.

Follow these instructions to turn on DHCP in your AirPort base station:

1. Run AirPort Admin Utility. (Find it in the Utilities folder, which is inside the Applications folder.)
2. Connect to your AirPort base station.
3. Click Show All Settings.
4. Click the Network tab.

5. Check Distribute IP Addresses (**Figure 7**).

FIGURE 7



Click the buttons below to set up or make changes to your AirPort Base Station.

To configure or change advanced settings, click Show All Settings.

Settings in this section determine how this base station's Internet connection is shared with computers connected to its AirPort network.

☑ Distribute IP addresses

AirPort client computers:

● Share a single IP address (using DHCP and NAT)

Use 192.168.1.1 addressing

○ Share a range of IP addresses (using only DHCP)

Beginning: 192.168.1.2 DHCP lease: 29 Days

Ending: 192.168.1.200 Message:

□ Enable PPP Dial-in

□ Enable AOL parental controls

NAT and DHCP will be used to share a single IP address. Client computers on the network should configure TCP/IP to obtain an IP address using a DHCP server. The base station will act as a bridge between the AirPort and local Ethernet network.

Set DHCP and NAT options in the AirPort Admin Utility's Network tab.

6. Set the DHCP Lease to a high number if you don't want machines to be reassigned addresses frequently. A lower number recycles addresses faster; a higher number is better for machines that stay on the network indefinitely.

   If your ISP gives you a single IP address that you wish to share with all the computers on your network (the most likely scenario), continue on; otherwise you're done.

7. Select the Share a Single IP Address (Using DHCP and NAT) radio button.

8. Typically, you can leave the Use 192.168.1.1 Addressing option selected in the pop-up menu, and just click Update.

If you want to switch the private, NAT-generated addresses assigned by the base station, use the pop-up menu to choose one of two other ranges of reserved addresses that don't overlap with real addresses: 10.0.1.1 or 172.16.1.1.

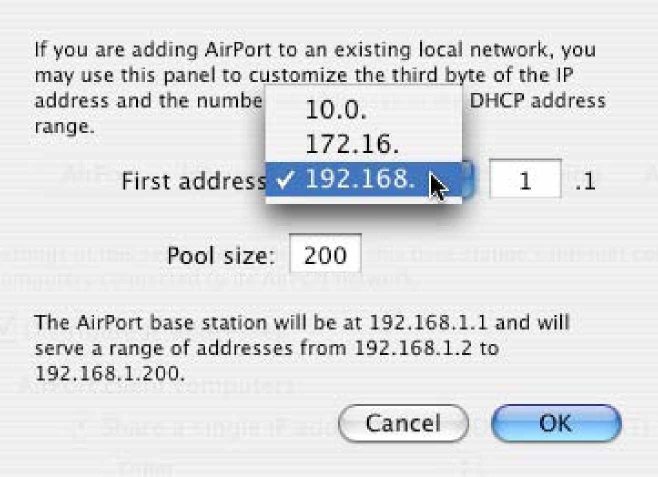
NOTE Private Internet addresses are non-routable; that is, they can be reached only from other machines on the private network, not from the rest of the Internet—or even the rest of a network that uses a different network range.

The group that assigns Internet numbers reserved several ranges for the purpose of private, local networking. These include 192.168.0.0 to 192.168.255.255, 10.0.0.0 to 10.255.255.255, and 172.16.0.0 to 172.31.255.255.

You can use any of these addresses or ranges within them with 100-percent assurance that no real computer on the Internet has an overlapping address. Of course, computers with these addresses require a gateway running NAT in order to communicate with the rest of the Internet.

You can also choose Other from the pop-up menu to open a dialog where you can define the third number in the IP range (**Figure 8**). You would choose a third number in the IP range other than the default that Apple provides if you were already using the identical network range for some other purpose. For instance, if you already have a network that starts 192.168.0, you could set your AirPort gateway to feed out address that start 192.168.1. The .1 address, such as 10.0.1.1, is always reserved for the AirPort base station as the gateway address.

FIGURE 8



If you are adding AirPort to an existing local network, you may use this panel to customize the third byte of the IP address and the numbe DHCP address range.

First address: 192.168. 1 .1

Pool size: 200

The AirPort base station will be at 192.168.1.1 and will serve a range of addresses from 192.168.1.2 to 192.168.1.200.

Choose an alternative set of private networking addresses from the First Address pop-up menu.

If you have a range of static addresses provided by an ISP that are fully routable over the Internet, reachable from anywhere, then you can enter all or part of that static range here. If you have a NAT server running elsewhere on your network to map private addresses to one or more public addresses, you can still let your AirPort base station assign IP addresses in that range without running NAT on the base station.

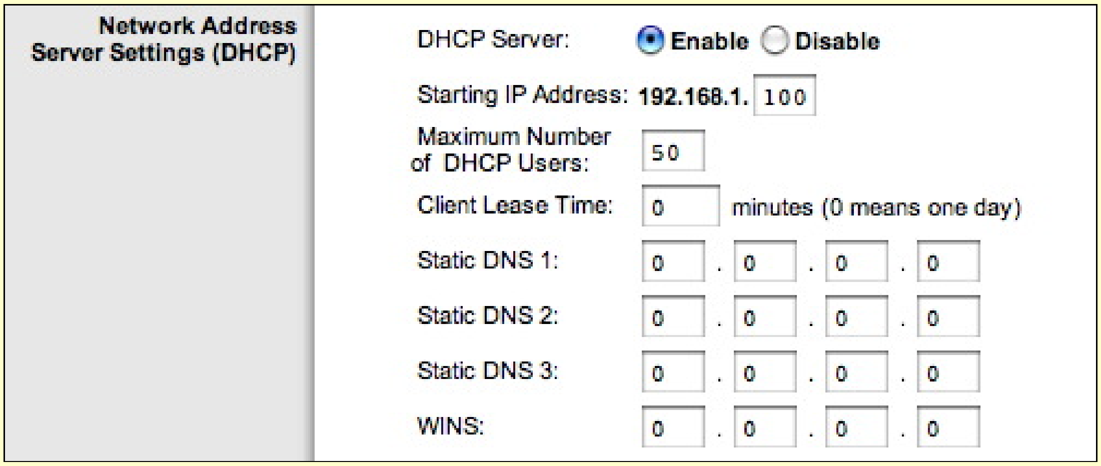
1. Working in the AirPort Admin Utility's Network tab, select the Share a Range of IP Addresses (Using Only DHCP) radio button.
2. Enter the address range in Beginning and Ending.
3. Click Update to restart the AirPort base station with the new settings.

Configuring DHCP with the Linksys WRT54G

The Linksys WRT54G is designed to run NAT and DHCP as a system quite simply.

1. Connect to your WRT54G via a Web browser. The basic Setup tab displays by default.
2. In the Network Address Server Settings area, make sure that DHCP Server is set to Enable (**Figure 9)**.

FIGURE 9



Network Address Server Settings (DHCP)

DHCP Server: ● Enable ○ Disable

Starting IP Address: 192.168.1. 100

Maximum Number of DHCP Users: 50

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

DHCP service is ready to go with just a few entries on the Linksys WRT54G.

3. Set the starting IP address for the DHCP and NAT assignment, as well as the maximum number of DHCP users only if you feel the need to change those values.

TIP Because the WRT54G acts as an Internet gateway at 192.168.1.1 by default and since our example here is starting to assign DHCP addresses starting at 192.168.1.100, you can set other machines on the local network to static addresses in the 192.168.1.2 to 192.168.1.99 range by default.

TIP You can change the first three numbers in Starting IP Address by changing the IP address of the router on the local area network. You change the router's address by entering an IP address in the Router IP fields in the Network tab. You might change the router—and thus the LAN's—private network address if you already are using the Linksys default network 192.168.1.0 elsewhere on the LAN or if you just prefer using a different private network range.

4. Enter the static addresses of the Internet DNS servers that you're using. You may need to query your ISP for these values. (The WINS setting is needed only for certain kinds of Windows networks.)

5. Click Save Settings to restart the server and enable these changes.

Software-based DHCP servers

Software-based DHCP servers can provide more flexibility or substitute for missing software if you've purchased a gateway that lacks Internet connection sharing.

I've found four methods of adding DHCP and NAT with relatively little hassle. I'll start with free, move into a $100 piece of software that has lots of flexibility, try out the $500 or $1000 solution (Mac OS X Server), and finish with cheap hardware supplements.

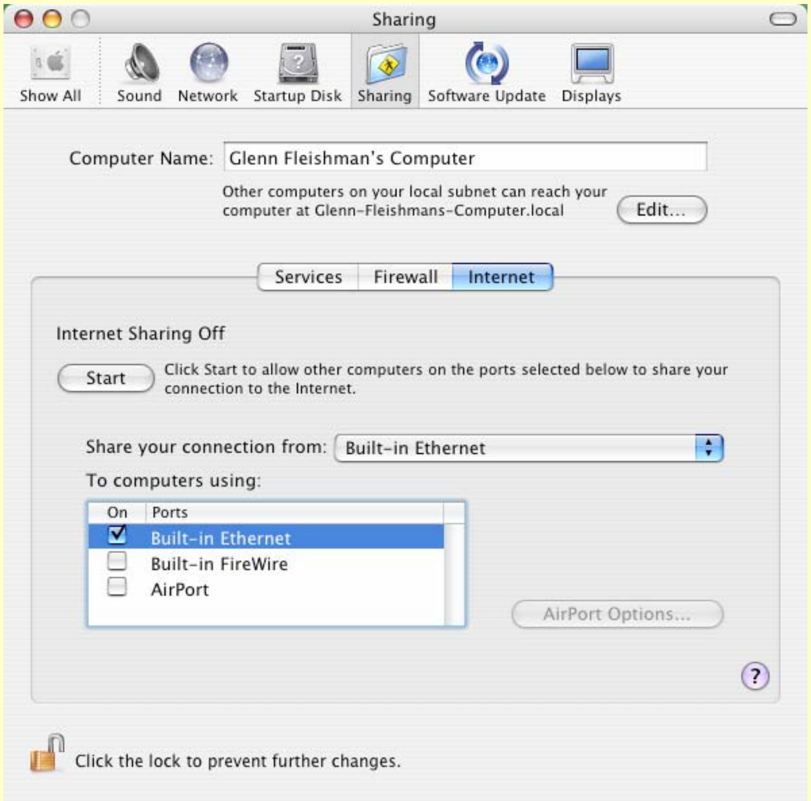
Except for the last, these DHCP server options work only with a network that uses static IP addresses, or in which a gateway is connected via its LAN ports to the local Ethernet network. If you use any of these methods, you must turn off DHCP and NAT in any existing gateways by unchecking DHCP service or Distribute IP Addresses or similar settings.

Panther’s Internet Sharing

Panther lets you run a simple DHCP and NAT server combination through its Internet Sharing feature found in the Internet tab of the Sharing preference pane. Although there are no dialogs for settings, you can still achieve many of the benefits of a more advanced server.

1. Select the Internet tab in the Sharing preference pane.
2. Choose Built-in Ethernet from the Share Your Connections From pop-up menu (**Figure 10**).

FIGURE 10



Computer Name: Glenn Fleishman's Computer

Other computers on your local subnet can reach your computer at Glenn-Fleishmans-Computer.local

Internet Sharing Off

Click Start to allow other computers on the ports selected below to share your connection to the Internet.

Share your connection from: Built-in Ethernet

To computers using:

☑ Built-in Ethernet
☐ Built-in FireWire
☐ AirPort

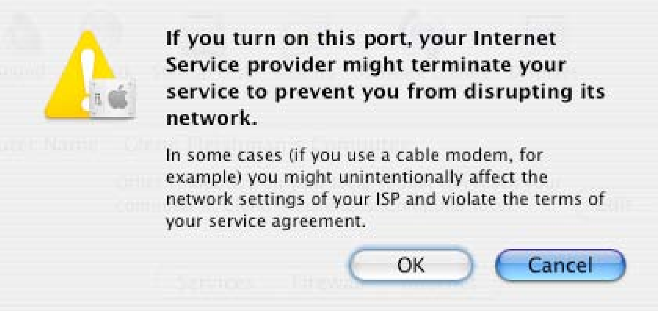
Click the lock to prevent further changes.

Internet Sharing settings within the Sharing preference pane.

3. In the To Computers using list, check the Built-in Ethernet box.

   Apple warns you about disrupting your ISP's network (**Figure 11**).

FIGURE 11



If you turn on this port, your Internet Service provider might terminate your service to prevent you from disrupting its network.

In some cases (if you use a cable modem, for example) you might unintentionally affect the network settings of your ISP and violate the terms of your service agreement.

Apple provides a strong warning to help you avoid problems with your ISP.

4. Click Start.

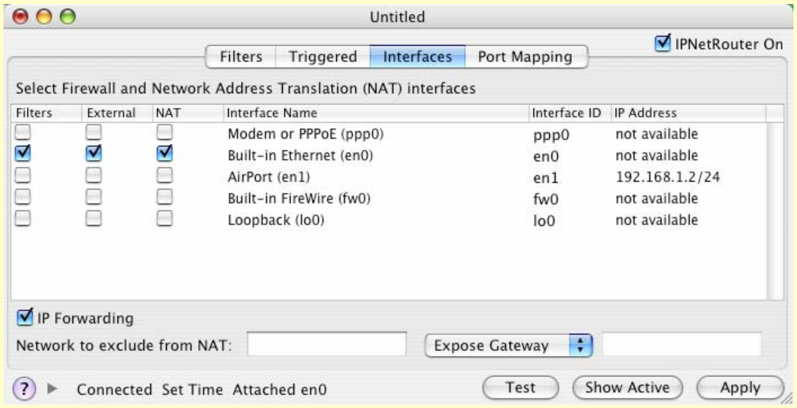
IPNetRouter X

If you'd like to specify exact network ranges and other parameters, you can use Sustainable Softworks's $100 IPNetRouter X (http://www.sustworks.com/site/prod_ipnrx_overview.html), which was still in final testing as I completed this book. IPNetRouter X offers a full-featured NAT and DHCP server that also has a behavior-based firewall and sophisticated filtering options.

Enabling DHCP and NAT is a snap:

1. Run IPNetRouter X.
2. Click the Interfaces tab (**Figure 12**).

FIGURE 12



☑ IPNetRouter On

Select Firewall and Network Address Translation (NAT) interfaces

Filters	External	NAT	Interface Name	Interface ID	IP Address
□	□	□	Modem or PPPoE (ppp0)	ppp0	not available
☑	☑	☑	Built-in Ethernet (en0)	en0	not available
□	□	□	AirPort (en1)	en1	192.168.1.2/24
□	□	□	Built-in FireWire (fw0)	fw0	not available
□	□	□	Loopback (lo0)	lo0	not available

☑ IP Forwarding

Network to exclude from NAT: Expose Gateway

Connected Set Time Attached en0

Main settings for IPNetRouter X.

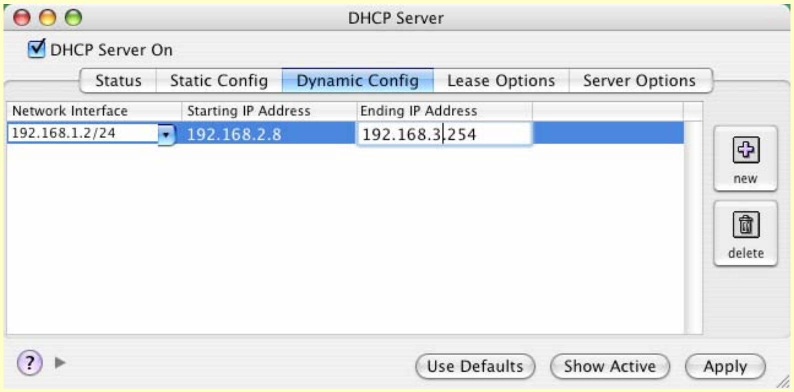
3. In the upper-right corner, check IPNetRouter On to enable it.

4. Check the row corresponding to the network that is your connection to the Internet; it should have External and NAT checked. The optional Filters checkbox activates IPNetRouter X's rules-based firewall.

5. Click Apply.

6. Choose Tools > DHCP Server and, in the resulting dialog, at the upper left, check DHCP Server On (**Figure 13**).

FIGURE 13



☑ DHCP Server On

Network Interface	Starting IP Address	Ending IP Address
192.168.1.2/24	192.168.2.8	192.168.3.254

DHCP Server settings in IPNetRouter X.

7. Click the Dynamic Config tab.

8. Make sure the range of addresses that's provided by default in the 192.168.1.0 network range doesn't conflict with any other service on your network. You might change the starting and ending addresses to 192.168.2.2 and 192.168.2.200 to avoid conflicting with many network products that use the 192.168.1.0 network.

9. Click Apply

10. Choose File > Save in order to save this configuration.

11. You should set this configuration file to load automatically on each restart by adding it to your account's Startup Items list in the Accounts preference pane.

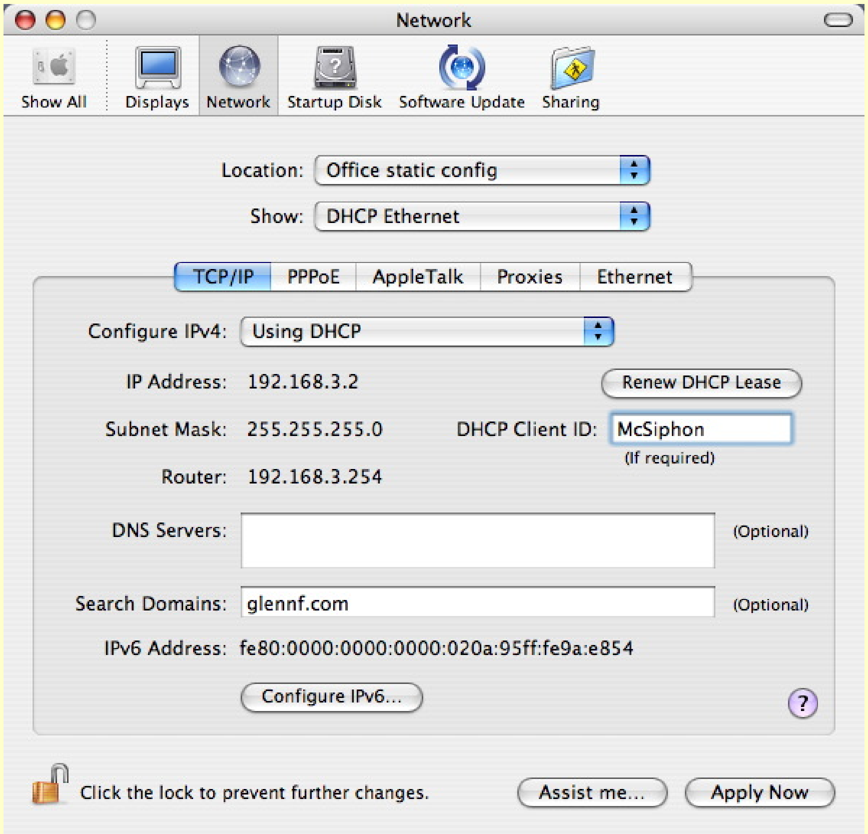
IPNetRouter X offers a trick that lets you use it over an Ethernet network in a way that I said wasn't allowed earlier. The Static Config tab restricts assigning addresses to only those computers that meet criteria. Substitute these two steps for those above:

7. Click the Dynamic Config tab, select the default address listed, and click Delete.

8. Click the Static Config tab. Add an entry for each computer on your network using either or both the MAC address and the DHCP Client ID to restrict which machines receive which fixed private addresses.

You can set the DHCP Client ID in Mac OS X by selecting an interface in the Network preference pane, like “DHCP Ethernet” (**Figure 14**), and entering a unique client identifier (anything you want) in the DHCP Client ID field. The MAC address is found in the Ethernet tab for Ethernet interfaces, and in the AirPort tab for AirPort adapter. (See the sidebar What and Where is a MAC Address? for more on finding MAC addresses.)

FIGURE 14



Location: Office static config

Show: DHCP Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.3.2

Subnet Mask: 255.255.255.0

DHCP Client ID: McSiphon (If required)

Router: 192.168.3.254

DNS Servers: (Optional)

Search Domains: glennf.com (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe9a:e854

Click the lock to prevent further changes.

The DHCP Client ID can be used with Static Config in IPNetRouter X to assign the same address to a computer every time it’s on the network.

During my research for this book, IPNetRouter X’s developer, Peter Sichel, said via email that when you assign fixed IP addresses in this manner, his DHCP server is entirely quiet until it hears an appropriate request from a machine with the right credentials.

Mac OS X Server 10.3

If you're already running Mac OS X Server 10.3 for some other reason, you can also have it act as a DHCP and NAT server. The configuration is quite complicated, unfortunately, requiring changes in the DHCP, NAT, and Firewall services. I've written a long article about this for O'Reilly Network, and it is available free online at: http://www.oreillynet.com/pub/a/wireless/2003/11/25/nat_panther.html.

Non-wireless broadband gateways

It's easy to overlook this last option as a cheap and simple method to add DHCP service to your network. While most broadband gateways are sold with Wi-Fi as a full wireless option, you can still purchase inexpensive hardware boxes that have all or most of the same features but no Wi-Fi.

These devices are the ideal solution when you're trying to use a single-port base station, such as the AirPort Express, with wired computers on the same network.

Take a look at the Asanté FriendlyNET FR1004 Internet Router, for instance, which has a street price of about $30 (http://www.asante.com/products/routers/FR1004/). On the LAN side, it's a four-port 10/100 Mpbs Ethernet switch with automatic cable type sensing—no uplink ports, in other words. Its WAN port runs at 10 or 100 Mbps, too, and handles all the major ISP login types.

The Asanté FR1004 is a perfect complement to AirPort Express: combined, you're getting the best firewall protection in a home device, an Ethernet switch, and the most robust home base station.

NOTE As I put the finishing touches on this book, it appears that the Asanté FR1004 is no longer shipping: I can't find in stock at any store that lists it. Although I haven't spent much time with it yet, you could consider the Linksys BEFSR41, which has somewhat similar features but costs about $50.

Improve Coverage Area and Range

The top question I receive about Wi-Fi is, “How can I extend the area served by my Wi-Fi network?” Several strategies let you cover more of your home or business without having to spend a fortune—$50 to $200 could double to quadruple your coverage area.

Add Additional Access Points for Roaming

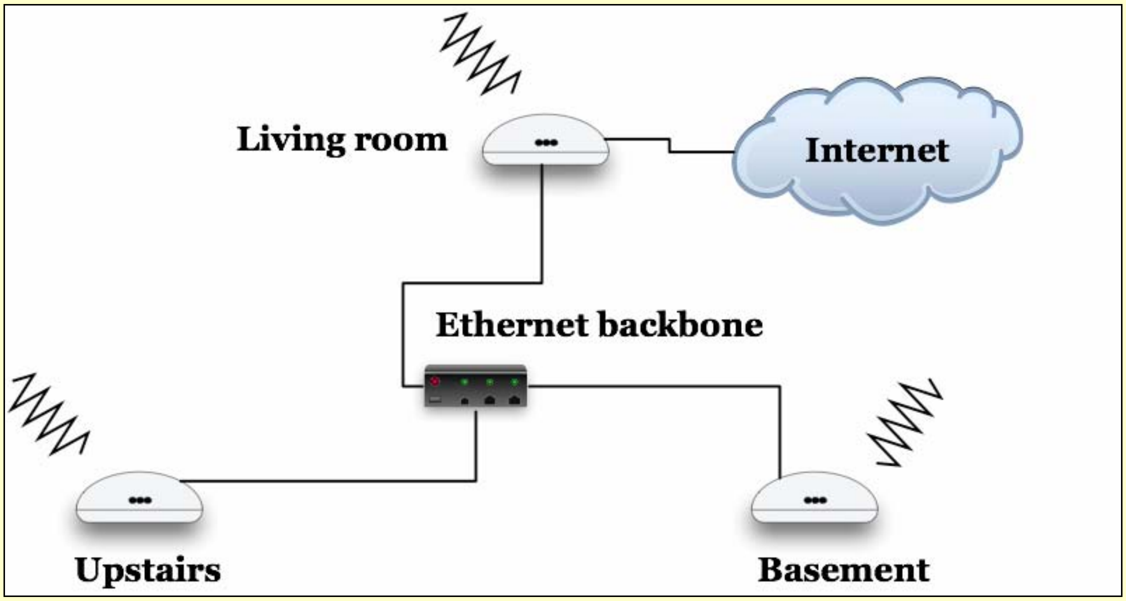
A relatively simple way to extend a network is to add access points. As noted earlier in Buy Subsequent Access Points More Cheaply, you want additional access points to be *dumb*. They should either lack features like providing DHCP service or have them turned off. Only your main access point should be *smart*, “firewalling” the outside world, connecting to the ISP, and handling other Internet and security tasks.

When you add additional access points, they must have the same network name, known as an *ESSID* (extended service set identifier). This enables computers to move around without changing their network settings because their AirPort cards automatically and seamlessly switch from one access point to another as needed to maintain a constant connection to the network. If you have encryption enabled, each access point must have the same options and keys set.

A very small number of wireless gateways don’t permit roaming: Asanté had one 802.11b model, for instance, that didn’t allow it, which surprised me. But all the 802.11g gateways from major manufacturers that I know about do allow roaming.

When adding access points to create a network that allows roaming, you need a network backbone that connects all the access points. Typically, you use Ethernet cabling to connect the access points (**Figure 15**). However, you can also use wireless connections or electrical connections to form that network backbone, as I describe in Bridge Wirelessly and Extend with HomePlug.

FIGURE 15



A simple network topology with one base station connected to the Internet in the living room; another base station upstairs; and a third in the basement. They're all connected by Ethernet to a switch.

The most important part of adding access points is choosing the Wi-Fi channels for them wisely. Wi-Fi has 11 overlapping channels in the U.S.; some countries have as many as 14, such as France. For best performance, you should use the farthest distant channels from one another in the same physical area at the same time: channels 1, 6, and 11 (U.S.) or 1, 7 or 8, and 14 (other countries).

TIP The important thing is to avoid overlapping channels, so if you have only two access points, for instance, you could make them channels 1 and 6, or you could set them to 2 and 10—the details don't matter as long as they're far enough apart.

You might consider using 802.11b access points to extend an 802.11g network unless you really need the speed everywhere. Often, an 802.11g base station has more advanced features or is easier to configure, making it worthwhile as your main hub, but potentially overpriced for outlying base stations.

TIP Although there's no problem with mixing 802.11b access points with an 802.11g base station, do note that your fastest extended network comes from using all 802.11g-capable devices connected to Ethernet.

SIDEBAR LIGHT UP WITH POWER OVER ETHERNET (POE)

It's relatively easy to pull Ethernet cable to remote locations, but running extension cords for power is more difficult. Power over Ethernet, or PoE, is an interesting way to position access points in areas where it's hard, expensive, or dangerous to bring electrical power. PoE used to be too expensive for all but institutional use, but it's come down in price.

With PoE, the Ethernet cable that brings the network to the wireless gateway also brings power at a low voltage over unused wires. This works because Ethernet is DC (direct current) electricity modulated in a certain manner, so running straight voltage is a small step. A PoE network needs power injectors on both ends that separate juice and data, or just on one end if you use a wireless gateway such as the AirPort Extreme Plenum model described in AirPort Extreme. Only a few Ethernet switches include PoE in each port and can be configured port by port to inject power into the cable. These are mostly expensive switches, but the feature should catch on over time.

PoE is most often used for exterior applications, like putting a base station in a rugged, weatherproof case on the roof of a house or building. An Ethernet cable carrying 12 volts at low amperage is much safer than the full 110- or 220-volt equivalent of a real outlet.

For beginners, your best bet is a kit from Macwireless.com, which sells several configurations for AirPort base stations (http://www.macwireless.com/html/products/poe/). HyperLink Technologies offers a more extensive but more technical set of PoE adapters (http://www.hyperlinktech.com/web/poe.php).

Don't run standard Ethernet cable outside unless you enclose it in conduit! The plastic shielding isn't designed to resist ultraviolet light or water, and it will likely break down within 6 months. Although it's more expensive and harder to work with, you need Ethernet cable rated for outdoor use, or even for direct burial. Ask at electrical supply stores or electronics stores. Some cable has a gel around the insulated wires inside a wrapper to avoid cracking during a freeze.

Also, look into proper grounding. You don't want lightning to destroy every device on your network or burn down your building. If in *any* doubt, consult a qualified electrician. A recent lightning strike near Adam Engst's entirely indoor network destroyed a Mac's Ethernet port—imagine if the cable had been outside!

Bridge Wirelessly

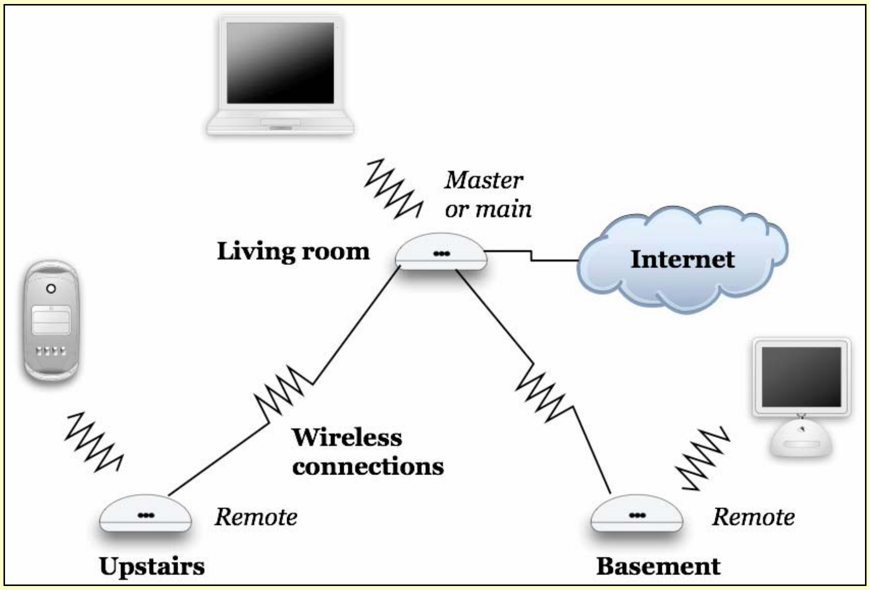
Wireless Distribution Service (WDS) is a neat way to extend an AirPort network without running wires between locations. As I note previously, if you want to extend a network by adding access points, you might connect them via Ethernet—which means more wires. Instead, WDS can connect an access point to other access points as easily as wireless clients connect to an access point.

How it works

WDS works in a manner very similar to plugging an Ethernet hub into an Ethernet switch. An Ethernet hub interconnects all the connected devices to each other as a single segment, just like wireless clients connecting to a wireless base station. An Ethernet switch, by contrast, isolates each port as a separate segment. A computer connected to a hub connected to a switch's port can reach computers on other ports' hubs because the switch knows to transfer data across segments based on where the computers are located.

Likewise, WDS allows access points to exchange information about where computers and other devices are located on a physical network. One access point can then route data to another or to a series of other access points to reach the destination computer (**Figure 16**).

FIGURE 16



The same basic set up used for an Ethernet-connected network can work with WDS. In this example, each base station is set to WDS and to serve access to local computers wirelessly as well.

WDS options in hardware

Unfortunately, WDS appears in different forms in each wireless gateway that includes it. The best implementations come from Apple and Buffalo Technology because these companies' base stations allow a base station to work as an access point serving access to local wireless clients while simultaneously connecting to one or more other base stations to exchange data across a wireless backbone.

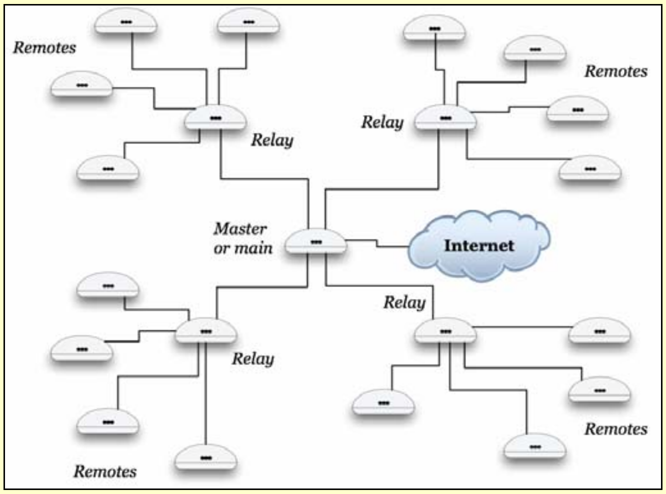
NOTE The biggest downside in WDS is that on a busy network, you effectively halve, quarter, or even eighth, your available bandwidth: All the network traffic that travels among access points over WDS reduces the overall throughput of the network. But with an effective network throughput of about 25 Mbps on an 802.11g network, even splitting that into pieces still provides plenty of usable bandwidth.

In general, to set up WDS you need to know the MAC address of each the wireless gateway you want to connect (see the sidebar What and Where is a MAC Address?). However, the AirPort Extreme Base Station will scan for other gateways, letting you simply select them by name.

Apple, Buffalo, and Linksys each have distinct approaches to how they allow WDS to be used. WDS suffers from a not-so-theoretical issue called the "hidden node" problem, which is exacerbated or mitigated depending on the approach.

Apple's WDS approach: Apple considers one device the master, which they call a main base station. This device is usually the one best positioned to connect to an Internet feed. Base stations that connect to the main are called remotes, and they relay traffic via the main to and from their clients, whether to other clients on the local network or out to the Internet. Finally, Apple defined a relay, which a remote can connect to and which is in turn connected to a main. You could have 4 remotes on each relay and 4 relays connected to a main for a total of 21 base stations (**Figure 17**), although bandwidth would be enormously reduced.

FIGURE 17



If one main base station tells four friends, and they tell four friends…well, this is what happens.

SIDEBAR THE HIDDEN NODE PROBLEM

In a mesh network in which multiple wireless access points connect to each other, the "hidden node" problem occurs when one node has at least two access points that can see the node but can't see each other. Because Wi-Fi works very much like Ethernet, it relies on collision detection that requires that every device on a segment can spot when other devices start transmitting and then back off.

With a hidden node, some devices can't tell when other devices are transmitting, resulting in crosstalk, interference, and problems. When designing a network to use WDS with more than a few points, you may have to give this issue some consideration. In some cases, you'll see a performance reduction if you ignore it; in others, the network might mysteriously vary in its quality and reliability.

TIP Based on the information available as the book goes to press, AirPort Express can function only as a main or as a remote, but not as a relay, due to its more limited function. AirTunes—streaming music from iTunes to a stereo via AirPort Express—works just fine over WDS, however. See Appendix C: Configuring AirPort Express.

Buffalo's WDS approach: Buffalo allows each base station to connect to up to six others. They don't all have to connect to one another, either, resulting in complicated topologies that might not always work because of the hidden node problem. Simpler is better.

Linksys's WDS approach: Linksys decided to allow its devices to be only in WDS bridging mode or in access point mode. As a result, you would have to buy two Linksys wireless gateways to have both the benefit of wireless bridging and to service local client computers. Although that scenario doubles your cost, you can set the bridges to an entirely different Wi-Fi channel, which essentially doubles your overall network throughput.

Configuring WDS on the AirPort Extreme Base Station

1. Open the Applications folder, then the Utilities folder, and run AirPort Admin Utility.

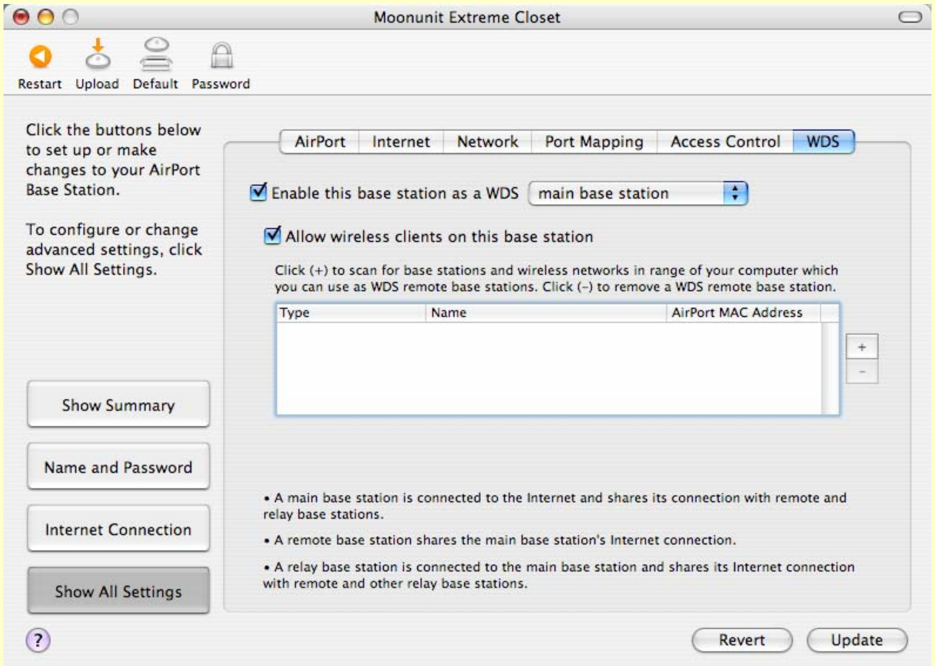
TIP If you don't have AirPort Admin Utility in the Utilities folder, then you haven't installed the AirPort software (or you've moved Airport Admin Utility). You can download the utility, which works on Macs without Wi-Fi, from http://www.apple.com/support/downloads/airportupdate.html.

NOTE I haven't seen the AirPort Express configuration options yet, as the unit hasn't shipped, but it's likely to use a similar or identical method to configure WDS. However, AirPort Express will also include a setup assistant to help you avoid these steps when you add it to a network.

2. Choose the base station that you are setting as the main base station from the left pane and connect to it.

3. Click Show All Settings and click the WDS tab (**Figure 18**).

FIGURE 18



Click the buttons below to set up or make changes to your AirPort Base Station.

To configure or change advanced settings, click Show All Settings.

☑ Enable this base station as a WDS: main base station

☑ Allow wireless clients on this base station

Click (+) to scan for base stations and wireless networks in range of your computer which you can use as WDS remote base stations. Click (–) to remove a WDS remote base station.

- A main base station is connected to the Internet and shares its connection with remote and relay base stations.
- A remote base station shares the main base station's Internet connection.
- A relay base station is connected to the main base station and shares its Internet connection with remote and other relay base stations.

The WDS tab of the Show All Settings view in AirPort Admin Utility.

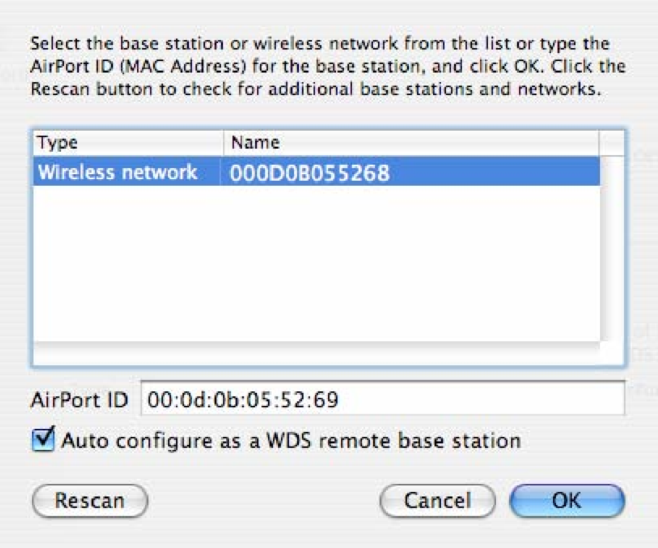
4. Check Enable This Base Station as a WDS, and choose Main Base Station from the pop-up menu.

5. Uncheck Allow Wireless Clients on This Base Station if you want this unit to act just as a bridge.

6. Click the + (plus) button to the right of the empty list box.

7. In the dialog that appears, you can see a list of other base stations (**Figure 19**). Select the base stations you want to add one at a time. Leave Auto Configure as a WDS Remote Base Station selected to skip connecting to the remote base station and configuring it through these steps as well—the software on the main base station handles that for you.

FIGURE 19



Select the base station or wireless network from the list or type the AirPort ID (MAC Address) for the base station, and click OK. Click the Rescan button to check for additional base stations and networks.

Type	Name
Wireless network	000D0B055268

AirPort ID: 00:0d:0b:05:52:69

☑ Auto configure as a WDS remote base station

Choose the other base stations, and optionally have the main base station automatically configure them for you.

8. I recommend testing each base station as you add it by clicking Update in the main Admin Utility screen, waiting for the base station to reboot, and then making sure clients can connect (if enabled) and bridge on all attached units.

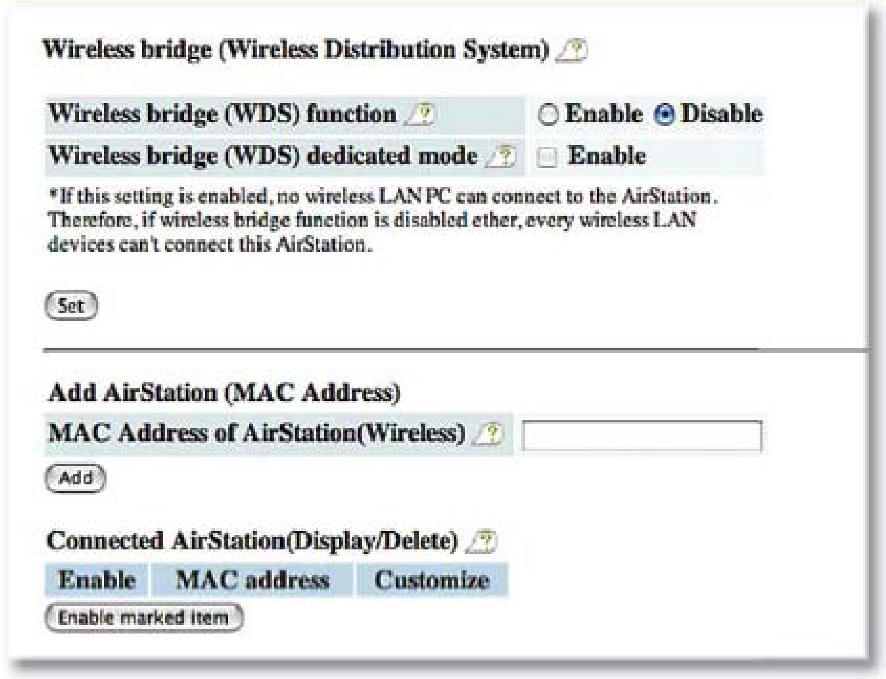
9. Repeat steps 1–8 for each additional manually configured remote base station and for every relay base station.

Configuring WDS on a Buffalo gateway

This configuration works for all 802.11g Buffalo gateways with WDS. My example uses the WLA2-G54 base station.

1. In the Web configuration screen of one bridge in the WDS set, click the LAN Setting option in the left navigation bar, and then click Wireless Bridge (WDS) below it (**Figure 20**).

FIGURE 20



Wireless bridge (Wireless Distribution System)

Wireless bridge (WDS) function	○ Enable ● Disable
Wireless bridge (WDS) dedicated mode	□ Enable

*If this setting is enabled, no wireless LAN PC can connect to the AirStation. Therefore, if wireless bridge function is disabled ether, every wireless LAN devices can't connect this AirStation.

Add AirStation (MAC Address)

MAC Address of AirStation(Wireless)

Connected AirStation(Display/Delete)

Enable	MAC address	Customize

Configuring Buffalo WDS settings.

2. Select the Enable radio button next to Wireless Bridge (WDS) Function.

3. If you want the unit to act just as a bridge and to not serve local wireless clients, check the Enable box next to Wireless Bridge (WDS) Dedicated Mode.

4. Click Set, and then return to this page after the unit reboots.

5. Enter the MAC address of the first unit in its colon form (00:00:00:00:00:00) and click Add. You may have to reboot the gateway, although that shouldn't be necessary.

6. Repeat steps 1–5 for a complementary unit to the one you just configured.

7. Test that the two work together and are carrying traffic. If they are, then repeat steps 1–5 for each additional unit. Each unit should contain the MAC address for each other unit that's part of the same WDS set.

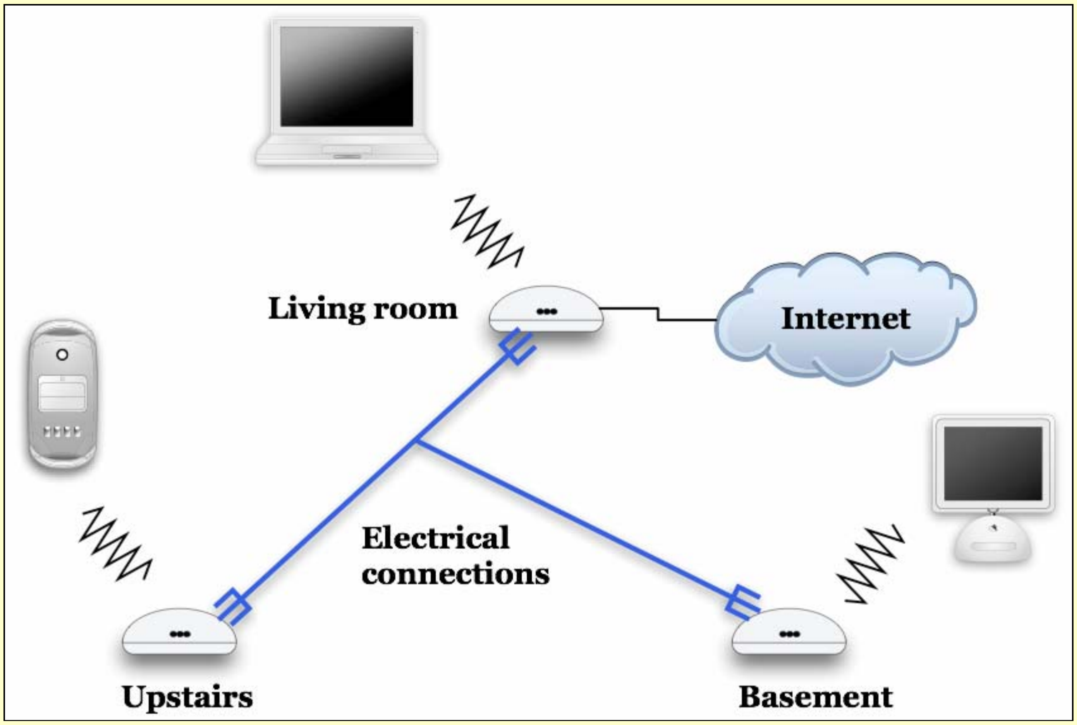
Extend with HomePlug

What's the most robust and ubiquitous wired network in your home? The electrical system! We don't think of data transmitting over power, but all wired networks use electricity to encode data. In the case of HomePlug, small adapters plugged into outlets modulate data over the 60 Hertz (Hz) cycle used in U.S. power. It's not the fastest network you'll see, offering a real throughput of about 6 Mbps, but that's about what you'll see from 802.11b, and very likely not much different from a network extended with WDS.

HomePlug has no central hub in most cases. Macintosh users should purchase $50 HomePlug Ethernet bridges, which offer a single Ethernet jack. You plug a cable from your Mac into this bridge, and you're done. The HomePlug system handles communicating among all the adapters on your electrical network.

To extend a wireless network, simply place access points in the appropriate locations, give them the same network name, set them to non-overlapping channels, and then plug them into HomePlug Ethernet bridges (**Figure 21**). And that's it.

FIGURE 21



HomePlug connects via the electrical wiring in your home using one Ethernet bridge per access point.

TIP You can enable robust encryption on the HomePlug network—it uses 56-bit DES—but you almost always need a Windows system to run the configuration software. Unless you're in an apartment building or other shared area in which you're concerned about people tapping in to your network via HomePlug, don't worry about it.

There's an interesting option for HomePlug and Wi-Fi: One form of HomePlug bridge is a wireless access point of the dumb variety, exactly the kind I recommend. For about $80, this HomePlug Wi-Fi adapter can be the compact extension to your network that you need.

Add an Antenna

If you can't reach every part of the area you want, the temptation is to boost the signal. Adding an antenna can increase the range of your Wi-Fi gateway, but it's not necessarily the best choice.

Because Wi-Fi is a two-way transmission, just boosting the access point's power and sensitivity doesn't necessarily mean that a client will magically work better. In many cases, adding a second inexpensive access point will offer superior advantages with less monkeying around (and in fact, Wi-Fi was designed around adding access points to extend range).

The fundamental problem with adding antennas is that it's technically illegal in many cases. Despite the fact that many wireless gateways come with antennas that can be removed or with jacks to add antennas, the FCC allows an antenna to be used if only it was tested and approved with a specific gateway. You cannot have an FCC approved antenna; only an FCC approved system. That said, there has never been a charge or arrest for this widespread activity, but I can't legally recommend it.

You can purchase antennas legally from several companies; HyperLink Technologies (http://www.hyperlinktech.com/), QuickerTek (http://www.quickertek.com/), and MacWireless.com (http://www.macwireless.com/) sell a variety of antennas, including ones designed specifically to work with AirPort and AirPort Extreme Base Stations and Linksys gateways.

Antennas come in several varieties, the most useful antenna for general purposes is *omnidirectional,* which means it can send signals in all directions.

For detailed advice about using antennas, consult Chapters 21 and 34 of *The Wireless Networking Starter Kit, Second Edition* (find it in print and electronic versions at http://wireless-starter-kit.com/).

Solve the Titanium PowerBook Range Problem

If there's one subject I've heard way too much about, it's the terrible range of the AirPort card in the Titanium PowerBook G4. The poor range is caused primarily by the poor placement of the antenna in the base rather than the screen.

Even though the Titanium PowerBook G4 has been replaced with the better-performing aluminum 15-inch PowerBook G4, there are hundreds of thousands of Titanium PowerBook G4s floating around, and many still-frustrated users who aren't ready to replace their machines.

Several suggestions have been made over the years to improve the Titanium PowerBook G4's range, but the simplest and most effective is to remove the AirPort Card (you can sell it on eBay for a decent price, amazingly enough) and add a third-party 802.11g PC Card from Linksys, Buffalo, or Belkin. Some people particularly like the Sony PCWA-C150S because it matches the titanium finish of the PowerBook G4 and doesn't stick out far.

As long as you're running Mac OS X 10.2.8 or later and AirPort 3.2 or later, you can simply plug in the replacement card, and the AirPort software treats it like a built-in device. With a PC Card, you'll enjoy terrific range because the card moves the antenna entirely outside the laptop's case.

You can also opt for a USB adapter or a variety of other older, cheaper cards or higher-powered cards, which I talk about in Appendix B: Connect without AirPort Adapters.

Talk to Your Neighbors

A frustrating part of Wi-Fi networking is that you can't control your "air space." This is a case of being hoisted, sometimes, by your own petard: The same regulations that allow everyone to use the spectrum means that everyone around you can also use the same parts of the spectrum. I often find that when someone is having problems using a Wi-Fi network in a volume of space in which it should have good reception, there's a neighbor at work.

Especially problematic is the so-called "108" or "Turbo G" technology made by Atheros, which works at its highest speeds only with equipment by the same maker. Some testing has shown that Atheros's technology can dramatically reduce the speed of close-by Wi-Fi networks using any channel and any other makers' chips. Those results aren't definitive, but it's a good place to start if you're trying to diagnose a problem.

If you're finding performance varies by time of day or even minute to minute, and you've eliminated your 2.4 GHz cordless phone and microwave oven as culprits—they can both put static on the Wi-Fi line—you should run MacStumbler (http://www.macstumbler.com/) or iStumbler (http://www.istumbler.com/) to determine whether other networks are running in the vicinity. These two programs each scan for networks and can identify characteristics about them, such as signal strength and whether security is enabled.

If you find other networks, you might think about knocking on neighbors' doors, introducing yourself, and proposing an informal channel usage agreement: if your neighbor and you are both using channel 6, switch to 1 and 11 to increase the distance between signals.

If your neighbor is using Turbo G equipment typically made by NetGear or D-Link, you might be able to convince them to download and install firmware upgrades that offer a dynamic version of the proprietary speed boost. This dynamic version scans for competing networks and backs off a bit if it might impact a network.

You (and your neighbor) could also consider moving your access points farther away from one another to reduce the signal strength conflict in the middle.

Secure Your Network

If you use a wired network in your home, someone would have to break into your house, plug into your Ethernet switch, and then crouch there in the dark to capture data passing over your network.

Wireless networks have no such protection: anyone with an antenna sensitive enough to pick up your radio signals can eavesdrop on all the traffic passing over your network. This could be a neighbor, someone parked in a car, or a nearby business. Many free, easy-to-use software packages make this a simple task for only slightly sophisticated snoopers.

However, you're not powerless to prevent such behavior. Depending on what you want to protect and whom you're protecting against, you can close security holes with tools that range from a few settings up to industrial-grade protection that requires separate servers elsewhere on the Internet.

But before I delve into the details of protecting yourself from snoopers, let's look at whether you even need to turn security on.

Likelihood, Liability, and Lost Opportunity

When Adam Engst and I were writing *The Wireless Networking Starter Kit, Second Edition*, we had a disagreement over how much security concern the average home Wi-Fi networker should have. Adam came up with a great formulation that I agreed with and want to walk you through. He calls it the three L's of security: likelihood, liability, and lost opportunity. This framework lets you evaluate how much security—if any—you need to apply to your network.

Note If you'd like to know more about any of the topics in this section, read *The Wireless Networking Starter Kit, Second Edition* (http://wireless-starter-kit.com/), which devotes 50 pages to the subject.

Likelihood

The first aspect of security to consider is likelihood: how likely is it that someone will violate your privacy, steal your data, or otherwise exploit you? If you live in a lightly populated area, and no one could easily come within range of your network without sitting in your driveway, you probably don't have much to worry about.

But if you live in an apartment building with neighbors who could pick up your connection, the likelihood of someone connecting to your network rises significantly, generating the question of whether you want to allow others to share your Internet connection or not.

The likelihood of attack increases significantly if you're running a business, since it's plausible that your network would carry sensitive information such as credit card numbers, business plans, and so on. Also, most businesses are located in areas or buildings where someone could easily sit and hack into your network without being noticed.

Liability

What is the realistic liability if someone were to record all the traffic that passed across your wireless network? For most home networks, the amount of network data that's at all sensitive is extremely low; perhaps a credit card number being sent to a unusual Web site that doesn't use *SSL* (a secure Web server standard), maybe some financial data, possibly some bits that would be embarrassing if made public.

Simply allowing someone else to use your Internet connection has a relatively low liability in most cases. However, you may think differently if you pay per byte, if you have a slow dial-up connection that would be impacted by someone else's use (with high speed DSL and cable modem connections, you're unlikely to notice another user), or if you're concerned that allowing someone else to use your connection would be violating your ISP's terms of service in a way that was likely to result in you being disconnected.

Businesses are, once again, a different story. The likelihood of sensitive and confidential information passing through a business's wireless network is much higher, of course, and the liability of an outsider learning that information is significantly greater. If a business's customer data were extracted from a wireless network, it could involve a disastrous loss of reputation and even lawsuits. And if a competitor learned confidential business plans, the ramifications could be catastrophic.

Lost opportunity

With home wireless networks, the opportunity cost for layering on security comes mostly in the form of troubleshooting irritating problems, which is more necessary and harder when security is on, and in the annoyance of dealing with passwords with new machines or when you have visitors.

Companies, even small ones, may have fewer lost opportunities because they might have a dedicated staffer or whole department that deals with installing, maintaining, and supporting the software that allows overall security.

Your spot in the security spectrum

It's up to you to determine the likelihood of someone breaking into your network and either using your Internet connection or eavesdropping on the data that flies by. Next, you must determine the severity of the problems that would ensue from someone using your bandwidth or using a network sniffer to record your data. Lastly, you need to figure out what the lost opportunity of different levels of security is: The higher the likelihood of attack and the higher the liability if your network were to be invaded, the more you're probably willing to spend and the more annoyance you're willing to endure.

Once you've worked through those three thought exercises, you can determine just how much money and effort you should expend to secure your wireless network. Now let's look at how you might apply such security precautions.

Simple Tricks That Don't Work

You may have read suggestions advising you to hide your network's name and make it hard to connect to, as a method of setting up basic network security. These techniques are called *closed network* and *MAC address filtering*.

Closed network

In a closed network, your base station turns off *beaconing*, which is a tag that lets other computers easily see your network's name. An open network appears by name in the AirPort menu or in other places in the Mac OS that show the name of networks you can connect to. But closing the network makes it only slightly obscure. With the addition of readily available software for any platform, someone can see your network's name. So you cannot rely on closing your network for any real security.

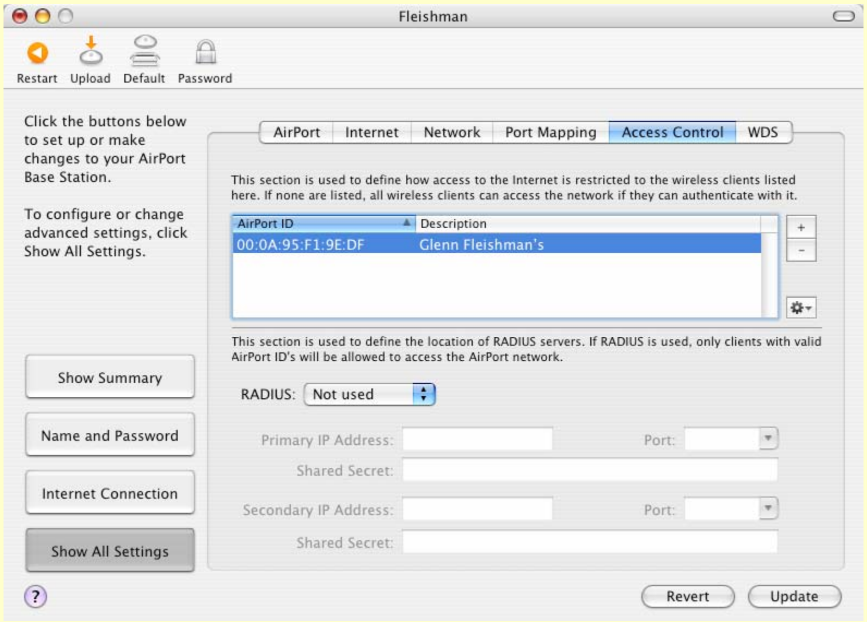
TIP Joining a closed network through the AirPort or similar interfaces just requires knowing its name. With an AirPort adapter, choose Other from the AirPort menu and enter the network's name precisely as you set it or as it was provided to you.

MAC address filtering

MAC address filtering sounds more promising initially. With this method, you enter the MAC address of every computer you want to allow to connect to your Wi-Fi network. If a computer's address isn't in the list, then it can't connect.

On the AirPort Extreme Base Station, for instance, you use AirPort Admin Utility to connect to the base station and, via the Access Control tab, add the MAC address of each computer (**Figure 22**). (The sidebar What and Where is a MAC Address? explains how to find adapters' MAC addresses.)

FIGURE 22



Click the buttons below to set up or make changes to your AirPort Base Station.

To configure or change advanced settings, click Show All Settings.

This section is used to define how access to the Internet is restricted to the wireless clients listed here. If none are listed, all wireless clients can access the network if they can authenticate with it.

AirPort ID	Description
00:0A:95:F1:9E:DF	Glenn Fleishman's

This section is used to define the location of RADIUS servers. If RADIUS is used, only clients with valid AirPort ID's will be allowed to access the AirPort network.

RADIUS: Not used

Adding MAC addresses to filter access.

The flaw with MAC address filtering is that any cracker worth her salt can easily monitor a network to see which MAC addresses are able to access the network. She can then use simple software to modify or *clone* the MAC address on her own network adapter to use one of those addresses, thus gaining access.

TIP If you use MAC address filtering and your network has multiple base stations, each one must have the same list of allowed MAC addresses.

Although MAC address filtering and a closed network will deter casual passers-by, they don't really constitute a defense. You can step up security through the methods described next.

SIDEBAR **WHAT AND WHERE IS A MAC ADDRESS?**

The *MAC*, or *Media Access Control,* address has nothing to do with Macintosh computers. Instead, it represents a unique address for every network device, including Ethernet and Wi-Fi adapters. A MAC address consists of six two-digit hexadecimal numbers separated by colons, such as 0A:F2:33:01:02:FC. The first three pairs of numbers are assigned to a manufacturer; Apple has at least two common ranges, which begin with 00:0a:95 and 00:03:93.

Because MAC addresses are now so frequently used for filtering, authentication, and WDS, the numbers are easier to find. Buffalo and Apple print the MAC address of the Wide Area Network Ethernet port and the Wi-Fi adapter on the back or underside of their hardware.

You can also find these numbers through the admin program or Web interface you use to configure a wireless gateway. For an AirPort Extreme Base Station, run the AirPort Admin Utility (found in the Utilities folder inside the Applications folder). Select the base station from the left pane, and the MAC numbers show up at the right. The AirPort ID is the device's wireless MAC address.

To find the MAC address of an AirPort or AirPort Extreme Card, open the Network preference pane in System Preferences and choose AirPort from the Show pop-up menu. The MAC number is listed as the AirPort ID. (Ethernet MAC addresses are labeled as Ethernet ID in the Ethernet adapter's settings in the Ethernet tab.)

Protect with WEP

From 1999 to 2003, the only straightforward way to secure a wireless network was by using *WEP* (Wired Equivalent Privacy). WEP is a system that enables you to invent an encryption key and enter that same key on a base station and all connected adapters. This key is used as the basis of encrypting all data that passes over the network. Without the key, the data appears to be gibberish.

The reason to turn WEP encryption on is twofold: first, to make sure that only people with the key can join and use the network; second, to obscure the traffic you're sending so that it remains private.

If neither of those issues is a concern, you can skip WEP and WPA in the next section. But most home Wi-Fi networkers feel safer with at least a little protection.

WEP basics

WEP comes in two key lengths: 56 bits and 128 bits; longer keys were seen as more secure, and hardware that uses them once cost more. WEP keys are generally entered as hexadecimal or base-16 numbers. A 56-bit WEP key is 10 hexadecimal digits; a 128-bit WEP key is 26 hexadecimal digits.

NOTE Because 16 bits of a WEP key aren't unique, you can also see WEP keys described as 40 and 102 bits. But that's just terminology—40-bit and 56-bit keys are the same, as are 102-bit and 128-bit keys.

Some gateways let you enter 5 or 13 text characters to create the short and long WEP key through simple mapping. These sets of characters are called *ASCII WEP keys* after the ASCII standard for text encoding.

Apple has always done a wonderful job of hiding the guts of WEP by allowing Mac users to enter a passphrase, such as "baby buggies," which the AirPort software converts into the appropriate hexadecimal number.

The primary difficulty in using WEP, which is found in all Wi-Fi equipment, is that Mac users sometimes have problems in interchanging Apple's friendly text WEP passwords and the more generally accepted hexadecimal and ASCII keys. And entering 26 hexadecimal digits is no one's idea of a good time.

WEP's weakness

Starting in 2001, unfortunately, several flaws began to emerge that made it possible to extract the WEP key by examining sufficient traffic passing over the network. A few pieces of free software now automate this process for crackers with no knowledge of WEP.

WEP is therefore no longer reliable for businesses that move substantial amounts of traffic over their wireless networks: As little as 15 minutes of Wi-Fi sniffing can enable software to break the key on a fully loaded network. But even busy home networks might require a day to a week of solid observation to break, which means that most home users have nothing to worry about.

If you're really concerned, you can upgrade your software or your gear to support *WPA* (Wi-Fi Protected Access), which is widely available in all newer Wi-Fi equipment, and described in Protect More Easily with WPA. WPA doesn't suffer from any of these flaws.

NOTE The new setup assistant that comes with AirPort Express will let you bypass some of the more obscure settings for WEP and WPA by answering questions or choosing from a list that explains the options. Watch for updates to this book for details when AirPort Express ships. Click the Check For Updates button on the cover of this book or click here to access update information.

Setting up WEP on an all-AirPort network

WEP works on AirPort networks that use graphite, snow, or AirPort Extreme base stations.

First, enter a key on the base station:

1. Run AirPort Admin Utility and connect to your base station.
2. Click Show All Settings.
3. Click the Name & Password tab or click Show All Settings.
4. Click Change Wireless Security.
5. From the pop-up menu, choose 128-bit WEP.

TIP You could choose 40-bit, but 128-bit does provide additional (but not exponential) security. However, if you are using AirPort and non-AirPort equipment together, using a 128-bit key requires entry of 26 hexadecimal digits on non-AirPort devices.

6. Enter your password phrase in Network Password and Verify Password, and then click OK.

7. Click Update to have the base station recognize the new encryption settings.

Next, enter the key on your AirPort or AirPort Extreme-equipped client Macs:

Mac OS 9:

1. Choose your network from the AirPort menu in the Control Strip (or run the AirPort application), expand the window by clicking the expansion triangle, and choose your network from the Choose Network pop-up menu.

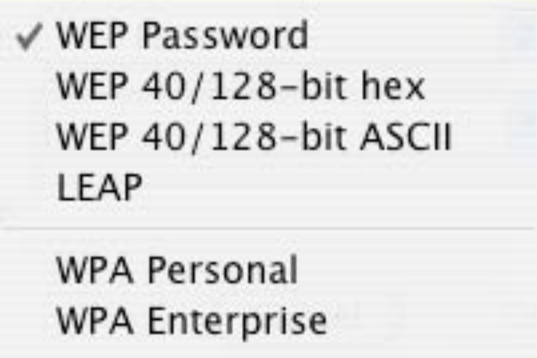
2. In the dialog box that appears, enter your AirPort password.

Mac OS X:

1. Choose the network from the AirPort menu (or run Internet Connect in the Applications folder and choose the network from the AirPort tab's Network pop-up menu).

2. In the dialog that appears, choose WEP Password from the Wireless Security pop-up menu (**Figure 23**), and enter it twice in the fields provided.

FIGURE 23



Apple's WEP password is the first choice. The other choices are explained ahead, in Joining a WEP-protected, non-AirPort network with an AirPort or AirPort Extreme Card.

Extracting an AirPort key for a non-AirPort adapter

Any computer that wants to join a WEP-protected AirPort network and doesn't have an AirPort or AirPort Extreme Card in it—whether it's a Mac or a Windows or Linux box—needs to have the hexadecimal equivalent of the Apple WEP password. Fortunately, it's easy to obtain:

1. Run the AirPort Admin Utility and connect to your base station.

2. Choose Equivalent Network Password from the Base Station menu.

TIP You may want to make a screen capture of this hexadecimal key or type it into a text document to have it handy, especially if the key is a 128-bit WEP password—26 characters long! Press Command-Shift-4 to select an area of the screen in Mac OS X to capture. Mac OS X records the selected area as a PDF file saved on the Desktop.

Joining a WEP-protected, non-AirPort network with an AirPort or AirPort Extreme Card

If you adopt a wireless gateway other than Apple's, you might run into some confusion when trying to enter a WEP key on a Mac with an AirPort or AirPort Extreme Card.

First, set your key in the wireless gateway in either hexadecimal or ASCII as either 40/56 or 102/128 bits. If you're joining a network set up by other people, obtain the key from them in either format.

In versions of the Mac OS before 10.2, including 8.6 and 9.x, you can enter WEP keys only in one of two ways in any dialog that prompts for the key when joining the network:

For a hexadecimal WEP key: Enter **`$`** (dollar sign) first, and then follow it with the hex key with no spaces, like **`$FEEB998877`**.

For an ASCII WEP key: Surround the key with double quotation marks, like **`"frech"`**. Those are straight quotes, not curly quotes.

Starting with Mac OS X 10.2, however, you can choose the kind of WEP key from a pop-up menu (**Figure 23**, on the previous page). Although you can still use a dollar sign or quotation marks, you can also just choose either WEP 40/128-bit Hex or WEP 40/128-bit ASCII from the pop-up menu and ignore the extra characters necessary in previous versions of the Mac OS.

Protect More Easily with WPA

When I said earlier that WEP had major security weaknesses that weren't entirely applicable to home and small-business users, I also noted that there was a solution: WPA (Wi-Fi Protected Access). WPA was developed by The Wi-Fi Alliance to bridge the gap between WEP and a future standard known as 802.11i. An engineering group ratified 802.11i in June 2004, but firmware and software updates to allow its additional features probably won't appear until September at the earliest. And none of its new features are a reason to wait on using Wi-Fi or deploying WPA security.

WPA fixes the methods by which security can be compromised, and makes the overall system less likely to be broken. WPA is available as a firmware upgrade for almost all older adapters, and either as an upgrade or as part of the shipping product for all newer hardware released since late 2002.

WPA's big advantage is that although it can use a hexadecimal key—one that's 64 hex digits long!—all platforms, not just Apple's, allow you to enter a more easily remembered text passphrase with punctuation, like `Rufus ate_my!water ba1100n`.

TIP Researchers believe that WPA keys are susceptible to cracking through brute force if you choose keys that are shorter than 20 characters long and contain only dictionary words. Choosing short random numbers, letters, and punctuation, or longer passphrases with a few punctuation marks defeats this problem, as in the example passphrase above.

The original AirPort Base Station cannot be upgraded to WPA, but the AirPort Extreme and the AirPort Express Base Station supports it. All AirPort and AirPort Extreme Cards can use WPA, but only within Mac OS X 10.3: older systems lack WPA support.

TIP If you want to upgrade an older non-AirPort adapter for WPA, check out this article I wrote that links to the various firmware upgrades scattered around the Internet for cards as old as those made in 1999: http://wifinetnews.com/archives/002875.html.

Although it's technically possible for a base station to simultaneously support WPA and WEP, only SMC offers units with both—which reduces the network's security down to WEP's weaker level! More typically, you must set either WPA or WEP as the encryption mode and make sure that if you choose WPA all your computers have the right updates to handle it as well.

Turning on WPA with AirPort Extreme

1. Run AirPort Admin Utility and connect to your base station.
2. Click Name & Password or click Show All Settings.
3. Click Change Wireless Security.
4. From the pop-up menu, choose WPA Personal.

NOTE WPA Personal uses a fixed key entered manually in the base station and all connected adapters. WPA Enterprise requires a special authentication server that allows you to log in with a user name and password but not a key; the server creates a unique key for each computer that's connected and rotates them frequently. This adds to security.

With a Personal key, each user on the network can still potentially see all the traffic of other users; with Enterprise, that's impossible.

5. If you leave the pop-up menu that appears set to Password, enter a key of 8 to 63 characters, including most punctuation. If you change the pop-up to Pre-Shared Key, you must enter 64 hexadecimal digits.
6. Click Update and wait for the base station to reboot.

You can now use the same password to connect from any WPA-capable system.

Connecting with AirPort to a WPA network

1. Choose the network you want to connect to from the AirPort menu.
2. At the prompt to enter a password, choose WPA Personal from the pop-up menu.
3. Enter the password or hexadecimal key, and click OK.

Deploy Application Security

The earlier sections about security primarily cover methods of securing your network against someone joining it, and secondarily against having your traffic decoded and observed. There are times when you might, in fact, want to allow anyone to join a network, but protect your own traffic over the network. This allows the best of both worlds: you can offer an open access point while keeping your data private.

The tips in this section are equally useful for a protecting data across a local network as they are for using a public hotspot network which, by its nature, tends to lack any data encryption.

Each of these techniques encrypts data—from a single password up to all traffic entering and leaving your computer. Depending on what level of security you want, these tips should provide you peace of mind and freedom from interception.

Secure Webmail

Reading email via a Web browser is an increasingly common task, especially with Webmail services that can connect behind the scenes to a "real" email server running the common POP or IMAP standards. But anything you read via a Web browser is sent in plain text.

To protect Webmail sessions, choose a provider that offers *SSL* (Secure Sockets Layer) connections. An SSL connection encrypts all traffic, rendering it impenetrable to anyone else.

Fastmail.fm (http://fastmail.fm/) and Google's Gmail service (currently in beta at http://gmail.google.com/) offer secure Webmail. Fastmail.fm requires a $14.95 one-time payment for SSL-based access, while Gmail includes it (currently) for free.

TIP Gmail isn't advertising its SSL feature in beta, but it's easy to reach. Enter **`https://gmail.google.com/`** to log into your Gmail account instead of **`http://gmail.google.com/`**.

FTP over SSH

If you're exchanging files via FTP with remote servers, you might try a newer form of secure FTP that uses *SSH* (Secure Shell) to encrypt the connection. To use FTP with SSH, the remote server must have an SSH software server running.

SSH is a built-in part of Mac OS X, and can be enabled through System Preferences alongside FTP:

1. Open the Sharing preference pane in System Preferences.
2. In the Services tab, check the Remote Login box to enable SSH and check the FTP Access box to enable FTP.

On the client side, you need FTP software that can handle the SSH connection, such as Interarchy from Stairways Software (http://www.stairways.com/). In Interarchy, select options from the File menu's SFTP submenu to connect to an FTP server over SSH.

SSL email

Some ISPs offer SSL email in which your email client initiates an SSL connection for sending and receiving mail. All current versions of popular email clients for Mac OS X, including Entourage, Mailsmith, Apple Mail, and Eudora, support SSL email. Check with your ISP to see if that's an option; you may have to do no more than check a few boxes in your account setup to turn SSL email on for either or both POP/IMAP and SMTP.

APOP and Authenticated SMTP

If you're concerned only with protecting your email passwords (which may be the same as passwords used for other services) and not at all about the potential of the contents of your email being read, you can encrypt your email passwords by using *APOP* (Authenticated POP) and *Authenticated SMTP*.

Both require that your ISP offer the service at the server level, and both are simple to set up in any mail client. With APOP, you enter your password in your email program, but the program sends a unique one-time password to the server—it's essentially a disposable password that you don't have to manage.

Authenticated SMTP allows you to send email from any network, and it typically uses an encrypted login that protects your email password in the process. It can also use a fully encrypted SSL session, which is increasingly typical and, in fact, recommended by a recent anti-spam report issued by major ISPs.

VPN

The whole 9 yards of data-in-transit protection is a *VPN* (virtual private network). A VPN protects all the data entering and leaving your computer by encrypting it on its departure and decrypting it on its arrival.

A VPN requires that you connect to a VPN server that manages the secure tunnel formed between your computer and itself. Mac OS X Server 10.3 includes both major flavors of VPN servers: *PPTP* (Point-to-Point Tunneling Protocol) and *IPsec-over-L2TP* (IPsec protocol over Layer 2 Tunneling Protocol).

TIP Mac OS X Server 10.3 is just $499 for 10 simultaneous users—and VPN users aren't counted against the total maximum simultaneous logins. This 10-user license can be an inexpensive solution for a small business to maintain local and remote network security.

Mac OS X 10.2 included an easy-to-use PPTP client, whereas 10.3 has both PPTP and IPsec. Both clients are built into the Internet Connect program found in the Applications folder.

To use a VPN, you first set up accounts on a server, and then turn on the VPN service in either or both flavors. Then you run a VPN client, provide the VPN server's address, enter a user name and password (for PPTP and IPsec) and an additional "shared secret" (for IPsec), and connect.

Once you've connected, all your traffic is encrypted until you once again disconnect. I've found that I can set up a VPN connection even over the slowest cellular data connection—9600 bits per second!

VPNs aren't for everyone, but they are an efficient way to protect your data when you have the right pieces in place.

Appendix A: AirPort Management Tools

Apple released the AirPort Management Tools 1.0 at the same time as the AirPort Software 3.4 release. You can download the tools from http://apple.com/support/airport/ by following a link in the Resources section at the right.

The tools comprise two packages:

- AirPort Client Monitor
- AirPort Management Utility

I discuss AirPort Client Monitor in Testing with an AirPort or AirPort Extreme Card or compatible varieties.

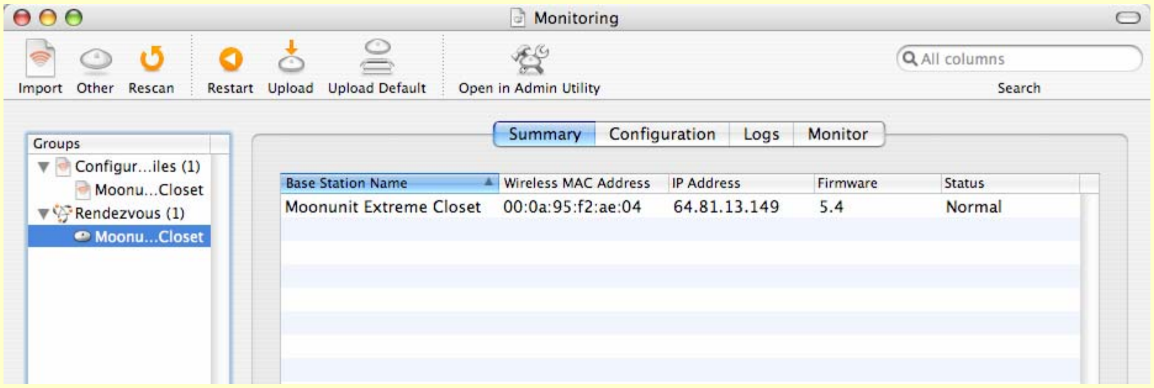
AirPort Management Utility is a much more sophisticated package designed to ease administration of many AirPort and AirPort Extreme Base Stations. It does not work with AirPort Express, which Apple considers a home gateway that will be used as a stand-alone item.

AirPort Management Utility provides a number of distinct features:

- Discovering base stations on the local network via Rendezvous
- Storing links to base stations by their IP addresses
- Allowing settings changes to be applied against several base stations at once
- Storing configuration files for individual base stations, or model files so that they can be applied to new base stations
- Viewing logs of events at base stations, such as client associations and network time synchronization
- Monitoring the signal strength over time of clients connected to a given base station, along with transfer statistics

The left bar of the AirPort Management Utility shows stored configuration files for base stations, base stations you've added manually by address that are stored in groups you define, and Rendezvous-enabled base stations that the program has discovered (**Figure 24**).

FIGURE 24



Base Station Name	Wireless MAC Address	IP Address	Firmware	Status
Moonunit Extreme Closet	00:0a:95:f2:ae:04	64.81.13.149	5.4	Normal

The Summary tab shows information for selected base stations.

Add base stations that have a static address by clicking Other (in the toolbar) and then entering the IP address and password for the unit. When you click OK, the base station shows up in the list at left in a group called New Group. You can create your own groups and drag base stations in and out of them.

You can select base stations and then click Open in Admin Utility (in the toolbar) to connect to them individually and use the AirPort Admin Utility interface for configuration.

One of the AirPort Management Utility's most useful features is the Configuration Files group. You can export a configuration from AirPort Admin Utility and then import it into AirPort Management Utility to then apply this file to other base stations as a model configuration. Follow these steps:

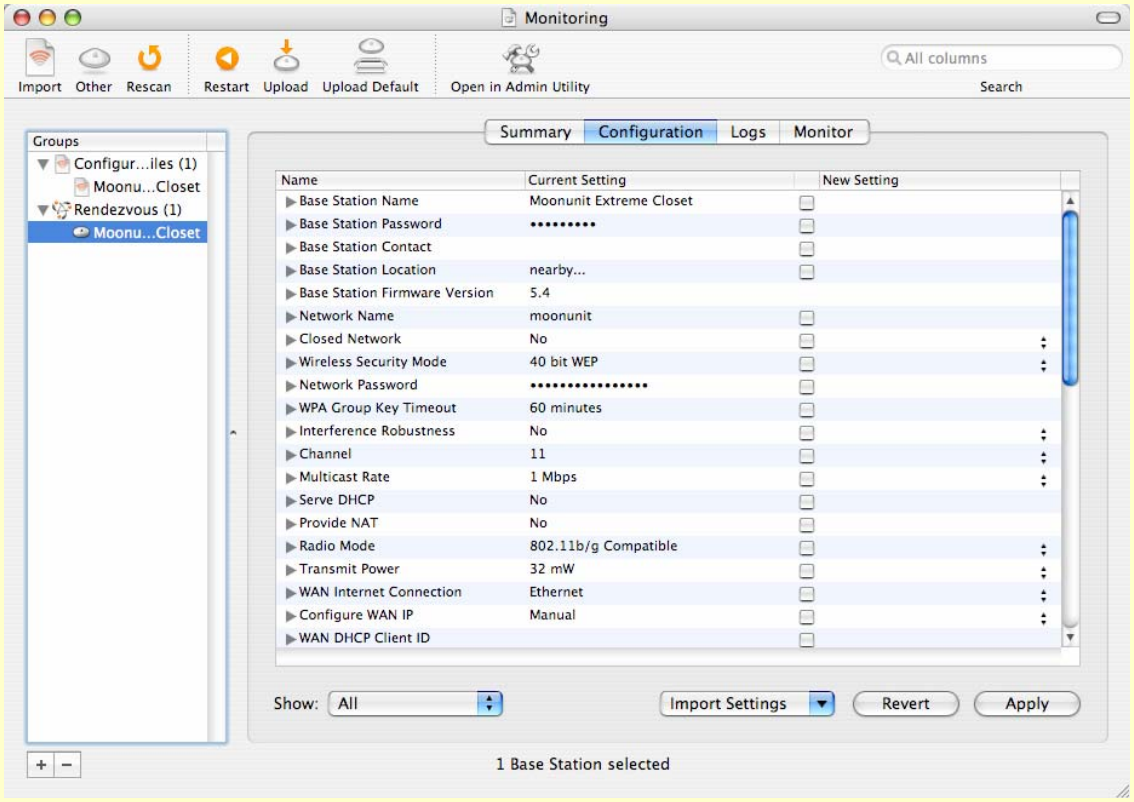
1. Connect to the base station in AirPort Admin Utility.
2. Choose File > Save a Copy As. Name the file descriptively and save it in a place that's easy to find, such as the Desktop.
3. Switch to AirPort Management Utility.
4. Click the Import button on the toolbar.
5. Navigate to and select the exported configuration file.
6. Click Open.

The file now appears in the list of Configuration Files.

An irritating feature in AirPort Management Utility is that when you run it by itself, it opens with an Untitled window. You should save a document that contains all your settings for base stations and only open that document to use the AirPort Management Utility in the future. Otherwise you'll find yourself having to re-enter settings.

Selecting one or more base stations and clicking the Configuration tab allows you to configure settings for one or more base stations at a time (**Figure 25**). If you need to change the DNS settings for all base stations on your network at one shot, you can enter that setting once for all units and click Apply: all systems will reboot and have the new settings available.

FIGURE 25



Name	Current Setting		New Setting
▶ Base Station Name	Moonunit Extreme Closet	□	
▶ Base Station Password	•••••••••	□	
▶ Base Station Contact		□	
▶ Base Station Location	nearby...	□	
▶ Base Station Firmware Version	5.4		
▶ Network Name	moonunit	□	
▶ Closed Network	No	□	
▶ Wireless Security Mode	40 bit WEP	□	
▶ Network Password	•••••••••••••••	□	
▶ WPA Group Key Timeout	60 minutes	□	
▶ Interference Robustness	No	□	
▶ Channel	11	□	
▶ Multicast Rate	1 Mbps	□	
▶ Serve DHCP	No	□	
▶ Provide NAT	No	□	
▶ Radio Mode	802.11b/g Compatible	□	
▶ Transmit Power	32 mW	□	
▶ WAN Internet Connection	Ethernet	□	
▶ Configure WAN IP	Manual	□	
▶ WAN DHCP Client ID		□	

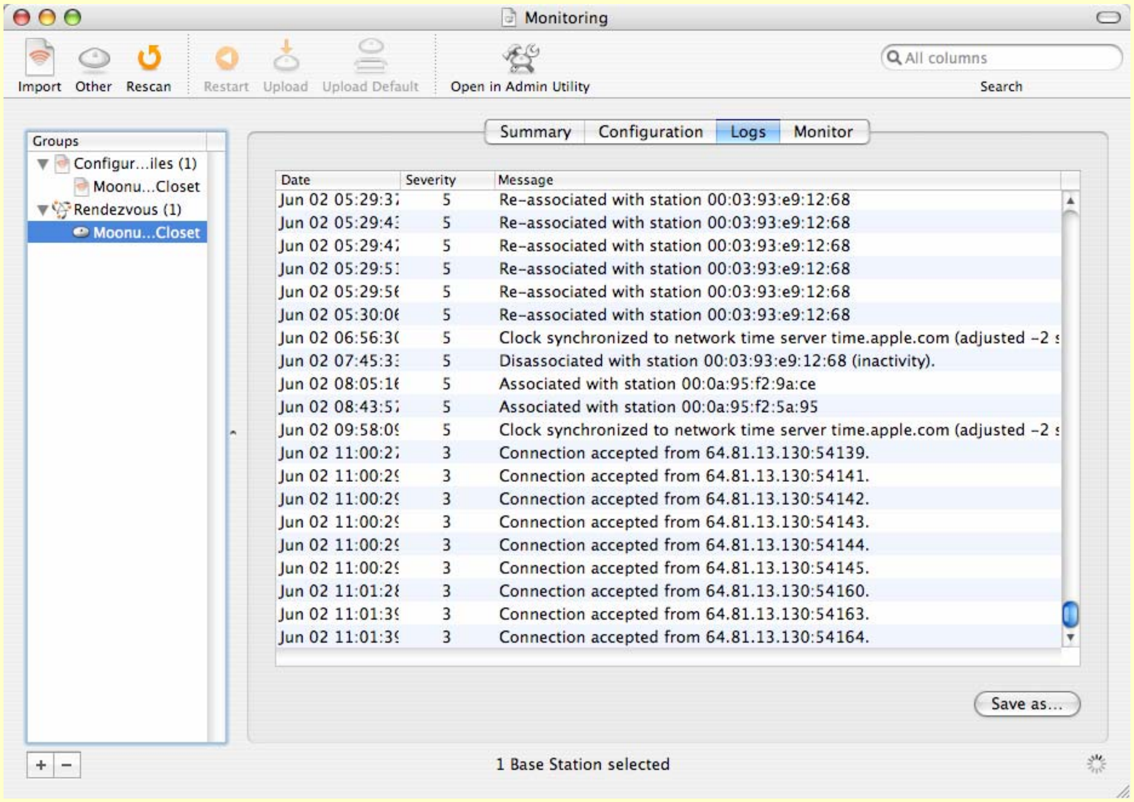
1 Base Station selected

The Configuration tab lets you change settings for one or more base stations at a time.

Click the triangle next to each setting in the list to choose specific base stations to which you want to apply a setting change.

The Logs tab shows information for a single base station, such as the association of wireless clients or reboot times (**Figure 26**). These logs can help you troubleshoot problems by providing specific information about what's happening in the base station.

FIGURE 26



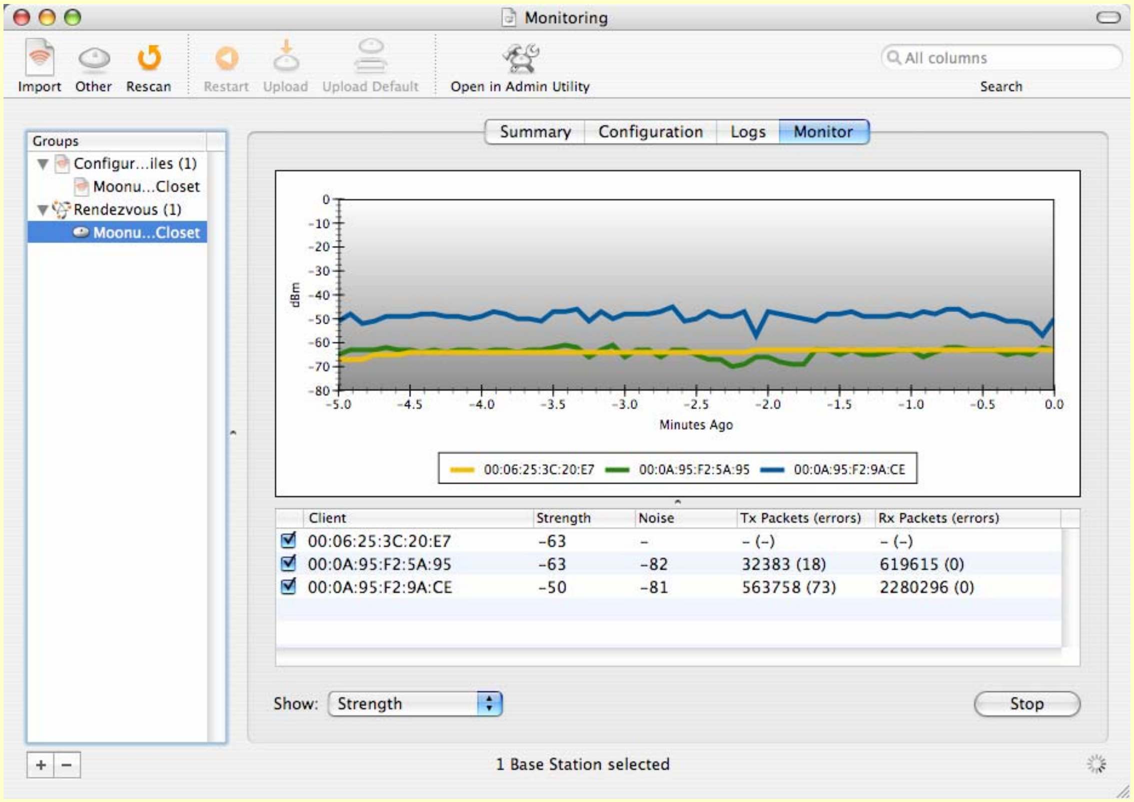
```
Date             Severity  Message
Jun 02 05:29:3      5      Re-associated with station 00:03:93:e9:12:68
Jun 02 05:29:4      5      Re-associated with station 00:03:93:e9:12:68
Jun 02 05:29:4      5      Re-associated with station 00:03:93:e9:12:68
Jun 02 05:29:5      5      Re-associated with station 00:03:93:e9:12:68
Jun 02 05:29:5      5      Re-associated with station 00:03:93:e9:12:68
Jun 02 05:30:0      5      Re-associated with station 00:03:93:e9:12:68
Jun 02 06:56:3      5      Clock synchronized to network time server time.apple.com (adjusted -2 s
Jun 02 07:45:3      5      Disassociated with station 00:03:93:e9:12:68 (inactivity).
Jun 02 08:05:1      5      Associated with station 00:0a:95:f2:9a:ce
Jun 02 08:43:5      5      Associated with station 00:0a:95:f2:5a:95
Jun 02 09:58:0      5      Clock synchronized to network time server time.apple.com (adjusted -2 s
Jun 02 11:00:2      3      Connection accepted from 64.81.13.130:54139.
Jun 02 11:00:2      3      Connection accepted from 64.81.13.130:54141.
Jun 02 11:00:2      3      Connection accepted from 64.81.13.130:54142.
Jun 02 11:00:2      3      Connection accepted from 64.81.13.130:54143.
Jun 02 11:00:2      3      Connection accepted from 64.81.13.130:54144.
Jun 02 11:00:2      3      Connection accepted from 64.81.13.130:54145.
Jun 02 11:01:2      3      Connection accepted from 64.81.13.130:54160.
Jun 02 11:01:3      3      Connection accepted from 64.81.13.130:54163.
Jun 02 11:01:3      3      Connection accepted from 64.81.13.130:54164.
```

The Logs tab summarizes administration connections, associations, and other actions.

TIP The AirPort Extreme Base Station's 5.4 firmware lets you send the system messages shown in **Figure 26** to a syslog daemon, a common Unix server package that can receive messages and dump them to a text file. The syslog daemon typically gathers server reports of all kinds to provide a kind of central console.

Finally, you can use the Monitor tab to view the signal strength and bytes transferred for client connections to a given base station (**Figure 27**).

FIGURE 27



	Client	Strength	Noise	Tx Packets (errors)	Rx Packets (errors)
☑	00:06:25:3C:20:E7	-63	-	- (-)	- (-)
☑	00:0A:95:F2:5A:95	-63	-82	32383 (18)	619615 (0)
☑	00:0A:95:F2:9A:CE	-50	-81	563758 (73)	2280296 (0)

The Monitor tab shows clients connected to a base station and their various strengths and traffic transferred.

Appendix B: Connect without AirPort Adapters

If you own a computer with an AirPort or AirPort Extreme slot but that omits either a PC Card (CardBus) or PCI card slot, I recommend using Apple's solution. But if you have a slot free, you might consider an alternative that could cost $20 to $50 for a fully functional, third-party option.

Older Power Macs That Predate AirPort

These computers can use Ethernet adapters, Wi-Fi PCI cards, and USB adapters, but each option comes with issues.

- A Wi-Fi Ethernet adapter like the 802.11b Linksys WET11 doesn't require specific Mac drivers like the cards do. It's configured with a Web interface. (Don't bother with the 802.11g WET54G since these older Macs have only 10Base-T Ethernet, which runs at 10 Mbps, and is thus slower than 802.11g's 54 Mbps throughput.) I recommend the WET11 for any older machine, including those that predate the PowerPC G3 processor and have 10Base-T Ethernet. A WET11 can bridge dozens of wired computers if you attach it to an Ethernet switch or hub, too. http://www.linksys.com/products/product.asp?grid=33&scid=36&prid=602

- If you are running Mac OS 8.6/9.x, you can use the MacWireless.com 802.11b PCI card. It's a little expensive because it's unique. http://www.macwireless.com/html/products/11g_11b_cards/11bPCI.html

- If you can run at least Mac OS X 10.2.8 and AirPort Software 3.2 or later on your older Power Mac, the 802.11g PCI cards made by Belkin, Buffalo, MacWireless.com, and Linksys work just as if they were AirPort Extreme Cards. No additional software is needed.

- If you lack a USB port, you could add a PCI card that provides USB (and FireWire, while you're at it) ports, and then use a Wi-Fi USB adapter from MacWireless.com or Belkin, as I describe next.

Older USB-only iMacs

These computers lack the PCI slots of Power Macs, so you're down to either a Wi-Fi USB adapter or a Wi-Fi Ethernet adapter (such as the Linksys WET11, discussed just previously).

- Belkin (http://www.belkin.com/) now offers Mac OS X drivers for its Wi-Fi USB adapter, making it the best choice for putting an older iMac on a wireless network. Find the Belkin Mac OS 9.2 and X 10.1, 10.2, and 10.3 drivers at: http://web.belkin.com/support/download/download.asp?download=F5D6050.
- MacWireless.com offers a USB adapter that has drivers for Mac OS 9.0.4 up to the latest releases of Mac OS X 10.3. http://www.macwireless.com/html/products/11g_11b_cards/11bUSB.html.
- If you desperately want to make another vendor's USB adapter work with Mac OS X, and you're not afraid to get your hands virtually dirty, Thomas McQuitty has posted instructions on modifying the Belkin driver to work with a similar USB adapter from Netgear at: http://www.mcquitty.net/Thomas/projects/USBWirelessOSX.html.

PowerBooks and Power Macs (G3s and G4s)

Any PowerBook or Power Mac that can run at least Mac OS 8.6 has one or more options that allow you to use the least expensive Wi-Fi adapter with your computer. In some cases, these adapters take advantage of Apple's built-in drivers, providing the best of both worlds.

Titanium PowerBooks are special candidates for these alternatives because of the heavy electromagnetic shielding the case provides due to Apple's poor placement of the Wi-Fi antenna. (See Solve the Titanium PowerBook Range Problem for more information.)

- On PowerBooks running Mac OS X 10.2.8 and at least the AirPort Software 3.2 update, Apple's drivers automatically support 802.11g PC Cards that use the Broadcom chip set from Belkin, Buffalo, Linksys, and MacWireless.com.

- To use PC and PCI adapters from D-Link, NetGear, and others that use Atheros's chips with a proprietary faster Turbo mode (108 Mbps raw/30-odd Mbps net), try OrangeWare's $15 driver. There's a free trial version. The driver supports the corporate 802.11a mode, and works with a/g dual-band cards, too. http://www.orangeware.com/endusers/wirelessformac.html

- Mac OS 8.6/9.x and Mac OS X 10.1.5 or later users can also try the IOXperts $20 driver, which works with a large range of very cheap 802.11b cards. A trial version lets you test compatibility. See http://www.ioxperts.com/80211b.html for 8.6/9.x, and visit http://www.ioxperts.com/80211b_X.html for OS X.

- If you use Mac OS 9 on a PowerBook, your best bet is to buy an Orinoco Silver or a WaveLAN Silver (same card, different name), since it uses the same hardware as Apple's AirPort cards and will work with Apple's AirPort drivers.

PCs Running Windows XP

Windows XP has terrific built-in support for Wi-Fi. Every piece of Wi-Fi equipment introduced in the last two years has a Windows XP driver; older equipment also often works without complaint. Because Wi-Fi is compatible across all manufacturers, you can use Windows XP computers to connect to AirPort networks.

Pre-Windows XP PCs

An older Windows system can connect to AirPort only if you install a driver compatible with the particular system release, typically Windows 98 Second Edition (SE) through Windows 2000. Your best bet is probably the same recommendation I give for older PowerBooks: the Orinoco Silver or Gold adapter.

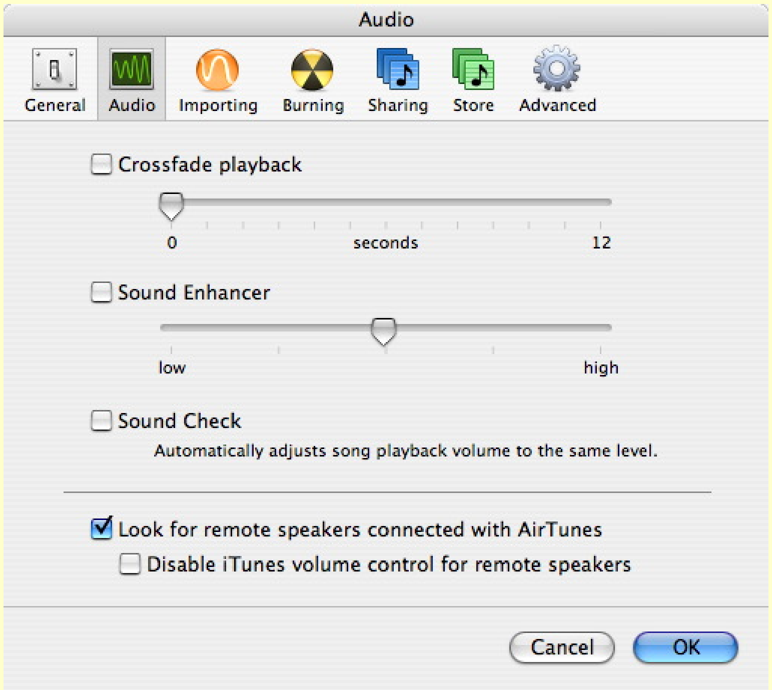
Appendix C: Configuring AirPort Express

As we went to "virtual press" with this edition of the book, AirPort Express hadn't shipped. When it does, I will revise this appendix to offer more details about its unique configuration options.

In the meantime, iTunes 4.6 with AirTunes support for streaming music from iTunes to an AirPort Express base station is available, and I can tell you how to use it with AirPort Express.

In iTunes, choose File > Preferences, and then click the Audio tab. Near the bottom, the checkbox Look for Remote Speakers Connected with AirTunes is checked by default (**Figure 28**). This option causes iTunes 4.6 to be aware of AirPort Express base stations that are plugged into stereos or powered speakers. (AirPort Express automatically senses these connections and sends out Rendezvous messages to that effect.)

FIGURE 28



☐ Crossfade playback

☐ Sound Enhancer

☐ Sound Check
Automatically adjusts song playback volume to the same level.

☑ Look for remote speakers connected with AirTunes
☐ Disable iTunes volume control for remote speakers

Check Look for Remote Speakers Connected with AirTunes to automatically discover AirTunes-equipped base stations.

Checking Disable iTunes Volume Control for Remote Speakers allows you to control the volume entirely from your stereo, instead of also via iTunes.

Appendix D: Configuring Software Base Station

You can use a computer equipped with a Wi-Fi adapter card not just as a client on a Wi-Fi network, but also as a base station. I discussed the pros and cons of this technique in Consider a Software Base Station. This section explains how to set up a software base station under Mac OS 8.6/9.x (next) and under Mac OS X (see Configuring Internet Sharing in Mac OS X).

TIP You can set up a software base station in Windows XP, too, through a combination of setting up an ad hoc network using one piece of configuration software, and the Internet sharing feature that's similar to Mac OS X's. Adam Engst and I wrote several pages about this topic in *The Wireless Networking Starter Kit, Second Edition* (http://wireless-starter-kit.com/).

Configuring Software Base Station in Mac OS 8.6/9.x

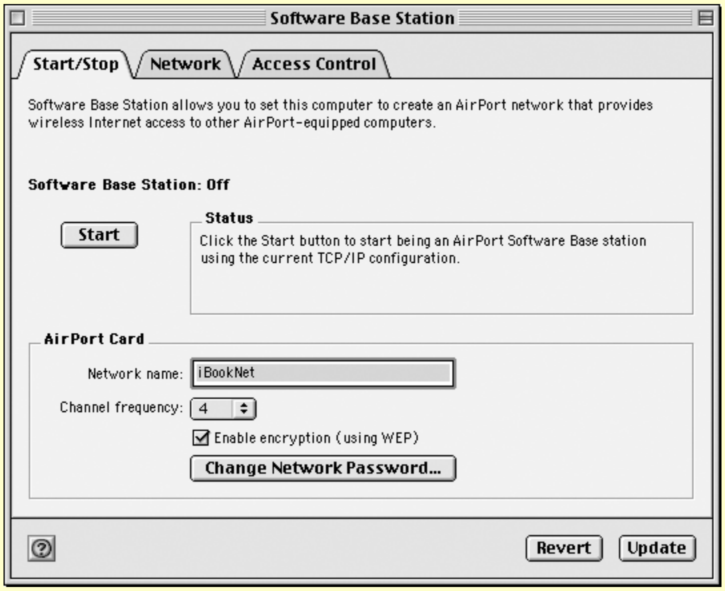
To share an Internet connection among the wireless computers that connect to your Software Base Station, you must also have a working Internet connection via Ethernet from a cable or DSL modem, or via standard dialup.

You configure the Software Base Station feature in Mac OS 8.6 and 9.x via the AirPort application, typically found in the Apple Extras folder inside your Applications folder.

Here are the steps:

1. Open the AirPort application and click the Software Base Station button in the main screen's lower-left corner to open the Software Base Station dialog box (**Figure 29**).

FIGURE 29



Software Base Station allows you to set this computer to create an AirPort network that provides wireless Internet access to other AirPort-equipped computers.

Software Base Station: Off

Status
Click the Start button to start being an AirPort Software Base station using the current TCP/IP configuration.

AirPort Card
Network name: iBookNet
Channel frequency: 4
☑ Enable encryption (using WEP)

Software Base Station dialog box in Mac OS 8.6/9.x.

2. In the Start/Stop tab, enter a name for your network—its service set identifier or SSID—in the Network Name field and choose the channel from the Channel Frequency pop-up menu.

3. If you want to protect your wireless data, check Enable Encryption (Using WEP) and click the Change Network Password button to enter the WEP key. Although Apple calls this WEP, you enter a plain text password that it converts into the actual WEP key.

WARNING! You can't use a non-AirPort wireless adapter to connect to an encrypted software base station because Apple didn't provide a tool in Mac OS 8.6/9.x's configuration that lets you extract the hexadecimal key necessary outside the AirPort environment. You can only enter an AirPort password and then use that password with other AirPort and AirPort Extreme Cards. See Protect with WEP.

4. Click Start to begin sharing the Internet connection.

Software Base Station always automatically provides private, non-routable IP addresses to client computers; in the Network tab, you can select if you also want to provide IP addresses to wired computers connected via Ethernet. Finally, use the Access Control tab to restrict access to specific network adapters by entering their MAC addresses, or the unique number assigned to the adapter.

TIP If you’re using a third-party wireless network adapter or want more control than Apple’s Software Base Station feature provides in Mac OS 8.6/9.x, check out Sustainable Softworks’ IPNetRouter (http://www.sustworks.com/site/prod_ipr_overview.html). It can do everything Software Base Station can do and much more, in part because Sustainable Softworks wrote much of Software Base Station for Apple.

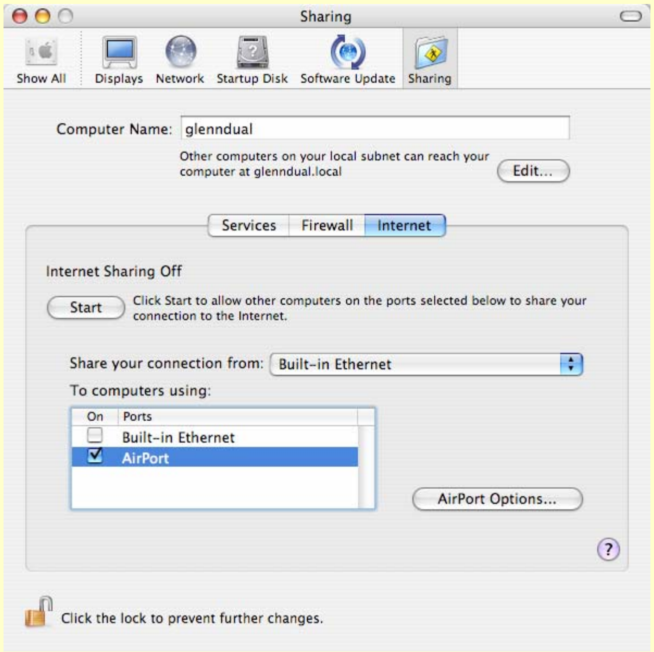
Configuring Internet Sharing in Mac OS X

In Mac OS X 10.2 Jaguar and 10.3 Panther, Apple relocated the Software Base Station feature from the AirPort utility to the Sharing preference pane in System Preferences.

Before starting, make sure you have either an Ethernet or an Internal Modem connection set up in the Network preference pane, as you can’t create a software access point without one or the other active. For this example, I assume your Internet connection comes via Ethernet from a cable modem.

1. Open System Preferences, click Sharing, and click the Internet tab (**Figure 30**).

FIGURE 30



Computer Name: glenndual

Other computers on your local subnet can reach your computer at glenndual.local

Internet Sharing Off

Click Start to allow other computers on the ports selected below to share your connection to the Internet.

Share your connection from: Built-in Ethernet

To computers using:

On	Ports
☐	Built-in Ethernet
☑	AirPort

Click the lock to prevent further changes.

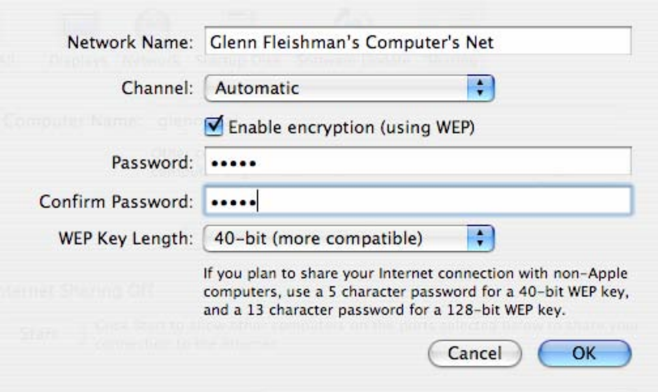
The Internet Sharing tab of the Sharing preference pane in Mac OS X 10.3. Choosing Built-in Ethernet and checking AirPort lets you share your wired Internet connection as a software base station.

2. In Panther, choose either Built-in Ethernet or Internal Modem (whichever matches how you access the Internet) from the Share Your Connection From pop-up menu, and then select AirPort in the To Computers Using list.

3. If you want to enable DHCP service to provide IP addresses to client computers across both your wireless and your connected wired network, check the Built-in Ethernet item in the To Computers Using list. (Before enabling this option, please read Don’t Get Your Service Canceled.)

4. Click AirPort Options to set the network name, channel, and WEP key (**Figure 31**).

FIGURE 31



Network Name: Glenn Fleishman's Computer's Net

Channel: Automatic

☑ Enable encryption (using WEP)

Password: •••••

Confirm Password: •••••

WEP Key Length: 40-bit (more compatible)

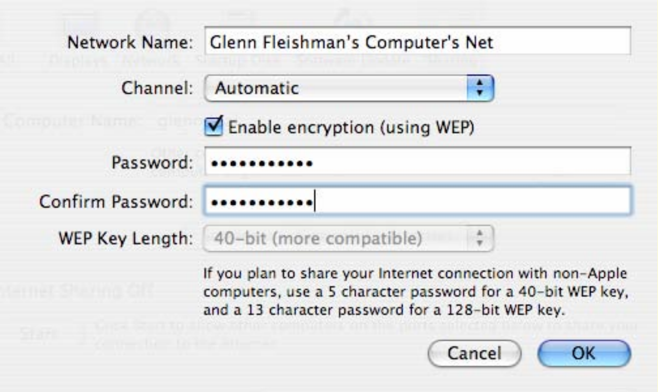
If you plan to share your Internet connection with non-Apple computers, use a 5 character password for a 40-bit WEP key, and a 13 character password for a 128-bit WEP key.

Set the specific wireless options you want for your software base station, including a WEP password.

5. Back in the Internet tab of the Sharing preference pane, click Start.

TIP If you turn on WEP in Mac OS X 10.2 or 10.3 and anticipate PCs or Macs without AirPort cards ever wanting to access your network, I recommend you set the WEP key using a dollar sign, followed by the 10-digit or 26-digit hexadecimal key (**Figure 32**). I talk more about this issue in Protect with WEP.

FIGURE 32



Network Name: Glenn Fleishman's Computer's Net

Channel: Automatic

☑ Enable encryption (using WEP)

Password: •••••••••••

Confirm Password: •••••••••••

WEP Key Length: 40-bit (more compatible)

If you plan to share your Internet connection with non-Apple computers, use a 5 character password for a 40-bit WEP key, and a 13 character password for a 128-bit WEP key.

Although you can't see a dollar sign, I've typed it at the beginning of the Password and Confirm Password fields. The WEP Key Length pop-up menu dims when you type the dollar sign, and the OK button won't light up until you type the right number of identical digits in both password fields. The dimmed pop-up menu even switches from 40-bit to 128-bit when you enter a longer key.

READING AND PRINTING TIPS

This ebook was designed to be read onscreen or printed. These tips help you get the most out of reading online and provide advice about printing.

Onscreen reading tips:

- Work with the Bookmarks tab (in Adobe Acrobat/Reader) or drawer (in Preview) showing so you can always jump to any main topic by clicking its bookmark.
- Blue text, including the blue text in the table of contents on the first page, indicates links.
- In Adobe Acrobat 5, the Take Control default settings on the View menu are Fit in Window and Continuous. For most people with larger monitors, those should be fine. To focus only on reading, in Acrobat 5, choose View > Full Screen, or in Acrobat 6, choose Window > Full Screen View. (Press Esc to leave full screen mode.) Preview ignores our default settings, but to emulate our defaults, choose View > Continuous Scrolling and select Scale Pages to Fit Display in the PDF tab of Preview's Preferences window.
- In Acrobat, you can increase the size of the text by clicking the window's Zoom button to make the window as wide as possible, and then choosing View > Fit Width. You can eke out more horizontal width by closing the Bookmarks tab (click the Bookmarks tab at the far left of the Acrobat window). In Preview, resize the window manually and click the Zoom In button; to save more horizontal space, close the bookmarks drawer (Command-T).
- To scroll using keyboard shortcuts you must first click in the main text area. The Page Up and Page Down keys may be the easiest (and they scroll by screen when you are viewing less than a full page). In Acrobat, the Left and Right arrow keys scroll to the previous and next page starts.

Printing tips:

- In the unlikely event that Adobe Acrobat or Adobe Reader cannot successfully print this PDF, try Preview; several readers have solved printing problems by using Preview.

- If you prefer a tighter layout that uses fewer pages, check your printer options for a 2-up feature that prints two ebook pages on one piece of paper. For instance, your Print dialog may have an unlabeled pop-up menu that offers a Layout option. Choose Layout, and then choose 2 from the Pages per Sheet pop-up menu. You may also wish to choose Single Hairline from the Border menu.
- When printing on a color inkjet printer, to avoid using a lot of color ink (primarily on the yellow boxes we use for tips and figures), look for an option to print entirely in black-and-white.

About This Ebook

Keep reading in this section to learn more about the author, the Take Control series, and the publisher.

About the Author

Glenn Fleishman has written for hire since 1994, starting with *Aldus Magazine*. He currently contributes regularly to *Macworld*, *InfoWorld*, *PC World*, *The New York Times*, and *The Seattle Times*. He's the regular Macintosh columnist for *The Seattle Times*, and a contributing editor at *TidBITS* and *InfoWorld*.

Glenn spends much of his time writing about wireless networking. He co-wrote two editions of *The Wireless Networking Starter Kit* with Adam Engst (Peachpit Press, 2003 and 2004). He edits the daily Web log Wi-Fi Networking News (http://www.wifinetnews.com/), and he and is the senior editor of Jiwire (http://www.jiwire.com/).

Author's Acknowledgements

Thanks to Adam Engst, my editor and co-writer, for helping develop this title as a useful, self-contained book. Thanks also to my colleagues writing Take Control books; they are a wonderful, supportive group.

Take Control of Panther: The Series

Take control of computing with the Take Control series of highly practical, tightly focused electronic books! Written by leading Macintosh authors, edited by TidBITS Electronic Publishing, and delivered to your electronic doorstep within moments of "going to press," Take Control ebooks provide the technical help you need.
http://www.tidbits.com/takecontrol/

Take control of Panther with:

- *Take Control of Upgrading to Panther,* by Joe Kissell
  http://www.tidbits.com/takecontrol/panther/upgrading.html
- *Take Control of Customizing Panther,* by Matt Neuburg
  http://www.tidbits.com/takecontrol/panther/customizing.html
- *Take Control of Users & Accounts in Panther,* by Kirk McElhearn
  http://www.tidbits.com/takecontrol/panther/users.html
- *Take Control of Sharing Files in Panther,* by Glenn Fleishman
  http://www.tidbits.com/takecontrol/panther/sharing.html

Take control of your applications with:

- *Take Control of What's New in Entourage 2004,* by Tom Negrino
  http://www.tidbits.com/takecontrol/entourage-2004.html
- *Take Control of Making Music in GarageBand,* by Jeff Tolbert
  http://www.tidbits.com/takecontrol/garageband-music.html
- *Take Control of Spam with Apple Mail,* by Joe Kissell
  http://www.tidbits.com/takecontrol/spam-Apple-Mail.html

About TidBITS Electronic Publishing

Take Control ebooks are a project of TidBITS Electronic Publishing. TidBITS Electronic Publishing has been publishing online since 1990 when co-publishers Adam and Tonya Engst first created their online newsletter, *TidBITS,* about Macintosh and Internet-related topics. *TidBITS* has been in continuous, weekly production since then, and it is the leading online Macintosh newsletter.

To stay up to date on Wi-Fi and other Macintosh topics be sure to read *TidBITS* each week. At the *TidBITS* Web site you can subscribe to *TidBITS* for free, participate in TidBITS Talk discussions, or search 14 years of news, reviews, and editorial analysis.

Adam and Tonya are well-known in the Macintosh world as writers, editors, and speakers, and they have written innumerable online and print publications. They are also parents to Tristan, who is five years old and thinks ebooks about trains, clipper ships, and dinosaurs would be cool.

TidBITS Web site: http://www.tidbits.com/

Adam's home page: http://www.tidbits.com/adam/

Tonya's home page: http://www.tidbits.com/tonya/

Publisher's Production Credits

Cover: Jeff Carlson

Editor in Chief: Tonya Engst

Publisher: Adam Engst

…and the many friends and relatives that helped in large and small ways by providing technical expertise, dinner, childcare, and more.